The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity

Edited by
Demosthenes Chryssikos, Nikos Passas, Christopher D. Ram

Selected papers and contributions from the International Conference on
“The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity”
Courmayeur Mont Blanc, Italy
30 November – 2 December 2007
Acknowledgements

ISPAC wishes to thank the “Fondazione Centro Internazionale su Diritto, Società e Economia” and its President, Dr. Lodovico Passerin d’Entrèves, for their generous contributions towards the publication of this book.
Deve rimanere bianca
CONTENTS

Keynote Address

KUNIKO OZAKI 9

Introduction

CHRISTOPHER D. RAM 21

Selected Papers and Contributions

PATRICK CUNNINGHAM, An overview of the meaning of fraud in different jurisdictions and the problems posed by it (scope and elements of fraud offences, types of fraud encountered and criminalised at the national level) 33

GIOVANNI BUTTARELLI, Protection against identity fraud – finding the balance between effectiveness and civil liberties 45

CHRISTOPHER D. RAM, Identity related crime as a global issue: the nature, concept and types of identity related crime 53

ROBIN CHALMERS, Biometric identification technologies and the use of e-security to protect identity 63

BRIGITTE ACOCA, Online identity theft: a growing threat to consumer confidence in the digital economy 71

KEVIN McNULTY, The relationship between identity-related crime and economic fraud 87

NIKOS PASSAS, Identity-related crimes: a review of research and suggested typologies 95
Jean-Louis Bruguiere, *Use of identity-related crime to facilitate organized crime and terrorist activities* 103

Demosthenes Chrissikos, *Criminalization and jurisdiction issues* 113

Joanne Klineberg, *Canadian identity theft legislation: a case study in domestic criminalization of identity-related crime* 129

Alexander Seger, *Identity theft and the convention on cybercrime* 153

Rutsel Silvestre J. Martha, *International cooperation to combat identity-related fraud: operational aspects* 159

Nicole Van der Mueleen, *Victims of identity theft: an uphill battle or an impossible fight?* 177

Conclusion 195

Annex

Results of the study on fraud and the criminal misuse and falsification of identity (identity-related crime) 207
KEYNOTE ADDRESS
I. Introduction: the growing threat of identity theft/fraud and the efforts to raise awareness about it

Although the criminal misuse of personal identity itself is not a new issue, national and transnational cases of theft and falsification of identity are now becoming serious and rapidly expanding problems for both developed and developing countries. First, the spread of modern information and communication technologies, coupled with the growing transnationality of criminal activities, have created a vast range of new opportunities for perpetrators of such crimes. Second, the increased reliance on personal and corporate identification in both public and private sectors and in a wide range of transactions has made our society extremely vulnerable to misuse of identities and fraudulent practices linked to them.

Harm caused by these crimes includes not only the large amount of losses of victims of fraud or other ordinary crimes committed through identity theft, but also harm to persons whose identities were misused and who have to face extremely difficult and costly struggles, often transnational, to restore their tainted identity, reputation and their position in a society at large. On the other hand, organized criminal groups can have access to vast amount of resources through illegally gained or falsified identities, which will be most likely used for further criminal activities.

The true extent and seriousness of such crimes, however, and their relationship with other criminal activities, including fraud, organized crime, cybercrime, money-laundering and terrorism, remain under-reported and underestimated, thus resulting in lack of reliable data. However, statistics from recent surveys indicate trends and the scope of the problem. For example:

- in the United Kingdom, the cost of identity-related crime to the British economy was calculated at 1.3 billion British Pounds per year (source: 2002 Cabinet Office Study);
- estimates of losses caused by identity-related crime in Australia vary from less than 1 billion US dollars to more than 3 billion US dollars every year (source: Paget, McAfee White Paper, 2007);
losses in USA are estimated at 56.6 billion US dollars in 2005 (source: Javelin Strategy and Research 2006 Identity Fraud Survey, Consumer Report).

Moreover, as crimes related to identity abuses are still a novel concept for criminal justice systems in many countries, basic conceptual framework remain uncertain and fluid and there are few legislative definitions. As a result, different terms, such as identity theft and identity fraud, are used in various jurisdictions to describe the same conduct and, in addition, there is lack of concerted action to combat such conduct. What is clear is the imperative need for Governments and the business community to work together to deal with the problem.

There is, of course, a positive movement such as extensive publicity regarding severe cases of identity theft and fraud in the print and electronic media and portrayal of the related risks in a number of television commercials which have raised public awareness about the problem. The consequence is that a broad range of stakeholders, both at the national and international levels, have started to streamline their efforts to develop effective counter-action against these emerging forms of crime.

II. The criminal diversity of the problem

A. Types of, and means used to commit, identity-related crime

In determining the range of identity-related crime (a term which will be used hereinafter as a “catch-all” concept encompassing identity theft/fraud and identity abuses in general), it is important to gain a better understanding of the means used for its commission. They depend on the nature and purpose of the identification structures involved, and the means available to offenders. In most cases, identification information is taken, copied or plausibly fabricated, rendered into some usable form and then used. Offenders obtain identification information through the theft or copying of complete documents or by getting partial information to build identities and procure genuine documents.

One of the most commonly used methods for committing identity-related crimes is that of “phishing” or “pharming”, whereby users of computer networks are deceived into providing offenders with user names, passwords and other electronic identification information. Other forms of crime are also encountered in practice, including malicious software that infects individual victim computers, capturing personal information and
transmitting it to offenders, and the hacking of commercial websites to obtain credit card data and other customer identification information.

Other methods used to gain identity information relate to debit and credit cards, primarily for subsequent use in economic fraud. For example, some information is gathered by skimming (running the card through a data-reading device). There are also cases where identity information is obtained by officials with inside access to government or commercial systems or by outside offenders by means of bribery or other corrupt means.

Information and communications technologies have also brought some means of forgery within the reach of a large number of offenders, triggering an evolution of criminal techniques that, in turn, requires a similar evolution of document safeguards.

B. Legislative measures, including criminalization aspects

The need to define the nature of identity-related crime and to develop a typology of pertinent conducts is fundamental for structuring effective criminal justice responses at the domestic level.

It is true that currently domestic laws and policy-making in most States are limited to dealing with identity problems primarily in terms of the further crimes that can be committed through identity abuses.

However, a new concept has emerged over the last years which put emphasis on the abuse of identity itself rather than on other crimes supported by identity abuses. Under this new approach, abuses of identity or identification information are established as specific offences and this is opposed to the traditional approach of criminalizing other activities committed using false identities.

In determining whether the problem of identity abuses is sufficiently serious to warrant the application of offences and other criminal justice measures, and if so, how to frame appropriate criminal offences, it is important to consider what specific legal rights or interests should be protected by the criminal law, including:

- the interests of individuals whose identity information is taken, copied, altered or misused;
- the extent to which relevant rights exist and are affected by the abuses, including privacy rights, intellectual property rights (corporate identity), and if applicable, the right to have an identity;
• the need to protect the integrity of various models of identity infrastructure, including national identity systems, subject-specific identity systems (such as passport systems), and relevant private sector commercial identity systems;
• within the scope of each identity infrastructure, what specific types of document and information should be protected;
• whether the criminalization of specific identity abuses per se is necessary or justified to prevent or suppress secondary crimes such as fraud, money-laundering, terrorism, or the smuggling of migrants or trafficking in persons;
• whether criminalization is needed or justified on national security grounds;
• which specific forms of conduct should be criminalized and how offence provisions should be framed (for example, in respect of conduct such as acquiring, taking or copying, falsifying, possessing, transferring or trafficking in identity information or documents, or the subsequent illicit use of identity documents or information in other offences); and
• at a general level, how the scope of identity offences would fit within each State’s existing criminal law, bearing in mind the need to avoid gaps.

C. Relationship with other crimes

1. Relationship with organized crime

Identity crimes that are transnational in nature often tend to involve falsification of, or tampering with, identification systems and documents that are increasingly beyond the means of individual offenders and likely to require a degree of expertise and resources associated with organized criminal groups.

Organized criminal groups may use identity-related crime to protect their members and operations from surveillance and to carry out routine activities such as international travel. Evidence provided by Member States indicates the specialization of criminal groups and the treatment of identity documents and information as an illicit commodity. Such groups develop expertise to fabricate sophisticated identity documents or exploit weaknesses in issuance schemes, deceiving or corrupting authorities, in order to obtain genuine documents, which could then be sold to others for use in crime, terrorism, illicit travel, illegal migration or other activities.
2. Relationship with terrorism

Similarly, terrorist organizations commit identity-related crime to obtain identification information and documents that can, in turn, be used by terrorist operatives to evade surveillance or arrest. In general, many basic scenarios of resorting to identity-related crime are common to organized criminal groups and terrorist groups. Moreover, terrorist groups that lack their own expertise may simply purchase false identification documents from organized criminal groups. Identity-related crimes can be employed for the financing of terrorism much the same way as for money-laundering.

3. Relationship with fraud

A substantial amount of identity-related crime is associated with economic fraud, as a means of avoiding fraud prevention measures and criminal liability and, in many cases, as a means of deception central to the fraud offence itself. Identity abuse has much the same role in economic fraud as it does in other crimes, along with the added role that identity abuse plays in deceiving victims in many fraud schemes. For example, the impersonation of officials of banks, credit card issuers and telecommunications providers is a common element of many reported economic and telecommunications frauds. Frauds, such as credit card fraud, could also be considered identity fraud, because the offender is using a copied or stolen card as a form of identification, effectively impersonating the legitimate cardholder.

4. Relationship with money laundering

Many measures to counter money-laundering heavily depend on identity or identification elements and the means used by offenders to launder proceeds often involve identity-related crime. Money-laundering methods make use of information, communication and commercial technologies, which enable offenders to generate false identification information and further facilitate, through the use of such false identification, remote transfers aiming at concealing laundered assets. These technologies have also led to a dramatic expansion of international transfers and offshore banking, complicating the regulatory environment and putting offshore banking and concealment within the reach of a much broader range of offenders.
5. Relationship with corruption

Identity-related crime can also be used as a means of avoiding detection or criminal liability when committing corruption offences, as used in other crimes. More important aspect of the relationship is the use of corruption to support identity-related crime. For example, passports and similar documents have become difficult to forge or falsify, making the active and passive bribery of officials to obtain a genuine document an easier alternative in many cases. Similarly, crimes of corruption can be used to alter or falsify information in systems used to validate or verify identity.

D. International cooperation to combat identity-related crime

The rapidly growing number of cases of transnational identity-related crimes makes effective international cooperation to combat these crimes essential. The first step towards enhancing such cooperation is the adoption, to the greatest extent possible, of common approaches to criminalization that can form a good basis for mutual legal assistance and extradition. Proper legislation to criminalize identity-related crime is essential to any effective fight against such crime. At the same time, such criminalization should be done in a coherent way in the countries around the world so that it would enhance not only domestic prosecution, but also international cooperation by fulfilling the double criminality requirement and other conditions for streamlined international cooperation.

The next step is to establish and implement a broad range of measures which need to be in place to ensure that criminal justice and law enforcement authorities cooperate with each other across the national boundaries more effectively, in particular through mutual legal assistance, law enforcement cooperation and information-exchange. Such international cooperation should involve every country in the world, since a lot of sophisticated identity-related crimes are committed in developing countries reaching their long arms through cyberspace to rich targets in the developed countries. This necessitates truly global cooperation, as well as technical assistance to the countries where proper criminalization and law enforcement are most needed.

It is needless to say that international cooperation measures should include those techniques which have been proven effective to deal with cybercrime. At the same time, in most of developing countries, more basic measures, such as preventive action against corruption, are significant, because even the most technically advanced identification method could be easily hampered by corruption of relevant officials.
Where the misuses of computer data or any interference with the functioning of a computer system are involved, the Council of Europe Convention on Cybercrime has the potential to be used as a legal basis for cooperation in a much broader context than that of the Council of Europe Member States, as it is open for accession to other States as well.

However, global instruments adopted within the United Nations system can also be utilized, where applicable, with a view to fostering international cooperation in this field, such as the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption, and the 16 universal legal instruments against terrorism.

- Cooperation between the private and public sector – Prevention of identity-related crime

Identity-related crime has a substantial impact on both private and public interests, as it affects both public identification, such as passports, and private documents like credit cards. In countries where private documents are used for public purposes and public identification is used for private purposes, crimes against any form of identification affect both areas. It is therefore essential for criminal justice authorities and commercial entities to cooperate effectively in order to develop an accurate and complete picture of the problems, as well as implement both preventive and reactive measures.

Especially with regard to prevention of identity-related crime, the cooperation between the public and the private sector has the potential to function as a catalyst. The first aspect to be considered is the development of security countermeasures that can be incorporated into commercial technologies and practices, focusing on means intended to make it more difficult to tamper with identification documents, to subvert or corrupt identification systems and to obtain identification data. Thus, for example, a number of specific methods can be used to prevent identity-related crime, ranging from document security measures to system-based measures intended to protect authentic documents and issuance systems from theft, diversion and corrupt issuance. Document validation and verification practices can also be strengthened, especially through the use of telecommunications and databases protected by encryption. Biometric elements can further be used to link identity to unique physical characteristics.

The strengthening of technical means to prevent identity-related crime requires consultation between public entities, such as standard-setting
bodies, and private interests, including those companies which produce and sell new technologies and those which will use them. An important factor that needs to be taken into account, in this connection, is the need to ensure that the preventive measures are effective and do not unduly impede normal commercial activities.

Another key element is education and training of persons who are in a position to identify and report identity-related crime, in particular employees of banks and financial institutions. Such training and education require frequent updating, to reflect the latest developments in criminal methods and techniques, law enforcement measures and commercial practices.

Other preventive methods that can benefit from the close collaboration between public and private sector include:

- the dissemination of information about identity-related crime to potential victims. Such information may include both general information to raise awareness of the threat and timely information about specific forms of identity-related crime based on accurate and up-to-date monitoring of criminal activities by appropriate entities in both the public and private sectors. Information campaigns can be directed at the general population and at specific groups considered to be particularly vulnerable or at increased risk of being targeted;
- the rapid and accurate gathering and analysis of information to support effective and timely prevention measures. This entails the gathering of relevant information among law enforcement, commercial and other entities at the national level and, where appropriate, at the international level; and,
- the rapid sharing of information among appropriate law enforcement and private sector entities at the national and international levels. Such sharing must be subject to appropriate and applicable privacy and security considerations.

In assessing the cost, consequences and repercussions of identity-related crime, we need to start from the identification of the four main kinds of victims of such crime, that means Governments, private companies storing large amounts of data, financial services providers and customers (either businesses or natural persons). As for the consequences, they vary and the may be obviously direct financial losses, or indirect costs for businesses and for Governments insofar as they should upgrade their prevention and, in the latter case, law enforcement systems. There are also associated indirect costs for consumers, who may need to clean up their
own name. In many cases, repairing damages can be extremely time consuming. According to a joint study conducted recently in USA by the Council of Better Business Bureaus and Javelin Strategy and Research, the amount of time that victims have to spend on rectifying problems stemming from identity-related crime grew over a period of four years from 30 hours to 40 hours per person.

It would also be useful to discuss the reputational risks involved. First, to Governments, as the identification documents they deliver may suffer from discredit. Secondly, to the financial system itself, as consumers may lose confidence in non-cash means of payments. Additionally, there are reputational problems for data storage service providers and financial sector providers, which affect the entire market environment and the business model itself.

- **The way forward – The UNODC approach**

In July 2007, ECOSOC adopted resolution 2007/20, upon the recommendation of the Commission on Crime Prevention and Criminal Justice, entitled “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime”. The resolution, among others, requested UNODC to provide legal expertise to Member States in reviewing their legislation and also to facilitate cooperation between public and private sector entities to fight against identity-related crimes. In order to implement the resolution, UNODC decided to create a consultative platform on identity-related crime. The platform intends to bring together public sector representatives, business representatives, international and regional organizations and other stakeholders to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime.

The platform aims at:
- increasing knowledge and awareness about identity-related crime and its links to transnational organized crime, fraud, corruption, money-laundering and terrorism;
- promoting cooperation and dialogue among stakeholders in order to identify gaps and needs;
- developing, as appropriate, common concepts, definitions and legislative approaches to identity-related crime as a solid basis for concerted action;
- identifying effective preventive and criminal justice policies and measures;
- increasing the capacity of stakeholders to combat identity-related crime, including through technical assistance in legislation and international cooperation in criminal matters; and,
- considering measures to protect victims of identity-related crime.

The first step under the platform is the establishment of a core group of experts from Governments, private sector entities, international organizations, as well as research and academic institutions. This multi-stakeholder think-tank will brainstorm on the best way forward and provide advice and guidance on possible long-term strategies for further consideration. The Courmayeur Foundation kindly offered to host the first meeting of this group back-to-back to the ISPAC Conference on the evolving challenge of identity-related crime. The organization of both events provides a unique opportunity for utilizing the presence of all the experts involved and enabling more focused discussions on how to develop appropriate responses to the problems posed by identity-related crime.
INTRODUCTION
Deve rimanere bianca
First, let me thank ISPAC for taking this subject matter up. One of the most difficult challenges facing those of us who work in the area of economic fraud and identity crime is simply to persuade both governments and criminological experts of the true extent and seriousness of the problem. These are not violent crimes, and quite often the problem involves large numbers of relatively small offences, so they get relatively little media attention.

Ms. Ozaki has just given an overview of the nature and scope of the problem, some of what we have learned about it, and raised a few of the many gaps in our knowledge base. What she has said is largely based on a report that I prepared as Rapporteur for an intergovernmental expert group asked by the Commission on Crime Prevention and Criminal Justice to conduct a study of the problem of “fraud and the criminal misuse and falsification of identity” in 2004. This was in many ways a humbling exercise. While we were able to gather a great deal of information and assemble a good evidence base for future work, I think I can safely say that all of us in our deliberations were made aware that what we have accomplished barely scratches the surface.

Before I proceed with substantive matters, let me also take this opportunity to thank the Chairman of the group Judge Pedro David, and his substitute at the second session, H.E. Eugenio Curia, the Ambassador of Argentina to the Intergovernmental Organizations in Vienna, for their contribution to the work of the expert group. They are not able to join us for these proceedings, but both of them are well-known to many of you in the room. Let me also preface my substantive remarks by noting that both my remarks and the texts that I prepared for this session represent an attempt to report accurately on the proceedings and findings of the intergovernmental group, but they are my own observations, and not necessarily those of the group, which last met in January 2007. I would also note that the views expressed are my own, and not necessarily those of the Government of Canada or the Canadian federal Justice Department.
The proceedings of ISPAC in 2007 really began in 2002, when the United Nations Commission on International Trade Law (UNCITRAL) called for a study of commercial fraud. Anecdotal evidence suggested that this was a serious and growing problem for global commerce, and in 2003 the initial conclusions and recommendations of the UNCITRAL panel emphasized this fact. The experts concluded that transnational commercial fraud was increasing, suggested a possible link to the globalisation of trade and the spread of information and communications technologies, and recommended that further work be done by the Commission on Crime Prevention and Criminal Justice. In 2004, the Crime Commission and the Economic and Social Council adopted a resolution (E/RES/2004/26) calling for a broader study of the criminal aspects of the problem, expanding the scope of the work to include all types of economic fraud as well as the related problem of the “criminal misuse and falsification of identity”, later to become known as “identity-related crime”. After receiving responses from 46 Member States and a number of private-sector entities and groups, the results of the study were reported back to the Crime Commission in April 2007 (E/CN.15/2007/8, and /8/Add.1/Add.3).

Now that we have an evidence base, we have to decide what to do with it. In 2004, the Commission created two mandates. It called for the establishment of the intergovernmental expert group and the conduct of the study, which has now been completed, and it also called on UNODC to produce materials based on the results of the study. When it accepted the report earlier this year, it also called on UNODC to use the study and any materials produced to provide technical assistance, subject to the availability of resources. This is where we are now, and hope that the consideration of this matter by ISPAC will serve to generate some useful insights on how we can approach this problem. In addition to what Ms. Ozaki has already said, let me make a few preliminary observations about how the study was conducted and how its results should be interpreted.

Meaning of key terms

A key issue which confronted both the Crime Commission and the expert panel itself with the fact that there was no clear definition or consensus on some key elements of terminology. With respect to fraud,
there was actually fairly broad uniformity in the State responses describing criminal offences. These emphasized dishonesty, deception, and a causal link to economic or equivalent losses by victims or gains by offenders. However, many States also used the term “fraud” as a more general description of dishonest conduct. They referred to passport or visa fraud, identity fraud, and other forms of dishonesty without an economic element. Many of those were considered as being with on the identity crime side of the study, so it was decided to use the term “economic fraud” to limit the scope of the fraud component.

With respect to identity crime, in the absence of an agreed definition, the Crime Commission in its mandate refers to the “… criminal misuse and falsification of identity…” but it quickly became apparent that this would not address the full scope of the problem, and that some of the developing terms of art, such as “identity theft” and “identity fraud” were not being used consistently. Some States thought that identity fraud consisted of using deception to obtain another’s identity, while others thought that it meant using that identity to commit fraud regardless of how it was obtained. None of the terms addressed the links between various identity abuses and other crimes such as fraud, money laundering, organized crime, and terrorism, and none of them seem to include some of the emerging forms and identity crime, such as illicit trafficking in identity documents or identity information. For that reason, the experts ultimately decided to use the term “identity related crime”.

Results of the study of economic fraud

To summarize briefly the findings with respect to fraud, there was as I have said a great deal of consistency of offences. Almost all states had criminalized it, using roughly similar definitions, limited to economic crime. Some had a small number of very general offences and others had a large number of specific offences for specific types of fraud, but most had encountered the same fundamental types of criminality. Most considered fraud to be largely an organized crime problem. While fraud, including the occasional nature transnational fraud, can be committed by individuals, it appears that the vast majority involves groups of three or more persons such that, when the other conditions are present, the Palermo Convention would apply. This is significant, because it places the emphasis for future work on finding ways to use the legal instruments already available effectively, as opposed to attempting to develop new ones.
Links to terrorism were less common, but were reported by several States. The primary focus seemed to be on fraud as a means of financing terrorism, both through major fraud schemes used to fund groups, and more minor schemes, such as credit card fraud, used to fund daily operations. Another concern was the use of telecommunications fraud both by organized crime and terrorist groups, as a means of obtaining communications services under false identities, so as to frustrate attempts to trace them if intercepted by law enforcement. In number of states also mention links to money laundering. These are significant for identity related crime, but the relationship with fraud appears to be primarily that fraud is a source of proceeds for laundering, and most indicated that it was a predicate offence and their legislation.

There appear to be substantial links between the evolution of fraud and the recent proliferation of information, communications, and commercial technologies. The actual links described differed between developed and developing countries, but both reported substantial links. For developed countries with extensive information and communications networks, and extensive use of these for commercial purposes, technologies were seen as a link between the offenders and victims, a means of deception, a means of obtaining the proceeds from victims, and of transferring the proceeds for purposes of laundering. For developed countries, who still rely on paper-based document systems, the main concerns were the use of computers and sophisticated printers to produce high-quality document forgeries. There was also some concern about the effects of fraud on transnational commercial systems such as credit card networks. The actual effects of new technologies are too many and too complex to list here, but one of the most pronounced and troubling has been a substantial expansion in what the experts describe as “mass frauds”, in which to technologies are used to target very large numbers of victims on a global basis. More generally, the involvement of technologies appears to be an area that is common between economic fraud and identity related crime, and in many cases technologies form the link between the two.

Regarding the quantification of the problem, most States told the expert panel that fraud is under-reported. Victims are often embarrassed, they may feel that law enforcement will not take the claims seriously, they may report to banks and credit card companies instead of law enforcement, and in many cases they may never be aware that they have been victimized. There was some parallel between legal and natural persons as victims, in the sense that companies are also reluctant to report victimization for fear of loss of commercial credibility. There are also substantial obstacles to developing a global picture. Many victims report to commercial companies,
and companies detect unreported occurrences themselves, which means that the commercial sector often has better information than governments. However, companies collect data for specific commercial purposes, and in some cases regarded as sensitive. This raises a challenge of assembling and comparing commercial data, and integrating it into an accurate global picture. Based on opinion however, a substantial majority of the states which responded indicated that fraud is increasing both in scope and in the volume of proceeds, and at the rate of increase is greater than most other forms of crime.

The experts also considered the question of fraud in the exceptional economic circumstances that may arise in cases of major economic transformation or development, post-conflict reconstruction, or recovery from major natural disasters. Here the report notes that the challenge of preventing and suppressing fraud is greater, and the damage that it can create is also greater. Both economic regulation and crime control mechanisms tend to be weakened, which creates opportunities for all offenders. In major reconstruction and disaster relief efforts large sums of money must often be raised and spent very quickly, which he roads the effectiveness of audit and other controls. Funds from charitable sources are even more difficult to regulate, as donors often have no means of verifying whether the contributions were actually used for the purpose intended. Greater harm often results as well. Major fraud schemes have eroded public confidence in new economic transformations at a time when that confidence was most critical, and systems in transition or recovery are more vulnerable to the inroads of organized criminal groups and corruption that may be fuelled by the proceeds of fraud.

Another key area examined by the experts was the need for prevention, and the need to involve the private sector. As the report notes, fraud is a crime of commerce, which means that the commercial sector both controls much of the environment in which fraud occurs, and has the most to gain from the application of effective controls. Companies usually have better information about the latest developments, and better access to employees who can be trained to identify possible fraud schemes quickly, and to customers who can be warned about deceptive schemes and how to avoid them. Many States also wanted a greater level of cooperation with respect to investigation and prosecution.
Identity related crime is a new and emerging concept, which emphasizes abuses of identity *per se* rather than other crimes supported by those abuses. Thus, for example, some states are now considering criminalizing the taking, fabrication, or possession of false identities or identity information, in addition to the established offences which are committed using that information, such as economic fraud. Proponents of such criminalization argue that this allows the criminal justice system to intervene much earlier, potentially reducing the damage from major offences and ongoing schemes, and that it recognizes the fact that a person whose identity is taken and misused is victimized in a different way than those who may be deceived in offences such as fraud.

A number of States are considering this option, but few had proceeded with it at the time of the study. However, many did have specific, and long-established identity crime offences, often to protect specific forms of identification or identity systems, such as their passport systems. Many also reported more general offences that included identity crime elements. Document forgery offences often included the forgery of identity documents for example.

There appear to be several key challenges for addressing identity related crime. One of these is that such crime must be considered in the context of the underlying identity infrastructure, and these differ between public and private sectors, and from one Member State to another. Some countries have centralized national identity systems, and offences to protect the integrity of those systems, while others have largely *ad hoc* systems in which specific identification and identity databases are used for functions such as driver-licensing and the collection of tax and payment of social benefits, and in which those forms of identification are often used for other purposes. The private sector has been forced to become more globally consistent, especially with respect to debit and credit cards, which are now used for global travel purposes. It seems likely that differences from one country to another with respect to how individuals are identified will have to be taken into consideration. On the one hand, countries need definitions and offences which meet their domestic needs and protect their domestic identity infrastructures, while on the other hand the global nature of identity related crime argues for as much consistency as possible as offences are formulated, to support more effective international cooperation. This is already an established issue for the private sector, and for inherently transnational forms of identification, such as the passport, and one which
seems likely to become an issue for identity and identity related crime more generally in future.

A range of reasons for committing identity crimes were reported. Generally false identities are created either by taking the identity information of a real person, or generating a completely fabricated identity. False identities were then used to gain physical or electronic access, and to shield true identities in order to avoid detection and prosecution. The major motives appear to be either economic ones, such as fraud or money laundering, or the evasions of restrictions on travel or migration, through the use of false passports and visas. Another scenario raised in the study is that of deprivation of identity, which is widely associated with trafficking in human beings, where identity documents are taken from victims as a means of control, but it has also occurred in the course of war crimes.

The role of information and communications technologies was widely reported and appears to be largely similar to the role they play in the evolution of fraud, but there were some additional observations. Two key aspects raised were the fact that modern technologies now rely on digital forms of identification, which can be deceived, and the fact that such technologies concentrate large volumes of identity information, which can then be taken. These in turn have fuelled a substantial increase in a new form of identity related crime, the illicit trafficking in identity information or complete identities. Historically, the pattern appears to have been one in which identity crime was committed to incidentally to other offences such as fraud, but in recent years this may have changed. The ability to take or copy large volumes of identity information has resulted in a new commodity, and the same technologies also form a means of trafficking and the collection of proceeds. Several States reported incidents in which documents such as credit cards, or credit card information files were taken in one country, quickly transferred abroad using e-mail or Internet applications, sold to other offenders, and used to commit fraud offences within a matter of minutes.

Information about the links between identity related crime and other forms of crime were more speculative than for economic fraud, simply because few States have the criminal offences and legal definitions necessary to support statistical reporting. They were nonetheless informative. A number of States, and most of the experts, felt that, while drawing conclusions about the involvement of organized crime would be premature, a similar pattern to fraud was likely. Identity related crime is complex and sophisticated, which suggests the involvement of an organized criminal group, and many of the secondary crimes which it supports, such as money laundering and trafficking in human beings are already known to
be associated with organized crime. Concerns about links between identity crime and terrorism were similar to those with respect to organized crime. Terrorist groups also have the sophistication and motivation necessary to commit identity crime, including the need to travel and move within a State without attracting attention. As with organized crime, the use of telecommunications frauds, in which false user accounts were created so that communications could not be traced if they were intercepted, was a significant concern.

Efforts to quantify the occurrences and costs associated with identity related crime are much more speculative than for fraud due to the lack of legislative definitions. Most experts, and the limited data available, appear to suggest substantial and fairly rapid increases, and most experts believe that technological development will tend to produce similar patterns in identity related crime to those already observed with respect to fraud. With respect to costs, while losses cannot be quantified, a range of cost factors were reported, and these are substantial. At the Government and corporate level, costs included the need for prevention and security measures, both for identity documents and for the supporting infrastructures. Several observed that the establishment of very sophisticated physical documents for passport and other key functions have tended to simply displace offenders towards more vulnerable targets. For example, if a passport cannot be forged, offenders tend to obtain genuine documents using false information if possible. Not all costs raised were economic. For example, the risk of terrorism or major economic crime has an effect on non-economic behaviours in many societies.

At the individual level, costs tended to be generated for two separate categories of victims. Where false identities are used to commit economic crimes such as fraud, then the victims of identity crime include the victims of fraud, and the losses are quantifiable in the same way. With a false identity is that of a real person, however a second category of victim is created, and the economic and non-economic losses to persons whose identities are misused are considerable. Reports included cases where victims have been arrested and charged with criminal offences or put on terrorist watch lists, for example. Victims may lose reputation or economic opportunities, or their ability to travel may be curtailed. Particularly problematic, in a global information infrastructure, is the fact that false information generated by offenders may spread very quickly on a global basis, but tracking down and correcting that information once the offence has been discovered can be extremely difficult.
Conclusion

Those are some of the most interesting findings. By way of concluding I would like to highlight some of the key areas that we hope to cover in these proceedings. With respect to criminalization, the state of development is very different for fraud and identity crime. For fraud, offences are well-established and the main issue appears to be how to modernize them to deal effectively with the recent increases in transnational fraud, use of technologies, and the commission of so-called “mass frauds”. For identity crime, the question is more fundamental. There is still a debate with respect to whether offences based on the new concept of identity crime are useful development or whether they are redundant with existing criminal offences, and views appear to vary from a legal system to another. If a decision is made to criminalize, then further issues with respect to how to formulate offences and how to define key terms in ways which meet the needs of each country’s domestic identity infrastructure, while at the same time serving the broader need for effective international cooperation arise.

With respect to prevention, there is general agreement that prevention should be pursued, but many issues with respect to how best to do so, and how to integrate the efforts of the number of different entities. These include the need for coordination between the public sectors and private sectors in general, and individual entities within each. At present, for example, the insurance industry and the credit card industry both have sophisticated antifraud capabilities, but not much communication between the two. Similarly, some countries have highly developed fraud prevention strategies, while others do not, raising questions of technical assistance and interoperability. The question of cooperation between the public and private sector appears most acute with respect to prevention but is also a broader and more overarching challenge.

A final area to highlight, perhaps, is the need for more research and data analysis. As I noted at the outset, a major challenge for those working to prevent and suppress economic fraud and identity related crime is the fact that unlike many other forms of crime, these tend to be chronically underestimated by governments. There appears to be a great deal of data, but spread over such a wide range of sources that assembling and analyzing it will be a major challenge. Data are needed to generate a global perception of the full extent of the problem in order to focus expert resources and political commitment towards the development of effective countermeasures. On a more immediate scale, information is also needed with respect to the latest evolution in criminal behaviour. Unlike many
other crimes economic fraud and identity crime often involve ongoing schemes, such that prevention includes a significant reactive element: the more quickly new schemes can be identified and information about them disseminated, the more quickly investigations can be launched and measures to prevent further victimized nation can be instituted. While the need for data and analysis is critical, perhaps the need to develop and identify national experts is even more so, especially with respect to the emerging challenge of identity related crime.
SELECTED PAPERS AND CONTRIBUTIONS
Deve rimanere bianca
AN OVERVIEW OF THE MEANING OF FRAUD IN DIFFERENT JURISDICTIONS AND THE PROBLEMS POSED BY IT (SCOPE AND ELEMENTS OF FRAUD OFFENCES, TYPES OF FRAUD ENCOUNTERED AND CRIMINALISED AT THE NATIONAL LEVEL)

PATRICK CUNNINGHAM
Executive Director, South African Fraud Prevention Service

Applicable legislation

In the South African and indeed the Southern African region the crime of fraud, in general, is dealt with under the Roman Dutch Common Law.

There are a variety of definitions of the crime, one such being: *Fraud is a willful perversion of the truth, made with intent to deceive, and resulting in actual or potential prejudice to another.*

The requirements for fraudulent conduct:
- *misrepresentation* (Perversion of the truth);
- *prejudice* (Actual or potential);
- *unlawfulness* (Willful behaviour);
- *intention* (Intention to deceive).

The element of prejudice allows for actual or potential prejudice. Potential prejudice means that the making of the misrepresentation, looked at objectively, must have involved a risk of prejudice, proprietary or non-proprietary.

I am aware that in certain jurisdictions, the crimes of identity theft and identity fraud are prosecuted as different crimes. It would appear unlikely that in the South African legal system, as it presently stands, that the courts would consider the crime of identity theft as satisfying the common law which states.
Theft consists in an unlawful contractatio with intent to steal of a thing capable of being stolen

The requirements of contractatio or physical control or handling would appear to mitigate against the crime of identity theft being admitted in our courts.

There are statutory enactments which have enhanced the Common Law, most notably in South Africa the Prevention and Combating of Corrupt Activities Act.

The legislation applies to:
• public officers, foreign public officials, agents, members of legislative authority, judicial officers, prosecuting authorities;
• parties to employment relationship;
• proceedings, contracts, tenders, auctions, sporting events, gambling and games of chance;
• public bodies, witnesses, obstructing of investigations;
• conspiracy or accessory thereto.

However, this piece of legislation is primarily intended to address the problems associated with fraud and corruption especially within the public service and does not address the issues of identity fraud.

From a legislative perspective, the introduction of the Financial Intelligence Centre Act in 2003 was intended to curb white collar crime and fraud and money laundering. However there are serious doubts as to whether it has achieved its purpose. Some argue that the conviction rate of only 39 cases of fraud since FICA came into effect in 2003 proves the system is not working.

Unlike the United States with Sarbanes-Oxley, the UK’s Data Privacy Act and the EU’s directives on data privacy to the best of my knowledge South Africa, and indeed the Southern African States do not have specific identity fraud related legislation.

The extent of the identity fraud problem in Southern Africa looking at available data and specifically from the South African Fraud Prevention Service

From the outset I must emphasise that there is no single source of information available that can, with authority, state what the extent of fraud, let alone identity fraud, is in South Africa. Depending on who one
listens to, values relating to fraudulent activity range from ZAR 800 million per annum to ZAR R3 billion per annum. The simple truth is that nobody really knows.

Statistics available from the South African Police Service can be considered as unreliable as the greater majority of frauds are not reported to the Police because of issues which I will discuss later in this paper.

I have therefore confined the data which I present to that which is available from the South African Fraud Prevention Service fraud data management system with regard to identity related fraud.

In the period from 1st January 2005 to 1st November 2007, the SAFPS members have reported 16,876 cases of identity related fraud involving more than ZAR 455 (million).

Over this period these incidents increased from 4,678 in 2005 to 6,831 in 2006 and to 5,479 up to 1st November this year. If we extrapolate this year’s figures out then we will finish the year in the region of 7,100 identity fraud related filings to the system. The problem is certainly not getting any better. The following table and slide provides an indication of the various types of identity fraud over the 2 year period broken down into age groupings.

<table>
<thead>
<tr>
<th>Category</th>
<th>&lt;20</th>
<th>20 to 30</th>
<th>30 to 40</th>
<th>40 to 50</th>
<th>50 to 60</th>
<th>60 to 70</th>
<th>70 to 80</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-False Identity</td>
<td>14</td>
<td>795</td>
<td>1120</td>
<td>412</td>
<td>108</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>02-Impersonation</td>
<td>1</td>
<td>378</td>
<td>682</td>
<td>229</td>
<td>100</td>
<td>29</td>
<td>11</td>
</tr>
<tr>
<td>03-False Employer Details</td>
<td>4</td>
<td>1721</td>
<td>1906</td>
<td>773</td>
<td>265</td>
<td>46</td>
<td>0</td>
</tr>
<tr>
<td>05-Victim of Impersonation</td>
<td>3</td>
<td>434</td>
<td>791</td>
<td>336</td>
<td>118</td>
<td>68</td>
<td>9</td>
</tr>
<tr>
<td>06-Evading Liability</td>
<td>96</td>
<td>2752</td>
<td>2553</td>
<td>797</td>
<td>242</td>
<td>43</td>
<td>7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>118</strong></td>
<td><strong>6080</strong></td>
<td><strong>7052</strong></td>
<td><strong>2547</strong></td>
<td><strong>833</strong></td>
<td><strong>216</strong></td>
<td><strong>30</strong></td>
</tr>
</tbody>
</table>

Since its operational inception in 2001, members have filed more than 54,000 cases of fraud in general to the data management system and involving more than ZAR1.3 billion. I would also point out that many of the SAFPS members do not report financially on savings and losses. Our estimate is that the savings and losses can be increased by at least 20%.
The types of identity fraud being encountered in the Southern African environment

The most commonly used form of identity in South Africa is the identity book. Unfortunately this document is out dated and easily copied, forged or altered. The South African Ministry of Home Affairs intends rolling out a new identity document but the programme has been fraught with problems and is several years behind schedule. It is not known when the new system will become operational. Even when this occurs, it will still be many years before the total population has converted to the new system. The issuing of passports as with identity documents and drivers licences have been the subject of corrupt practice.

Some of the more widespread methods used to manipulate the true identity in the identity document include:

- Removal of the original subjects’ photograph and substitution with that of the person committing the fraud.
- Alteration of the identity document number.
- Forged manufacture of the identity book.
- Use of a deceased person’s identity document.
- Issuing of legitimate identity documents by corrupt employees of the Ministry of Home Affairs.

Although there are no meaningful statistics available for identity fraud committed electronically, there appears little doubt that this type of identity fraud in South Africa is increasing. An examination of the notifications we receive from members of the public requesting assistance due to Identity fraud on the Internet has show a significant increase in the past 2 years.

South Africa, due to its economic position in Africa is the happy hunting ground of people from other African countries such as Nigeria, Ghana, Kenya and not least Zimbabwe. It is estimated that there are 3 million Zimbabweans currently in South Africa. It is indeed surprising how quickly so many of these people are able to obtain South African identity documents whilst our own citizens can wait up to 2 years for a new identity document. The majority of cases involving Nigerian expatriates is money laundering through involvement in the drug trade and prostitution in the major South African cities. These people are hardened criminals and it is an acknowledged fact that the enjoy the protection of many Police Officers through corruption and buy offs. The SAFPS systems hold numerous cases of attempts to open bank accounts by Nigerian expatriates using “suspect” funds.
There is evidence to show that syndicates, especially from other African states have infiltrated our banking system and, utilising false documentation and in collusion with the bank employee, have siphoned off and transferred large sums of money. Again I regret to say that exact figures are not available.

The most common form of identity fraud utilising electronic media is “skimming”. In the majority of cases this occurs in restaurants when the client hands over the credit card to the waiter who takes it away to run the card through the POS terminal. The card data is skimmed and within 12 hours is being used in London and New York. This fraud is now being overcome by portable hand held POS terminals that are brought to the clients table. Not all restaurants have the portable devices and occasional cases of skimming are still being reported.

Other identity frauds on record include:
- Account take-over.
- Refund deposit scam.
- In collaboration with dishonest bank employees who have been infiltrated into the banks by the syndicates, the use of false identity to move funds of South Africans deposited in overseas financial institutions.
- Application fraud:
  - Telecommunications.
  - Retail.
  - Banking.
  - Property.
- Transactional banking fraud.

I have been unable to find any information relating to the possibility of terrorist connections and identity fraud in South Africa. If this is taking place then the States Intelligence services would be unlikely to divulge such information.

The response of Government to the problem of identity theft and fraud

At the behest of the South African Government a National Anti-Corruption Forum was formed in 2001 with UNODC as one of the primary sponsors together with the Embassy of France amongst others. The Forum held its second national summit from 22nd-23rd March 2005 and has held various workshops and conferences since then. The Prevention of
Corruption Act discussed above has been one of the outcomes of the Forum. Unfortunately the Forum has failed to address the problems associated with identity fraud and has concentrated its discussions around public sector corruption.

An examination of relevant documentation and reports emanating from the Forum fails to find any mention of identity fraud.

We are becoming known as the crime capital of the world and South Africa has a very high rate of violent crime. This attracts much public concern and media attention. The Government considers that this aspect must take first priority in its fight against crime.

Secondly, in an emerging economy like South Africa, the demands on social spending, schooling and health are enormous and Government must rightly direct its resources into these fields for the betterment of the population at large. Enactment of legislation related to identity fraud is therefore seen as some way off. However, the Common Law crime of fraud in the South African legal system would appear to be robust enough to be used in cases of identity fraud without the need, in the short to medium term, of legislation dealing specifically with identity fraud.

Thirdly it is unfortunate that the Government and especially the Ministry of Home Affairs, the department dealing with the issue of identity documents, despite the corruption legislation discussed above, is plagued by corruption. This is further exacerbated by alleged corruption at all levels within the South African Police Service with the National Police Commissioner presently under investigation for possible corrupt associations with criminal syndicates. High profile members of these syndicates are pending prosecution for huge drug trafficking crimes. There has been a plethora of papers written on this topic and it is not the intention of this paper to explore the issues further.

There is currently before Parliament draft legislation in the form of the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill which attempts to impose a form of identification process on the purchase of pre-paid cellular phone cards.

However as Professor De Koker rightly points out in his letter to the Select Committee on Security and Constitutional Affairs:

“Unfortunately there is little direct public communication regarding the matters under debate. Civil society has to rely on newspaper articles and other summaries of discussions on detailed and technical matters. This complicates the participation by civil society in the debate. This is unfortunate because the Bill holds grave implications for ordinary citizens. The debate seems to have shrunk to one
between the Department of Justice, that wishes to enforce an
identification process in relation to cellular phone users, and the
electronic communication service providers that have raised a variety
of practical objections in this regard. It seems as if it might be assist
the legislative process if the debate could be enriched with more
concrete information regarding two key matters. In the process of
probing these matters the Committee will also ensure that it
considers key issues relating to the interests of citizens”.

The perception that South Africa is a criminals paradise has been
occasioned by a number of factors, all of which are discussed in this paper,
namely.

A liberal Constitution that enshrines the values of human rights.
This allows for criminals to take advantage and manipulate the keystone of
our democracy to their own criminal advantage.

A Government that has many question marks hanging over its head
with regard to fraud and corruption.

An enforcement agency that is acknowledged has having large
scale corruption within.

A criminal justice system that labours under rules that cause huge
backlogs in prosecution.

An extremely low success rate in criminal prosecutions including
fraud.

*The effect of the criminal justice system on identity theft and fraud*

There is concern in legal circles around the time being taken to
bring criminal prosecutions to finality and it is not uncommon for financial
crime cases to take between 2-3 years before prosecution even starts. The
right of bail and the protection of the Constitution has given criminal
elements the opportunity to delay cases appearing before the courts by
simply firing their counsel just before trial and insisting that they acquire
another defense attorney, thus delaying trials and sentencing.

I have attempted to find cases of prosecution for identity fraud in
our courts, and although I am not saying there have not been any, I have
been unable to find any reported cases in the case law on the subject.

However, an examination of reported fraud cases involving
minimal amounts of money, usually result in either a fine or a suspended
sentence being imposed. There are cases, several in number, where
imprisonment has been imposed, but these appear to be more for employee
theft and fraud where the trust of the employer has been impeached.
In summary, the prosecution of identity fraud appears to be non-existent in South Africa. As previously indicated this can be the result of complainants failing to lodge an official complaint with the Police knowing in advance that the complaint will either not be dealt with at all, or badly investigated, and with little chance of a successful prosecution coupled with immense time delays in the process.

In the past few years a number of Commercial crime courts have been established in the major centres in South Africa. This very welcome step in the right direction has meant that prosecutors and investigators are involved with serious financial crime investigation and prosecution in tandem. The prosecution success rate in these courts is around 90%. However I must point out that cases referred to these courts are selective and prosecutions are usually of people already identified through audits and the Financial Services Board as having been fraudulent in their business activities involving many millions of rands. Identity fraud does not appear to feature in the Commercial Crime courts at this juncture.

The response of the private sector to the problem of identity theft and fraud

If I may digress for a moment and take you back to circa 1988 when Superintendent Keith Balchin of the UK’s Metropolitan Police at Scotland Yard’s Fraud Squad addressed a gathering of bankers and retailers.

In brief Keith Balchin told the gathering, inter alia, “Don’t expect the Police to do your work for you. Get your own houses in order and start preventing fraud instead of expecting the Police to investigate it”. This advice was taken to heart by many large UK organisations and led to the formation of CIFAS, and I am sure that many of you here today have heard of, if not have dealings, with CIFAS. Suffice to say that in the intervening years CIFAS and its members have prevented billions of Pounds of fraud through the concept of data sharing and have prevented many attempted identity frauds.

The CIFAS concept was introduced in South Africa in 2000 and I will talk on this a little later. There can be no doubt that from a private sector perspective “getting our house in order” is paramount.

Chairperson, it seems that the picture I have painted so far is one of doom and gloom. Yes, we do have challenges. Yes, both the public and private sector need to address the identity fraud problem more systematically, but South Africa is an emerging economy with massive challenges on the social front. We have come from a background of
repression and we move, albeit slowly and with some caution, into the future where we know we can play our part on the world stage. Our banking system is acknowledged as one of the most advanced in the world and our rating in the world’s financial markets is high. I know we will do it.

I have already indicated the contribution to the fight against fraud in South Africa that is being made by the South African Fraud Prevention Service and its members. SAFPS is confident that it is making inroads into fraud prevention and particularly that of identity fraud.

To this end our system not only allows for the filing of details of people who have committed fraudulent conduct but we also file data on victims of impersonation in order to try and protect them from further impersonation. In addition SAFPS provides a free public service whereby people can register the theft or loss of identity documents with us. These details are circulated to our members and in effect once that number is “in the system” it prevents its use in attempted identity frauds.

The success of this service has been tremendous and has saved a lot of South Africans from the trauma of impersonation.

Being Internet based, the SAFPS fraud data management system is open to members on a 24/7 basis without the need for expensive IT hardware and software and integration into complex banking systems. The success of SAFPS in South Africa is borne out by the fact that we are in the process of extending the service into adjoining countries, with Botswana and Swaziland being the first to “come on board”. Our objective is to provide the service to the whole of Southern Africa by the middle of 2008.

Without wishing to labour the virtues of the system, our members are able to:

- identify syndicate fraud;
- receive warnings of syndicate activity;
- identify identity fraud and impersonation;
- file data in 9 different categories including identity fraud and impersonation, both as the offender and the victim;
- search for information on a variety of search criteria.

I have already spoken on the monetary savings our members have achieved. I regret I cannot give figures on the number of people who have been saved from victim status nor the trauma that has been prevented by the service.

In 2005, having seen the success that SAFPS was achieving, we were approached by ATMIA/GASA, the International ATM industry Association to develop an ATM crime system based on our own system for
the recording of crime internationally by ATMIA/GASA organisations. Known as Cognito, the system now provides the international ATM industry with an Internet based ATM crime data management system.

SAFPS believes that it is the only organisation in South Africa that is effectively addressing the identity fraud crisis by proactive service provision to its members and to the public.

In the latter instance we offer a free service to the South Africa public for the registration of lost or stolen identity documents. These details are circulated to our members and should a lost or stolen document be used in an attempt to obtain goods or services our members are able to prevent the fraud. A simple, but what has been proved to be, a highly effective proactive deterrent against identity fraud.

Proposed regional and international remedies to reduce identity theft and fraud

Laws, Rules and Regulations are reactive, ladies and gentlemen. They do little to prevent fraud and crime. If they did, why is crime internationally increasing faster than laws are being passed to prosecute criminal behaviour, often with little effect? They allow for the prosecution of offenders once caught and set standards for prosecution and penalties for such offenders. From my experience over the past 40 years they seem to do little in the prevention arena.

It is my contention that in the field of identity fraud there has got to be a proactive approach to the challenge. The international community cannot sit back and wait for Governments to pass laws. As the age of technology becomes even faster, so to will the threats and cases of identity fraud become even more numerous. Protection of the individual must come about through proactive conduct on the part of countries and it is my further contention that it must be the private sector that must take the lead but obviously with the involvement of governments and bodies such as UNODC.

It is accordingly my humble submission to this Forum that we take up the challenge and I would place before you for consideration a set of guidelines that was the basis on which both CIFAS in the United Kingdom and SAFPS in South Africa were founded and which have proven to be the success they are:
• An international and regional data management system of identity fraud related crime. I have already mentioned the Cognito system developed for the international ATM industry.

• If I may quote Mr. Mike Lee the CEO of ATMIA/GASA with extracts from their documents:

   “The Objectives of an International ATM Crime’ Directory:
   - Standardised recording of ATM crime
   - Standardised reporting of ATM crime data
   - Systematic research on ATM crime data
   - Co-ordinated response by industry & by police to ATM crime
   - Appropriate allocation of resources to ATM crime response

The Benefits of an International ATM Crime Directory:
- Greater consistency of ATM crime data, definitions and terms at an international level
- Greater coherence of response to ATM crime
- Greater centralisation & mobilisation of ATM crime-fighting resources”.

• The technology is available and all that needs to be done is to change the cosmetics around names and agree through debate and engagement the reporting contents of the system.

• Such a system must be free of political and commercial interference, although obviously governments and commercial concerns would be members.

• The service provided must be non competitive in nature.

• It must operate in a non-profit environment.

• The system should be financed by member fees in equal part to ensure that there can be no pressure brought to bear in the effective operation of the system as well as government and hopefully UN support.

There is unquestionably a vacuum in international crime data management systems that are available to non government law enforcement agencies. In the field of identity fraud prevention this is a serious problem that must be confronted.

* Delegates may wish to substitute the wording “ATM crime” to read “Identity Crime”.

43
I thank the Chair and organising committee for inviting me to this Forum and for the privilege and honour of having been able to address you today.
I am grateful to the other Speakers for the interesting statistics they have provided. I have a number of recent ones of my own upon which to comment, both from Italy and abroad, including those published by the American Federal Trade Commission in February this year. We need to pay close attention to statistics from all countries, but a degree of caution is also needed. Fraud is generally under-reported and statistics can be incomplete and misleading if all of the variables are not taken into account. Many frauds are not discovered by victims or by the controllers of data banks, and many that are discovered may not be prosecuted. Reports of frauds which do trigger actions to prosecute or recover losses are also sometimes not occasionally transmitted to various organs which collect and analyse data. There are also definitional issues – it may be difficult for officials to distinguish between simple errors and actual frauds or swindles. So, we have to be careful.

We need caution also – as previous Speakers have pointed out – in dealing with the concept of “identity theft”. There are a number of different phenomena: alongside actual frauds and swindles that involve identity crime elements, there are also identity abuses which are separate from fraud. These include problems such as substituted personalities or impersonation, and conduct which damages another person’s identity. These can be intentional malfeasance, they may arise in the context of other malfeasance, such as computer viruses, or they could occur in accidental or relatively innocuous circumstances. Simply having or using another person’s identity may not always be a crime: identities may be exchanged consensually for example, which would not be a crime in its own right, but might become a crime if the exchanged identities were used for a criminal purpose. We also have cases in which false identities which are used to mislead are not the product of identity theft or the taking of identity information from real persons, but are instead completely fabricated
identities of nonexistent people. When real identities are taken and misused, those from whom they are taken can suffer substantial harm. In our Italian experience, victims of such crime have been themselves subject to criminal proceedings simply because a card for prepaid cellular telephone service used by others in connection with the commission of serious crimes was falsely obtained in their name.

As President of the Schengen Municipal Control Authority in Brussels, I can tell of the trauma of many people whose activities have been taken and misused, and the difficulties they have faced in re-establishing their identities and repairing their reputations following criminal identity thefts. The losses are not just economic. In addition to the risk of criminal prosecution and sentences, victims have been expelled from Europe under false names which properly belonged to others, when they were unable to establish their true identities. In some cases we found it virtually impossible to fully restore victims’ original identities and we have had to resort to the creation of a second, entirely new, identity for people who have been robbed of their true ones. We refer to this as the “alias” problem.

The offence of identity theft is often committed from a distance and I would like to say that, in my view, the future will see many more opportunities for the misuse of digitally-based credentials of citizens and consumers, even without knowledge of the victims’ identities.

One subject that we have begun to address in the Authority safeguarding data in Europe is identity theft in on-line social networks, such as blogs and newsgroups in which many young people spontaneously record and disseminate personal information. These seem innocuous, but collectively assemble large amounts of personal information and can represent a major identity crime problem. Offenders may gather sufficient information to assume another’s identity, including personal information needed to guess passwords or deceive institutions verifying identities. These scenarios also pose a challenge for criminalization, because the information is freely posted or made available on public networks, and taking it is not analogous to theft in most legal systems.

I have appreciated the statements that have been made up to this point on the need for a systematic approach and on the need to pay attention to the educative aspect as a means of preventing identity crime. As new technologies develop, there will, on one hand, be a greater prevalence of inexperience, well-meaning trust and naivety among common citizens, who take time to fully adapt to new technologies, while at the same time, on the other hand, new developments mean new opportunities for offenders, who adapt to the technologies much more quickly and find ways to exploit them for criminal purposes.
Another aspect that I would like to raise is the way in which countless millions of pieces of information are held inadequately by public and private handlers. In Europe there is a new right embodied in the Nice Charter which is now solemnly figuring as a fundamental right in the new European Union Treaty, replacing our failed European Constitution but destined to be recognized in the same light. This right is not entitled “the right to privacy” but “the right for data to be protected”. Of what then does this right consist? It goes beyond established rights to privacy and includes a right to have one’s personal data adequately protected, which imposes an obligation on custodians of data to protect it. It also includes a right to ascertain whether and how information is held securely by whoever is entitled to hold it. It entails the application of the principle of precautionary measures, because so often the collection of information is bulimic, or there is an exaggeration, or it is irrelevant to purpose, or it is excessive in amount.

The legal regime in Europe today views the management of data as a risky activity, but this is not a negative assessment. On the contrary, “risky activity” in Europe’s Civil Codes signifies an important activity, one which must be given an incentive by the system, but also one which may cause serious harm to citizens if certain measures are not adopted. Thus we do not only need to concern ourselves with the problem of legally reporting these facts on the part of private data handlers.

I share the preoccupations that have been voiced. I would like to note that the Computer Crimes Act in Italy makes it mandatory for some crimes to be officially prosecuted as opposed simply to being subject to an unregulated complaint by interested parties. The Act also provides that certain penal norms may be invoked by the managers of data-banks only if adequate security measures have been adopted. The state will not accept a request for protection from a data-bank manager or for prosecution, unless it can first be shown that the data have been held in a secure manner.

In addition to issues relating to the quantity and security of information, there is also the problem of how the interested parties are to be identified. New European normative acts frequently require the inclusion of secure identification measures such as digital photos in physical documents, often with lamination or other security measures, biometric data or RFID devices. These can be made resistant to tampering or falsification, but identification itself is only as good as the link to the actual person identified, and adequate attention is not always paid to verifying the physical identity of the person to whom such a sophisticated document is issued. In Italy it is possible for an identity card to be issued without the
production of the previous one only to a person who can produce four verifying witnesses.

The new Italian electronic identity card contains a splendid secure chip and even I have not been able to refrain from wanting one. However, when I applied for it, I did not need to produce the preceding identity card, and I was not asked for the four supporting witnesses. As a result, I would have been able to acquire a magnificent identity card bearing my own digital imprint, but perhaps also a name different from my true one. This issue calls for serious attention. We are preoccupied with requiring a fingerprint on key identity documents, such as the European passport, national passports or national identity cards, but these appear only on the card which the interested party carries with him. They are not included in the data banks used to verify identity, along with other information about the person being identified. Technicians call this a system of one to one verification, rather than a system of identification.

We are also focusing strongly on the problem of requests for photocopies of identity documents. People who go to a public or private office for whatever purpose are often asked for proof of their identity and sometimes it suffices to show a document or even perhaps a copy of a document. In the field of mobile telephone operations, for example, this has resulted in many thousands of cards for prepaid cellular telephone service being registered under incorrect or false names. These can be used by offenders to make telephone calls which, if intercepted by law enforcement, cannot be traced back to them. A few weeks ago, a short distance from here, a delicate police operation impounded hundreds of thousands of cellular telephone cards carrying false identity information, in many cases referring to citizens who probably even today have no knowledge at all of this fact. To deal with problems such as this, we have to concern ourselves with how information is held and what concrete security measures are in place. Given modern trends in the way data are processed and the ease with which they can be transferred and stored, this concern extends not only to government agencies, but also to the behavior of private companies in the outsourcing field, which can no longer be controlled solely by the managers of their core businesses.

Identity theft is a crime which often causes ongoing damage to victims over an extended period, and this is also true of many fraud schemes. All too often, those who lament the offences fail to give sufficient attention to the moment when information is taken and the need to alert potential victims, including those whose identities have been taken and those who might be victimized by offenders misusing them. In some countries, where there is the greatest level of fraud in the economic field
with regard to loans, bank advances and even credit cards, no policy exists
with regard to the right of access by interested parties who have suffered
damage. Other than the fact that they have been informed by the police,
they have no right to a timely report to put them in the picture prior to the
damage occurring. Alerting victims not only reduces the losses, it may also
be important for investigative reasons. This is why jurisprudence tends to
concentrate strongly on systems that consult victims in tracing losses and
proceeds. Currently available statistics in Italy and elsewhere in Europe
show that more than 50% of illegal activity in the information sector results
from criminal insider operations. Thus it is important to have alerts in
addition to tracing operations. For example, the Italian Guarantor has
required all operators in the mobile phone sector to have an alert system:
whenever a subscriber’s name appears on more than four telephone
accounts (seven in the case of a business), the subscriber receives an SMS
text message from the telephone company checking whether anyone is
improperly acting under their name.

There is work to be done in the way that public and private
undertakings are working today, because there is increasingly more
ubiquitous computing. We are increasingly working away from our offices,
conducting private activities in public places. We carry with us our laptops,
as well as our memory sticks, mobile telephones and web mail services.
The result is that we are carrying a wealth of information with us, and often
transmitting it wirelessly, and the storage and transmission media may not
always be properly protected.

Thefts of identity can occur even with the most mundane mailing of
a disk, as has occurred in England (as you will have read in all the
European newspapers), where two disks containing data on some twenty-
five million citizens, mailed in a perfectly normal envelope, went missing.
Where did they end up? What will the people into whose hands it comes do
with this information?

I would like to conclude by saying that, apart from dealing with the
criminal aspect, we must be concerned with the restrictions our democratic
societies have had to face since 9/11. Security measures in critical areas
such as air travel necessarily involve a mix of public and private sector
elements. For security reasons, which I fully understand, many legislative
provisions in Italy, Europe and the world at large, now require private
operators to obtain much more information. The air carriers have the names
of people who purchase tickets, and governments have the identities of
suspected terrorists, but unless private data flows to the public sector and
public data is given to the private sector, none of the data are of any use.
These data-exchanges are necessary, but they also entail some degree of risk and the need for adequate security and crime prevention measures.

Today, so far as air travel is concerned, the new American PIN-air system, and soon its European version, will enable much more data to be registered in relation to a simple flight. Nevertheless as this multitude of information accumulates, greater problems arise with regard to their security. We need all to reflect on the way to use the Personal Identification Number (PIN), the so-called common identifier numbers that will be used to identify passengers. These bring benefits in terms of quick and reliable identification, but also disadvantages in terms of theft of identity, because a number of violations have become easier to commit. Consequently we have proposals and efforts from the information sector on how to use the codes more securely. These include finding ways to “anonymize” part of the code itself or only utilize a given part of it in isolated transactions. This allows varying degrees of security depending on the requirements of each type of transaction, and limits the extent of the harm if the code is compromised in one transaction.

Here I cite the interesting Austrian experience, where there is a multi-use single national number, which permits, through the use of algorithms, different numbers to be memorized, different templates, according to whether the authorized holder is using the card in the health sector, the private sector or the public administration sector.

I conclude with a reference to the Seventh Framework Programme which the European Commission has initiated to give major financial backing for the study of new Privacy Enhancing Technologies. This involves funding for research into new developments in information and communications technologies to improve security and find new ways to protect data and prevent offenses, including identity thefts and frauds. In this sense, we have been at pains to propose to the private sector the application of the one box only principle, whereby data in a given category would preferably be retained by one holder and would not be duplicated in the archives of all the other public and private bodies needing to access it. Instead of retaining their own copies, other users would consult the original source. That, of course, carries its own security risks that the data will be intercepted in transit. To protect against this, sources would only be consulted through telecommunications under stringent conditions, including authentication of the parties and records of all such consultations.

1 See http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3402
being kept in two places – at the site of consultation and the site of reception. These records and identification systems should make it easy to discover the perpetrators of any fraudulent use.

We must also recognize – and this is truly my last word – that there are new categories of identifiers, like genetic data and biometric data, whose abusive utilization can produce serious difficulties. Biometrics are very unique, but as identification they are only as reliable as the information which is linked to them in identity data bases. As a member of the judiciary, I think that if my iris or retinal scans were to be stolen, perhaps the problem would be rather light, and if human odour were to be used as an identifier (there are some experiments in this direction), I would have few difficulties. However, if someone were to succeed – and this has already happened in Japan – in changing the data base template for the original fingerprint on my identity card, I would risk, without any other possibility, of being expelled from the bench for the rest of my days. If someone should then think in the future of using the prints in the criminal field also, we would have inflicted a severe vulnus on the reliability of proof in penal proceedings.

In one sense, the statistics that have been presented today show us how fortunate we are. Although the data emerging are very serious, in the sense that the number of thefts of identity is high, there are, nevertheless, millions and millions of pieces of identity-related information that are held in inadequately secure conditions and we remain fortunate that no-one at present is abusing them.

I believe that one day all of us must be free to enjoy an agreeable life in information science, but one where we will simply be able to say “I am”, and not have to admit that, “Without paper, I am not”.
IDENTITY RELATED CRIME AS A GLOBAL ISSUE: THE NATURE CONCEPT AND TYPES OF IDENTITY RELATED CRIME

CHRISTOPHER D. RAM
Counsel, Department of Justice, Criminal Policy Section, Canada

The first question we should ask with respect to identity-related crime is why we should be concerned about it at all, and why it should be an international issue. National governments rely on identity for key aspects of governance, such as controlling entry, regulating voting, and as the basis for identifying criminal and terrorist offenders or suspects. Private companies and individuals also use identity for banking, property ownership, and a range of commercial transactions. Underlying this is the reality that identity is everywhere. Identity does not just consist of a document, it encompasses identity documents and information, both on those documents and elsewhere, which is used to establish who we are as unique individuals, and to link all other information about us. Criminal subversion of identity documents and identity infrastructures is a major concern because of the universal nature of identity.

Identity crime is not new. Criminals have always used false identities. What is changing are the ways in which we establish identity and the ways in which identity can be abused. Technological change has substantially increased the threat, and globalization, travel and information technologies have made it a global threat. Technological change has centralised identification infrastructures, which concentrates data. Credit-card data is stolen by hackers en masse. As recent developments in the UK demonstrate, the identity information of millions can be stored on a disk and lost or stolen in a single act.

Once personal data is stolen and misused, the interconnected nature of identity infrastructures has made it much more difficult to correct the problem. The details of identity infrastructures and identity crime may be different in developed and developing countries, but the underlying issues are the same. The ability to establish and verify identity is critical to domestic stability, security and prosperity, and this makes it a critical factor in development and reconstruction.
Results of the study on identity-related crime

The Study had more difficulty with identity-related crime than economic fraud because it is a new concept. There was not much hard data on rates and trends, although a number of States reported that it was a serious and increasing problem, and some reported data on related crimes such as impersonation and forgery of identity documents.

The new focus is to criminalise conduct in respect of identity documents or information specifically, instead of focusing on frauds and other crimes committed using false, stolen or fabricated identities, but this is more complex than it might seem. Those looking into criminalisation options have had to address several distinct scenarios:

• Identities may be completely fabricated, which means that the offender is pretending to be a non-existent person, but there is no element of “theft” or illicit copying or taking of identity information.
• Identity documents or information from a real person may be physically taken (identity theft) or obtained by deception (for some States this was identity theft and for others, identity fraud) and the offender then pretends to be a real person.
• Identity information may be taken from open, public sources, such as public directories or Internet web pages, and used to create false identities for criminal purposes.
• Identification systems may be tampered with so that information linked to a real identity, such as a criminal or immigration record or bank account is falsified or altered.
• Identification information itself may be trafficked as an illicit commodity, especially if stolen en masse (e.g. hacking commercial sites for credit card files).
• For some States, the problem also included the secondary offences such as fraud or illegal entry committed using the false identities or documents.

To understand identity crime, it is essential to look at the underlying identity infrastructures. The forms of identity crime may be global, but the identification systems differ from one country to another, and this triggers differences in the approaches to criminalisation and other responses. Some States have centralised identity systems, while others rely on specific identification for purposes such as drivers’ licences and passports and private identification for purposes such as banking, credit, and insurance.
Identities usually consist of specific bits of information which, when linked together, are unique to each individual, but which are not unique in isolation. Many people may share my name, for example. It only identifies me as a unique individual taken in combination with my address, date of birth, photograph, fingerprints or other identifiers. As traditional identity information such as names, birth information and addresses have become easier to misuse, identity infrastructures have increasingly turned to information which only the individual would know, such as passwords or PIN numbers, or physical or biological data such as photographs, fingerprints and DNA radiographs.

A critical concept in developing criminal law will be the idea of “identity information” and distinguishing it from other forms of personal information and other justifications for protecting it. My health records and bank account balances, for example, are “personal information” and subject to legal protections for privacy reasons, but they do not identify me. The concept of “identity information” and the legal and policy justifications for requiring it to be protected and for criminalising misuses of it, are relatively new developments. One clear finding of the study was that, while there seem to be clear reasons for protecting identity information as such, very few countries do so. Even European and other countries which protect personal information do not usually differentiate between personal information such as financial or medical records, and the much narrower class of information needed to uniquely identify the subject of such records. To some extent, the choice of identifiers has also depended on the importance of establishing identity. The more costly and in some cases, intrusive means, such as DNA radiographs and fingerprints, tend to be reserved for functions such as criminal records, for example. Photographs have been used for some time on passports, and the use of fingerprints to identify criminal offenders dates from the 19th century.

Only one of the States which responded to the study, the USA, has criminalised “identity theft”. A few other countries, including Canada, reported that they were considering legislation, and Canadian legislation was introduced in the legislature just before these proceedings. Some US and Australian States have also established specific identity offences.

A range of more traditional identity-related crimes were also described in the study:

- offences committed using false identification, including fraud, illegal migration-entry, privacy offences, impersonation;
• offences to protect specific identity documents, most commonly passports or national identity cards (e.g., failure to update information or providing false or misleading information); and,
• offences which protect the integrity of identity, such as privacy or disclosure offences, offences of using false information to obtain identification, and a range of general or specific corruption offences.

Some identity crimes were also included within broader offences. For example, forgery offences generally include the forgery of identity documents, and theft offences may include the taking of identity documents or information. In some countries, especially States Parties to the Council of Europe Convention on Cyber Crime, cyber crime offences such as “hacking” also included the taking or copying of identity related data. A number of States also had or were considering offences to deal with “phishing” and related conduct in which identity information is obtained by deception. A key issue for many systems is whether intangible data, including identity information, is “property” so as to bring it within the existing scope of theft offences.

In criminological terms, most identity-related crime starts with offenders obtaining either identity documents or the sorts of personal identity information needed either to obtain documents or to impersonate others while committing other crimes such as fraud. This may involve either physical identity documents and offences such as the use of documents stolen by pickpockets or taken from waste, or parallel activities used to obtain digital information. This includes sophisticated computer hacking and the use of malicious software to take personal details such as names, addresses and credit-card information en masse or less-sophisticated means such as the use of personal surveillance or small video cameras to obtain PIN numbers.

Once obtained, identity documents or information may be used immediately to commit other offences, especially credit-card fraud, where the information is usually quickly changed when the card-holder or company realises the card has been compromised. More sophisticated operations tend to transfer the information and use it to obtain further ID, building more sophisticated false identities. Several States reported credit card operations where e-mail was used to quickly transfer compromised information to associates or groups in other countries, and lists of potential fraud victims are sometimes sold from one criminal group to another.

The identification process includes both physical indicia or documents and the underlying systems that issue and verify identity.
Offences commonly involve deceiving issuance systems to generate genuine but false ID, especially for elaborate documents such as passports. Not reported but also possible is tampering with identity systems so illegitimate identities are recognized as valid. States where paper documents are common also reported old-style forgery, often with the use of new technologies such as document scanners and high-quality printers.

An overarching finding of the Study was that changes in information and communications technologies are closely linked with criminal opportunities and increases in both fraud and identity-related crime. Most of the hard evidence is for fraud, but States and experts expect ID crime to follow a similar pattern. A number of ways in which technologies may influence of identity related crime patterns were raised:

- Greater dependence on digital and automated identification rather than face-to-face recognition has created new opportunities whereby offenders can use false digital information to deceive the systems.
- The concentration of large volumes of identity data in single systems has created the potential for large-scale thefts, and the technologies also have provided the means for both hacking and copying the information. The same technologies have also provided a means of rapid and relatively secure global trafficking in the data and a means of collecting and laundering proceeds from trafficking.
- Technologies have also provided a new means of contact between offenders and victims. This is a critical element of modern fraud, but also for fraud related types of identity crime, especially, “phishing”, in which inexperienced users of technologies are deceived into providing computer passwords and other identity information.
- Aside from providing an infrastructure for trafficking in stolen or copied and identity data, as with other forms of cyber crime information and communications technologies also provide the means whereby offender expertise and techniques are disseminated. When a new form of identity related crime is created by an innovative offender, it quickly spreads, both geographically, and to broader and less sophisticated groups of offenders.
- As discussed at the beginning of these proceedings, the role of information and communications technologies may differ between developed and developing countries but the technologies are clearly a factor in both. Developed States were more concerned about mass-hacking and other common forms of cyber crime, whereas developing States tended to be more concerned about use of
technologies to forge paper identity documents and other documents used to commit fraud.

Increasingly, identity infrastructures are themselves becoming global. Specific identity infrastructures tend to be reserved for national governments or specific companies, but in both public and private sectors, global inter-operability has become a major challenge. Banks, credit card issuers and other financial institutions must now serve a global market. In the public sector, the need for a global passport and visa system has been supported by Passport Agreements, and more recently by the work of the International Civil Aviation Organization on technical standards for passports.

Regarding costs, States had no real data because they had no legal definitions on which to collect it. There was some private sector data, but it tends to be business-specific, which raised issues of comparability and analysis. Identity related crime tends to be closely related to other secondary crimes committed using the false identities, and a major challenge is the difficulty in distinguishing between the costs of identity related crime per se and the costs of secondary crimes such as economic fraud. This is further complicated in the area of economic crime by the fact that both the predicate offences and the identity related crime are also closely related to money laundering. One can easily imagine the same costs being calculated three times.

Costs linked exclusively to identity crime also tend to be indirect and intangible, compared to fraud. For example, a company whose credit card files are stolen might face a series of direct and quantifiable fraud losses, but also a loss of customer trust or confidence. For identity crime, costs tend to be allocated against two separate sets of victims. Direct costs arise for third-party victims of offences using false identities, such as fraud, but there are also both direct and indirect costs to victims whose identity is taken and misused. These include:

- loss of reputation, business opportunities etc.;
- cases of surveillance, arrest, travel restrictions and other inconveniences as the victim is identified as a possible offender; and,
- the costs associated with of searching out and replacing false data in domestic and foreign data-bases, and of obtaining new identity documents.

In addition to costs to victims, there were also general economic costs associated with factors such as the loss of confidence in banking, finance and commercial structures. There was a range of general damage to
public identity systems, such as the costs of interference with voting systems, would the corruption of licensing systems. Inappropriate candidates might be elected based on fraudulent votes, or incompetent individuals might be licensed to drive, for example. A further range of costs were the security in prevention costs of making identity systems resistant to tampering, and left the public and private sectors. Finally, they were the substantial costs of investigating and prosecuting offences in the public sector, and the corresponding costs associated with the recovery of losses in the private sector.

Most of the countries which responded indicated that prevention was a key issue. It was seen both as a major need, in the sense that it was preferable to prevent an incident then to have to react to it afterwards, and a major opportunity, in the sense that much identity related crime was seen as preventable. A key issue raised by a number of respondents was the need for cooperation between the public sector and the private sector. Public and private identity documents and infrastructures often overlap – passports or national identity cards might be required in order to open bank accounts for example – and one respondent even suggested that as major beneficiaries of its national identity system that some of the costs of operating a system might be allocated against the private sector. Most States also use their criminal law to protect commercial interests to some extent. The most obvious example were offences relating to fraud itself, but a number also had offences dealing with critical commercial technologies such as credit cards. While the companies had an interest in maintaining commercial competitiveness and minimizing economic losses, the governments themselves had an overarching interest in protecting the stability and integrity of commerce.

Responses on prevention had several focal points. They addressed both strategic prevention, which related to the general need to develop and implement infrastructures that resistant to crime, and situational prevention, which related more to the rapid identification of ongoing criminal schemes and dissemination of specific information to those likely to encounter the schemes in order to generate both criminal investigations and preventive countermeasures in order to minimize the damage.

Many reported measures focused on physical identity documents, such as technical measures against forgery and counterfeiting, limits on periods of validity of the documents had to be regularly renewed, and the use of photographs and other identifiers. Other reported measures focused on the protection of identity infrastructures themselves, from a range of threats which included external tampering or deception, as well as
corruption or interference by insiders. To be valid and reliable, the process of creating identity and issuing documents had to be protected from deception. The most sophisticated biometric identity systems, for example, become unreliable if the link between the biometric information and the other information concerning the individual is unreliable. In addition to establishing basic identity and issuing documents it was also necessary to protect the verification process. Once in circulation identity documents are used and those uses involve retrieving information from the infrastructure. At the simplest level is required elements such as photographs on documents so that those responsible could verify them on the spot. For more complex systems verification and use involves the transmission of data back and forth which requires encryption and other protections against interception. One widely reported safeguard was the use of multiple identifiers. Some referred to triple redundancy systems which included something the person identified:

- knows (PIN number);
- has (keys, cards, documents); and,
- is (photographs and other “biometric” identifiers.

Aside from technical preventive measures, situational and strategic prevention also extend to education and training elements. Situational measures included the training of employees and other key workers on how to identify prevent and react to identity related crime, and strategic measures included widespread public education on how to recognize identity crime schemes, how to protect their own identities, and what to do to minimize the damage if an identity related incident occurs.

One of the most striking aspects of identity related crime is that it is almost always associated with some secondary form of crime and analogous to the concept of the predicate offence and money laundering. Recent developments suggest a trend in which identity crime elements were often committed by offenders engaged in offences such as fraud, organized crime or terrorism on an incidental basis, but are increasingly being committed by more specialized offenders who take or fabricate identity information the symbol complete identities, and then sell these as a form of illicit commodity to other offenders who use them for secondary crimes. The most common form of secondary crime, both in volume of proceeds and number of occurrences would appear to be fraud, and this was a major concern of the private sector. Many governments also saw this is a serious problem, but rank it behind tampering with travel related identity documents such as passports and visas in terms of seriousness. This is probably because for governments, national security elements, the security
of borders, and the ability to identify those who cross them raise substantial non-economic issues.

Many respondents saw links between identity-related crime and both organized crime and terrorism as being similar. Organized crime and terrorist activities tend to involve fairly sophisticated groups with a significant incentive to conceal their identities and the nature of their activities from a law enforcement and security agencies. Both need to travel domestically and internationally without surveillance, to be able to transfer and use resources, and to communicate without interception and tracing. The relationship between identity related crime and money laundering is long established, and underlies many of the established anti-money laundering measures, such as “know your customer” requirements. The relationship between identity related crime and trafficking in persons is more novel and complex, having been raised during the negotiation of the Palermo Protocol only in 1999-2000. One aspect is similar to travel related crime in general. Those seeking to move persons from one place to another without being caught by traveler immigration restrictions use essentially the same methods to conceal identity, whether they are themselves traveling illicitly, whether they are smuggling migrants, or whether they are moving victims of trafficking from one place to another. An added element in the case of trafficking in persons has been the tendency of offenders to strip victims of their identities once the transfer process is completed, as a means of exerting ongoing control.

All of these connections represent significant challenges for researchers, but they can also be seen as significant opportunities for the prevention and suppression of various forms of crime. In considering prevention, it quickly became apparent to the expert panel that to the extent that identity related crime was also an element of many fraud schemes, the prevention of identity related crime could also be seen as a means of preventing fraud. The same is true for other crimes such as money laundering and terrorism, and the same is equally true both of prevention and investigative elements. The development of more secure identity infrastructures, and means which identify cases of tampering and other illegal activity not only serves as a control and identity related crime, but also a valuable means of detecting preventing or prosecuting the secondary crimes associated with identity crime. The same argument can also be extended to criminalization. The existence of identity crime offences may, in many cases provide the basis for detection and investigation which starts with the identity offence, but then spreads into a broader range of criminal activities.
In conclusion, approaches to identity crime, and views about the merits of identity crime as a new perspective may vary, but this is clearly an area which merits further consideration.
BIOMETRIC IDENTIFICATION TECHNOLOGIES
AND THE USE OF E-SECURITY TO PROTECT IDENTITY

ROBIN CHALMERS
Head of International Policy,
United Kingdom Identity and Passport Service

One of the major challenges that border authorities face is the need to be able to satisfactorily identify travellers. Up until recently this has traditionally meant reliance on the ability of the border inspector to spot something out of place either with the passenger or their document. However as the numbers of travellers increases worldwide, the amount of time that inspectors have to make a judgment on the person or the document is being reduced. There are higher levels of expectation from the traveling public about the time they should be kept in a queue waiting at passport control. Increasing the number of border inspectors is usually not an option. Technology has a part to play in the solution to these problems. In particular the use of electronic passports (“e-passports”) which record information about the traveller that can be read and recorded automatically whenever the passport is used at a border-control point, can make transit faster and easier for travellers, while at the same time providing enhanced security by increasing the reliability of the information on the passport and the ways it is checked against other records. In this presentation I will be covering the following:
- Background to the introduction of e-passports.
- Choice of biometrics.
- Technical Specifications.
- Benefits of e-passports.

The term “biometrics” refers simply to some form of characteristic which is measurable or observable and can be observed or recorded visually or by apparatus, and which is sufficiently unique to each individual that it can be used for identification purposes. Some forms, such as photographs and the use of fingerprints, have been in use for some time, while other, newer forms are now emerging as more is learned about
unique biological characteristics and new technologies are developed that can read, record and verify these characteristics.

The introduction of biometrics in travel documents was based on a vision that saw the value of developing technology that would allow biometrics to be used at the border as well as by carriers and by those issuing documents. The ultimate goal was for improved document security through use of biometrics to create a much stronger and more secure link between the document and the bearer. The technology would have to be capable of allowing retrieval of biometrics over a 10 year period (as this fits in with the maximum period of document validity). It could not contain any proprietary element to protect against changing infrastructure or changing suppliers. Given that travel documents are by definition issued in one country and used in others, global interoperability was seen as essential. There was a need for inspection personnel and systems (manual or automated) in different countries worldwide to be capable of reading biometric data from the documents and using these to provide immediate information to identify the traveller and to permit manual or automated checks against stored records. A critical challenge is that this must be done in countries with varying degrees of development and access to technologies, and in some cases at border-crossings ranging from major urban centres to remote rural locations. This required, *inter alia*, a standardized approach to how biometric data are stored in the documents themselves. This concept is not unique to e-passports. For the same reasons, global interoperability is also a major objective of the standardised specifications for placement of both visually-readable information and electronic data in Machine Readable Travel Documents (MRTDs) of all kinds.

The New Technologies Working Group in ICAO began looking at use of biometrics around 1999. At that point the reason for considering biometrics was not only to improve identity checking but also assist facilitation of increasing numbers of travellers though use of automated processing. Biometrics appeared at first to be primarily a way to increase the throughput of passengers through airports. However the events of 9/11 increased pressure on ICAO and the NTWG to develop a biometric solution more quickly as a form of security-enhancement. The selection report in early 2002 had identified the biometrics that could be used. Further work was done to settle on one primary globally interoperable biometric characteristic. The use of the human face was chosen for the following reasons.

There is no disclosure of personal information that the person does not routinely disclose.
The use of photographs is already socially and culturally accepted. Photographs are already collected and widely used for travel documents.

Recording and verification are seen as non-intrusive compared to some other biometric identifiers such as fingerprints or scans of eye (iris or retinal) tissues.

New automated storage and retrieval technologies are available, but are not essential to the use of photographs. Records can still be kept and used in existing ways.

Photographs taken for other purposes often already exist and can be re-used (if still current), a factor especially useful for children.

Human verification of the biometric data by comparing the photograph to the actual traveller being identified is a relatively simple and familiar process for border guards, and can be done without any new or special apparatus.

Even though facial recognition is seen as the most globally-interoperable biometric for travel documents, it is not the only possibility. Other biometrics can be, and in some cases are, also used as identifiers, and in the case of travel documents, some other identifiers such as fingerprints are used in conjunction with facial photographs. The introduction of EU regulation on minimum security standards in travel documents mandated the inclusion of photographs and fingerprints in the passports of all EU Member States. Photographs became a requirement in August 2006, and both biometric identifiers will be required for new documents starting in mid-2009. Germany has already started producing such documents (November 2008).

I do not propose to spend a lot of time on the technical specifications. Suffice to say that there are four pillars of interoperability:

- **Common data structure.** ICAO has developed a logical data structure (LDS) so that data items are recorded, organized and stored in a standard way to achieve global interoperability.

- **Common biometrics.** The actual biometric standard of using the human face was adopted for the reasons given above.

- **Common data storage.** To ensure that stored data can be read everywhere, there was agreement on using a contactless Integrated Circuit which conforms to the ISO 14443 standard.

- **Common Security.** Security requires that information be retrievable and readable only by those authorised to do this, that it be resistant to tampering or falsification, and that it be possible to verify authenticity. This requires forms of PKI (Public Key Infrastructure, a form of encryption), and specific applications were developed to
provide a means of securing the data in the IC chip and allowing for its verification and authentication. One challenge is to ensure that data are recorded securely, but that they can be read and authenticated at many entry points. With PKI technologies, a “private” encryption key is used to write the data on the chip, which can then be read and authenticated by anyone with a device equipped with the corresponding “public” key. The matching of the two keys authenticates the data (“digital signature”), but those with public keys cannot alter the data. As discussed by other speakers, these technologies are reliable, but there is still a debate as to how effective the present arrangements are.

The introduction of biometrics posed a number of challenges and these were not all technical. One of the biggest issues relates to the quality of the facial image. Good quality images are very important to make the most reliable use of the biometric identifier. ICAO has developed guidelines on photographs but even with these, the standard of images can vary significantly depending on local factors such as equipment quality, lighting and the skill of the operator. Poor image quality may reduce the reliability of the biometric, increase verification times or cause other problems that erode the gains used to justify the substantial investment that biometrics entails.

As with any form of personal information, privacy issues are always a factor. As previously mentioned, one reason ICAO selected facial recognition to begin with is that faces are on public display, and some of the privacy issues with other identifiers do not arise. Once collected and recorded with other information, however, facial photographs are still personal information, and privacy issues have arisen with respect to the potential for data on the chip to be skimmed or read without the holder’s knowledge. Eavesdropping (ie listening electronically to the communication whilst the chip is being accessed by a reading device at the border) is also a concern. However, States have introduced access controls that make this difficult.

Another area that has become very important is the need for border control authorities and document issuers to work together to ensure that governments are obtaining value for money from the investment that has been made in e-passports. Making sure that the potential contribution they can make to enhanced border security is being maximized by border authorities.

With the introduction of fingerprints in EU passports, there has also been a need to develop a much more secure method of protecting
fingerprint data which is understandably seen as much more sensitive than the face.

So what is the difference between an e-passport and a non-e-passport? A principal driver behind the introduction of e-passports is that the technologies being incorporated enhance the ability to verify that the person carrying the document is truly the person to whom it was issued and that the document is not counterfeit and that the data and document have not been tampered with since issuance. This is achieved through the inclusion of the IC chip containing the bio data and photo which is stored and secured in accordance with an ICAO specification.

The use of PKI to encrypt the data makes it difficult to access and read the data without a public key, and the use of a form of private key as a “digital signature” makes it effectively impossible to alter the data without the changes being apparent when data in the chip is checked against the source file, when the passport is verified. Alteration or tampering is much more difficult than forms of paper-based forgery or alteration, and therefore a significant step forward in document security. This can also be done using fairly basic equipment at border crossings by officials without extensive training. A passport reader equipped with the basic technology needed and the appropriate public key information (or connected to a larger system with access to it) will immediately highlight any tampering or discrepancies in the encrypted data. With conventional passports, detecting any form of skilful counterfeiting or tampering with the document usually needs careful examination of the document, and will often elude the cursory inspections of officials.

The e-passport is much more of a challenge for the fraudster or forger – providing the data is protected and validated using the PKI system. Once established, this provides a much stronger link between the passport holder and the document. In addition to the rapid and accurate verification of the e-passport and identification of the person using it, the use of biometrics and related technologies also facilitates speed and accuracy in a number of other security-related processes. One example is in the background checking performed as part of the passport, visa or other travel document application and entitlement adjudication processes. It becomes much easier to verify the identities of applicants against other data-bases.

Editor’s note: see also, however, BUTTARELLI, infra, who makes the point that, while biometric and related technologies can be very secure in protecting data from tampering, the data themselves are only as reliable as the verification that was made at the time the individual was identified and the biometric data were created.
Thus far, this paper has discussed the use of biometric technologies to record and access data, but not the means whereby the data are compared to the passport holder in person. The selection of facial photographs by ICAO is based in part on the fact that these can be “read” by border officials simply by viewing the decrypted digital photograph and comparing it to the physical photograph, if any, in the document itself, and comparing these to the actual face of the traveller. To further enhance both reliability and the speed with which travellers can be checked, however, facial recognition technologies have also been developed. These scan the actual face of the traveller and compare specified proportions or dimensions to the digital image, alerting officials when there is not a match or where there is doubt, but the number of variables increases complexity. The function is similar to electronic reading and comparison of other biometrics such as fingerprints and retinal scans, in that by automating the first part of the verification process, some elements of human error can be reduced and larger numbers of travellers can be screened more quickly. The use of fingerprints and retinal scans is more reliable, but usually requires the voluntary participation of users by enrolment to allay privacy concerns. The following are examples of some of the current schemes:

- **Privium** – A Dutch system operating at Schiphol Airport. This been operating for a number of years and uses IRIS (retinal scan) technology. It requires voluntary enrolment of users, who can then pass through passport control more quickly.
- **IRIS** – The original IRIS system is in use at a number of UK airports. It means that there is no need to use an actual passport at control, but also requires enrolment and the voluntary recording of retinal scan image data.
- **RAPID** – A more recent use of technology, this does use a combination of passport and facial recognition technology, which alleviates privacy concerns.

There is also increasing interest in passport validation by non-government bodies such as banks where travel documents are often required to prove identity. There is no reason why in future a bank might not use a passport reader to verify and authenticate a travel document to

---

in the first place, and Mr. CHALMERS’ conclusion to the same effect, below. Biometric data uniquely identify biological individuals, but the possibility of falsification or error in the identity information which is linked to biometrics can still not be completely excluded.
prevent ID fraud. Airlines and other carriers are also interested in the use of biometrics to confirm that the document is held by the right person.

However whilst biometrics is a significant development in the travel document environment, it is not a panacea for ID fraud. It does freeze the identity and this makes it very difficult for that person to obtain a second identity providing there are proper checks in place. But even more important is the need to have a reliable system of establishing identity in the first place especially if this relies on supporting documents that may be relatively easily obtained or counterfeited. Additionally the whole end to end travel document application and issuance system needs to be adequately protected against fraud.

In conclusion, the inclusion of biometrics in travel documents is a major step forward and around 40 countries are now issuing e-passports, and further countries are developing the necessary documents and infrastructure. The e-passport provides a much higher level of assurance on the identity of the document holder and can contribute also to safer and still secure automated processing of low risk travellers. However its value depends not only on the technology but also the integrity of the document issuance system.
ONLINE IDENTITY THEFT: A GROWING THREAT TO CONSUMER CONFIDENCE IN THE DIGITAL ECONOMY

BRIGITTE ACOCA
Policy Analyst, OECD Committee on Consumer Policy

Introduction

Over the past decade, views on the role that the Internet plays in the everyday life of millions of people in the world have evolved. In 1998, electronic commerce was regarded by many as offering “a radically new way of conducting commercial transactions”\(^2\). In 2008, strengthening consumer confidence in the established, yet not fully developed digital marketplace, has become a key concern.

If consumers today benefit from more choice and easier ways to purchase goods and services on the Net, business-to-consumer online transactions remain timid, in particular across borders. Cyber fraud has been identified as one of the main reasons for such limited success. As indicated in a 2006 OECD report on the implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders\(^3\), important steps have been taken in

---

1 The Committee on Consumer Policy is within the Directorate of Science, Technology and Industry of the Organisation for Economic Cooperation and Development (OECD), Paris, France. More information on its activities may be found at: http://www.oecd.org/sti/consumer-policy. The views and opinions expressed here are personal and should not be attributed to either the OECD or its member countries.


3 More information on the 2003 OECD Guidelines on Cross-border Fraud may be found at: http://www.oecd.org/sti/crossborderfraud.
recent years by governments to combat the phenomenon through the establishment of more effective consumer protection regimes and in particular empowered consumer protection enforcement authorities. However, despite these efforts, e-commerce continues to suffer from a remaining lack of trust, nourished by new and ever complex forms of fraud on-line.

Among these fraudulent activities is identity theft (“ID theft”). This longstanding problem off-line, recently imported to the digital world, has been pointed out as the source of growing concerns. Under the EU 2006 Special Eurobarometer, only 27% of the EU population purchased goods and services on-line over the past year, and mostly on a domestic basis. According to 2008 Eurostat data, in 2006, 12% of individuals aged 16 to 74 had not ordered goods or services over the Internet in the preceding 12 months because of worries about giving credit card or personal details on-line. Under a 2006 online survey in the United States, nearly one in three adults said that security fears compelled them to shop on-line less, or not at all, during the 2005-2006 holiday season.

The OECD, notably through its Committee on Consumer Policy (“CCP”), has devoted efforts to address the issue. Its 2008 Scoping Paper on Online Identity Theft, which provides background on the scope and scale of the problem in OECD countries, offers ideas on possible enforcement initiatives that stakeholders – including governments, business, and industry – could further develop in their collective fight against the challenge. In the light of the report’s conclusions, policy principles on ways to prevent online ID theft through education have been further developed by the CCP in 2007 and 2008. These principles, which

---

will be considered at the 2008 OECD Ministerial on the Future of the Internet Economy\textsuperscript{9}, call for enhanced international enforcement cooperation to combat online ID theft, taking into account actions that are being carried outside the OECD, such as those of the United Nations Office on Drugs and Crimes (UNODC).

The International Conference on The Evolving Challenge of Identity-Related Crime: Addressing Fraud and the Criminal Misuse and Falsification of Identity, jointly organized in 2007 in Italy by the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (“ISPAC”), in cooperation with the UNODC, provided a good opportunity for many stakeholders, including the OECD, to exchange views and experience on the issue and cooperate in this area.

The following aims at providing a brief overview of the characteristics of ID theft (I); the techniques and methods used to perpetrate it (II); its goals (III) and scale (IV); as well as what measures have been put in place (V) or should be put in place (VI) to prevent, detect and deter online ID theft. All these elements were discussed extensively at the above mentioned conference, as well as at the first meeting of the core group of experts on identity-related crime that was set up by the UNODC in 2007\textsuperscript{10}.

\textsuperscript{9} For more information on the OECD Ministerial Conference, to be held on 17-18 June 2008 in Seoul, Korea, see: www.oecdmisterialseoul2008.org.

\textsuperscript{10} The core group of experts was set up by the UNODC as a follow-up to the recommendations in the UN Results of the second meeting of the Intergovernmental Expert Group To Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, E/CN.15/2007/8, 2 April 2007, pp. 5-20. The group, including experts from various criminal and economic organizations, including the OECD and UNCITRAL, met in November 2007 in Courmayeur, Italy, back to back to the above mentioned ISPAC International Conference. It discussed about the various elements of ID-related crimes and agreed to work further on the development of recommendations for best practices in the fight against ID related crime.
I. What is “identity theft”?

Absence of a harmonized definition

Although the concept of identity theft (“ID theft”) is widely used at both domestic and international levels by various bodies, whether from the public or private sector, or the media, it has not yet been globally understood. This may be explained by the fact that ID theft is an illicit activity with multiple facets, which is itself generally included in a larger chain of wrongs or crimes. More specifically, ID theft, whether on-line or off-line, is committed over different sequences of actions.

This complexity has opened the path for different legal characterisations of the concept in the 30 OECD Member countries, as well as in regional and international organisations. ID theft is indeed qualified as a crime in some countries, as a civil wrong in others, and/or as a preparatory step in the commission of other more serious offences such as terrorism, or money laundering.

In some countries such as in Australia, the United States, Canada, or Korea, the concept of ID theft prevails. In contrast, in other countries, such as Japan, the concept is as such unknown. Most Member States from the European Union (“EU”) use the terms “identity fraud” or “identity crime” as synonyms. French-speaking countries refer to the terms ID theft (“vol d’identité”) or impersonation (“usurpation d’identité”) interchangeably. Some even argue that the terminology used is inappropriate. Indeed, how could an identity ever be “stolen”? Isn’t it more about misusing an identity than anything else? This question is even more accurate online, since the concept of digital identity is itself still unclear. Are passwords or PIN-codes elements of a digital identity?

For Europol, ID theft and ID fraud are subsets of ID crime. ID theft is itself a sub-category of ID fraud, as “identity fraud is broader than identity theft in that identity fraud refers to the fraudulent use of any identity, real or fictitious, while identity theft is limited to the theft of a real person’s identity”

For the UN Intergovernmental Expert Group to prepare a study on Fraud and the Criminal Misuse and Falsification of Identity (“the UN IEG”), ID theft and fraud are also sub-categories of ID crime, which covers

---

all forms of illicit conduct involving identity. The group distinguishes ID theft from ID fraud as follows:\textsuperscript{12}:

- \emph{ID theft} refers to occurrences in which information related to identity, which may include basic identification information and in some cases other personal information, is actually taken in some manner analogous to theft or fraud, including theft of tangible documents and intangible information, the taking of documents or information which are abandoned or freely available, and the deception of persons who have documents or information into surrendering them voluntarily.

- \emph{Identity fraud} refers to the use of identification or identity information to commit other crimes or avoid detection and prosecution in some way.

The UN IEG takes the view that the element of deception, and hence the term “fraud,” lies not in the use of deception to obtain the information, but \textit{in the subsequent use of the information to deceive others}. As with economic fraud, this element of deception includes the deception of technical systems as well as human beings.

\textit{Towards a common understanding}

Despite the above described divergent approaches, all of the countries and organisations addressing the issue aim at preventing fraudulent or criminal activities resulting from the unauthorized acquisition and subsequent misuse of someone’s personal information. The OECD Committee on Consumer Policy has thus agreed to understand the concept of ID theft as follows:

\textit{“ID theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes”}\textsuperscript{13}.

\textsuperscript{12} UN IEG, \textit{Results of the second meeting of the Intergovernmental Expert Group To Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity}, Report of the Secretary-General, E/CN.15/2007/8, 2 April 2007, pp. 5-20.

\textsuperscript{13} OECD \textit{Scoping Paper on Online Identity Theft}, Section I.
II. How is ID theft perpetrated on-line?

ID thieves employ a variety of methods to obtain victims’ personal information. Some online tools include the activation of malicious software (so-called “malware”), understood as a program installed on a computer system for the purpose of causing harm to that system or to others. Phishing\(^\text{14}\), is also an important technique that ID thieves use to lure Internet users on-line: deceptive e-mails or fake websites are sent out or used to trick users into disclosing their personal information. These phishing messages are themselves widely distributed by spam, so as to ultimately install malware on users’ computers.

Phishing techniques are becoming more sophisticated and more difficult to detect. Some of the principal forms, which are mainly based on malware, are:

- **“Pharming:”** as in a classic phishing attack, users are redirected from an authentic website to a fraudulent site that replicates the original in appearance.
- **“SMiShing:”** cell phone users receive short text messages whereby a company confirms to them that they have signed up for one of its services, indicating that they will be charged a certain amount per day unless they cancel their order at the company’s website.
- **“Spear-phishing:”** the sender impersonates a company’s employee/employer to steal their colleagues’ passwords/usernames to ultimately access the company’s computer system.
- **“Vishing:”** a classic spoofed e-mail, disguised so as to appear from legitimate businesses or institutions, invites the recipient to call a telephone number. Victims feel usually safer in this way as they are not required to go to a website where they would transmit their personal information. When calling, the target reaches an automated attendant, prompting her to enter personal information such as account number, password or other information for pretended “security verification” purposes. In some cases, the phisher skips the e-mail altogether and cold calls consumers, fishing for financial information.

\(^\text{14}\) Like ID theft, the concept of “phishing” is not clearly and consistently defined in OECD member countries. Some law enforcement authorities or industry often use it as a synonym of online ID theft. Others distinguish the two notions.
One could expect that new forms of ID theft techniques will emerge in the next years. As in a chess game, thieves have to date demonstrated an incredible capacity to quickly adapt so as to circumvent prevention and deterrence efforts deployed by stakeholders. In recent years, the classic and basic phishing attack attempting to lure internet users through fake financial institutions’ emails has, for example, been progressively replaced by well designed messages targeting smaller and more intimate communities, such as chat rooms, companies’ intranet or even international organisations’ employment websites, where trust is the central element of communication.

III. What drives identity theft?

ID thieves misuse personal information in furtherance of a variety of different unlawful schemes. Typically, these schemes involve the misuse of existing accounts, opening new accounts, fraudulently obtaining government benefits, services, or documents, health care fraud, and unauthorized brokering of personal data. ID theft is also used to perpetrate serious financial crimes such as money laundering or terrorist financing.

IV. Scale of the problem

Due to the original lack of understanding of what ID theft is about, available statistics reflecting the scale of the problem are oftentimes inconsistent from one country or authority to another, complicating cross-border comparisons. Most data based on complaints may not effectively reflect the seriousness of the problem as many identity theft victims do not report their case to the authorities. Whether collected by public or private entities, identity theft data vary greatly: some sources (not surprisingly, security vendors) conclude that the scale of ID theft has gone down in the past years, resulting in growing consumer confidence. In contrast, other sources advance figures reflecting an increase in ID theft. According to the US Federal Trade Commission (“US FTC”), in 2006, for the sixth year in a row, ID theft topped the list of consumer complaints, accounting for 246,035 of more than 674,354 fraud complaints filed with the agency.\(^\text{15}\)

Many law enforcement agencies or medias often describe ID theft as the “fastest growing crime of the 21st Century,” that business, consumers, and governments constantly face on-line. Whether ID theft is severe or not, or more important on-line than off-line, it is certainly a rising issue that has already resulted in substantial direct economic losses for all stakeholders including individual victims, private sector entities such as, in particular, financial institutions, and country economies. In the United Kingdom, for example, the Home Office estimates that ID fraud costs GBP 1.7 billion to the UK economy, compared to GBP 1.2 billion in 2002.\(^\text{16}\) According to APACS, the UK payments association, online banking fraud continues to increase, costing the UK industry GBP 22.5 million in the first half of 2006, against GBP 14.5 million in the same period in 2005.

Victims also bear indirect costs which are themselves difficult to measure. Recovering their reputation, trying to make loans or even just applying for a professional position may prove difficult if not impossible in some cases. According to the US FTC’s 2006 Identity Theft Survey Report\(^\text{17}\), 16% of ID theft victims reported having difficulty obtaining or using a credit card, 10% reported being refused a cheque account or having cheques rejected. According to CIFAS, the UK’s Fraud Prevention Service, in cases where a “total hijack” has occurred, victims may need over 200 hours before things are back to normal.\(^\text{18}\)

As mentioned above, financial institutions, although often reluctant to divulge the number of ID theft attacks they have been subject to, for fear that their reputation could be harmed, have been the targets of most phishing attacks in recent years. Despite growing education and awareness efforts to alert their customers about the threat, they – and, with them, e-commerce as a whole, remain particularly vulnerable to the problem.

\(^{16}\) See: www.identity-theft.org.uk/.


\(^{18}\) See CIFAS’ website at: www.cifas.org.uk/identity_fraud_is_theft_serious.asp.
V. What has been done?19

There is no one solution to the problem. An effective fight against online ID theft would require that all stakeholders get involved in the battle, at both domestic and international levels, and put in place various prevention, detection, deterrence and redress mechanisms to stop ID thieves’ activities. As recommended by the UNODC20, authorities, whether of a criminal or economic nature21, the private sector and civil society, are particularly well placed to eradicate the problem. They should co-operate with each other through, for instance, information sharing and mutual assistance in investigations, to prevent ID thieves from evading jurisdiction and liability. The following only provides some examples of what countries have undertaken at domestic level to fight ID theft. Much more has in fact been done at both domestic and international levels22.

Education and awareness

In its 2008 policy guidance on online identity theft, the OECD Committee on Consumer Policy focuses on the prevention efforts that should be implemented to alert potential victims about the threat. The guidance takes note of the various initiatives carried out at both domestic and international levels to educate consumers about the forms, techniques of ID theft, and what to do if it occurs. Education initiatives have been carried out in various ways, ranging from government websites specifically dedicated to alert consumers about the ID theft threat, to videos, leaflets, or kits.

---

19 Detailed information on enforcement initiatives carried out at both domestic and international levels may be found in the OECD’s Scoping Paper on Online ID theft, Section V.
20 United Nations Intergovernmental Expert Group To Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Results of the second meeting of the Intergovernmental Expert Group To Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, E/CN.15/2007/8, 2 April 2007, pp. 5-20.
21 Such co-operation took place for example on the occasion of the above mentioned 2007 core group of experts meeting.
22 For more details on enforcement initiatives against ID theft, see Section V of the OECD Scoping Paper on Online Identity Theft.
The Australasian Consumer Fraud Task Force (ACFTF)\textsuperscript{23}, a group of 18 government regulatory agencies and departments from Australia and New Zealand responsible for consumer protection regarding frauds and scams, has for example, within the framework of its March 2006 Consumer Awareness Month (CAM), run a campaign educating consumers about phishing scams, noting the lack of awareness among Australians who seem to be responding to these scams at a much higher rate than other countries\textsuperscript{24}.

The private sector has also devoted much efforts to make consumers aware of the problem. The Anti-Phishing Working Group for example maintains a website containing information on the latest phishing trends, and methods and allows users to report about any phishing message.

Education efforts are not limited to consumer information. Much has been done by governments to also educate businesses about the problem. In Canada, for example, the Consumer Measures Committee\textsuperscript{25} has developed two ID theft information kits addressed respectively to consumers and businesses\textsuperscript{26}. While the consumer kit includes information to help consumers reduce the risk of identity theft, assess whether they have become a victim, and advises them on what to do if they do fall victim, the business ID theft kit informs businesses on how to reduce the risk of compromising consumers’ information, what to do when a thief strikes and how to tell consumers about a breach. Both kits have been developed based on consultations with both consumers and business’ representatives.

\textsuperscript{23} More details about the ACFTF can be found at: www.accc.gov.au/content/index.phtml/itemId/781937/fromItemId/622554.


\textsuperscript{25} The CMC provides a federal-provincial-territorial forum for national cooperation to improve the marketplace for Canadian consumers, through harmonization of laws, regulations and practices and through actions to raise public awareness. For more information, see http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00127e.html.

\textsuperscript{26} For more details on the CMC Consumer ID theft Kit, see: www.cmcweb.ca/idtheft. For more details on the CMC Business ID theft Kit, see: http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00091e.html.
**Criminalisation**

The transition of traditional forms of ID theft to the online marketplace raises the question of whether existing OECD member country schemes adequately address the new aspects of the problem.

Few OECD member countries have developed legislation which specifically addresses ID theft. In most countries, it is a constituent element of common wrongs, and as such it is covered by a multitude of rules including unlawful access to data, fraud, forgery, or intellectual property rights.

In the United States, under Federal and various state laws, ID theft is a specific criminal offence. In 2004, the *Identity Theft Penalty Enhancement Act* ("ITPEA") introduced aggravated penalties. In Australia, ID theft is a stand-alone offence in two jurisdictions – Queensland and South Australia.

In most other countries, ID theft is absorbed by other offences. In some of these countries, the idea of criminalization has been simply rejected. In France for example, in 2006, questioned about the possible adoption of new legislation criminalizing ID theft, the French Ministry of Justice objected that that ID theft (whether committed on or off-line) is already adequately sanctioned under French law through various criminal and civil wrongs such as the use, without authorisation, of someone’s name, if such a use exposes the victim to criminal sanctions (Article 434-23 of the French Criminal Code), fraud ("escroquerie" – Article 313-1 of the French Criminal Code), or defamation (Article 131-12 et al. of the French Criminal Code). In other of these countries, the issue is being discussed. In Canada for instance, in 2007, the Government introduced a bill making ID theft a specific criminal offence. The new Bill would help ensure that the

---

27 See the United States Code ("U.S.C.") Title 18, Section 1028 (a) (7).
preparatory steps of collecting, possessing and trafficking in identity information, which are generally not captured by existing offences, be covered by the prohibition. Under the new legislation, each of the three created offences would be subject to five-year maximum sentences.

Would criminalization improve the fight against ID theft and more specifically online ID theft? And how? According to the US Identity Theft Task Force, in cases where the foreign country does not have laws criminalising ID theft, it impedes the investigating country’s ability to collect evidence and prosecute ID theft crimes that have foreign components.33

This issue has been recently examined by the European Commission. In its 2004-2007 Action Plan on the prevention of fraud on non-cash means of payment, the European Commission suggested examining i) the merits of establishing an EU single contact point for individuals against ID theft, which could include a register of bodies engaged in the prevention of this illegal activity; ii) the creation of a database of original and counterfeit identity documents accessible to public authorities and the private sector. The Commission also reinforced the role of the EC Fraud Prevention Expert Group (FPEG), an independent body, chaired by the Commission, whose main objective is to intensify cooperation between interested parties, especially at the international level.34 Various law enforcers, banks, retailers, consumer groups and network operators are members of the EU FPEG and exchange information and best practice to prevent fraud. In October 2007, its subgroup on ID theft issued a Report on Identity Theft/Fraud in the financial sector with a particular focus on payment and retail banking areas. The paper notably contains a number of recommendations for more tailored and consistent policy measures across the EU.

Several Directorates of the European Commission are now focusing on the issue of criminalisation, considering whether specific EU legislation on ID theft would be beneficial. For example, the Commission’s

---

34 Reference to the EC FPEG may be found at: http://ec.europa.eu/justice/home/news/information_dossiers/conference_integrity/doc/payment_fraud_en.pdf
Directorate General for Justice, Freedom and Security (DG FJS) organised in November 2006 a high level conference on the integrity of identities and payments to further strengthen public-private co-operation against identity theft and credit cards fraud\textsuperscript{36}. In May 2007, the Commission adopted a Communication on a general policy on the fight against cybercrime announcing a series of actions including the launching of an in-depth analysis aimed at preparing a proposal for specific EU legislation against identity theft\textsuperscript{37}. On that basis, in July 2007, DG FJS launched a comparative study on ID theft, examining the various definitions used in EU Member States and exploring the idea of criminalising the offence across the EU.

\textbf{VI. What could be done further?}

In its aforementioned report, the UNODC recommends that “States that have not done so should consider the modernization of fraud offences and investigative powers to deal effectively with domestic and transnational fraud committed using … electronic mail, the Internet and other types of telecommunication technology”\textsuperscript{38}. It further adds that “lawmakers need to develop appropriate concepts, definitions and approaches to the criminalization of a range of conduct, including identity theft…”\textsuperscript{39}.

Both the aforementioned 2008 OECD \textit{Scoping Paper on Online ID Theft} and policy guidance go in this direction and suggest a set of ideas for further actions that international and/or domestic bodies could undertake to enhance cross-border enforcement co-operation against online ID theft. For example, they both point out to the need for the development of a common understanding of the concept of ID theft, on which the dissuasive character of possible sanctions is inherently dependent. Taking

\textsuperscript{36} Presentations at the conference may be found at: \url{http://ec.europa.eu/justice_home/news/information_dossiers/conference_integrity/interventions_en.htm}.


\textsuperscript{38} UN IEG, Report of the Secretary-General, Section II, D, 1 a), paragraph 20, p. 11.

\textsuperscript{39} UN IEG, Report of the Secretary-General, Section II, D, 1, paragraph 21, p. 12.
into account of the horizontal nature of ID theft, which cuts across many other issues such as privacy, security or competition, they also call for the development of side legislation on data protection. Such legislation already exists in some countries, such as the United States, where many states have adopted rules imposing a duty on companies to disclose security breaches or risks of security breaches affecting sensitive personal information of their customers.

There are no such data breach disclosure rules in the EU. Article 4 of the 2002 EC Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (“the e-Privacy Directive”)\(^{40}\) requires ISPs to notify their subscribers about security risks, without however imposing on them to notify actual security breaches. However, in 2006, the European Commission issued a communication on a proposed reform of the regulatory framework for electronic communications\(^{41}\). Under the communication, ISPs would be required to notify both the national regulatory authorities and their customers of any breach of security that led to the loss of personal data and/or to interruptions in the continuity of service supply and their customers of any breach of security leading to the loss, modification or destruction of, or unauthorised access to, personal customer data. The proposal has been welcomed by the EC Article 29 Data Protection Working Party\(^{42}\).

Identity management, and more specifically electronic authentication, may constitute other helpful means to combat online ID theft. Although – once again – the concept of identity management is itself difficult to define, it is more and more designated as one potential solution – but not the only one – to prevent the misuse of digital identities. In some

---


countries, such as Korea, authentication tools have been put in place to safeguard personal information. In October 2006, an improved online identity system was introduced in the country to help verify Korean citizens’ identity in the digital environment\(^43\). The old 13-digit citizen registration number, which contained Korean citizens’ personal information, was used as an identity verification means online. However, this number, which was stored on firms’ online databases, had been the subject of numerous thefts\(^44\). The Korean authorities decided to replace it by a new “i-PIN” number which does not contain any personal data and could be replaced in the event someone’s i-PIN number has been copied or misused. Identity authentication tools may not only be aimed at protecting users’ identities, but also at helping business verifying their customer’s identity.

In its fight against money laundering and terrorist financing, the Financial Action Task Force (FATF)\(^45\), an independent intergovernmental organisation which is a member of the UNODC and whose Secretariat is housed by the OECD, recommended that “Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers”\(^46\).

Public or private entities storing sensitive personal information should also ensure that adequate security measures are in place to protect their customers’ personal data. Recent government data leakages in the United Kingdom have shown how individuals may be easily exposed to the potential misuse of their identity, whether in the near or distant future.

\(^43\) Reference to this new Korean identity verification means may be found at: www.vnunet.com/articles/print/2165834.

\(^44\) In early 2006, 1.2 million Korean citizens noticed that their citizen registration number was used without their knowledge or consent to sign up for accounts in *Lineage*, a series of online games.

\(^45\) The FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. See: http://www.fatf-gafi.org/pages/0,3417,en_32250379_32235720_33625510_1_1_1_1,00.html.

\(^46\) More information on this issue may be found in Recommendation 5 of the FATF, at: http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html#r5.
VII. **Conclusion**

The above discussion only provides a snapshot of the problem of online ID theft. It aims at illustrating the complexity of the issue, which represents a serious threat for individuals, public and private entities, and countries’ economies. In today’s ever convergent digital economy, the risk of ID theft may become exponential.

For example, it now not only affects fixed computers, but also all sorts of external devices linked to the Internet often on an “always on” basis. As discussed in a draft *OECD M-commerce Policy Guidance* (being developed by the CCP and which should also be examined at the 2008 *OECD Ministerial on the Future of the Internet Economy*), mobile devices such as mobile phones are, for instance, a rising source of concerns in a number of OECD countries. Users are increasingly exposed to the unauthorized use of their device, resulting in high charges on their account, often far later after they can find out about the theft.

At the 2008 OECD Global Forum on Competition, the expansion of ID theft to many sectors of the economy has also been denounced as a barrier to vigorous competition in the online marketplace. It is in the interest of all stakeholders to actively participate and co-operate in the fight against online ID theft.
THE RELATIONSHIP BETWEEN IDENTITY-RELATED CRIME AND ECONOMIC FRAUD

KEVIN MCNULTY
Head of Identity Fraud Reduction Team, Identity and Passport Service, United Kingdom

In looking at the link between identity related crime and economic fraud there are a number of key questions which are raised. These include:

• What purposes are identity crimes committed for?
• What is the relevant scale and importance of each of these purposes?
• What are the precise links between identity crimes/fraud and economic fraud?
• Is economic gain ultimately the sole motivating factor for those who undertake identity crimes?

In seeking some answers to these questions, I first revisited the UN Commission on Crime Prevention and Criminal Justice Experts Group study on fraud and the criminal misuse and falsification of identity. The key findings from this were:

• That there are significant areas of overlap between identity crime and economic fraud;
• the most common offences associated with identity crime are either economic offences such as fraud, or offences related to travel or identity documents; and,
• that there is no statistical information about the relative prevalence of identity-related crime and links to other offences was available.

In order to further understand the associations between identity related crime and economic fraud it is helpful to examine some case studies from the UK.

Abuses of identity details can take a number of different forms, from lone individuals seeking to fund drug habits or lavish lifestyles, to
collusion of individuals through an organised or organised criminal group. The first example is an example of the operation of a lone individual.

**Case study 1**

In 2005 Cleveland Police undertook a prosecution against Stephen Hoyle who was involved in the fraudulent abuse of over 80 identities. He enjoyed frequent foreign holidays, drove an expensive car and built up a portfolio of buy-to-let homes. Hoyle took out seven fraudulent mortgages, worth £273,700, and had applications for a further eight, worth £543,000, being considered when police caught up with him. Police discovered driving licences containing Hoyle’s picture but with different names, 70 credit cards and details of up to 140 identities when they raided his home. The investigation also revealed he had taken out other loans totalling £75,000 in other people’s names, and racked up almost £63,000 debt on bogus credit cards. Police found deposits of £390,000 on 21 bank or credit card accounts, and more than £130,000 going through his girlfriend’s three accounts in one year. A lap-top computer had a spreadsheet with 69 names, detailing bank accounts, credit cards, pin numbers, addresses, email addresses, and passwords. Hoyle was eventually charged with 59 offences, involving the sum of £1,412,000, and was eventually sentenced to three and a half years imprisonment.

More usually, cases involve more systematic and organised abuses involving a number of individuals, and collusion and or coercion.

**Case study 2**

In May 2007 bank employee Shana Campbell was sentenced to 4 years imprisonment. She was involved in passing customer details on to fraudsters, and other bank employees were threatened or coerced in to assisting. New accounts were set up in the same name as victims to avoid detection (these were plundered at a later date). High value accounts and those belonging to the recently deceased were targeted, and £1.3 million was stolen in this way – with one account drained of £158,700. A further £1 million was stolen through use of Trojan viruses. The leader of the fraud known as Olawasegun Adekunle had, among other luxury goods, an £18,500 18-carat gold Rolex, an £87,000 Bentley Continental and a “palatial” Thames apartment. Adekunle was sentenced to 5 years, the bank
insider (Campbell) was sentenced to 4 years. Whilst the judge in the case indicated that Adekunle would be deported upon release, his true identity and country of origin remain unknown.

Finally, identity frauds are often perpetrated by organised criminal groups.

We know that Government departments are often the victims of identity fraudsters. In late 2005, the Tax Credits system operated by Her Majesty’s Revenue and Customs was targeted by organised fraudsters; 62,000 attempts were made to defraud the tax credits e-portal using stolen identities, and of these 33,000 were successful at a cost of £55 million, leading to the closure of the portal in December 2005.

Case study 3

In July 2007 Abdulqudri Bolaji Hazzan was sentenced to 30 months imprisonment for his part in a £1 million fraud against the tax credit system. Hazzan was charged with 7 counts of fraud, including money laundering offences and the loss attributable to him alone was £123,847. He is the first member of a gang identified as being involved in this fraud against the tax credit system. It is expected that a further 9 individuals will be prosecuted for their part in the fraud. The gang have used over 125 stolen identities to make false tax credit claims and opened over 50 bank accounts in order to receive the payments. When arrested a substantial amount of property was seized, including identity details, banking documentation, IT equipment and mobile phones.

Case study 4

The final case study relates to the prosecution of Anton Gelonkin and Aleski Kostap.

Gelonkin was controlling an organised criminal group in London and involved in multiple criminal offences. He had also been involved in the collapse of The Moskovsky Gorodskoi Bank in Moscow in 1995 with losses amounting to £61 million. In respect of their fraudulent activities in this case:

- £1m benefit calculated;
- 25 passports recovered;
- 200 + bank accounts;
• 60 aliases;
• 100 addresses;
• 20 companies established.

Their operation was financed by utilising multiple compromised credit card details to commit customer not present fraud. Once card details had been obtained, information used as passwords and security codes was usually obtained from online directories – Mother’s Maiden Name through 1837online.com and date of birth through 192.com. Cards which utilised these details as security questions were specifically chosen. Once the account had been taken over they were used to fund on-line gambling accounts and to buy high value goods – subsequently sold on eBay. They utilised mailboxes & mail redirect services and false documentation to facilitate the frauds, and as well as producing forged passports and driving licences, by way of supporting secondary identification documents they also produced multiple bank statements – targeting bank letterheads where fonts are easier to reproduce – and utility bills. The subjects were eventually charged with Conspiracy to Defraud UK Central Clearing Banks, possession of forged passports and attempting to pervert the course of justice (Kostap). Gelonkin pleaded guilty to all charges at the onset of their trial on 30 October 2006 and was sentenced to 6 years imprisonment. Kostap elected trial and the jury unanimously found him guilty on all counts on 27 November 2006 – he was sentenced to 5 years imprisonment.

Ultimately these are just isolated case studies which illustrate cases of identity fraud being committed for large economic gains. There are numerous others, as there are also examples of identity crime being committed for purposes other than economic gain.

It remains the case that there is a lack of definitive research on this issue. Most research and reports into identity fraud focus on the estimates of the scale of financial loss, or on the impact on the victim. Fewer studies focus on offenders and their motivation for committing identity theft. One which does, however, is the October 2007 Center for Identity Management and Information Protection (CIMIP) study50. In providing an analysis of 517 cases from an offenders perspective, it is one of the largest such documented studies.

50 http://www.utica.edu/academic/institutes/cimip/publications/index.cfm
CIMIP provided a comprehensive study of offenders M.O. from closed secret service cases where there was an identity theft element. The data was examined to determine the modus operandi of the offenders. The most prevalent motive of the offenders in fraudulently obtained personal identifying information was personal gain.

Use of stolen identity documents (motive-percentage):
- Obtain and use credit 45.3%.
- Procure cash 33%.
- Conceal actual identity 22.7%.
- Apply for loans to buy vehicles 20.9%.
- Manufacture and sell fraudulent IDs 7.7%.
- Obtain cell phones and services 4.6%.
- Gain government benefits 3.8%.
- Procure drugs 2.2%.

Of these motivating factors, all but the third, to conceal actual identity, involve direct economic gain.

Where this was the motivating factor the reason for stealing the personal information was to:
- gain employment;
- conceal credit history;
- obtain “new” identity documents.

Going back to the analysis of all the cases, in most of them the identity theft facilitated other offences, which in descending order of commission were:
- fraud;
- theft;
- forgery;
- credit card fraud.

Through this detailed and extensive analysis it is arguable that the purpose of stealing identities and subsequent offences committed in this study were all ultimately linked to economic gain.
Another interesting study in the UK, was a 2006 analysis of over 55,000 victims of identity fraud. Part of this work looked at what false identities were used for:

- apply for a store card (56 per cent);
- credit card (43 per cent);
- mobile phone account (35 per cent).

In many cases respondents’ personal details were used to open a number of different accounts, for example to apply for both a store card and a mobile phone account.

To conclude, from the available studies and research on identity related crime, the evidence overwhelmingly suggests the primary motivation for committing identity related crimes is economic gain. However it is important to remember that much of the available good quality data and surveys undertaken relate to the financial services sector, and in reaching such a conclusion on available evidence one must bear in mind that the origin of the data will skew the motivating factors.

There is also a paucity of good quality data on this subject and in particular few studies which focus on offenders’ motivation. More work is clearly needed in this area in order to advance our understanding of the links between identity related crime and economic fraud.

In addition identity crimes are undoubtedly committed for other purposes, as others have spoken about at this conference. These include:

- concealment for travel/employment;
- terrorist related purposes;
- avoiding surveillance; and
- preventive measures before and during offences.

However I would maintain that identity crimes are primarily being undertaken for the purposes of fraud or other offences for financial gain, or by individuals or groups with an ultimate view to furthering or realising economic gain.

In respect of what we can do to combat identity related crimes in the future the following represent some key areas to begin to effectively combat the problem.

http://www.cifas.org.uk/?edit_id=577-73
How to combat in future?
• Prevention better than cure;
• Public/private sector collaboration essential;
• Sharing of data to authenticate and verify customers identity;
• Staff fraud databases;
• Authentication services – ease of proving identity quickly to a high standard;
• Uptake of such systems by Government and private sector.

Where frauds continue to occur there is a need for:
• appropriate legislation – offences and deterents;
• effective investigation and prosecution;
• wider linked offences – proceeds of frauds legitimised through money laudering;
• robust asset confiscation system;
• effective international co-operation – prosecutors, police and judicial.
IDENTITY-RELATED CRIMES: 
A REVIEW OF RESEARCH AND SUGGESTED TYPOLOGIES

NIKOS PASSAS  
Professor, Northeastern University, Boston; Editor of “Crime, Law and Social Change: an International Journal”

The ISPAC theme and conference prompted me to rethink research into illegal enterprises I have conducted over the last 23 years, in order to consider the role played by false or stolen identities. This exercise was revelatory in that it brought out a new angle through which to analyze criminal activities and ways in which to seek more effective controls.  

This paper reviews a range of crimes in which identity misconduct plays a significant role and seeks to offer ways of usefully organizing cases and materials relative to identity crime through typological exercises.

Identity misconduct and other crimes

Just looking at the list of criminal activities in which one form or another of identity-related misconduct is involved shows the wide range of crimes in which mis-identification plays an important role:

- Accounting and bank fraud – the BCCI Affair.
- Informal economies – hawala and benami accounts.
- Trade in commodities.
- Tele-marketing/false lottery fraud.
- Terrorism.
- Sanctions violations.
- Proliferation and arms traffic.
- Tobacco smuggling.
- EU/VAT/Customs fraud.
- Theft of art and cultural property.
- Corruption.
In more detail, the case of Bank of Credit and Commerce International, the criminal activities by bank officials, by bank clients and bank committed against the bank included anything from money laundering and terrorist finance to corrupt practices and illegal technology transfers. One of the most significant offenses was accounting fraud, which included a systematic misrepresentation of the bank’s finances in order to hide non-performing loans to a shipping concern and losses from investments and derivatives. The cost was more than $2 billion and the bank would have been declared bankrupt, had the true state of its activities been revealed. In the shipping companies fraud, millions of dollars went into merry-go-rounds from company and BCCI accounts set up in Switzerland, USA, the Cayman Islands, Panama, the Middle East, Luxembourg and other countries. Accounts were set up in the name of front companies with false commercial histories and in the name of company employees, who were tricked into signing false documents (Passas, 2001).

Another deceptive practice involved the secret and illegal takeover of a US financial institution, Financial General Bankshares, which was renamed First American Bankshares (FAB). The FAB takeover took place through a series of holding companies and a group of investors who acted merely as nominees for BCCI, despite assurances given to the authorities by very prominent Washington DC lawyers (Passas, 1995).

Research into the field of informal economies and value transfers through ethnic networks shows that many legitimate clients and interests are served. This benefits national and regional economies as well as migrant communities and their families. Yet, there are many illicit transactions that also go through informal channels. The many types of methods and modi operandi in hawala and similar informal value transfer systems include the use of false names (benami accounts) or the names of nominees in order to hide the true identity of senders, beneficiaries or both parties (el Qorchi et al, 2003; Maimbo, 2002; Passas, 1999, 2003a, 2003b, 2004a).

Turning to a comparatively neglected economic area, studies have pointed to significant crime risks and vulnerabilities in the trade sector. While much attention focuses on financial transactions and institutions, imports and exports amounting to trillions of dollars go on around the world with little scrutiny and accountability. Despite rules requiring the honest declaration of origin, destination, value, and identity of all parties involved (buyer, seller, importer, exporter ultimate consignee, broker, shipper etc.), authorities routinely receive incorrect, misleading or completely fabricated information on these items. In practice, by hiding the identity of importers, nominee trade amounts to billions of dollars of
commercial transactions only in the US diamond sector (Passas 2004b; Passas and Jones, 2006). The misconduct facilitated by such false declarations ranges from tax evasion, VAT and subsidy fraud to embargo and sanctions violations, money laundering and terrorist finance.

In the case of conflict diamonds, the origin and beneficiaries of the trade are misrepresented in order to hide the fact that parties to violent conflict in Africa gain from this trade and sustain their war efforts through barter deals or profits. In some cases soldiers have worked on the diamond extraction but very frequently, this occurs through forced or slave labor.

A series of frauds committed against wealthy and elderly through telephone and marketing methods shows how vulnerable citizens are led to believe that they have won prizes and lotteries. They are then asked to send cashiers checks to persons who do not exist and PO box addresses, ostensibly to pay for taxes before receiving these prizes. Sophisticated telephone callers give fake names and pretend to represent lotteries based in Canada, the UK or elsewhere and invite the victims to send significant amounts, sometimes more than once – in one case involving US victims, the checks they sent ranged from 5,000 to more than 100,000 dollars each. In one instance, the fraudsters were able to mirror the website of a true lottery and make it appear as if the real website showed the targeted victims as winners. They referred victims to the ‘stolen website’, so that the victims would have no doubt about the legitimacy of the whole enterprise.

In terrorism cases, supporters and participants frequently employ false or stolen identities in order to raise, transfer and spend fund for their operations. A manual discovered in Manchester and attributed to al Qaeda specifically instructs members of the group not to use their true name or to use other people’s names for transactions related to the group’s activities. In addition, many instances of terrorist finance have involved identity frauds as well as welfare, credit card and bankruptcy frauds in order to raise funds for their cause.

The outline and analysis of instances of serious crimes in which identity theft and fraud play an important role can and fill an entire book. The main question, however, is how to best organize the empirical data on such crimes in a meaningful and helpful way. Some useful questions that can be raised aiming at the construction of useful typologies are the following:

1. Whose ID is affected and how?
2. For what purpose?
3. Who is ultimately victimized?

Let us consider tentative answers to these questions in turn.
1. Types of ID offenses

In some cases, offenders wish to simply obscure their true identity. In other cases, they make up a false identity, in order to perpetrate or facilitate other illegal activities. In yet other cases, they use someone else’s identity, so that illegal activities cannot be attributed to them.

It is precisely because of the high demand for secrecy that several jurisdictions have been offering confidentiality and opportunities for tax avoidance or tax evasion. The market for secrecy caters not only to those committing fiscal offenses but also anyone wishing to secure privacy against family members, to avoid disclosure of sensitive undercover law enforcement or intelligence operations or to protect a company from competitors curious about activities, transactions and likely future moves (Walter, 1985). People seek to hide their own identity, also when they receive corrupt payments or favors, or more generally when they facilitate or participate actively in illicit activities.

Assistance to this masking of identities can be provided by entire jurisdictions, such as secrecy and tax havens, organizations, professionals (e.g., lawyers; see di Nicola and Zoffi, 2005; Levi et al, 2005) or nominees on a continuing basis or for ad hoc/one-off transactions (Passas, 1995).

In other cases, a completely fake identity is manufactured. In the example of the telemarketing fraud mentioned above, the victims were tricked into sending cashier checks to persons with Ango-Saxon sounding names that did not exist. Mailed checks were picked up by the fraudsters at Postal Office boxes and sold off to a money laundering network of money changers in Canada and the Middle East.

More sophisticated was the creation of false identities by a group of offenders committing tax evasion, tobacco smuggling across state borders, money laundering and terrorism finance. In this case, the group took advantage of low tobacco taxes in Southeastern US states and smuggled cigarettes to Midwestern states, where the taxes were much higher. In the process of committing these crimes, the group created false identities, opened fraudulently bank and credit card accounts (USA v. Mohamad Hammoud et al., US Dist. Court, Western District of N. Carolina, 2000).

In yet other cases, someone else’s identity is used to hide one’s operations or activities. This type of misconduct can be committed with the knowledge of the persons whose identity is used or without that knowledge. In many instances in the BCCI affair cited earlier, the illegal acquisition and control of a US bank was perpetrated with the use of nominees, most of whom were aware of the transactions and misrepresentations.
It is likely that the more frequent use of someone else’s identity is done without the person knowing what is happening. Such misconduct may victimize the person whose identity is used, as in the instance of stolen credit or debit cards. It may also victimize other persons, such as the issuing bank or third parties from whom goods and services are purchased. So, the different types of ID misuse can be organized as outlined in the typology below:

- hiding one’s own ID;
- making up a false ID;
- using someone else’s ID:
  - knowingly;
  - unknowingly:
    - against those whose ID is used;
    - against third parties.

2. For what Purpose are Identity Crimes Committed?

Three possible categories are conceivable under this typology.

Firstly, one can consider identity offenses are crimes by themselves. The criminal conduct in such cases starts and ends with the identity. The identity is the aim and target of offenders.

Secondly, identity offenses may be mere instruments for the commission of other crimes, in a way similar to the way money laundering is a complement to or result of the predicate offenses. This is possibly the largest category of identity crimes, which as we have seen can be instrumental to tax evasion and fraud, terrorist finance or capital flight, proliferation or bribery, etc. In this instance, identity crimes are facilitative of other crimes.

Thirdly, identity misconduct is a response to state actions. As governments fight terrorism or seek to sanction particular actors or states, the incentive is provided for the targeted legal and physical persons to alter their identity for self-protection or in order to avoid sanctions and penalties (see, for example, official lists of designated terrorists or terrorist supporters, targeted financial sanctions, etc.).

So, another way of organizing identity-related offenses could be summarized as:

- Identity crime as an offense per se.
- Identity crime as facilitative of other crime.
- Identity crime a response to state action.
3. Who is Victimized?

An alternative way of classifying types of misconduct is by asking the question: what types of identities are affected? Three possible answers are 1) the identity of a physical person, 2) that of a legal entity or organization and 3) that of a website, as in the example of fraudsters creating a mirror of the website of a government agency or a lottery, in order to deceive large numbers of victims. Thus, another way of organizing cases and data would be as follows:

- identity of a physical person;
- identity of a legal person;
- identity of a website.

Conclusion

All contributions to this volume as well as my previous research suggest that multiple crimes and offenses, domestic and transnational, are linked in various ways to false and stolen identity or other misrepresentations. Some ways of rethinking such diverse linkages are offered through the above typologies. The most productive use of typologies is heuristic and supportive of research, analytical or policy-making purposes.

For instance, typologies can assist in organizing meaningfully the mass of cases, materials and associations as they emerge from the writings in this book and elsewhere.

They may be used to identify priority needs for policy, law enforcement, regulatory action.

They can help efforts to specify the kind of legislative or other control responses authorities deem appropriate.

Further, typologies like the ones outlined in this chapter (e.g., the one regarding victimization) can clarify and illustrate which social actors should be concerned, involved, or bear (part of) the cost of remedial actions.

Moreover, as they also raise the question of identity crimes as a reaction to state actions, they can assist in efforts to anticipate or analyze the effects of particular policies or regulation, which may drive the demand for certain kinds of identity crimes.
Finally, they can facilitate the assessment of policy and regulatory actions, in order to improve the efficiency, fairness and legitimacy of particular policies or norms.

It is hoped that the thoughts offered in this chapter provide a springboard for constructive typological thinking that can assist in better analysis, prevention and sanctioning of identity misconduct.

References


USE OF IDENTITY-RELATED CRIME TO FACILITATE ORGANIZED CRIME AND TERRORIST ACTIVITIES

JEAN-LOUIS BRUGUIERE
premier vice président, Tribunal de Grande Instance, France

Introduction

La chute du communisme et le développement de la mondialisation, celui des échanges économiques, la promotion des valeurs démocratiques mais corrélativement une plus grande ouverture sur l’extérieur a eu pour conséquence de conférer à la criminalité une dimension planétaire.

La recherche d’un profit accru dans des secteurs devenus de plus en plus lucratifs, en particulier le trafic des stupéfiants, a tiré profit de l’opportunité offerte par un monde de plus en plus ouvert et par les outils technologiques permettant une plus grande circulation du renseignement.

Dans l’euphorie de la chute du monde bi-polaire et bercés par l’illusion de l’entrée dans une nouvelle ère de prospérité, de liberté et de sécurité, les Etats occidentaux n’ont pas pris garde aux extraordinaires mutations qu’allait engendrer ce basculement du monde nouveau beaucoup plus chaotique et antagonique que le précédent où chaque camp conscient des enjeux stratégiques de cette confrontation géopolitique et de ses propres responsabilités sécuritaires a maintenu pendant des années un sentiment artificiel de sécurité.

Car, en définitive, le paradoxe de cette époque de la division du monde en deux blocs opposés dont les relations étaient régies par la dissuasion nucléaire, réside dans le fait que, au-delà de cette crainte permanente et souvent manipulée à des fins de propagande, de l’apocalypse nucléaire, le monde était beaucoup plus stable qu’aujourd’hui. Certain au prix d’une confiscation drastique des libertés civiles dans le camp soviétique.

Dans chaque camp – constitué d’Etats responsables – tout a été mis en œuvre pour que le pire n’arrive pas. Et les quelques épisodes de tensions entre l’Est et l’Ouest (la crise de Cuba et celle de Berlin) ont finalement
apporté la démonstration rassurante de la volonté de Washington et de Moscou de ne pas franchir des limites considérées comme inacceptables par l’autre.

Il en est résulté l’élaboration d’une stratégie de contournement consistant à créer des zones de tensions voire même des situations de belligérance limités aux marges des deux blocs, dans des zones de glacis comme au Moyen Orient et en particulier au Liban.

L’activisme terroriste des années 1980 qui a particulièrement touché la France au Liban et sur son sol procède de ces stratégies. Les organisations terroristes étaient “sponsorisées” par de Etats de la région (la Syrie, l’Irak, la Libye) qui étaient liés au camp socialiste.

En revanche, dans ce même camp les préoccupations sécuritaires étaient prégnantes, même en ce qui concerne l’activisme de réseaux terroristes agissant contre les pays occidentaux. L’exploitation que j’ai pu faire de la volumineuse documentation de services secrets du Pacte de Varsovie (MFS de l’Allemagne de l’Est, Services hongrois, KGB) ont mis en exergue que les autorités de ces pays ont étroitement contrôlé les activités de mouvements terroristes comme le “groupe Carlos” pour éviter tout dérapage susceptible de nuire à leur sécurité. Ces services devaient encadrer les projets terroristes de ce groupe pour en canaliser les effets, notamment en contrôlant les déplacements de leurs membres. Ces derniers disposaient de passeports diplomatiques de complaisance fournis par des Etats du Moyen Orient. Lorsque les membres de cette organisation sont devenus incontrôlables, la Hongrie qui les hébergeait et même l’Allemagne de l’Est les ont expulsés.

Cette référence historique documentée met en exergue la dimension stratégique pour les réseaux terroristes de l’époque de la mobilité de leurs membres et donc de la nécessité pour eux de disposer de titres de voyages surs, en l’occurrence de passeports de complaisance. Mais ces groupes en grande partie manipulées par des Etats étaient relativement contrôlés.

La chute du communisme devait libérer toutes les énergies confinées par des décennies de régime totalitaire. Corrélativement le développement rapide de la mondialisation accélérerait le rythme des échanges. En Europe la création de la Zone Schengen créait un espace inter communautaire de libre circulation des personnes et des biens sans qu’aucun mécanisme de contrôle ou de répression des activités illégales facilitées par cette espace n’ait été mis en place. Il faudra attendre les attentats du 11 septembre 2001 pour que les États Européens consentent à la mise en œuvre du Mandat de Arrêt Européen.

104
Ce rappel historique souligne le rôle essentiel joué par la liberté de circulation dans le développement des activités criminelles et terroristes. J’axerai mon propos sur le phénomène terroriste que je connais mieux pour les avoir observés depuis plus de vingt ans.

D’autant plus qu’il existe – au delà d’aspects purement logistiques – une différence qualitative et pas seulement de degré entre la criminalité organisée et les Terrorisme.

La criminalité organisée ne développe une contestation politique et ne porte pas directement atteintes aux structures de l’État, à ses institutions ou à ses intérêts stratégiques. Elle se situe à l’intérieur du corps social auquel elle appartient. Sa stratégie – quantitative – consiste par des activités criminelles à valoriser un profit illicite. La déstabilisation des institutions qui peut en résulter n’est que la conséquence de ses activités. Jamais un but en soi.

Le Terrorisme en revanche se situe en dehors de l’État qu’il combat, même si ses acteurs se trouvent physiquement dans le périmètre géographique de ce dernier.

Plus que pour délinquants de droit commun, la clandestinité est une composante essentielle, “l’épine dorsale” de l’activité terroriste comme le disaient les “Brigades Rouges” italiennes.

Or pour garantir cette clandestinité et autoriser les déplacements de leurs membres dans de bonnes conditions de sécurité, la possession de documents d’identité et de voyage falsifiés ou contrefaits est indispensable.

Le développement anarchique depuis une dizaine d’années des réseaux islamistes radicaux liés à la mouvance Al Qaida qui constituent la mouvance islamiste européenne a jeté une lumière crue sur l’utilisation massive par ces réseaux de documents administratifs falsifiés.

Il existe donc incontestablement un lien direct entre le recours par des réseaux terroristes à des documents administratifs falsifiés ou contrefaits et leur capacité opérationnelle. L’utilisation abusive de tels documents est en outre valorisée par les politiques d’immigration qui en Europe ne sont pas suffisamment harmonisées.

Aussi de notre efficience dans la lutte contre l’utilisation illégale de documents administratifs dépend en grande partie le succès de notre entreprise dans l’éradication de la menace terroriste.

Je me propose dans un premier temps d’évoquer les principales caractéristiques et l’évolution des réseaux islamistes opérant en Europe en lien avec d’autres structures basées dans la zone pakistano-afghane ou en Irak et la place occupée par la recherche de faux documents d’identité et de voyage dans le développement de leurs activités avant d’envisager les
mécanismes de riposte que se doivent de mettre en place la communauté internationale et les États.

I. La typologie fonctionnelle des réseaux terroristes

L’utilisation de documents d’identité ou de voyage falsifiés ou contrefaits a toujours joué un rôle primordial dans le fonctionnement de ces réseaux en raison des exigences de la clandestinité. Pour toutes les organisations, la sécurité est la préoccupation la plus prégnante. C’est notamment le cas aujourd’hui pour l’ETA comme ce le fut hier pour l’IRA, la RAF allemande et les Brigades Rouges italiennes.

Pour la mouvance islamiste radicale, l’utilisation de ces documents s’est avérée différente. Elle s’inscrit dans une méthodologie opérationnelle différente plus difficile à contrer. Ces réseaux sont moins structurés. Il en résulte une situation diffluente. Les groupes ou cellules constituant ces réseaux évoluent de façon réactionnelle et souvent aléatoire obéissant à des logiques comportementales difficiles à anticiper même s’ils s’inscrivent dans une dynamique terroriste cohérente.

Ces réseaux se développent par ailleurs sur un mode horizontal et ont une grande propension à se ramifier sur une large échelle. Par ailleurs leur structure interne a les mêmes caractéristiques: ils sont polymorphes et très évolutifs. Dans ce contexte de mutation, la capacité de franchir des frontières aisément et sans plan préétabli est essentielle.

L’émergence de la menace islamiste radicale remonte au début des années 1990. La France a été un des premiers pays touchés par ce phénomène avec le GIA algérien (le détournement d’un vol Air France Paris Alger en décembre 1994 et, six mois plus tard, une campagne d’attentats sur notre sol).

De 1994 à 2001 la menace terroriste et les groupes qui l’ont sous- tendu ont fortement évolué. Ils se sont atomisés tout en prenant une dimension planétaire.

L’utilisation de documents d’identité ou de voyage falsifiés ou contrefaits a suivi cette évolution.

Assez peu utilisés au début des années 1990 par des réseaux peu mobiles, l’utilisation de ces documents s’est développée de façon croissante à partir des années 1996-1998.

Après 1998, avec les structures du GSPC, du FIT tunisien et du Takfir Wal Hijra, cette évolution est devenue exponentielle.

De fait, c’est surtout la mise en place à partir de 1994-1995 de véritables filières d’acheminement de moudjahidin européens en
Afghanistan qui va donner un essor sans précédent à l’utilisation frauduleuse des documents administratifs falsifiés ou contrefaits, surtout les passeports.

Le tropisme afghan a en effet nourri ces filières sur lesquelles nous avons beaucoup travaillé. Londres était le passage obligé.

Les candidats au Jihad étaient chargés de trouver leurs documents de voyage dans leur pays d’origine – en général auprès de la criminalité de droit commun. Mais la fourniture de faux visas pakistanais ou d’empreintes de cachets de services d’immigration était de la responsabilité des structures islamistes basées à Londres sous la direction d’Abou Koutada et d’un tunisien surnommé Abou Iyad.

Quelques exemples – sans alourdir le débat – peuvent être donnés sur l’utilisation de ces documents dans un contexte terroriste.


Surtout nombre de militants de cette mouvance, plus radicale que la précédente mais aussi – ce qui n’a pas été suffisamment appréhendé – très proche de l’idéologie d’Al Qaida ont émigré clandestinement au Canada, utilisant pour ce faire des passeports français falsifiés.

Pourquoi le Canada; A cela trois raisons principales. Le Canada est une terre d’émigration. Les lois y sont moins restrictives qu’aux Etats Unis. En deuxième lieu la province du Québec est francophone et enfin il est facile de pénétrer sur le territoire américain par la voie terrestre.

La cellule d’Ahmed Ressam était basée à Montréal. Fateh Kamel comme d’autres militants islamistes ont pu se rendre aisément au Canada et de là gagner clandestinement le territoire américain. Or il s’agit de la première tentative d’Al Qaida de frapper les Etats Unis sur leur sol.

Autre exemple l’assassinat du Commandant Massoud. Il a été établi que le réseau responsable de cette opération était basé en Europe, en Belgique et en Grande Bretagne et que les faux passeports belges utilisés par les auteurs de cet attentat ont été obtenus et falsifiés dans ces deux pays.

Les membres de la cellule islamiste arrêtés en France en décembre 2002 et qui s’apprêtaient à commettre des attentats chimiques sur le sol français, après s’être entrainés dans le Nord de la Géorgie avaient fait un large usage de documents de voyage falsifiés.

Après ce bref exposé de la typologie fonctionnelle des réseaux islamistes, il convient de s’interroger sur les facteurs permettant cette utilisation frauduleuse de documents administratifs.
II. Les facteurs qui permettent ou facilitent cet usage frauduleux

Ils sont de deux ordres:
• La constitution de filières criminelles organisées permettant d’alimenter les structures terroristes.
• Les carences ou faiblesses des États dans le contrôle transfrontalier et les politiques d’immigration.

1. Les filières criminelles

Elles sont elles aussi de deux ordres:

a. celles qui appartiennent à la délinquance de droit commun ou à la criminalité organisée.

Ce sont les rares cas de passerelles entre criminalité ordinaire et terrorisme. Encore qu’il ne s’agisse pas à proprement parler de passerelles. Les relations sont purement “économiques” de fournisseurs à clients, sans dimension idéologique. C’est notamment le cas pour les explosifs et les armes provenant des Balkans. Un trafic qui profite à la fois aux réseaux terroristes et à la grande criminalité. Il en est de même pour les faux passeports dont certains contrefaits proviennent de Thaïlande. En 1994 le réseau “Lounici” lié alors à l’AIS, le bras armé du FIS algérien, était lié dans ses activités logistiques notamment orientées vers la fourniture de faux documents italiens avec des organisations criminelles, notamment la Camorra napolitaine.

b. Des activités criminelles organisées agissant avec la complicité tacite de certains États:
• La zone des Balkans (cf. supra) pour la fourniture d’armes mais aussi de pièces documentaires. L’action de la communauté internationale et notamment de l’Europe n’a pas permis d’endiguer le phénomène.
• La Thaïlande (cf. aussi supra) avec les passeports et autres documents contrefaits à Bangkok.
• L’Afghanistan avec le trafic du pavot qui s’opère notamment dans la région de Kandahar-Quetta avec la complicité d’organisations criminelles ayant des liens avec des structures étatiques pakistanaises.
2. La carence des États

a. Le refus de certains États de lutter contre cette forme de criminalité (la Thaïlande) ou qui se montrent incapable de le faire (Pakistan). D’autres encore sont soupçonnés d’agir délibérément dans cette voie à des fins politiques voire même terroristes (c’était le cas de certains pays du Moyen Orient pendant la guerre froide liés au Bloc de l’Est. C’est aujourd’hui encore le cas pour l’Iran ou la Syrie par l’intermédiaire de leurs services.

D’autres États ne sanctionnent que légèrement la fraude documentaire et surtout l’utilisation de faux documents administratifs. On peut citer à cet égard le Royaume Uni qui, conscient de l’importance de ce phénomène pour l’activité des réseaux terroristes a, depuis les attentats de Londres, renforcé sa législation. Il est vrai que l’absence de contrôle d’identité rend la répression de la fraude documentaire plus difficile.

b. L’immigration.

Surtout en Europe; aucune politique commune. C’est même un sujet de contentieux politique (France Espagne).

L’espace Schengen qui s’élargit. Peu de parade. Le mandat d’arrêt Européen est un bon instrument mais il n’est pas appliqué dans tous les États (notamment en Allemagne). Les équipes communes d’enquête ont également démontré leur efficacité. Mais elles ne sont pas encore généralisées.

III. Comment réagir: les procédures de riposte

La dimension stratégique de la fraude documentaire pour les réseaux terroristes doit impérativement être prise en compte par tous les États eu égard à la mondialisation de la menace terroriste et à la porosité croissante entre grande et petite criminalité et activités terroristes.

Cette nécessaire prise de conscience par les États exige la mise en œuvre de moyens de riposte adaptés.

Ces moyens devraient – selon moi – se développer à deux niveaux.
1. En amont, par une action politique et technique.
2. En aval en durcissant les armes juridiques insuffisamment adaptées au phénomène et en renforçant la coopération internationale.
1. **En amont**

C’est l’action politique.


Le cadre Européen plus intégré et normatif paraît être le mieux adapté pour faire progresser les législations et les politiques en cette matière.

Par ailleurs, on pourrait imaginer l’adoption par le Conseil de l’Europe d’une convention sur la fraude documentaire. Une telle convention qui devrait entraîner l’adhésion des pays membres : elle aurait un effet d’entraînement certain à l’égard de la communauté internationale. En tout état de cause cette action politique devrait être conduite dans le cadre plus général de la lutte contre la contrefaçon.

*b.* L’action technique.

La généralisation des cartes d’identité et des passeports biométriques – les techniques existent.

La généralisation – ce qui ne sera pas sans poser des problèmes d’ordre politique – du visa électronique (Australie, Bahreïn). Un système souple et finalement peu contraignant Cette mesure pourrait dans un premier temps n’être applicable que pour certains pays.

2. **En aval**

Des mesures essentiellement juridiques.

*a.* au niveau international.

Il rejoint ce qui a été dit plus haut concernant l’action politique. Se doter de nouveaux instruments internationaux. L’Union Européenne pourrait prendre des initiatives dans de domaine.

*b.* au plan national il conviendrait de mieux incriminer et réprimer la fraude documentaire lorsqu’elle s’inscrit dans un contexte terroriste. C’est ce que la France a fait d’une certaine façon avec l’association de malfaiteurs (article 421-2-1 du Code Pénal).
Conclusion

La fraude documentaire dans le contexte de l’activisme terroriste n’est pas un sujet académique. C’est une exigence opérationnelle.

Sa répression se heurte à la difficulté d’harmoniser les législations car elle soulève d’autres problèmes politiques, comme l’immigration.

Cette exigence de prendre en compte ce phénomène est d’autant plus prégnant que la menace terroriste s’aggrave et que l’Europe est de plus en plus visée.
I. Introduction: defining concepts and developing terminology as a starting point

The fact that identity-related crime has become perhaps the defining crime of the information age is itself an indication of the huge challenges that need to be addressed when developing appropriate domestic and international criminal justice responses to the problem. In doing so, however, serious consideration should first be given to the clarification of crucial terminological and definitional issues, as it is impossible to study the real threat of the phenomenon and evaluate appropriate countermeasures without conceptual clarity.

The concept of false identity or the falsification of identity or identity documents encompasses three types of misconduct:

• the invention or fabrication of a wholly fictitious identity;
• the alteration of a genuine identity or the use of parts of a genuine identity; and,
• the use of a genuine identity by a person other than the individual to whom it properly belongs or, in the case of documents, the lawful holder of the document.

In the UN study on “fraud and the criminal misuse and falsification of identity” (2007), the general term “identity-related crime” was used to cover all forms of illicit conduct involving identity, including identity theft and identity fraud. The approach followed was to use this descriptive concept as an “umbrella term” to cover all punishable activities having identity as a target or a principal tool. In some contexts, the term “identity abuse” was also used with a similar meaning, but without carrying any implicit assumption about whether a given conduct is already a criminal offence or should be criminalized. The reason for using such generic terms was the diversity in definitional approaches followed in national jurisdictions in that the same conduct designated as “identity theft” in some countries is seen as “identity fraud” in others.

The UN study further specified that the term “identity theft”, in particular, refers to occurrences in which information related to identity (basic identification information/other personal information) is actually taken in a manner analogous to theft or fraud, including theft of tangible documents and intangible information and deceptively persuading individuals to surrender documents or information voluntarily.

2 Pursuant to Economic and Social Council (ECOSOC) resolution 2004/26 of 21 July 2004, the United Nations Office on Drugs and Crime commissioned a study on “fraud and the criminal misuse and falsification of identity”, which was released in early 2007 as the result of the work of an intergovernmental expert group and was submitted to the United Nations Commission on Crime Prevention and Criminal Justice at its sixteenth session (E/CN.15/2007/8 and Add. 1-3). The findings of the study were based on the information provided by 46 Member States. The study tackled differences and deviations in definitional and conceptual approaches at the national level with regard to the criminal misuse and falsification of identity and shed light on various aspects revealing the complexity of the problem and its criminal diversity. Crimes involving identity abuses were examined jointly with fraud given their close relationship and the specific directions of the ECOSOC mandate. The full text of the study is available at the UNODC website: http://www.unodc.org/unodc/en/organized-crime/index.html.

3 See also Koops/Leenes, “Identity Theft, Identity Fraud and/or Identity-related Crime”, Datenschutz und Datensicherheit 30 (2006), p. 554.


On the other hand, the term “identity fraud” generally refers to the subsequent use of identification or identity information to commit other crimes or avoid detection and prosecution in some way\(^6\). This includes both fraud against private entities (e.g. credit card fraud) and fraud against the public sector (e.g. illegally obtained social benefits or procurement contracts).

**II. Criminalization of identity-related crime per se**

The present state of legislation and policy-making in most States is limited to dealing with identity problems primarily in terms of the further crimes that can be committed through identity abuses, such as forgery and impersonation\(^7\).

However, some States have already begun to address the problem from the perspective of identity itself and treat identity abuses such as taking, copying or fabricating identity and the various forms of tampering with identity systems, as **new and distinct forms of crime**. The criminalization of identity-based offences in a number of legal systems reflects the recognition that primary abuse of identity can lead to a range of secondary crimes, thus enabling the criminal justice system to intervene at an earlier stage. This approach also results in broadening the scope of victims to include both those whose genuine identity is used to commit other crimes and those targeted by subsequent crimes.

\(^6\) Ibid.

\(^7\) Some of the Member States that provided information for the purposes of the UN study reported on a number of specific identity abuses which were also subsumed within broader crimes, such as cybercrime offences, including the theft of data and unauthorized access to or tampering with computer systems. Some States highlighted the criminalization of offences that were specific to types of identification or identity such as passports or government identification. States parties to the Council of Europe Convention on Cybercrime reported that they were required by article 7 of that Convention to ensure that their legislation on forgery covered computer – or data – related forgery. Several States made reference to offences related to computer “phishing” and similar conduct. In other States, that activity may also be covered by more general cybercrime legislation, such as that covering the theft or illicit possession of passwords.
Examples of this new approach are the **US legislation**, which criminalizes identity theft at both federal and state levels, as well as the legislation in some **Australian States**. In addition, the Government of

---

9. Sec. 530.5 of the Penal Code of California sanctions every person who wilfully obtains personal identifying information of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the name of the other person without the consent of that person. Moreover, it sanctions every person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information of another person.

Sec. 530.5 of California Penal Code also gives a definition of “personal identifying information”, which is defined as the name, address, telephone number, health insurance identification number, taxpayer identification number, school identification number, state or federal driver’s license number, or identification number, social security number, place of employment, employee identification number, mother’s maiden name, demand deposit account number, savings account number, checking account number, PIN (Personal Identification Number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voice print, retina or iris image, or other unique physical representation, unique electronic data including identification number, address, or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person.

Sec. 13-2008 of Arizona Revised Statute sanctions the act of taking the identity of another person. A person commits this crime when he/she knowingly takes or uses any personal identifying information of another person, without the consent of that other person, with the intent to obtain or use the other person’s identity for any unlawful purpose or to cause loss to a person.


In 2003, *South Australia* introduced specific identity theft offences. The offences, in Part 5A of the Criminal Law Consolidation (Identity Theft) Amendment Act, criminalize the following conduct:

- the assumption of a false identity (including falsely pretending to have a particular qualification or have, or be entitled to act in, a particular capacity) – s 144B;
- the misuse of personal identification information – s 144C;
- the production and possession of prohibited material – ss 144D(1) and (2); and,
Canada introduced on 21 November 2007 a new bill making identity theft a specific criminal offence.

The federal Identity Theft and Assumption Deterrence Act of 1998, in particular, is a landmark in the evolution of US identity theft legislation. It was the first statute to define identity theft as an act

- the possession of equipment for making prohibited material – s 144D(3).

Section 144A of the Act defines key terms including “false identity” “personal identification information” and “prohibited material”. “Personal identification information” is broadly defined as information used to identify the person, including the person’s name, address, date of birth and voice print, and biometric data relating to the person. The definition of personal identification information specifically includes “the person’s credit or debit card, its number, and data stored or encrypted on it”. For a body corporate, “personal identification information” includes the number of any bank account established in the body corporate’s name or of any credit card issued to the body corporate.

The offences do not apply to under-age persons who attempt to enter age-restricted venues or purchase age-restricted items, such as cigarettes or alcohol.

The Criminal Law Consolidation (Identity Theft) Amendment Act also amended the Criminal Law (Sentencing) Act 1988 by providing for the issue of a certificate, on application by the victim of the offence, where a court convicts a person for an offence involving the assumption of another person’s identity or use of another person’s personal identification information. The certificate contains details of the offence, the name of the victim and any other matters the court considers relevant.

Queensland’s new section 408D is based on the model credit card skimming offence that was endorsed in March 2004. The Queensland offence is quite broad to ensure that the full range of conduct that can constitute identity theft is captured. The new provision applies to a person who possesses “identification information” for the purpose of committing or facilitating the commission of an indictable offence.

The definition of ‘identification information’ covers a broad range of conduct which can be described as “identity theft” and “identity fraud”.

For more information, see Model Criminal Law Officers’ Committee of the Standing Committee of Attorneys-General, Discussion Paper on “Identity Crime”, April 2007.

The adoption of ad hoc legislation against identity theft was motivated by the need to modify the existing criminal code (18 USC 1028), which was originally intended to tackle crime in the fields of drug trafficking, alien smuggling and credit card fraud. The problem with the old law on identity theft appears to have been that the documentation had to be physically presented as part of the crime. This meant that “card not present” crimes using the telephone, computer or the Internet were not covered by legislation.
involving one who “knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law”\textsuperscript{12}. This definition/provision contains three elements – the object (means of identification), the act (transfers, possesses, or uses) and the intention that links the acts to further criminal activities (intent to commit, or to aid or abet, or in connection with, any unlawful activity). With regard to the acts and the intended offences, the provision is following a broad approach, whereby the possession of personal information may be criminal even if no further offence is committed\textsuperscript{13}. The penalty for a simple breach is a maximum of 5 years imprisonment and an aggravated offence attracts a penalty of 15 years imprisonment and a maximum fine of $250,000\textsuperscript{14}.

The Act also defined personal information (referred to as “means of identification”) broadly, to include government-issued identifiers, such as

\begin{quote}

The US Secret Service – the main law enforcement group in the USA responsible for this type of crime detection – testified to the Senate Judiciary subcommittee that law enforcement was frustrated that the unlawful use of personal information was not a crime, and that identity theft was being perpetrated by organized criminal groups which knew that this activity could be committed with relative impunity. The Federal Trade Commission testified to the same subcommittee that victims of identity theft were suffering real tangible harm, with the effects of the theft being both significant and long-lasting in nature. The direct harm was exacerbated by the fact that the consumer victims had great difficulty obtaining help from law enforcement, since US law did not at that time recognize these individuals as victims.

Under the 1998 Act, the US Secret Service leads the law enforcement fight against identity theft, while the Federal Trade Commission is responsible for the complaint process, as well as education, awareness and prevention.


\textsuperscript{12} 18 USC § 1028(a)(7).


\textsuperscript{14} The aggravated offence was introduced by the \textit{Identity Theft Penalty Enhancement Act (ITPEA)} in 2004.
social security and passport numbers, biometric information and telecommunication and electronic identifiers.\textsuperscript{15}

The Act was seen by many commentators as an important first step with regard to the fight against identity theft, while others, without questioning the necessity of establishing a criminal offence, argued that trying to deal with identity theft through criminalization alone could not serve as an effective means of control and therefore more comprehensive strategies were needed. Matejkovic and Lahey claim that the Act accomplished a number of significant tasks. Among them is the classification of individuals as primary victims as opposed to financial institutions, as well as the federalization of the crime which gives victims the opportunity to request aid from law enforcement officials\textsuperscript{16}.

With regard to the European legal framework, no specific criminal provision targeting identity theft or identity fraud \textit{as such} exists\textsuperscript{17}, nor does the Council of Europe Convention on Cybercrime\textsuperscript{18} or the European Union Framework Decision on attacks against information systems\textsuperscript{19} contain identity-specific crimes. Rather, most relevant regulations are those contained in Directives on either privacy protection in

\textsuperscript{15} In May 2006, the US Government issued an executive order to supplement the criminal legislation against identity theft. Executive Order 13402 on “Strengthening Federal Efforts to Protect Against Identity Theft” established an Identity Theft Task Force. The Task Force is assigned to develop a strategic plan to enhance the effectiveness and efficiency of government efforts to deter, prevent, detect, investigate, and prosecute identity theft.


\textsuperscript{17} See Mitchison/Wilikens/Breitenbach/Urry/Portesi, ibid., p. 23.

\textsuperscript{18} Opened for signature in Budapest on 23 November 2001 and in force since 1 July 2004 (European Treaty Series No. 185).

general, or on ICT crime\textsuperscript{20}. Identity theft/fraud, being at the crossroads of these areas, are usually covered by both\textsuperscript{21}.

At the national level, most European Union Member States, in view of the lack of specific legislation, cover most or all incidents of identity theft under other headings within criminal law. Thus, in France, Germany and the Netherlands, for example, there are laws that can be used to prosecute offences such as forgery or data abuse\textsuperscript{22}.

In the United Kingdom, to take another example, identity theft is not yet a crime under the current legislation, although the Government is consulting on whether it should enact relevant legislation. The use of a false identity or the adoption of another person’s identity can be a criminal offence if proved that there was some conspiracy to commit a criminal act or fraud, or that a criminal act or fraud took place. However, in these circumstances, the defendant would be prosecuted for the conspiracy or criminal act itself as this would be the more serious offence and would carry a higher penalty. Nevertheless, there have been some recent laws that target identity crime offences. The Identity Cards Act 2006 created new criminal offences of being in possession of or controlling false identity documents, including genuine documents that have been improperly obtained or were issued to another person, without reasonable cause. These offences came into force on 7 June 2006 and cover both domestic and foreign documents.

Despite the reluctance of national law-makers in Europe to resort to the criminalization of identity theft/fraud as a component of the overall efforts to address the problem, the challenges posed by related criminal


activities have already been recognized at the European Union level as a considerable policy issue\textsuperscript{23}, while the European Commission has further proposed that “EU law enforcement cooperation would be better served were identity theft criminalized in all Member States”\textsuperscript{24}. This proposal paved the ground for conducting consultations to assess whether specific legislation is necessary and appropriate in Member States, as it is reasonable to suggest that there will be increasing public attention in Europe to preventing and responding efficiently to identity abuses for criminal purposes. The Commission (DG on Justice, Freedom and Security) has already launched a comparative study in July 2007 on the definitions of identity theft used in the EU Member States and their criminal consequences. This study will include, upon its finalization, recommendations on best practices.

The overview above indicates that the abuses of identity as distinct criminal offences represent a fresh approach for most States and extensive work is needed. In this connection, the UN study on “fraud and the criminal misuse and falsification of identity” recommended that “law-makers need to develop appropriate concepts, definitions and approaches to the criminalization of a broad range of conducts, including identity theft, identity fraud and other identity-related crimes. It is also critical for most States to ensure consistency with their respective private and public identity systems and with other already established crimes”\textsuperscript{25}.

\textsuperscript{23} As part of an awareness campaign to improve the prevention of identity theft and payment fraud, Directorate-General Justice, Freedom and Security (DG JLS) and Directorate-General Internal Market of the European Commission organized a conference on “Maintaining the integrity of identities and payments: Two challenges for fraud prevention”, which took place on 22-23 November 2006 in Brussels. The Conference intended to emphasize the importance of the wider involvement of policy makers and high ranking representatives of national administrations and to provide a platform for policy makers to discuss possible EU initiatives in this field. Among the issues discussed at the Conference were possible EU criminal legislation on identity theft, training models for law enforcement/financial investigators, exchange of information and privacy issues.


\textsuperscript{25} E/CN.15/2007/8, para. 22.
III. Why to treat identity-related crime as a separate category of offence?

The same study, however, pointed out that “given the concerns expressed about the links between domestic means of identification, international and travel-related identification and transnational forms of identity-related crime, criminal offences that provide a good basis for international cooperation are desirable”. Therefore it recommended that “States consider the establishment of new identity-based criminal offences” and that “in developing new offences, common approaches to criminalization be taken, to the greatest extent possible, to facilitate future transborder evidence-sharing, extradition of offenders and other forms of international cooperation”.

Bearing these recommendations in mind, it would be useful to examine whether criminalization of identity-related crime per se would be an effective policy option and whether it would bring about definite advantages in the fight against this form of crime.

A first reason for which identity-related crime seems to merit special treatment is that it occurs in forms and on a scale that have no precedent in the past. Because of the spread of modern information and communication technologies, identity management has now gained a new and more challenging role. Face-to-face transactions have rapidly been replaced by e-commerce and on-line arrangements. Along with the new role of identity in the information society, new opportunities for the commission of crimes involving the misuse and falsification of such identity have emerged as an unavoidable consequence. Given the increasing seriousness of the problem, criminalization of identity-related crime provides, to a certain extent, a particular way of raising awareness among individuals as well as businesses.

Professors Koops and Leenes use an eloquent example to justify the treatment of identity-related crime as a separate offence by resorting to a comparison with the legal framework on computer-related crime. Although computer-related fraud can be examined as simply another means to commit fraud, it has been considered a category of fraud on its own. As a result, article 8 of the Council of Europe Convention on Cybercrime established a separate offence of computer-related fraud aiming at combating any undue manipulation in the course of data processing with

\[\text{Ibid.}\]
\[\text{See Koops/Leenes, ibid., p. 553 et seq.}\]
the intention to effect an illegal transfer of property. The primary reason for this development was not that forms of computer-related fraud were not punishable under traditional criminal provisions, such as those on fraud or forgery, although there were certainly specific legislative gaps. Rather, ad hoc criminalization was chosen because combating computer fraud requires special expertise and knowledge of computer systems and data.28

The same argument can also be raised with regard to identity-related crime. The new forms and scale of identity management create new opportunities for fraudulent practices. In order to combat such practices in an effective manner, attention should be devoted not only to the potential extension of current legal provisions and schemes, but also, and more importantly, to assessing whether new strategies should be developed to focus on the specifics of identity-related crime, including the feasibility and effectiveness of developing ad hoc legislation that treats such crime as a self-standing offence.

Another reason for such an approach is the need to protect victims of the crime more efficiently. Unlawful identity takeover can cause separate social harm that needs to be addressed by criminal law. Moreover, it differs from traditional fraud in two fundamental ways. First, it takes time for the victim to notice the crime and the harm caused by it and often this occurs until long after the perpetrator “has booked a one-way ticket to the tropics”. Secondly, the victimization of persons whose identity is targeted may well continue long after the crime, since, contrary to the traditional cases of fraud, a feature of identity takeover is that the victim is blacklisted and faces difficulties in regaining credit history and trustworthy image (“associated indirect cost for consumers”). It is therefore altogether important to deal with the specifics of identity-related crime in order to ensure a sufficient level of protection and support for victims.29

In addition, in many legal systems, the criminalization of specific abuses of identity information can increase the effectiveness of investigations, by triggering the application of investigative powers as soon as it is clear that identity information may have been compromised, rather than having to wait until secondary offences such as fraud or acts of terrorism were committed. As it is true that perpetrators can use the obtained identities to hide their own identity, being able to prosecute the chronologically first act could avoid difficulties in the identification of the

29 See also Van der Meulen, ibid., p. 25.
offender committing the subsequent acts. As the UK Cabinet Office Study of 2002 indicates, focusing on identity theft in particular, “prosecution of offenders should be pursued more vigorously. One way to ensure this might be through the creation of a new offence of identity theft, which might make successful prosecution both more worthwhile and easier.”

Furthermore, specific identity offences can respond more effectively to changes in criminality related to the involvement of technologies and organized criminal groups. Some organized criminal groups are sophisticated enough to use multistage identity schemes in which identity information from one source is used to submit fraudulent applications for genuine documents in an effort to build and maintain even more solid and elaborate fictitious identities. Another factual scenario is that specific stages of identity-crime schemes may be carried out by offenders in different jurisdictions, usually with a view to facilitating organized crime activities. By resorting to specific identity crimes, each

31 Cases and relevant information reported by Member States in the context of preparing the UN study on “fraud and the criminal misuse and falsification of identity” indicated that a substantial percentage of identity-related crime is associated with, and facilitates the transborder commission of, specific offences involving an organized criminal group such as trafficking in persons and smuggling of migrants.

Article 12 (security and control of documents) of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children (General Assembly resolution 55/25 of 15 November 2000, annex II) and the Protocol against the Smuggling of Migrants by Land, Sea and Air (General Assembly resolution 55/25 of 15 November 2000, annex III), both supplementing the United Nations Convention against Transnational Organized Crime, requires States parties to ensure that travel or identity documents issued by them are of such quality that they cannot easily be misused and cannot readily be falsified or unlawfully altered, replicated or issued; and to ensure the integrity and security of travel or identity documents issued by them and prevent their unlawful creation, issuance and use.

Article 13 (legitimacy and validity of documents) in both the Trafficking in Persons Protocol and the Migrants Protocol further requires States parties, upon request, to verify within a reasonable time the legitimacy and validity of travel or identity documents issued or purported to have been issued in their name and suspected of being used for trafficking in persons or the smuggling of migrants.

Article 6 (criminalization) of the Migrants Protocol requires States parties to establish as criminal offences, when committed intentionally and in order to obtain a financial or other material benefit, not only the smuggling of migrants, but also,
offender could be prosecuted for each element of the criminal conduct in the place where it was committed, whereas criminalization based on proof that the activity is in preparation for another crime requires proof of the other crime, which may not exist or may be in another State. In this way, specific offences increase the likelihood of successful investigations and prosecutions, and may alleviate some of the challenges encountered in the field of international cooperation.

There are, of course, legal challenges that need to be addressed such as the divergent national attitudes with regard to the delineation of the preparatory acts at the early stages of the conduct. The legal concept of preparation raises questions as to how each legislation defines, or will define, the crime and the preparatory steps associated with it. Therefore there is a need to identify and describe criminal behaviours, as well as develop concrete typologies before undertaking legislative action at the national level.

IV. The treatment of identity-related crime as a “serious crime”

In addition to the treatment of identity-related crime as a self-standing offence, it may also be necessary for law-makers to examine the threshold of applicable penalties. There is currently the perception that those penalties are generally too low to be dissuasive and this is mainly due to the fact that identity-related crime is still treated in many States only in conjunction with fraud or other potential crimes, the latter being considered as more serious crimes.

However, if more States establish in future domestic crimes to address identity abuses per se, it seems highly likely that, in view of the sophistication and the criminal expertise involved, the relevant national laws will treat identity-related crime as a serious crime. A reliable indication of the serious nature of a crime is that provided for by the United Nations Convention against Transnational Organized Crime (Palermo when committed for the purpose of enabling the smuggling of migrants, producing a fraudulent travel or identity document; procuring, providing or possessing such a document; and enabling by such means (that is, by producing, procuring or providing a fraudulent document) or other illegal means a person who is not a national or a permanent resident to remain in the State concerned without complying with the necessary legal requirements.
Article 2, subparagraph (b), of the Convention defines “serious crime” as an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. The UN study “on fraud and the criminal misuse and falsification of identity” includes a relevant recommendation that the scope of application and appropriate definitions contained in articles 2 and 3 of the Palermo Convention be taken into consideration by Member States engaged in the development of new offences pertaining to identity-related crime.

In case of identifying such a level of seriousness for offences targeting identity, Member States will be provided with convincing and reliable arguments regarding the use of the Palermo Convention as a legal basis for international cooperation to combat those offences. As far as the other “enabling factors” for the application of the Convention are concerned, the transnational aspect seems to be in most cases an inherent element of identity-related crime, whereas the involvement of an organized criminal group is more or less implied where the means used to commit the crime are beyond the capabilities of individual offenders.

V. Jurisdiction issues

As it is possible for offenders to route communications or target a specific group of victims to take maximum advantage of any gaps in offence provisions or investigative powers or capacity in certain national territories (“forum shopping”), the establishment of flexible jurisdictional

---

32 General Assembly resolution 55/25 of 15 November 2000, annex I.
33 E/CN.15/2007/8, para. 20 (e).
34 The United Nations Convention against Transnational Organized Crime defines an organized criminal group as such if one of its objectives is to generate a “financial or other material benefit” (Article 2). Although identity-related crimes are not necessarily economic in nature, almost all of them fall within the scope of the Convention, as even non-economic identity-related offences are covered if they are linked to an organized criminal group that is also involved in economic crime.

Moreover, the meaning of the term “financial or other material benefit” is relatively broad and includes, for example, trafficking in child pornography for reasons of sexual gratification. It therefore encompasses identity crimes where stolen or fabricated identification or identity information is treated as a form of illicit commodity and bought, sold or exchanged, as well as instances where identification is misused for personal or organizational gains, including non-financial gains such as securing entry into another country.
regimes plays a pivotal role in ensuring effectiveness of the international cooperation mechanisms used to combat identity-related crimes of transnational nature.

In the context of the UN study on “fraud and the criminal misuse and falsification of identity”, it was highlighted that modern transnational identity-related crimes tend to take place in many national jurisdictions at the same time and therefore may not be well addressed by strictly territorial jurisdictional principles, unless laws have been updated to provide for more flexibility. Furthermore, narrow approaches can lead to cases where no State with the ability to prosecute effectively has sufficient jurisdiction to do so. The study therefore recommended the review of the relatively narrow jurisdictional approaches to ensure that they keep pace with the ongoing evolution of identity-related crime.\[35\]

With regard to extraterritorial jurisdiction, information reported by some Member States for the purposes of the study indicated the establishment of jurisdiction on an extraterritorial basis where fundamental national interests were affected, such as in cases of offences relating to the forgery of passports or counterfeiting of currency.

Extraterritorial jurisdiction is definitely of relevance and usefulness in cases of domestic prosecutorial action where extradition is not possible. The study recommended that all Member States consider establishing jurisdiction to prosecute identity-related crime where the accused offender is found in their territory and they cannot extradite him/her for any reason to another State that has territorial jurisdiction to prosecute the offence.\[36\]

However, broad approaches to territorial jurisdiction may often result in conflicts of jurisdiction, ne bis in idem and other problems. The study therefore recommended that States should consult and collaborate with each other to ensure that cases are prosecuted, where possible, by the State that is in the best position to do so, taking into account factors such as the availability of witnesses and evidence, the rights of accused persons, the capacity of the State to mount a fair and successful prosecution and the ability of other interested States to provide cooperation in support of the prosecution.\[37\] Because of the nature of the crimes at stake, early

\[35\] E/CN.15/2007/8, para. 23(a).


\[37\] E/CN.15/2007/8, para. 23(b).
identification of the States concerned and early investigative coordination and cooperation are deemed to be particularly important.

VI. Conclusion

The fight against perpetrators attempting to obtain and use identity-related information goes along with a number of challenges for law enforcement and criminal justice authorities. In order to respond effectively to these challenges, appropriate conceptual and definitional approaches to identity-related crime are needed as a prerequisite for having in place clearly defined and delineated legal frameworks, including relevant criminalization provisions. Ensuring conceptual clarity in efforts to address this particularly complex problem is of crucial importance keeping in mind the classic Roman axiom “nullum crimen nulla poena sine lege certa”.

However, effectiveness in the fight against identity-related crime can only be ensured if the legal measures in place are combined, in the context of an integrated and comprehensive counter-strategy, with appropriate preventive and technical measures geared towards establishing stronger identification management and verification systems and limiting the risks stemming from this form of crime. As eloquently pointed out and described in the literature, identity-related crime is the “consequence of the vulnerabilities of the identification architecture and such vulnerabilities are not created by the perpetrators; rather, they are exploited by them”.

---

CANADIAN IDENTITY THEFT LEGISLATION:  
A CASE STUDY IN DOMESTIC CRIMINALIZATION OF IDENTITY-RELATED CRIME

JOANNE KLINEBERG
Legal Counsel, Department of Justice, Canada

Introduction

The international community has begun in earnest to take a close look at the growing problem of identity crime. One of the bodies that is exploring the issues is the United Nations Office of Drugs and Crime. From 2005 to 2007, the UNODC conducted an international study in which Member States were queried about their experiences, laws and practices in relation to both fraud and identity related crime. The study revealed, among other findings, that while States have a relatively good grasp on economic fraud both in terms of what it looks like and having legislation to prohibit it, identity related crime is much less well understood and, save for a small number of countries, not explicitly addressed by criminal laws.

Building on the results of that study, the UNODC has brought together a core group of experts to delve more deeply into the problem to advise it on how best to assist Member States in understanding the nature of the problem and possible best practices to address any shortcomings either domestically or in relation to cooperative international efforts. In addition, and to further the efforts of the UNODC, ISPAC also took up the matter at its annual proceedings in November 2007 and brought together experts and interested individuals to further develop the international community’s understanding of the issues. The basic content of this paper was presented by the author at that conference, and has now been formalized following from the discussions held at the conference.

1 The author was involved in the development of legislation in Canada in this area, but the opinions contained herein are those of the author alone and do not represent the views of the Government of Canada or the Department of Justice.
There are a vast range of approaches that could be employed to address concerns over identity abuses, ranging from privacy legislation, enhanced security in the banking and private sectors, improved technology on credit cards and computer systems and consumer protection measures, to name just a few. The focus of the work of UNODC, ISPAC, and this paper, lies in the area of crime prevention and criminal justice responses to the problem, but it should be borne in mind that, given the nature of identity abuses and identity itself, any comprehensive, effective response must be of a multi-disciplinary nature.

Criminalization of identity related misconduct is often discussed as a possible approach. Proponents of this approach tend to characterise “identity-related crime” as either a new and emerging problem, or one which has been made sufficiently more serious by technological advances that it requires a thorough review of the adequacy of existing criminal law measures and consideration of novel approaches to criminal liability. Others take the view that such crime is nothing more than the modern technologically enhanced version of the traditional crimes of fraud and impersonation. This view suggests that the emphasis should be placed on increasing capacity to conduct domestic and transnational investigations and prosecutions, and that the enactment of new criminal offences would only duplicate existing offences and could generate false expectations on the part of the public and divert attention away from enforcement efforts.

The urge to “over-criminalize” conduct can certainly sometimes infect legislatures across the globe. This is a serious issue which should not be overlooked or minimized in the identity crime area. Indeed, the potential for duplication in this area is large. However, it would similarly be a mistake to assume, without closely examining the issue, that nothing is to be gained by consideration of criminalization. It is only after a careful and thorough study that one can resolve the matter with any degree of confidence.

While bodies like the UNODC explore ways in which States can work together to improve international enforcement measures and set out best practices for the world community to strive for in a variety of domains, including possible recommended elements for criminalization, it is ultimately for each State to decide what policies to pursue, and this includes whether to enact new offences or modernize existing ones to criminalize identity abuses per se.
The Government of Canada has recently introduced legislation to amend the Criminal Code to introduce new offences and amend existing ones in relation to identity related crime. This paper will briefly describe the Canadian legislation as a case study which may be illustrative of the process that other states might wish to undertake domestically in order to assess the adequacy of its criminal laws. For obvious reasons, the domestic criminal law of each country will differ in substance and underlying principles in both minor and significant ways. Therefore, this paper will attempt to emphasize the processes that were undertaken and the obstacles that were faced, in the hopes that it might act as a possible guide should other states decide to undertake the same analysis. The legislation introduced by the Government of Canada will be described briefly at the end of the paper.

The problem of defining the problem

Any consideration of identity theft almost immediately reveals a significant problem of terminology. When Canadian officials began to look at the issue, even a cursory survey of existing legal provisions in the few countries that have expressly legislation in this area (principally the United States and Australia), of the multitude of media reports of “identity theft” and of publicly available materials of law enforcement bodies expressing concern over the issue revealed a lack of uniformity in both the understanding of the precise limits and contours of the term “identity theft”, and of the use of that term as either synonymous or merely contiguous with other related terms such as “identity fraud” and “identity crime”.

In Canada, many institutions had already taken a strong interest in the issue of identity theft before the Government introduced specific legislation in Parliament in November 2007. The banking sector, law enforcement agencies, privacy commissions, consumer protection associations, and even federal and provincial government departments and


agencies had developed their own working definitions of the key terms. None of these definitions exactly match any other. While they may share many similar features and common elements, they also vary in ways which might appear subtle and insignificant to the casual reader, but which could be highly significant to criminal courts, persons accused of crime, or victims who might expect government action. For constitutional and practical reasons, a much higher degree of clarity and certainty is needed as the definitional basis of any criminal offences.

For instance:

- recol⁴ – an online site for intake of complaints of economic crime – appears to use “identity theft” and “identity fraud” interchangeably and defines them as conduct that involves “stealing, misrepresenting or hijacking the identity of another person or business and [which] provides an effective means to commit other crimes”⁵;
- the Royal Canadian Mounted Police website states that “Commonly referred to as identity theft, identity fraud involves the unauthorized acquisition, possession or trafficking of personal information where that information is used to create a fictitious identity, assume or takeover an existing identity that results in financial gain, goods or services, or conceals criminal activity”⁶;
- the Privacy Commissioner of Canada states that “identity theft” is “the unauthorized collection and use of your personal information, usually for criminal purposes”⁷;
- the Government of the Province of Ontario’s Ministry of Government and Consumer Services has defined “identity theft” as what “occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud or theft”⁸;

---

⁴ Reporting Economic Crime Online (RECOL) is an initiative that involves an integrated partnership between International, Federal and Provincial Law Enforcement agencies, as well as, with regulators and private commercial organizations that have a legitimate investigative interest in receiving a copy of complaints of economic crime in Canada. The service is administered by the RCMP and other participating law enforcement agencies.

⁵ https://www.recol.ca/scams/Identity_Fraud.aspx


⁷ http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp.

• “Phonebusters”, a Canadian law enforcement site for gathering complaints, describes the following under the heading “identity theft”: “When an imposter co-opts your name, your Social Insurance Number (SIN), your credit card number, or some other piece of your personal information for their use – short when someone appropriates your personal information without your knowledge – it’s a crime, pure and simple”9.

To be fair, none of the extracted texts above hold their definition out as an actual legal definition, although they do imply that the conduct described is criminal. In fact, it is far from clear that all of the conduct described in these working definitions is actually criminal under Canadian law, especially in the absence of more detailed definitions of key phrases such as “stealing” or “appropriating” information.

These problems of terminology are likely to be more acute in jurisdictions that do not have specific identity theft legislation. In the absence of criminal (or other) legislation that explicitly defines what is meant by “identity theft” or related concepts, various bodies interested in the subject are free to, and indeed may arguably be required to, define the terms for themselves as they proceed to try to understand the problem and identify possible solutions10.

Looking even more closely, one sees buried within the current supply of inconsistent terms in use in Canada an even more basic problem: “What conduct should be encompassed by the selected term(s)?” or more fundamentally “What conduct should be criminal?” No two definitions above describe exactly the same conduct, and these definitions reveal some fairly subtle but difficult and significant policy questions. For example: Should the absence of consent of the person whose identity is used be relevant? Must the information have been wrongfully obtained (in addition to or as an alternative to being wrongfully used)? Could the conduct involve the hijacking of the identity of a legal person or only a natural person? Is the actual commission of a further crime, using the identity


10 Whether a State has adopted legislation dealing with cybercrime may also be a factor, as this often requires legislatures to deal with questions such as whether pure data or information are “property” which can be the basis for theft and similar offences.
information, necessary? Does identity theft encompass the creation and use of fictitious identities?

In addition to revealing certain underlying policy difficulties in assessing criminal law issues in this area, the ongoing terminological/definitional situation is itself problematic. Domestically, these terminology issues can be an obstacle to effective communication across relevant public bodies such as law enforcement agencies and departments responsible for criminal law policy development. This means that as a State embarks upon an analysis to determine whether or not criminalization is appropriate, its ability to communicate with key stakeholders, and to comprehend the representations made to it by key stakeholders, could be negatively affected unless all parties are cognizant of the definition problem and take it seriously by devoting sufficient time and attention to defining their use of terms with adequate precision.

Another way in which the absence of universally accepted definitions creates a problem is in relation to public awareness and public expectations. All of the definitions selected above were extracted from material made available specifically for dissemination to the general public in Canada. All of the organizations which had prepared those materials play a vital role in communicating information to the public, advising them on risk identification and avoidance, self-help measures, and remedial actions that can be taken if they feel they have been victimized. When multiple agencies with important public education roles define “identity theft” in different and to some degree conflicting ways, one must acknowledge the potential for confusion among the citizenry. The use of labels such as “identity theft” can create the impression that the label corresponds to a concrete forensic and criminological definition of the problem, and that something can and will be done about it when it occurs. The public may be led erroneously to believe that it could expect action from the State, either by way of prosecution for a perceived wrong or some form of compensation for a loss, among other measures, when such may not be possible in law or available in practical terms. Public expectations are sometimes not seen as a pressing problem by governments, but they can be significant and should not be ignored. To the degree that the State has a responsibility to its citizens to be clear about what conduct is and is not criminal, States should at least be aware of the legislative environment and whether it permits, or even encourages, a variety of agencies to present potentially erroneous or confusing information to the public about the state of the law on such an important issue.

These difficulties of terminology and definition can also exacerbate the already difficult tasks of data collection and data analysis. If police
agencies, consumer industries and various government statistics agencies employ different terminology and/or define each chosen term to encompass a different set of behaviours, any data that are collected by them will have uncertain value, will not easily be subject to comparison, and if taken together may present an inaccurate or misleading picture of the current environment. As there are relatively few available statistics on identity theft in Canada, any organization's attempt to collect data is appreciated, but one is left to speculate about how much more useful such statistics would be if the conduct at issue was defined in law, as that could form the basis for determining what should be measured in the first place, as is generally the case for crime statistics.

It also bears mentioning that this sort of terminological confusion can be greatly multiplied in the international context as language and methodological differences complicate the already challenging terminological and definitional exercises. If caution is not exercised in this context, there could be negative impacts on international cooperation in criminal law matters, such as where extradition or mutual legal assistance is sought. There is good reason to believe that identity related crime does cross borders in several ways. Because so much information is stored electronically in today's modern world, sensitive information can be accessed in one country by individuals in another and easily sold or transferred across borders, and used by an individual in one country to access goods or services in another country. Some of the crimes commonly associated with identity abuses, especially those involving passports and other travel or immigration-related documents and processes, are also inherently transnational in nature. The realities of the information age coupled with the vulnerability of information to exploitation demand a

For instance, in Canada, a service called Phonebusters receives complaints from the public and collects information about a variety of fraudulent schemes, among other functions, using categories which are partly law-enforcement and partly complainant-driven. Statistics published reflect these classifications rather than specific criminal law definitions, which do not yet exist for most identity crime offences. Case volumes and loss reports overlap significantly with economic fraud, which is a defined offence. While such data are of limited use, they are often the best available information until appropriate legislative definitions are adopted. Further inaccuracies and biases are probably generated by the reluctance of some victims, especially of frauds, to report the crime, and the fact that victims of some forms of identity crime may never be aware that they have been victimised. See the Report of the UN expert panel, E/CN.15/200718, para. 17.
strong and coordinated international criminal enforcement response, which in turn requires at least common understanding of the underlying criminal behaviour.

**Diagnosing the state of the problem and the state of the criminal law**

There may be a tendency among many confronted with the identity crime problem – which is unmistakably complex and far-reaching and difficult to grasp in its human terms let alone in its legal aspects – to simply assume that existing offences in one way or another cover the conduct that is at issue. The temptation to form such a conclusion should be resisted. Even a cursory look at a small sampling of material available to Canadians shows that the terms which are already in common usage do not lend themselves easily to definition, and do not yet benefit from universally accepted meanings. If this is true, how could it be known that existing criminal law regimes are adequate without actually examining the question in detail?

In Canada, once the terminological/definitional problems were identified, a process described as a “legislative diagnostic” was conducted. This involved a detailed and thorough review of existing Canadian criminal legislation in order to determine the law’s adequacy for dealing with identity related crime, and the existence of any limitations that might call for legislative action. A related exercise was conducted, involving a detailed examination of the various stages, aspects and forms of conduct that are involved in identity related crime, understood at its broadest level, and a distinct assessment of the criminalization questions in respect of each form of conduct. The results of the two “diagnostics” taken together led the Government of Canada to develop introduce Bill C-27\(^\text{12}\).

\(^{12}\) The author does not necessarily have a view as to which of the two diagnostics should be commenced or completed first, but it does seem imperative that both be undertaken if a truly sound decision on domestic criminal law reform in this area is to be achieved.
Diagnostic of legislation and legislative issues

The following will provide a brief description of the major offences that Canadian officials reviewed as part of their legislative diagnostic to illustrate the process that was undertaken.

In the UNODC fraud study, most States reported legislative measures against a variety of criminal offences in relation to fraud. This consisted of either a general fraud offence, offences in relation to fraud in specific contexts or by specific fraudulent schemes, or all of the above. Canada shares in this pattern, with a generic fraud offence as well as several more particularized fraud offences\(^\text{13}\). The Canadian fraud offence is particularly broadly drafted – the conduct can be “deceit, falsehood or other fraudulent means” – and has been interpreted by the courts to have a large reach. The offence can be proved not just by proof of actual economic deprivation, but also by a mere risk of deprivation\(^\text{14}\). In short, fraud consists of deceit coupled with deprivation (or risk thereof) of property.

Because most identity related crime is committed for the purpose obtaining financial reward or other forms of property, fraud offences are the most directly applicable and useful crimes with which to address the problem. From this perspective, a significant percentage of identity crime can be viewed as a sub-category of economic fraud.

Other categories of crime that are also commonly found in domestic criminal regimes, including Canada’s, are also directly applicable to aspects of identity related misconduct. Impersonation (or “personation” as the offence is labelled in Canada) is another immediately obvious applicable offence. In Canada, personation is a rather broad offence that prohibits fraudulently impersonating any person, living or dead, with either the intent to gain a personal advantage or an advantage for another person, to obtain property or an interest in property, or to cause a disadvantage to the person who is personated or to another person\(^\text{15}\). The advantage mentioned above has been held to include a non-economic advantage. Personation only

\(^{13}\) Subsection 380(1) of the\textit{ Criminal Code} provides the general fraud offence. Subsection 380(2) and sections 382, 383 and 383, for instance, provide fraud offences specific to the capital markets. Canada’s\textit{ Criminal Code} is available online at: \url{http://laws.justice.gc.ca/en/home} (English) and \url{http://laws.justice.gc.ca/fr/home} (French).


\(^{15}\) Section 403 of the\textit{ Criminal Code}. 

137
applies where a real person has been impersonated; it does not cover the creation and use of fictitious identities.

The offences of personation and fraud have large areas of overlap, and also certain areas of exclusive application. Where someone impersonates a real person and gains an economic benefit thereby, the personation offence is essentially a fraud – the identity deception that is core to personation doubles as the deception element of the fraud. Fraud could have application where personation would not apply, however, where a person uses a fictitious identity rather than that of a real person to obtain property. Conversely, personation could apply where fraud would not if the impersonation were carried out with intent to gain an advantage of a non-economic nature, such as to evade police detection or to obtain a lease that he or she could not otherwise have obtained (for instance owing to their own bad credit rating).

Forgery is another grouping of offences that have obvious application as many identity related crimes involve the use of false documents to support the misused identity. Canada currently has two general forgery related offences, making a false document and uttering a false document. In both cases it is required that the person either make or use the document with intent that it should be treated as genuine by someone else. Making a false document expressly includes altering, making an addition to or removing something from a genuine document. It also includes creating a wholly false document where such document purports to be made by or under the authority of, or in the name of, someone who did not actually make or authorize it. Thus, fraud offences are certainly applicable to prosecute those who create and who use fraudulent identification documents, or other forged documents in support of identity related crimes (such as, for instance, a fraudulent title document to support a title fraud). However, those who profit from the traffic in forged documents, even where they do so knowing that their end use will likely be criminal, do not appear to be committing any forgery related offences.

Many states, including Canada, also have distinct offences in relation to credit cards. In Canada, credit cards are different from debit cards (cards which permit access to bank accounts and banking services via

---

16 Section 366 and 368 of the *Criminal Code*. Specific forgery offences have also been adopted to protect specific documents, such as passports. See *Criminal Code*, s.57.

17 Subsection 366(2) of the *Criminal Code*.

18 Section 321 of the *Criminal Code*. 
automated teller machines), but both are included in the term “credit card”\(^\text{19}\). Canada’s credit card offences cover a wide range of conduct involving possession, use, trafficking and forgery of the cards themselves. In addition, there are offences in relation to credit card data. Specifically it is an offence where a person “fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use credit card data, whether or not authentic, that would enable a person to use a credit card”\(^\text{20}\).

In fact, the enactment of offences specifically in relation to the possession and trafficking of credit card data was in recognition of the fact that the real value lies in the information (data) that is embossed or otherwise contained in or on the card, and not the card itself. A similar situation is now being recognized with respect to identification information. Indeed, in Canada at least, one could argue that credit card data is a sub-category of the larger category of identification information as it is commonly understood (even in the absence of universally accepted definitions). As such, credit card data is more or less fully protected by existing criminal laws. What this reveals, however, are the limitations of Canadian criminal law insofar as it the protection of other valuable and criminally exploitable categories of personal identity information are concerned.

Computer crimes could also play a role in the battle against identity crime. Computer offences in Canada prohibit, where the actions were done fraudulently and without colour of right: obtaining any computer service; interception of any function of a computer system; using a computer system with intent to commit another computer related offence; and use, possession, trafficking in a computer password to enable a person to commit one of the other offences.

Certainly some of the largest and most well-reported instances of data breach have involved computer hacking to obtain the valuable information. However, other types of computer based techniques for obtaining sensitive information are not captured by existing computer offences, such as the use of mass emails designed to deceive recipients into voluntarily divulging their personal information (commonly known as “phishing”) or the creation of false websites that mimic those of genuine organizations or otherwise purport to be genuine and thereby seek to deceive others into voluntarily providing information.

\(^{19}\) Section 342 of the *Criminal Code* for credit card offences; see section 321 for the definition of “credit card”.

\(^{20}\) Subsection 342(3).
Other offences that might appear at first to be capable of addressing conduct in relation to the acquisition and possession of sensitive personal information are those of theft and possessing property obtained by crime. In Canada, theft requires taking or converting “anything” with intent to deprive the owner of it either temporarily or permanently. The offence of possession of property obtained by crime requires that a person possess “any property or thing” that the person knew was obtained by crime. Courts in Canada have held essentially that information is not property, as it is not subject of proprietary rights. In addition, the nature of information is such that its acquisition or conversion by one person does not deprive another of possession of it (except of course where it is only available in a tangible form and that tangible item is stolen, but in this case it is the tangible item, and not the information, which is stolen). These offences, therefore, would certainly apply where identity documents or other tangible items that contained information were stolen (or possessed after having been stolen), but are not available in situations involving the taking of intangible information such as by copying it from another source.

The offence of conspiracy in Canada requires two or more people to actually agree to carry out a crime together and put their plan into action. It is not required that any concrete steps toward the commission of the offence actually be taken. However, mere knowledge of, discussion of, or passive acquiescence in a plan of criminal conduct (as opposed to an agreement to do something) is not enough. It is generally agreed that, absent wiretap evidence, it is difficult to prove conspiracy. In addition, the larger an organization and the more segmented its activities, the less likely it will be to prove that each member of the organization had agreed to commit one or more specific offences with someone else, as each may play only a small role in the overall scheme.

Canadian law generally holds a person criminally liable for an offence committed by another person based on aiding, abetting or counselling another person to commit a crime. An accused can be liable where they know which crime the other person intends to commit, and they do something or omit to do something for the purpose of helping the other

21 Section 321.
22 Section 354.
24 Paragraph 465(1)(e).
to commit that crime, or where the accused person encourages or advises the person to commit the crime. As with conspiracy, proving that any particular person knew the precise nature of the crime that others might commit could be difficult in the absence of wiretap evidence or evidence of insiders. In addition, the offence must actually be committed for someone to be found guilty as a party to it.

Special offences in relation to organized crime and terrorism activities were also reviewed to determine their degree of applicability. Canadian offences in relation to organized crime and terrorism do permit prosecution for activities that are not in themselves criminal, but which are motivated by a desire to further the activities of such groups. Specifically, these participatory offences require proof of, respectively, an intention to “enhance the ability of a criminal organization to facilitate or commit an indictable offence” or to “enhance the ability of any terrorist group to facilitate or carry out a terrorist activity.” The emphasis of the offences on the purpose behind the commission of the acts calls for evidence that, as for conspiracy and party liability provisions, in most cases will not be readily available. For this reason, while these offences are in theory applicable in the most serious cases of identity related crime, in practical terms, their utility may be somewhat reduced.

Diagnostic of the criminal conduct itself

A complementary exercise that was carried out could be termed a “conduct diagnostic” and involved a detailed examination of the steps, aspects, components, functions and practical realities of identity related misconduct. A determination about the adequacy of the law could only be made by comparing the legislative diagnostic against a clear and full appreciation of the various elements of the behaviour and their respective potential for harm.

At its core, identity related crime is about the exploitation of an identity: the false use of identity to deceive. Fundamentally, an identity

---

26 Section 21 of the Criminal Code.
27 The organized crime provisions are set out in sections 467.1 to section 467.2 of the Criminal Code. The definition of “criminal organization” expressly excludes “a group of persons that forms randomly for the immediate commission of a single offence”. For terrorism offences in Canada see section 83.18 of the Criminal Code, RSC 1985, c. C-46, as amended by S.C. 2002, c. 41
consists of information about an individual that is projected outwardly so that they can be distinguished from other individuals. Thus, the nature of both identity and identity-related crimes are closely associated with information, and how it is collected, stored, transferred, and used. The central role of information to identity-related crime differentiates this typology of crime from most traditional criminal offences. Pure information, distinguished from any tangible aspect, is a notoriously challenging “thing” to deal with in law generally, and this is no less so in the criminal law domain. There is no single clearly definable act in relation to information that constitutes the crime — indeed, can sometimes be difficult to describe acts in relation to information at all. For instance, what does it mean to “use” or to “possess” information?

Philosophical questions aside, at the more concrete level, identity-related crime involves a multi-step enterprise that can often follow a linear progression of conduct. The earliest stages of the enterprise are those involved in the obtaining of crucial pieces of identity information for later manipulation and/or use. As we have seen, some means of acquiring this information are crimes themselves, such as theft of documents from a wallet or computer hacking, while other methods may not be readily identifiable as crimes, such as looking over someone’s shoulder to see and memorize their credit card number (often referred to as “shoulder surfing”), scavenging in garbage to find discarded mail or bills (often referred to as “dumpster diving”) or by deceiving either the person or someone else into divulging the information (often referred to as “social engineering” or “pretexting”).

In a simple one or two person consumer fraud operation, following its acquisition, the information might then be used immediately or shortly thereafter to access goods or money, as in the case of a credit card fraud or the taking over an existing account and associated withdrawal of funds.

If a card or document is required to support the claim of identity, there might be an intermediate step involving the fabrication of one or more forged documents for eventual use to deceive. Forged documents could be used to perpetrate a fraud or an immigration or travel related offence, or to obtain yet further documents to bolster a false identity.

In more elaborate schemes, often conducted by more sophisticated criminal organizations, there could be multiple people involved in the...
various stages, each of whom is only ever involved in one or two of those stages and who may be kept safely ignorant of the intended end uses of the information. False identities may be produced by a criminal group in support of its own other illicit activities, or as an end-product, for sale to other offenders. Indeed, the increasingly complex and sophisticated nature of organized crime activities, coupled with rapid advances in technology, has led to the ability of criminals to stratify and segment their operations such that individuals may be involved in only one or two aspects of a larger criminal scheme without personally being party to an entire crime.

Identity deception can be the beginning or the end, or the middle, of a larger criminal enterprise. In addition to following a linear progression, it may also be part of a circular process within a larger enterprise. It can be perpetrated to obtain goods, to evade detection by authorities on an ongoing basis so as to facilitate the continuation of unrelated criminal activity, to obtain even more information that will later be combined with it or with other information for eventual further use, or for all of those reasons. Identity deception and manipulation are believed to be connected to organized crime and terrorism, both as revenue generating techniques and as methods of true identity concealment. Identity theft is a simple and effective tool for economic fraud on a small scale (small in terms of the value of each individual fraud but large in terms of the number of such frauds that are perpetrated). Identity deception can be used to cover up child abduction or as part of schemes engaged in trafficking in persons or the smuggling of migrants, in which cases false identities can be used to shield the true identities of both the perpetrators and the victims. When what appears to be a simple identity theft case is discovered, it is often impossible to know without a thorough investigation what associated criminal activity, either already committed or in the planning stages, will also be uncovered.

The usefulness of the identifying information for such a vast range of criminal purposes has led to its commodification. Not only might large criminal organizations have segmented their own operations, but there may also be individuals or organizations now filling niche markets by engaging

having three or more persons, a low threshold which includes the vast majority of major fraud cases. The recent report of the UN expert panel observed that there was not sufficient evidence to make a similar conclusion with respect to the involvement of organized criminal groups in identity-related crime, but that such a pattern seemed likely to emerge as evidence accumulates. See E/CN.15/2007/8/Add.2, para. 21, and E/CN.15/2007/8/Add.3, para.18.
in only one aspect of identity related crime that is ancillary to, but which facilitates, criminal operations. These individuals or groups are otherwise unconnected to those to whom they provide their services. For instance, some may have become expert at acquiring large amounts of personal data by computer hacking, large scale phishing scams, becoming insiders in legitimate organization, social engineering or other such techniques. They may supply that information to others who are in the business of buying and selling that data, but who remain uninvolved at both the front end (the acquisition of the information) and the back end (its criminal use or incorporation into forged documents). There may also be individuals who do nothing other than make forged documents.

Identity crime is different from typical criminal offences. It may be both a discrete crime – the one-time use of another person’s information for a single purpose (depending on how one defines it) – but it is also a methodology of crime that covers a vast range of conduct that may be committed for any of a number of different purposes.

These realities in all of their subtle manifestations must be analysed and appreciated as part of the larger project of determining whether criminalization is appropriate, in addition to being important factors weighing heavily in favour of enhanced enforcement of existing laws.

Limitations identified

The legislative diagnostic, combined with the conduct diagnostic, revealed in Canada a situation in which could generally be summarized as follows: Canadian criminal law is, on the whole, relatively adequate for dealing with the deceptive use of identity to gain economic or other types of advantages and for dealing with conduct in relation to the making and using of false documents, but it has limitations in terms of effectively addressing the early stages of identity related crime, specifically the acquisition, possession and trafficking of identity related information for criminal purposes.

With the exception of the newer offences concerning computers and credit card/debit cards, most of the offences in the Criminal Code reflect a time that pre-dates the advent of the computer, the Internet and other elements of modern technology. Other than these offences, Canadian criminal law is generally concerned with property, which does not include information, even though information has now become a powerful tool for accessing property, and itself has become a commodity that people are willing to pay for. This makes all property related offences inapplicable to
the early stages of identity information acquisition unless something tangible containing the information, such as a physical document, was appropriated.

Even computer related offences to date in Canada only prohibit various forms of physical interference or unauthorized use of a computer system. They focus on a certain type of misuse of this one device, which conduct accounts for only some of the many ways in which identity information is acquired. There are other computer related identity theft techniques, such as phishing, and non-computer based techniques which are excluded from the reach of the law. Thus, with the exception of credit card data, the situation in Canada is that some “thefts” of identity information are criminal offences, others are not. None of the applicable offences is directly concerned with the truly blameworthy aspect of the conduct from an identity crime perspective. Rather, they are concerned with conduct such as theft or interference with a computer system, which are blameworthy for clearly valid reasons, but reasons which have little or nothing to do with the risks associated with identity theft.

Some more specific provisions are applied to specific documents such as passports, but even these are not entirely effective in the modern context. Identity documents are property, but they have legitimate uses and cannot be made contraband *per se*. One has a right to possess one’s own identity documents, and in some scenarios transfers to and possession of documents identifying one person by another person are legitimate and justifiable. Further, in many identification schemes legal title or ownership of the actual documents lies with the State or issuing authority and not with the holder or user of the documents themselves.

This means that the discovery of persons with one or even many documents that clearly do not identify or belong to them, such as drivers licences, health insurance cards, and even passports, may not constitute a criminal offence unless there is sufficient evidence that the documents were stolen, forged or otherwise obtained by the commission of a crime. There may be a strong inference of such circumstances, but this will frequently not rise to the level of proof beyond a reasonable doubt.

The legislative diagnostic combined with the conduct diagnostic revealed a number of limitations in current Canadian criminal law. The limitations in the applicable law may not be egregious or enormous, but there are more than a few. We now live in a world where information alone can unlock a treasure box located anywhere in the world, from anywhere else in the world, and can allow criminals or terrorists to pass anonymously from one country into another and conduct their affairs without arousing suspicion. A body of domestic criminal law that continues to employ 19th
century ideals of property as the cornerstone of social life and criminal conduct, with piecemeal additions designed only to address individual technologies as they may emerge, could arguably do more to meet the challenges that identity and information present to the modern world.

Much of the conduct at the early stages — the acquisition, possession and trafficking of information — can be thought of as “preparatory” to the crimes of fraud, personation, forgery or travel and immigration related offences. It is behaviour that arises even prior to an attempt to commit one of those other offences. The criminalization of “preparatory conduct” is controversial with good reason. It pushes the boundaries of criminal law to the edge of what is acceptable.

In the author’s view, however, there are sound reasons to consider the criminalization of these modes of preparatory conduct in this case. While the harm associated with the end stage uses of identity crime are readily apparent, there is still a great deal of potential harm, and some actual harm, that results from the early stages of information acquisition and trafficking. Once information of such a sensitive nature has been acquired by someone with criminal intentions, the person to whom the information pertains (or the person who was storing it) has effectively lost control over the information, which can never be regained. There may be considerable time in between the collection of the data and its use, and during this period of time, that information could be moved, copied, shared between criminal organizations, manipulated and merged with other information, incorporated into forged documents, and prepared for use for any number of purposes. The risk of harm could materialize into actual harm at any moment of the criminal’s choosing; the person to whom the information belongs could remain ignorant for this entire period of time and completely vulnerable. In the author’s view, it can not be said that this state of affairs necessarily falls, or should fall, outside the scope of the criminal law.

We have already seen some of the limitations in using general rules and principles of inchoate liability or party liability to attack those who

---

29 In addition to the economic loss that could be incurred by one or more persons or institutions. The person whose identity was misused suffers emotional distress and associated feelings of frustration, vulnerability and violation related to the loss of control over that most fundamental aspect of ourselves, our individual identity. In addition there are impacts in terms of time and money spent rehabilitatating one’s credit record. In the worst cases a person could be wrongly implicated in criminal activity.
participate in identity related operations. Many of these rules seem to emanate from an era where people, alone or with a small group, committed individual and discrete crimes, one at a time. Today, however, crime is more fluid and the start and end points of a criminal act are not always easy to identify, especially where sophisticated organized crime or terrorist organizations are involved.

One other difficulty with the approach that focuses on party liability is that it requires that the ultimate crime actually be committed or at least attempted. One can not be a party to a crime that is not committed, even if the intentions of all parties are clear and provable. Must the law require that a crime of fraud or personation actually be attempted before action can be taken? One might be guilty of conspiracy in these circumstances, but again this requires a significant amount of evidence that will rarely be available. Expressly criminalizing the early stage identity related conduct could overcome at least some of these limitations.

The narrow focus of existing offences also imposes some practical limits on what law enforcement can do in actual cases. Even if potential offenders are actually found in possession of information pertaining to others, and are preparing it for use in crime, they could not be arrested and charged with any crime, and in the absence of an offence, powers to seize the information are limited. The information, which itself is so vulnerable to exploitation, can usually not be removed from the criminal supply chain unless and until it is associated with a crime. Criminalizing the preparatory conduct itself can therefore also be justified as a means to enable law enforcement to intervene at an earlier stage than is currently possible. Identity information can be treated as an instrumentality, or evidence, such that it can be seized, removed from the hands of those who would exploit it. This generates advantages with respect to investigation, the collection of evidence, prosecution and international cooperation, but it also reduces the exposure of victims’ identity information to future criminal use, thus reducing economic, reputational and other damage to the victims, and costs to law enforcement and identity infrastructures.

Further, while the impulse to avoid criminalizing preparatory conduct is generally appropriate, it may be that there is no bright line in law or policy between “preparatory” conduct and conduct that justifies the criminal sanction. Upon deeper examination, many of the more traditional offences in this area already demonstrate a flavour of preparatory-ness. For instance, the offence of forgery – the making of a false document with intent that someone should be deceived by it – is arguably a preparatory offence to fraud (or to uttering a false document, which in Canada applies regardless of whether or not the person utters the document with intent to
gain an economic benefit). Clearly, the making of the document is preparatory to its use, and in and of itself the making of the document does not directly cause measurable harm, yet forgery would appear to be a common offence worldwide, even though harm is only realized when the document is used to deceive someone. Until then, there is only potential harm. Canada also has many criminal offences in relation to the making or possessing of instruments for use in other crimes, such as: possession of housebreaking instruments\(^{30}\); possession of instruments for use in forgery\(^{31}\); and possession of instruments to unlawfully obtain computer service\(^{32}\). It is certainly arguable that these offences are also preparatory to other offences, and yet policy dictated that they were warranted.

There is also an argument to be made that it is preferable to enact specific preparatory offences rather than relying on general provisions and principles such as conspiracy, party liability and attempt. This is because the operation of general principles to more concrete offences leave a great deal of uncertainty as to precisely what conduct is and is not criminal, as so much will be fact and circumstance dependent, as well as dependent upon the interpretation of the law and its application to those facts and circumstances. If the prohibition of preparatory conduct in one area is thought to be justified, then it might well benefit the citizenry, both as potential accused persons and victims, to know in advance, with a greater degree of certainty, exactly what conduct is and is not permitted. Creation of new offences directly outlining the prohibited conduct could accomplish these objectives.

*The Canadian Response to Identity-Related Crime: Bill C-27*

Bill C-27 was introduced in Parliament on November 21, 2007\(^{33}\). The main objective of Bill C-27 is to create three new “core” identity theft offences designed to target the early or preparatory stages of identity crime.

\(^{30}\) Section 351.

\(^{31}\) Paragraph 369 (b).

\(^{32}\) Section 342.2.

\(^{33}\) For full text of the Bill see: http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3125690&Language=e&Mode=1. At the time of writing, the bill was being studied by Committee in the House of Commons. There are other somewhat more technical amendments and revisions to existing offences that will not be discussed here.
(1) An offence that would be called “identity theft”

This would be cover the preparatory acts of obtaining or possessing identity information with intent to use that information to commit an offence that has “fraud, deceit or falsehood” as an element.

(2) An offence that would be called “trafficking in identity information”

This offence would cover the transfer or sale of information to another person, where there is knowledge or recklessness that the information would be used to commit a criminal offence that involves “fraud, deceit or falsehood”.

These two new offences would complement the existing offence of personation, which already exists in Canadian criminal law. Personation involves pretending to be another person, with intent to gain an advantage for anyone, or cause a disadvantage to anyone. A further amendment contained in Bill C-27 would rename the existing crime of personation as “identity fraud”. This is meant to demonstrate the continuum of activity, from “identity theft” – in which the information is taken and handled in preparation for criminal use – to “identity fraud” – those later stages in which the information is actually used to deceive or perpetrate a fraud.

A definition of “identity information” would also be provided. This is a narrower concept than what many States describe as “personal information”, being limited to information which, alone or in combination with other information, is capable of identifying an individual. This definition would expressly include biometric as well as traditional forms of identifying information such as name, address, and date of birth, and also various forms of alphanumeric identifiers such as driver’s licences, passports, and financial account numbers. It would be a non-exhaustive list of items of identifying information, such that it would encompass any other information of type that is commonly used to identify a person.

It would also be clear that the information would not only include that information that actually pertains to a real person, but would also include information that “purports” to identify a person. The intention of this is to ensure that fictitious information would also be included in the definition, where it has the appearance of being genuine. Fictitious identity

---

34 By way of illustration, one’s name, date of birth or bank-account numbers would be identity information, whereas other personal information, such as the balances of bank accounts or personal health information would be protected by other (e.g. privacy) measures as personal information, but not by the proposed new offences as identity information.
information was included as the offences are preparatory to both personation and fraud (among other offences), the former of which applies only to acts in relation to real people, the latter of which could also encompass the use of a fictitious identity. This also has the effect of easing the burden of proof on the prosecution, which would not be required to show who the real person was to whom the identity information related. In practical terms, it may be sufficient to show only that the information was not the genuine information of the accused (although proof of the applicable mens rea with respect to future criminal conduct would obviously also be required).

For the offence involving acquisition or possession of identity information, it would not matter how the information was obtained (e.g. whether via “phishing”, combing through garbage, hacking into a computer, watching over a person’s shoulder, or any other technique, and whether or not that technique was a separate crime). Likewise, for the offence involving trafficking of the information, it would not matter how the information was originally obtained. For both offences, the blameworthy aspect of the conduct would lie in the person acquiring, possession or passing on to another information that is destined for use in the commission of a crime.

(3) An offence for unlawful handling of government-issued identity documents

Bill C-27 would also enact another new offence directly targeting the unlawful possession and transfer of key government issued documents commonly used for identification purposes. The offence would prohibit the procuring, possessing and trafficking in authentic or forged government-issued identification documents where they contain false identity information or information pertaining to a person other than the accused. It would not be an offence where the conduct was done with a lawful excuse, and explicit exemptions are provided for conduct done with the consent of the person who owns the document or whose information is contained in the document, for law enforcement purposes, in the ordinary course of business, or for genealogical purposes. This offence is meant to avoid the problems associated with having to prove that the accused knew the documents were obtained by crime, as there would be no such knowledge element. Nor would there be a requirement that the accused intended to use the documents. The policy underlying these amendments is that certain government issued documents – health insurance cards, passports, drivers licences, and citizenship and immigration related documents – are of such a sensitive and crucial nature for identification purposes that citizens should
be prohibited from possessing or transferring any documents that do not pertain to them, unless they have good reason to do so.

With the exception of existing offences with harsher punishments which would be amended by the Bill, the same penalties are applied to all of the new crimes. These range from an expedited procedure and minimal penalties for less serious cases up to maximum terms of imprisonment of five years. This ensures that they meet the requirements of a “serious crime” set out in Article 2, subparagraph (b) of the Palermo Convention, so that the extradition, legal assistance and other cooperation provisions will be available when the other triggering requirements are present.

In terms of victim assistance, Canadian criminal law provides for some restitution, but current provisions would only apply to direct financial losses and compensation for physical harm, which does not cover all of the harm which results in identity-related crime cases. To address this, the Bill would also create a power for a court which convicts the offender, as part of the sentence, to order the restitution of reasonable costs associated with rehabilitation of the victim’s credit rating and identity. Such costs could include the costs of obtaining new documents and the costs associated with clearing debts or obligations falsely incurred in the person’s name.

Conclusion

Evidence from multiple sources seems to confirm that identity related misconduct is on the rise, that it harms individuals both economically and psychologically, it jeopardizes national security, and that it is a subject worthy of careful consideration as governments and the international community strive to catch up to criminals who have turned the identities of others into a potent tool for criminality.

One of the many issues for consideration in this area, ranging from regulatory enhancements to the security of banking and credit card information to privacy legislation to consumer measure and public awareness to improved criminal enforcement of existing laws, is the issue of direct criminalization of the relevant conduct. To date, very few states have sought to criminalize identity theft directly. It is the author’s hopes that the description of the Canadian experience in this regard can shed

---

Principally that the offence alleged must be “transnational in nature” and involve an “organized criminal group”. See generally, A/RES/55/25, Annex I, Article 3, paragraph (2) and Article 2, subparagraph (b).
some light both on the need to consider whether or not criminalization is appropriate within each state, and on some of the major obstacles and processes that such an analysis might entail.
IDENTITY THEFT AND THE CONVENTION ON CYBERCRIME

ALEXANDER SEGER
Head, Technical Cooperation Division, Directorate General I - Legal Affairs, Department of Crime Problems, Council of Europe

As societies worldwide are becoming highly dependent on information and communication technologies they are also increasingly vulnerable to cybercrime. This includes:

- Malware, that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets.
- Botnets which are one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware).
- Spam, not only as a nuisance but also as carriers of malware.
- The use of the internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda).
- The growing risk of cyber-attacks against critical infrastructure.
- Child pornography and the increasingly commercial sexual exploitation of children on the internet.
- Offenders who are increasingly organising for crime aimed at generating illicit profits.
- A shift in the threat landscape from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes.

Many forms of cybercrimes are related to identity theft in one way or the other, whether ID theft is defined as “the misuse of the identity (name, date of birth, address, financial information or other personal details) of another person without knowledge or consent” or as “assuming the identity

1 Head of Economic Crime Division, Council of Europe, Strasbourg, France. The views in this paper do not necessarily reflect official positions of the Council of Europe. For further information see www.coe.int/cybercrime.
of another person by stealing Personally Identifiable Information (PII) to commit fraud” or as “the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive”.

Conceptionally, ID theft can be separated into three distinct phases:

1. The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from the outside (illegal access to computer systems, trojans, key-loggers, spyware and other malware), or phishing and other social engineering techniques.

2. The possession and disposal of ID information, which includes the sale of such information that now plays an important role in the e-underground economy where credit card information, bank account details, passwords or full identities are among the most offered goods.

3. The use of ID information in order to commit fraud or other crimes, for example by assuming another person’s identity to exploit bank accounts and credit cards, create new account, take out loans and credit, order goods and services or disseminate malware.

Action against identity theft in connection with cybercrime requires a multi-pronged approach involving:

• prevention (measures to be taken by individuals, data security in the public sector and in the private sector, measures to protect privacy and personal data);
• legislation (to criminalise illegal access, interception, data and system interference, misuse of devices, computer-related forgery and fraud; but also liability for data security and civil remedies);
• enforcement (facilitating reporting of ID theft, the investigation and prosecution of ID theft, the building of law enforcement capacities, coordination, intelligence and analysis, and public-private cooperation);
• extensive international cooperation, including the full implementation and accession to the Convention on Cybercrime of the Council of Europe.

The Convention on Cybercrime is the only binding international treaty in this field. It was elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA, and opened for signature in Budapest in November 2001 (thus also known as the “Budapest Convention”). It is in force since July 2004 and has become a treaty with a global scope in that it serves countries worldwide as a
guideline for the development of national laws against cybercrime, in that an increasing number of countries are moving towards accession and in that it serves the Parties to the Convention as a framework for international cooperation.

The Convention requires countries to criminalise certain conduct such as the illegal access to a computer system (“hacking”, circumventing password protection, key-logging, exploiting software loopholes etc), the illegal interception (that is, violating the privacy of data communication), data interference (malicious codes, viruses, trojan horses etc), system interference (such as denial of service attacks through botnets and other means of hindering the lawful use of computer systems), the misuse of devices (including the development of tools to commit cyber-offences), computer-related forgery (including phishing attacks), computer-related fraud, child pornography, the infringement of copyright and related rights, and – in a separate protocol – hate speech, xenophobia and racism.

It asks countries to introduce a range of procedural law measures to give law enforcement and other criminal justice authorities the means to investigate, prosecute and adjudicate cybercrimes more effectively. Among other things this should allow for the possibility to take immediate action to preserve electronic evidence, to search and seize computer data or to intercept communications, while putting the necessary safeguards in place to prevent abuse of such powers and unnecessary infringements of privacy, freedom of expression or other civil rights.

Finally, it provides for a range of measures for more effective international cooperation against cybercrime.

The Convention is focusing on criminal conduct and not on specific techniques or technologies. There are thus no specific provisions on identity theft. However, the full implementation of its substantive law provisions will allow States to criminalise conduct related to the first and third stages of the ID theft process:
With regard to substantive criminal law, the question that remains is whether the possession, disposal, sale or other use of ID information, that is, stage two of the process, is to be made a separate criminal offence, such as for example in the USA. In Europe, this question was also raised by the European Commission in a Communication in May 2007\(^2\). This will certainly trigger further discussions and possibly actions.

In addition to the substantive law provisions, the Convention offers further tools to facilitate criminal justice measures against ID theft committed through computer systems. The scope of the procedural provisions mentioned above is very broad and applies to any criminal offence involving a computer system. This means they can be used for the investigation of any conduct related to ID theft which is made a criminal offence in a country even if this conduct is not specifically mentioned in the Convention.

Finally, the chapter of the Convention on international cooperation is highly relevant as cybercrime is probably the most transnational of all crimes.

In conclusion, countries that are determined to take action against ID theft in relation to cybercrime should make every effort to implement the Convention on Cybercrime. This will help cover many needs in terms of substantive law, procedural law and international cooperation.

It is nevertheless worthwhile to continue the discussion as to whether in addition it is necessary to criminalise identity-theft as a separate offence or to develop a separate international instrument on the criminalisation of identity theft in general (that is not limited to the internet or computer systems), or whether the full use of the existing legal framework and a stronger emphasis on prevention would serve the purpose.
INTERNATIONAL COOPERATION TO COMBAT IDENTITY-RELATED FRAUD: OPERATIONAL ASPECTS

RUTSEL SILVESTRE J. MARTHA
General Counsel, Office of Legal Affairs, INTERPOL

Introduction

1. At the 16th International Conference of the International Society for the Reform of Criminal Law held at Charleston (SC, USA from December 6-10, 2002), Michael J. Elston and Scott A. Stein examined the issue of international cooperation in on-line identity theft investigations, and they concluded their paper with the following words:

“The current structure of international mutual legal assistance is simply too slow and cumbersome for the Internet Age. Electronic evidence is ephemeral, and the delay inherent in the current structure significantly lessens the chance that such evidence will be obtained and cyber criminals will be caught. On-line identity theft will continue to be lucrative and difficult to stop or to investigate. The Council of Europe Convention on Cyber crime, while not aimed directly at identity theft (a crime that can be committed off-line as well as on-line), provides some hope for future efforts to identify, track and catch international on-line identity thieves. Law enforcement officers in the United States and other countries may well have better access to electronic evidence in the near future, but the promise of the Cyber crime Convention will not be fulfilled if it is implemented largely (or exclusively) through the existing, slow, cumbersome MLAT [mutual legal assistance] process. The Internet Age demands a system that will put front-line prosecutors and investigators in contact
with their counterparts quickly so that precious evidence is
not lost due to delay”.  

2. Interestingly, a similar view, at least in part, can be found in
paragraph 137 of the study on “fraud and criminal misuse and
falsification of identity” that was prepared at the request of the
United Nations Office on Drugs and Crime and submitted to the
ECOSOC. It reads:
“The major challenges identified included the complexity of
cases and the length of time needed for cooperation. Several
States highlighted the importance of fast and informal
coopereation amongst investigators”.  

3. I will suppress my inclination to take issue with the distinction made
between formal and informal cooperation, save to say that as a matter
of public international law, that distinction is non-consequential.

More important, however, is the finding in the study that the
“existing international legal instruments, including the Convention
against Transnational Organized Crime, the Council of Europe
Cybercrime Convention, and other regional and bilateral instruments,
were sufficient as a legal basis for cooperation, and that the focus

1 “International Cooperation in On-Line Identity Theft Investigations: A
Hopeful Future but a Frustrating Present” Michael J. Elston* and Scott A.
Stein, 16th International Conference of the International Society for the Reform
of Criminal Law held at Charleston, SC, USA from December 6 - 10, 2002, at
www.isrcl.org/Papers/Elston and Stein.pdf

2 In 1961 this was confirmed as good in law in Temple of Preah Vihear
(Preliminary Objections) by the International Court of Justice: “As regards the
question of forms and formalities, as distinct from intentions, the Court considers
that, to cite examples from the field from private law, there are cases where, for the
protection of the interested parties, or for reasons of public policy, or on other
grounds, the law prescribes as mandatory certain formalities which, hence, become
essential for the validity of certain transactions, such as for instance testamentary
dispositions; and another example, amongst many possible ones, would be that of a
marriage ceremony. But the position in the cases just mentioned (wills, marriage,
etc.) arises because of the existence in those cases of mandatory requirements of
law as to forms and formalities. Where, on the other hand, as is generally the case
in international law, which places emphasis on the intention of the parties, the law
prescribes no particular form, parties are free to choose what form they please
provided their intention clearly results from it”, Case concerning the Temple of
Preah Vihear (Cambodia v. Thailand), Preliminary Objections, ICJ Reports 1961,
p. 31; see also Case concerning the Northern Cameroons (Cameroon v. UK),
should be on finding and disseminating ways to use the available tools effectively as opposed to creating new ones.”

4. My focus here will be on shedding some light on the relevance of INTERPOL’s legal framework and on explaining how the INTERPOL tools and mechanisms can be used effectively to effectuate cooperation in combating fraud and the criminal misuse and falsification of identity. As will become clear, INTERPOL’s legal framework and tools have undergone significant changes since 2001, precisely to deal with the need of speedy, real time, and user friendly tools and mechanisms.

5. Some general information about INTERPOL will help to appraise the scope and potential of its legal framework, tools and mechanisms, when it comes to combating fraud and the criminal misuse and falsification of identity.

About INTERPOL

6. Created in 1923, INTERPOL facilitates cross border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat crime.

7. The Organization provides four principal services, referred to as its core functions:

(i.) Secure global police communications services – the fundamental condition for international police co-operation is for police forces to be able to communicate with each other securely throughout the world.

(ii.) Operational data services and databases for police – Once police can communicate internationally, they need access to information to assist in their investigations or help them to prevent crime. INTERPOL has therefore developed and maintains a range of global police databases.

(iii.) Operational police support services – INTERPOL currently prioritises crime-fighting programmes on fugitives, terrorism,

---

drugs and organized crime, trafficking in human beings, financial and high tech crime, and corruption.

(iv.)  Training.

8. How can then INTERPOL be relevant to the fight against fraud and the criminal misuse and falsification of identity?

The principles of availability and spontaneous information: INTERPOL Global Police Databases

9. One of the challenges mentioned by Eston and Stein in their 2000 paper is that when on-line identity theft investigators in one country need information, the process through which they have to go “is too slow and cumbersome to be useful”.

10. This problem is of course not limited to investigations concerning fraud and criminal misuse and falsification of identity; it is known as the problem of trans-national availability.

11. The principle of availability gained notoriety as a consequence of the European Union draft Council Framework Decision of 12 October 2005 on the exchange of information. The aim of this proposal was to introduce what was perceived to be a form of cooperation in criminal matters which did not previously exist: the principle of availability. This new legal concept concerns law enforcement authorities in one Member State granting access to the information they hold to authorities in other Member States for the purposes of prevention, detection and investigation of criminal offences.

The principle of availability is defined in the Hague Programme as the possibility whereby “a law enforcement officer in one Member State who needs information [in the pre-trial phase] in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose”. The EU Heads of State or Government called for the principle to be operational by 1 January 2008. The proposal would require EU Member States to “ensure that information shall be provided to equivalent competent authorities of other Member States and Europol, under the conditions set out in the future Framework Decision, in so far as these authorities need this information to fulfil their lawful tasks for the prevention, detection or investigation of criminal offences”.

162
12. The principle is innovative in that when a law enforcement officer or Europol needs information to perform their lawful tasks (preventing, detecting or investigating criminal offences), they may obtain this information. The Member State that controls this information would be obliged to make it available for this purpose unless it provides specific grounds for the refusal (Article 14 of the proposal).

13. In its own way, the Cybercrime Convention also contains a concept that can be related to the notion of availability. I refer to the principle of “spontaneous information” enshrined in Article 26 of the convention. According to that Article 1, a Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations. It can do so when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

14. Both the principle of availability and the notion of spontaneous information relate to INTERPOL’s second core function.

15. Indeed, within the spirit of the notions of trans-national availability and spontaneous information, INTERPOL has developed and maintains a range of global databases. INTERPOL provides all of its member countries with instant, direct access to a wide range of criminal information. This enables the global law enforcement community to connect seemingly unrelated pieces of data, thereby facilitating investigations and enhancing international police co-operation.

16. The legal framework that enables this global implementation of the principle of availability spontaneous was first put into place in 1982, 1986 and 1990 by INTERPOL’s General Assembly when it adopted the following sets of rules:
• ‘Rules on International Police Co-operation and on the Internal Control of INTERPOL’s Archives’;
• the ‘Rules on the deletion of police information held by the General Secretariat’; and,
• the ‘Rules governing the database of selected information at the ICPO INTERPOL General Secretariat and direct access by NCBs to that database’.

17. In 2003 these sets of rules were replaced by an integrated framework, the ‘Rules on the processing of information for the purposes of international police co-operation’, which were adopted by the General Assembly at its 72nd session (Benidorm, Spain, 2003) in Resolution AG-2003-RES-04, and entered into force on 1 January 2004. They were lastly amended by Resolution AG-20054-RES-15 adopted by the General Assembly at its 74th session (Berlin, Germany, 2005).

18. The rules regulate the purposes for which information can be recorded in INTERPOL’s police databases, the conditions that need to be met in order for such information to be recorded and retained, the review dates (deletion rules), the access of national authorities to the global police files, the communication of information, as well as the modification, blocking and cancellation of information. Based on these rules over the years, the following databases have been built with information provided by national authorities and information collected by the General Secretariat itself:

(i.) Nominal data – contains records on known international criminals, missing persons and dead bodies, with their criminal histories, photographs, fingerprints, etc.
(ii.) Stolen and lost travel documents – contains information on more than 15 million travel documents reported lost or stolen by 125 countries. This database enables NCBs and other law enforcement entities, such as immigration and border control officers in countries which have expanded access to front-line units, to ascertain the validity of a suspect travel document in seconds.
(iii.) Stolen administrative documents – contains information on 185,000 official documents which serve to identify objects, for

---

5 Resolution AGN/51/RES1.
6 Resolution AGN/55/RES/2.
7 Resolution AGN/59/RES/7.
example, vehicle registration documents and clearance certificates for import/export.

(iv.) *Stolen motor vehicles* – provides extensive identification details on approximately 3.9 million vehicles reported stolen around the world.

(v.) *Stolen works of art* – permits member countries to research records on more than 31,000 pieces of artwork and cultural heritage reported stolen all over the world.

(vi.) *DNA profiles* – DNA profiles, which are numerically coded sets of genetic markers unique to every individual, can be compared to create opportunities for person-to-person, person-to-scene or scene-to-scene matches with no previous connections, or help identify missing persons and unidentified bodies. Records do not contain nominal information, and member countries control their own data.

(vii.) *Fingerprints* – provides access to INTERPOL’s automated fingerprint identification system database, enabling fingerprint submission in compliance with the INTERPOL standard for electronic file exchange. It contains information entered directly by scanning or importing electronic files and latent finger marks collected from crime scenes.

(viii.) *Child sexual abuse images* – the INTERPOL Child Abuse Image Database (ICAID) contains hundreds of thousands of images submitted by member countries. It uses image recognition software to connect images from the same series of abuse or images taken in the same location with different victims. The database has helped investigators identify and rescue more than 550 victims throughout the world.

24/7 Network

19. The availability of INTERPOL’s global police databases by itself does not serve to quench the criticism of slowness in the traditional mutual assistance procedures

20. To address this problem, the Cybercrime convention introduced the concept of a 24/7 Network in its Article 35:

"1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences"
related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a. the provision of technical advice;
b. the preservation of data pursuant to Articles 29 and 30;
c. the collection of evidence, the provision of legal information, and locating of suspects.

2. a. A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network”.

21. In addition, the convention requires each Party to designate a central authority responsible for sending or answering requests for mutual assistance, the execution of such requests or their transmission to authorities competent for their execution. The central authorities shall communicate directly with each other (Article 27:2(a) and (b)).

22. Article 27, paragraph 1(1) of the Convention against Transnational Crime carries the same idea but is less compulsory and precise in what it prescribes:

“1. (...). Each State Party shall, in particular, adopt effective measures:

(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities; (...)”

23. Obviously, only a global gateway would be able to overcome the problems that these provisions aim to address. It is submitted, that currently, INTERPOL has a system in place in 186 countries that provides a unique and efficient solution to the problem that the 24/7
network and central authority system. I am referring to the I-24/7 global police communicated system, which was launched in 2003 and provides the gateway to international police data.

24. To understand this assertion, one must be aware that a key feature of INTERPOL’s structure is the INTERPOL National Central Bureaus.

25. Article 32 of INTERPOL’s Constitution prescribes that in order to ensure constant cooperation of INTERPOL’s members, “each country shall appoint a body which will serve as the National Central Bureau” (NCB). According to the same provision the NCB, which is listed in Article 5 of the Constitution as pertaining to the structure of the Organization, shall ensure liaison with the various departments in the country, with those bodies in other countries serving as NCB, as well as with the Organization’s General Secretariat.

26. In carrying out their liaison function – as defined in Article 32 (a) of the Organization’s Constitution – between the General Secretariat and the authorized national institutions, the National Central Bureaus are responsible vis-à-vis the General Secretariat for the entities and persons they have authorized to consult, or supply information for, the INTERPOL global police information system.

27. With regard to their responsibility vis-à-vis the authorized national institutions, prior to authorizing them to consult, or to provide information through, the INTERPOL global police information system, the National Central Bureaus shall first establish that procedures conforming to their national laws have been put in place to ensure and to continue to ensure that the said entities respect the INTERPOL rules.

28. INTERPOL’s I-24/7 global police communications system connects law enforcement officials in all 186 member countries and provides them with the means to share crucial information on criminals and criminal activities.

29. As criminals and criminal organizations are typically involved in multiple activities, I-24/7 can fundamentally change the way law enforcement authorities around the world work together. Pieces of seemingly unrelated information can help create a broader picture and solve trans-national criminal investigations.

30. Using I-24/7, National Central Bureaus (NCBs) can search and cross-check data in a matter of seconds, with direct access to databases containing information on suspected terrorists, wanted persons, fingerprints, DNA profiles, lost or stolen travel documents, stolen motor vehicles, stolen works of art, etc. These multiple
resources provide police with instant access to potentially important information, thereby facilitating criminal investigations.

31. Using the I-24/7, INTERPOL National Central Bureaus can be either responsible themselves for sending or answering requests for mutual assistance, the execution of such requests or their transmission to authorities competent for their execution as envisaged by any of the international conventions.

32. The I-24/7 system also enables member countries to access each others’ national databases using a business-to-business (B2B) connection. Member countries manage and maintain their own national criminal data. They also have the option to make it accessible to the international law enforcement community through I-24/7.

33. Although I-24/7 is initially installed in NCBs, INTERPOL is encouraging member countries to extend their connections to national law enforcement entities such as border police, customs and immigration, etc. NCBs control the level of access other authorised users have to INTERPOL services and can request to be informed of enquiries made to their national databases by other countries.

Integrated solutions

34. INTERPOL has developed two new integrated solutions which can provide member countries with direct access to its databases on wanted persons, stolen and lost travel documents and stolen motor vehicles through either a fixed or mobile network database, known as MIND and FIND.

35. These integrated solutions are now being offered to front-line law enforcement officers such as border guards in member countries. They allow an officer to submit a query to a national database and either the database at the INTERPOL General Secretariat (FIND) or a local copy of the data (MIND) simultaneously via I-24/7. The officer receives responses from both within seconds. An electronic alert system notifies member countries concerned of potential matches.

36. All INTERPOL global police databases, except the one of child sexual abuse images, are accessible through the I-24/7 Dashboard, a restricted-access Internet portal. An automated search facility (e-ASF) enables member countries to conduct searches and add or modify their own data in the databases on stolen and lost travel
documents, stolen administrative documents, stolen motor vehicles and DNA profiles.

**INTERPOL tools and mechanisms in practice**

37. Let me turn now to how the INTERPOL tools and mechanisms work in practice in relation to fraud, criminal misuse of identity and falsification.

(1) Criminal misuse of stolen and lost travel and identity documents

38. Responding to a questionnaire of the Intergovernmental Expert Group, governments have expressed a general concern with the misuse of passports and other identity documents to enter countries illegally or conceal the true identity of travellers. The study also reports stolen documents or information used to commit other crimes (fraud) or to obtain further ID and build false identity for later use, amongst the identity-related crimes encountered. Similarly, it reports of a link between identity related crime and fraud, terrorism, trafficking in human beings, illegal immigrations etc.

39. These findings correspond with INTERPOL’s own. Indeed, INTERPOL believes that the use of stolen and lost travel documents poses the single greatest gap in global security.

40. For that reason INTERPOL launched its Stolen and Lost Travel Document Database mentioned before.

41. INTERPOL experienced that at field level, most countries rely on their own national sources of information. Yet crime is increasingly globalized. Real-time access to up-to-date international information is vital to prevent criminals from travelling freely to escape from the law or commit further crimes. INTERPOL therefore designed and manages the database of passports, identity cards and visas reported as stolen or lost by countries known as the stolen and lost travel documents (SLTD) database. It enables front-line officers to check instantly whether a travel document is stolen or lost. INTERPOL also has databases on stolen motor vehicles and wanted persons.

42. To help countries connect easily and deal with the problem of speed, INTERPOL has developed two integrated solutions using either fixed or mobile integrated network databases, known as FIND and MIND. Both can integrate into the existing computer-assisted verification system in a country. In addition, MIND can be used in a country without an existing system.
43. There are two main benefits of using MIND or FIND: **The first is the access to international data** on a real-time basis via quick searches. An automatic functionality sends queries to national and INTERPOL servers and provides responses from both simultaneously. There are top-level security systems to protect the data. **The second benefit concerns the integration into existing systems, which means that no changes in the daily work of frontline officers and no special training are required.** There are also no language barriers, because the process is the same as when officers conduct searches of their national databases. It is easily adapted to individual countries’ requirements and capabilities.

44. **The way it works is as follows.** An officer can submit a query to the national system by simply passing a passport over a digital scanner or manually entering its identification number. The response indicates whether or not the document matches one in the database.

45. The query passes simultaneously to a national database (if existing) and either the database at the INTERPOL General Secretariat (FIND) or a local copy of the data (MIND) via INTERPOL’s I-24/7 global police communications network.

46. The officer will receive responses from both within seconds. An electronic alert system notifies member countries concerned of potential matches.

47. The choice for either FIND or MIND depends on the infrastructure in each country. MIND is proposed when a country cannot use FIND for whatever reason. INTERPOL officers will work with the country to identify the best technical platform for an integrated solution which satisfies the country’s specific technical, legal and operational criteria.

(2) **Using the available tools effectively**

48. At this stage it is useful to recall the finding in the study that the “existing international legal instruments, including the Convention against Transnational Organized Crime, the Council of Europe Cybercrime Convention, and other regional and bilateral instruments, were sufficient as a legal basis for cooperation, and that the focus should be on finding and disseminating ways to use the available tools effectively as opposed to creating new ones”.

49. There are at least three simple ways in which the use of INTERPOL tools can be enhanced:
Connecting the cybercrime points of contact to the INTERPOL i-24/7 Network: Some of the parties to the Cyber Crime Convention have appointed specific authorities as their points of contact. To my knowledge, none of these contact points are within the INTERPOL National Central Bureaus of their countries. Consequently, they are unlikely to be connected to INTERPOL’s I/24/7 global communication system. The competent authorities of these countries should be aware that INTERPOL’s rules allow that the designated cybercrime contact points can be connected to INTERPOL’s I/24/7 global communication system by the INTERPOL National Central Bureau within these countries. It is therefore recommended that National Central Bureaus are approached with a request to be connected. The same applies for countries which have not yet appointed a national cybercrime contact point. This would be consistent with the recommendation of the INTERPOL Working Party on IT Crime that National Cyber Crime Units be equipped with the necessary legal, technical and secure infrastructure to effectively communicate utilizing existing international networks, such as the INTERPOL network of National Central Reference Points for cyber crime (NCRPs)\(^8\).

Contribute to the global police data bases: By introducing the notion of spontaneous information, the Cybercrime Convention seems to feed the view that countries have a responsibility to forewarn other countries about individual situations that present a potential threat\(^9\). This is in fact a logical extension of the first principle. Countries should not only be mindful about protection of their own citizens, but should also warn other countries about potential threats they might face. The obligation to inform extends beyond wanted persons alone. It is equally important that countries share information about passports that were stolen blank or stolen from the bearer, because these are essential tools for identity criminals. Passports are a question of international trust, where countries assume that the information on passports has been verified and validated by the issuing country. Therefore, any risk of violating that process should

---


\(^9\) See Corfu Channel (UK/Albania) case, ICJ Reports 1949.
lead to immediate information sharing. The same is true for known hackers, suspicious IP-addresses etc. The practical implication is that countries have to ensure that they communicate all potentially relevant information to other countries and update the global police databases in a systematic and comprehensive fashion.

Consultation of INTERPOL’s global police databases: Once connected to INTERPOL’s I-24/7 global police communication system, these national contact points will not only be able to communicate worldwide with other relevant entities, but they could commit to systemically check international databases in order to ensure that identity related criminals are intercepted before being able to perform their unlawful acts.

INTERPOL may be used in non-emergency cases as well

50. Before finishing, I should like to clarify one point. Most of the criminal law agreements and conventions contain an obligation for the States Parties to co-operate in the field of law enforcement, for example, investigative assistance or information exchange\(^{10}\).

\(^{10}\) Examples are:

- Article 7(1) of the 1988 United Nations Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances: “The Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and legal proceedings.”
- Article 9(1) of this Convention: “The Parties shall co-operate closely with one another, consistent with their respective domestic legal and administrative systems, with a view to enhancing the effectiveness of law enforcement action to suppress the commission of offences […]”
- Article 9(1a): “They shall, in particular, on the basis of bilateral and multilateral agreements or arrangements establish and maintain channels of communication between their competent agencies and services to facilitate the secure and rapid exchange of information concerning all aspects of offences […]”
- Article 18(1) of the United Nations Convention against Transnational Organized Crime: “States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention […]”
- Article 48(1a) of the United Nations Convention against Corruption (not yet in force): “States Parties shall, in particular, take effective measures to enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and
51. Pursuant to these provisions the Contracting Parties are in principle obliged to co-operate to the widest extent possible. This commitment is also expressed in Article 31 of the Organization’s Constitution which states that, in order to further its aims, the Organization “needs the constant and active co-operation of its Members who should do all within their power which is compatible with the legislation of their countries to participate diligently in its activities.” Membership in INTERPOL entails a commitment to its aims, as expressed in Article 2 of the Organization’s Constitution.

rapid exchange of information concerning all aspects of the offences covered by this Convention [...].”

• Paragraph 2 of United Nations Resolution 1373, adopted under Chapter VII of the United Nations Charter: “All States shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.”

• Article 8 of the Inter-American Convention against Terrorism: “The States Parties shall work closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences established in the international instruments listed in Article 2. [...] In this context, they shall establish and enhance, where necessary, channels of communication between their competent authorities in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences [...].”

• Article 13(1) of the Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives and other Related Materials: “States Parties shall exchange among themselves, in conformity with their respective domestic laws and applicable treaties, relevant information [...].”

• Article 7(1) of the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime: “The Parties shall co-operate with each other to the widest extent possible for the purpose of investigations and proceedings aiming at the confiscation of instrumentalities and proceeds.”

• Article 25(1) of the Criminal Law Convention against Corruption: “The Parties shall co-operate with each other, in accordance with the provisions of relevant international instruments on international co-operation in criminal matters, or arrangements agreed on the basis of uniform or reciprocal legislation, and in accordance with their national law, to the widest extent possible for the purposes of investigations and proceedings concerning criminal offences established in accordance with this Convention.”
Read in that context, Article 31 of the Constitution underlines that the Members shall co-operate constantly with the Organization in order to further those aims. Through this co-operation with the Organization, Members effectively give mutual assistance between criminal police authorities and thereby contribute to the preventing and combating of ordinary law crimes. Hence, when Members subscribe to such international treaties and conventions, they are deemed to be acting within the spirit of Article 31 of the Constitution; particularly when these treaties refer to INTERPOL.

52. Indeed, many of the conventions Members have signed explicitly mention INTERPOL’s role in the field of international police co-operation and information exchange. The Organization is mentioned in the provisions dealing with the obligation for mutual legal assistance and international co-operation. Under these agreements INTERPOL serves as a communication centre for the Contracting Parties.

53. Two United Nations Conventions state that requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. Both mention INTERPOL in this context. Article 18(13) of the United Nations Convention against Transnational Organized Crime and Article 46(13) of the United Nations Convention against Corruption: “This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.”

Article 7(8) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: “Transmission of requests for mutual legal assistance and any communication related thereto shall be effected between the authorities designated by the Parties; this requirement shall be without prejudice to the right of a Party to require that such requests and communications be addressed to it through the diplomatic channels and, in urgent circumstances, where the Parties agree, through channels of the International Criminal Police Organization, if possible.”

The phrases in both conventions “where Parties agree” must be understood to refer to Article 31 of INTERPOL’s Constitution when INTERPOL Members are involved.
54. The situation is the same in the case of the European Conventions which mention such a role for INTERPOL in the context of international co-operation. Article 24(3) of the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 27(9b) of the European Convention on Cybercrime and Article 30(3) of the Criminal Law Convention against Corruption: “Any request or communication under paragraphs 1 or 2 of this article may be made through the International Criminal Police Organization (INTERPOL).”

55. Article 3 of the Co-operation Agreement on Police Matters between Benin, Ghana, Nigeria and Togo includes also an obligation for INTERPOL: “The INTERPOL National Central Bureaus shall serve as a liaison organ between the different security services of the Contracting Parties.”

56. All these provisions demonstrate that the Organization may provide its facilities to enable effective police co-operation between the member countries. INTERPOL may participate in the communication referring to requests for mutual legal assistance and may serve as a communication centre between the respective national authorities working on police matters. Therefore, the police authorities may communicate through INTERPOL channels. As a global coordinator, the Organization should help to make the communication and co-operation between the member countries more effective and rapid. By signing these conventions which refer explicitly to INTERPOL, Members of this Organization have undertaken to use INTERPOL channels for the exchange of information.
VICTIMS OF IDENTITY THEFT: AN UPHILL BATTLE OR AN IMPOSSIBLE FIGHT?

NICOLE VAN DER MEULEN
International Victimology Institute
Tilburg, The Netherlands

On October 2, 2007, newspaper headlines reported how New York Mayor Michael Bloomberg became one of the latest high profile victims of identity theft. While, as Sewell Chan writes, “[y]ou might think a man worth at least $5 billion would hardly notice if $400,000, or so went missing”¹ someone else did. Robert M. Morgenthau, the Manhattan District Attorney, charged two men with stealing or attempting to steal from personal accounts belonging to the Mayor. Despite the attention granted to his case, Bloomberg is simply another name on the long list of high profile identity theft victims. He follows into the footsteps of Oprah Winfrey, Tiger Woods and Steven Spielberg. In addition to joining the group of celebrity victims, Mayor Bloomberg also joins an even larger group of general, non-celebrity, victims of identity theft, in the United States and in other areas of the world. Fifteen years before the media broke the news about Bloomberg’s case, TransUnion LLC received 35,235 consumer complaints about identity theft². Throughout these past fifteen years, many developments have taken place with regard to society in general and with regard to identity theft specifically. Perpetrators managed to take advantage of developments within society, especially developments within the field of digital technology, to create innovative methods to gather personal identifying information and to subsequently abuse it for a variety of benefits.

Furthermore, identity theft began to spread across the globe\(^3\). Whereas many outside of the United States initially viewed identity theft as an exclusively American problem, complaints in, among others, the United Kingdom, Australia, Canada, Belgium, and the Netherlands provided evidence to the contrary. Identity theft, as many recognize and acknowledge now, is a global problem and generates victims all around the world. As a result, the challenge to counter identity theft is an international challenge which requires significant cooperation and coordination among different stakeholders at both national and international levels.

The following paper attempts to address one aspect of the complex problem of identity theft, its victims. Individual victims of identity theft constitute a novel category of victims which means they have encountered and continue to encounter other, perhaps more difficult, obstacles on their path as they try to resolve their case. In addition to individual victims, businesses also suffer significant damage both as a result of monetary losses and reputational scars after incidents of identity theft. Without trying to disregard the experiences of businesses and financial service providers, the focus of the following paper is on individual victims of identity theft and tries to answer a number of questions. First, what (dominant) types of identity theft currently exist? Second, what general and specific obstacles do victims of identity theft face when they try to resolve their case? Third, do certain citizens run a higher risk of becoming victims of identity theft? Fourth, what are the limitations of current research with regard to victims of identity theft?

1. Types of identity theft

Identity theft is a multi-faceted concept, which requires a closer inspection to separate its different faces. Types of identity theft differ based on the methods used and motives held by perpetrators of the crime. Through identifying the separate types of identity theft, the consequences for and experiences of victims can be placed in their appropriate context. Furthermore, the distinctions which exist between and among the different types of identity theft need to be addressed when policy makers introduce

measures to combat the problem. The following overview introduces and emphasizes a number of different, dominant types of identity theft.

1.1 **Financial identity theft**

Financial identity theft is without a doubt the most common type of identity theft. The majority of countermeasures introduced so far focus primarily on this type of identity theft. In general terms, financial identity theft occurs when a perpetrator uses personal identifying information to gain financial benefits, through, for example, opening a new credit card account. Financial identity theft is an umbrella type which captures two forms of identity theft, true name fraud and account take-over. With account take-over, a perpetrator manages to abuse an existing account of a victim. Activities can range from a single purchase with an existing credit card account to changing the billing address of the card and completely taking over the account. The second form, true name fraud, occurs when perpetrators take personal identifying information of the victim and open a new credit card account, a mortgage or request a loan, without the victim’s knowledge or consent. Consequences for victims of financial identity theft differ depending on the form. Account take-over victims generally encounter less difficulties or obstacles when they try to resolve their case than victims of true name fraud. More information on the experiences of victims of financial identity theft will follow in section two.

1.2 **Criminal identity theft**

Criminal identity theft is a second type of identity theft. With criminal identity theft, the perpetrator commits a (serious) crime and provides a ‘stolen’ identity to escape prosecution. When individuals become victims of criminal identity theft they may, for example, be initially stopped for a minor traffic violation, but upon checking their records the law enforcement officer finds a warrant out of their arrest for a serious crime like murder. The identity theft victim is then wrongfully arrested and subsequently locked up in prison.

1.3 **Medical identity theft**

Medical identity theft is a third type of identity theft. According to Pam Dixon of the World Privacy Forum, “[m]edical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information – without the person’s knowledge
or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods”\textsuperscript{4}. Furthermore, medical identity theft often leads to crucial errors or fictitious information in existing medical records of victims. The World Privacy Forum convincingly claims that medical identity theft “…is the least studied and most poorly documented of the cluster of identity theft crimes”\textsuperscript{5}.

2. Victims: experiences and obstacles

2.1 Introduction

Victims of identity theft face many challenges and obstacles. Sarah E. Berg rightfully notes how “[a]s crimes become more complex and high tech, victimization also shifts from traditional into more complex forms”\textsuperscript{6}. Precisely this complexity challenges traditional means of law enforcement agencies and victim support groups. While anecdotes about significant experiences often make their way into the media to create headlines which shock and terrify many, in-depth research into the experiences of victims of identity theft appears to be relatively scarce. Previous and ongoing research on victims of identity theft predominantly focus on the size and scope of the problem\textsuperscript{7}. Numerous studies try to provide reliable data on the prevalence of identity theft, especially financial identity theft. Debates generally arise as a result of these studies due to the implications individuals, whether policy makers or officials from the private sector, extract from the results.

\textsuperscript{5} Dixon (2006), p. 5.
\textsuperscript{7} For a complete overview of previous prevalence studies: Privacy Rights Clearinghouse (2007). ‘How Many Identity Theft Victims are There? What is the Impact on Victims?’ available online at http://www.privacyrights.org/art/idtheftsurveys.htm
This section, and this paper in general, however, do not focus on prevalence data nor on the many challenges associated with trying to gather such information. Instead, this section tries to provide an insightful and thought-provoking overview of the experiences of victims of identity theft, the obstacles they encounter and the way their lives are shaped during the aftermath of the crime. Studies on these elements are less available than studies on the prevalence of identity theft. In addition, anecdotes in the media provide a glimpse of what victims of identity theft go through after they discover the crime and have to regain control over their lives.

2.2 Types of impact

Identity theft can have a number of different impacts on individual victims and their lives. The Australasian Centre for Policing Research (ACPR) recognizes the following types of impact:

- direct financial impacts – including the loss of savings; the cost of reporting and preventing the continued use of the identity; and the cost of restoring reputation;
- indirect financial impacts – including the damage to credit rating; the damage to personal/business reputation; and creation of a criminal record; and
- psychological impacts – these may vary considerably depending upon how the stolen identity is used. They may include the impact upon a family of the theft of a deceased person’s identity; the impact of the use of one family member’s identity by another family member; and the impact of the use of a stolen identity in criminal activity such as terrorism, people smuggling or drug offences.”

In the following sub-sections, these three different types of impact are elaborated upon through a number of studies, which have been conducted over the past few years with the specific aim to investigate victims and their experiences.

---

2.3 Direct and indirect financial impacts

Initially victims of identity theft failed to receive the necessary attention and recognition. Before identity theft became a federal crime in the United States, in 1998, through the Identity Theft Assumption Deterrence Act, law enforcement officials did not acknowledge victims of identity theft as victims. During the years after identity theft became a separate crime, non-profit organizations began their research. The Privacy Rights Clearinghouse came in 2000 with an important overview of victims, their experiences and their recommendations for better public policy. The Privacy Rights Clearinghouse spoke to 66 victims of identity theft and produced a groundbreaking document ‘Nowhere to Turn’ which provides crucial insights about these victims and their experiences. In ‘Nowhere to Turn,’ the Privacy Rights Clearinghouse describes how victims of identity theft spent an average of 175 hours actively trying to resolve their case. Victims generally need to contact the creditor, the debt collector, and the credit reporting agencies (CRAs) in an attempt to remove the bad credit charges from their records. The inaccurate bad credit charges ignite the most problems because they generally prevent victims from obtaining a new credit card, opening a bank account, renting an apartment, or even finding a job. These findings are not out of the ordinary as later studies prove. The Identity Theft Resource Center (ITRC) produced a more comprehensive and thorough analysis about the long term impact of identity theft on its victims. Through in-depth surveys, the ITRC attempted to surpass previous studies conducted by the Federal Trade Commission (FTC), the Government Accountability Office (GAO), and other consumer groups and explore other areas of victimization.

For its 2003 analysis, the ITRC used responses of 180 victims, and in its 2004 analysis 197 victims responded to the survey, which is a larger group than used during previous studies conducted by the Privacy Rights Clearinghouse and the GAO. According to the analysis provided by the

---

ITRC, victims of identity theft spent an average of 600 hours to resolve or at least try to resolve their case, which is considerably longer than the 175 hours reported by the Privacy Rights Clearinghouse. The following year, in 2004, however, the number had been significantly reduced to an average of 330 hours, with half of the victims spending less than 100 hours to resolve their case. Usually, these hours are spread out over various years, which means the crime continues to haunt its victims. Another negative effect of the time intensive procedure to resolve the crime is the potential for job loss of the victim. In ‘Nowhere to Turn,’ ‘...victims reported missing several days or weeks of work to put their lives back together, and two people even reported losing their jobs due to the time devoted to identity theft resolution’.

The crime manages to have a domino effect on the lives of victims through not only stealing financial assets but also depriving victims of time which subsequently leads to potential job loss, deteriorated interpersonal relationships, and severe stress. As the ITRC concludes, ‘[e]ven after the thief stops using the information, victims struggle with the impact of identity theft. That might include increased insurance or credit card fees, inability to find a job, higher interest rates and battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime. This ‘tail’ may continue for more than 10 years after the crime was first discovered’. The costs to individual victims appear to be significant and diverse. As the ITRC notes, ‘[v]ictims of identity theft experience various costs as a result of the crime. These costs include lost wages or vacation time, diminished work performance, increased medical problems, impact on family and friends, financial and other costs’.

2.4 Psychological impact

Victims of identity theft also experience severe emotional reactions after the crime. In order to discover more about the emotional reactions of victims of identity theft, Tracy Sharp et al. (2004) conducted an exploratory study which examined the psychological and somatic impact of identity theft. Additionally, the study also investigated the coping mechanisms used

---

13 Privacy Rights Clearinghouse, 2000, p. 5.
by victims of identity theft. Within their study, Sharp et al. recruited 37 identity theft victims and placed them in six focus groups. The researchers provided the victims with two victim impact questionnaires. The first was administered two weeks after the victims discovered the incident of identity theft and the second six months after the discovery. The results of the first questionnaire indicated the following common reactions: irritability and anger, fear and anxiety, and frustration. During the second impact measurement, the results demonstrated how “...the emotional responses shifted such that the majority (26%) of participants indicated that they were distressed and desperate, 24% stated that they were irritated and angry, and 14%...endorsed feelings of anxiety, fear, mistrust and paranoia”\(^\text{16}\). These emotions demonstrate how victims of identity theft experience similar feelings as victims of other crimes. Consequently, they generally need and deserve treatment which other victims have a right to during the aftermath of a crime. Sharp et al. recognize how “[t]he results of this study suggest that psychological impact is indeed great on victims of identity theft. Not only are there immediate emotional and physical consequences to the victimization, but also lasting effects are seen, especially in cases that have not met resolution”\(^\text{17}\).

2.5 Secondary wounding and secondary victimization

A particularly problematic aspect for victims of identity theft is their inability to prove their innocence. Due to lack of evidence, victims have to fight an uphill battle to convince law enforcement officials, among others, that they fell victim to identity theft. The burden of proof rests with the victim, which is a significant weakness. The misplacement of the burden proof along with the inability of law enforcement agencies to adequately investigate identity theft cases generally leads to secondary victimization. Other reasons for secondary victimization include roadblocks victims run into with creditors and CRAs when they try to resolve their case. Victims need means of prove to provide sufficient evidence for their case. Without any kind of evidence, however, CRAs, debt collectors, and creditors appear unwilling to help the victim and as a result the bad credit charges continue to


\(^{17}\) Sharp et al. (2004), p. 133-134.
contaminate the records of the victims. As one victim notes, “[t]o the large creditors, don’t treat victims as though they are the culprits. We are having a difficult enough time without having to suffer more run-around. Hire people who do nothing but deal with these issues”\textsuperscript{18}. Throughout the years, however, research has demonstrated an increase in responsiveness from law enforcement agencies which is an encouraging result especially due to the fact that many victims criticize the treatment they receive from law enforcement officials. With regard to financial service providers, businesses, and utility companies, no significance change occurred between 2003 and 2004\textsuperscript{19}.

2.6 Medical identity theft

Victims of medical identity theft encounter similar challenges as victims of other types of identity theft. As Dixon describes, “[v]ictims of medical identity theft may experience the now-familiar consequences of financially oriented forms of identity theft. These can include the loss of credit, harassment by debt collectors, and inability to find employment”\textsuperscript{20}. In addition to these consequences, however, medical identity theft introduces different and perhaps more dangerous consequences. As a result of medical identity theft, victims may receive the wrong medical treatment or find their health insurance exhausted. On top of that, they might fail to obtain an insurance company which is willing to insure them for health as well as life insurance\textsuperscript{21}. An overview of cases described by the World Privacy Forum indicates both the severe damage the crime causes along with the nearly unimaginable creativity expressed by perpetrators. One victim found her blood type altered in her medical records, which could lead to a life threatening situation if she found herself in an accident and in need of a blood transfusion. Dixon asserts how this as a worst-case scenario especially when “...a victim does not learn about medical identity theft, or only learns about it during the course of a medical emergency when obvious medical discrepancies that have been introduced into the medical file by the criminal are discovered”\textsuperscript{22}.

\begin{itemize}
\item \textsuperscript{18} ITRC (2004), p. 26.
\item \textsuperscript{19} ITRC (2004).
\item \textsuperscript{20} Dixon (2006), p. 5.
\item \textsuperscript{21} Dixon (2006).
\item \textsuperscript{22} Dixon (2006), p. 33.
\end{itemize}
The creativity is also further demonstrated through other cases. A number of individuals, for example, fell victim to a lucrative scheme of a Boston area psychiatrist who created false entries in records of individuals who were not even his patients. The psychiatrist used the records, of drug addiction and severe depression, to submit false bills to insurance companies. Victims feared for their insurability and one victim told an investigator how she was “...concerned about obtaining future health insurance coverage...because her husband is self-employed”\textsuperscript{23}.

Many of the problems medical identity theft victims run into are a result of the unfamiliarity of the crime. The World Privacy Forum describes how victims of medical identity theft lack the ability to rely on their rights to see and correct errors in their medical records. Victims of financial identity theft do have those rights now with regard to their credit reports. Along similar lines, “[m]edical identity theft victims do not have an easy way to discover who, if anyone, to call for help. Because of how this crime is committed, in some situations, the same people victims may call for help may be among those perpetrating the crime”\textsuperscript{24}. Initially, victims of financial identity theft were also unaware of who to contact for help or information, but through the actions of non-profit organizations and public awareness campaigns this problem is largely eliminated. With regard to victims of medical identity theft, however, these problems are still there and these require a different, more specific, type of advice and help to resolve their situations.

2.7 Criminal identity theft

Victims of criminal identity theft, just as medical identity theft victims, encounter more challenges and obstacles than victims of financial identity theft. This is a result of two problems. First, criminal identity theft remains to be an area which receives less attention than financial identity theft. Consequently, policy makers focus more on policy which prevents or reduces the occurrence of financial rather than criminal identity theft. Second, victims of criminal identity theft face distinct problems due to the nature of the type of identity theft. The perpetrator has committed a serious crime and abused the victim’s identity. Law enforcement officials subsequently treat the victim as a serious criminal which many times means victims end up in prison without the ability to prove their innocence. The

\textsuperscript{24} Dixon (2006), p. 9.
prison element may lead to general and specific consequences. The general consequences, such as potential job loss, attorney fees, and loss of time, are similar to those experienced by all victims of identity theft. Specific consequences for victims of criminal identity theft, however, are the introduction of a criminal record which can basically ruin the life of the victim. As Beth Givens from the Privacy Rights Clearinghouse writes, “[c]redit-related identity theft can ruin your life for a couple of years. Criminal record identity theft can ruin your life forever. It is virtually impossible to wipe the slate clean.”

Givens provides a number of case histories which illustrate the extreme consequences for victims of criminal identity theft. Certain victims proved to be unable to find employment time and time again. One victim K., tried to find employment in the retail sector, after he was let go from his current retail store position. With his experience, he assumed finding a new position would not pose too many difficulties, yet he received numerous rejections. When he finally did receive a position to sell men’s clothing, the store ultimately changed its mind when he showed up. After K. demonstrated significant persistence to find out why the store withdrew the job offer, he found out his name popped up in a database “…used by all the department stores in that part of the state [which stated] that he was wanted for arson and shoplifting.” The act of criminal identity theft on the part of the perpetrator consequently prevented K. from obtaining any kind of employment relevant to his previous experience, which also led him to become homeless. While certainly K.’s case may be an extreme victim experience, this type of case helps to illustrate the possibilities of identity theft victimization along with the needs of victim assistance. As Givens notes, “K. contacted us in 1996 and has been instrumental in our learning about this worst-case scenario of identity theft and in working with the legislative process to pass laws to prevent his situation from happening to others.”

---

2.8 Conclusion

The available, but limited, research on victims of identity theft, their needs, and experiences provide significant insights which policy makers along with other stakeholders ought to incorporate into their public policy proposals and other countermeasures. The above sections paint rather tragic pictures of victims and their experiences both with regard to primary and secondary victimization. The main issues to remember are the reversed burden of proof placed on the victims and their subsequent inability to prove their innocence, which ultimately leads these victims to be trapped in a nearly irreversible situation of crime and injustice.

3. Risk assessment

In general, identity theft is a crime which can occur to anyone. The story about Mayor Bloomberg in the introduction and the stories about other celebrities certainly support this claim. Regardless of the fact that identity theft is indiscriminate with regard to its victims, certain citizens appear to be more prone to fall victim to the crime. Keith B. Anderson conducted a study to analyze whether certain citizens are indeed more likely to become victims of identity theft. While Anderson initially acknowledges how “[o]ne does not do something to become a victim – it just happens to you”\(^\text{28}\). He also describes how “…a little deeper reflection suggests that this is really not the case. The risks faced by consumers do differ, and these differences may manifest themselves in differences across groups with different demographic characteristics”\(^\text{29}\). Without trying to blame the victim, Anderson identifies a number of factors which may increase the likelihood of identity theft victimization for certain consumers. Anderson predicts that factors such as having a good credit record, engaging in more transactions, and having a higher income level may make a consumer more likely to fall victim to identity theft. Furthermore, Anderson also identifies the potential correlation between falling victim to identity theft and the place where a consumer does business and the victim’s household

\(^{29}\) Anderson (2005), p. 11.
composition\textsuperscript{30}. Important to note, however, is how all consumers need to take the necessary precautionary measures in an attempt to prevent identity theft, but that some may indeed be more likely to fall victim, even if they take measures to protect themselves. Anderson concludes in his study how, “\textit{the likelihood that a person will be a victim of identity theft does appear to be related to demographics}”\textsuperscript{31}. He identifies the following relevant demographic characteristics in particular: level of income, education, gender, age and household composition. According to Anderson, “[c]onsumers with higher levels of income are more likely to be victims of ID theft...Similarly, those with more education may be somewhat more likely to be victims”\textsuperscript{32}. Anderson’s results furthermore indicate how the elderly run a lower risk to become victims of identity theft, but that households with only one adult are more likely to be victimized. Just as women appear to be more likely to fall victim to the crime than men. As Anderson rightfully notes in the end, however, “Socio-Demographic Characteristics do matter. However, no one is immune from the risk of ID theft”\textsuperscript{33}.

4. Needs for future research

Stories about victims of identity theft surface on day-to-day basis in the media, but comprehensive and in-depth research about their experiences, needs, and problems remain scarce. While in the United States, non-profit organizations such as the ITRC and the Privacy Rights Clearinghouse conduct ground-breaking studies on the experiences of victims of identity theft, other countries appear to lack these crucial interest groups and subsequently the pivotal studies about victims. Without research on the plight of victims of different types of identity theft, law enforcement agencies and businesses, including financial service providers, fail to gain insights into the experiences of victims, to acknowledge their needs for assistance, and stakeholders ultimately fail to learn from their own mistakes or missing links.

A major obstacle to conduct future research on victims of identity theft is the lack of specific legal provisions which criminalize identity theft.

\textsuperscript{30} Anderson (2005).
\textsuperscript{31} Anderson (2005), p. 23.
\textsuperscript{32} Anderson (2005), p. 23.
\textsuperscript{33} Anderson (2005), p. 24.
Many countries appear to criminalize various elements of identity theft and these are scattered among various provisions which means victims of identity theft are not recognized within their own category. Future research, however, is undeniably necessary due to the increasing number of threats along with the expanding transnational character of identity theft. On 16 November, 2007, McAfee provided its Top 10 Threat Predictions for 2008. Within its predictions, McAfee notes how “[t]he old threats will persist, but a new crop is on its way”\textsuperscript{34}. Together with a new crop of threats and attacks come more and different types of victims of identity theft, who will all inevitably need help to recover their assets and resolve their case. Finally, due to the fact that no one is immune from the crime, policy makers and researchers in cooperation with each other need to discover what kind of consumer behaviors and attitudes may potentially lead to victimization of identity theft. Berg advocates for more comprehensive surveys which can also discover behavioral characteristics which may indirectly facilitate the occurrence of identity theft. She describes how “...while steps have been undertaken in the last five years to better understand the problem of identity theft, there has been little research done in the areas of high tech crime victim profiling and prevention. Most studies, whether one-time or ongoing, focus on victim demographics without examining ways in which their victimization may have been facilitated technologically”\textsuperscript{35}.

5. Conclusion

The increasing availability and accessibility of personal identifying information along with relatively easy ways for perpetrators to pretend to be someone else leads to many cases of identity theft. These cases lead to a novel category of victims who face significant challenges during the aftermath of the crime. The reversed burden of proof along with the victims’ inability to provide evidence in order to proof their innocence often leads victims into a state of desperation. They spend numerous hours in an attempt to restore their credit record, their medical record, or their criminal record. The restoration of these records is crucial for the


\textsuperscript{35} Berg, p. 26-27.
successful continuance of their lives. Without these records restored, they could face job loss, jail time or even death in the case of medical identity theft. Certainly, the past years have demonstrated a sense of progress for victims and their needs, but still many victims remain without recognition or assistance. And many remain with their lives ruined by perpetrators of identity theft. In the near future, more international and comparative research is needed to develop a more insightful and useful overview of victims, their needs, and their experiences.
CONCLUSIONS
The challenge of dealing with transnational and global crime problems is often dominated by asymmetrical factors. The evolution and proliferation of information and communications technologies has led to a rapid and accelerating evolution in the ways those technologies are used, both in legitimate commercial and communications practice, and in the hands of criminal offenders. Crime prevention and prosecution responses, on the other hand, are characterised by a much slower, more deliberative evolution, dominated by the sovereignty of States, the need to maintain basic rule of law and human rights protections at the international level that correspond to those applied at the domestic level, and the time-consuming process of disseminating information and building international consensus on what should be done, how, and by whom.

The subject-matter taken up by ISPAC in November 2007 is no exception. The problem of transnational economic frauds has emerged as a commercial challenge that has expanded substantially with the globalisation of trade and as a major criminal law enforcement problem as technologies have given a new class of offenders access to a new form of low-risk and very lucrative crime. The problem of identity-related crime has always been a significant element of the larger fraud problem, but has also emerged as a major issue for States, which need to identify not only their own nationals, but also foreign nationals who seek entry or residence in their territories. For commercial entities, the challenge is to establish and maintain identity infrastructures for their customers and their commercial needs, which range from personal credit cards to the identification of major corporate entities engaged in very large transactions.

As the Rapporteur for the Crime Commission Study, I welcome this opportunity to examine the problems of economic fraud and identity-related crime. While the Study establishes that much has been learned about the problem, it is also clear that much more remains unknown, and that a greater commitment to research, analysis, and the development of preventive and reactive countermeasures is needed. The Study has shown that the seriousness of the problem of economic fraud is consistently under-
estimated by governments, and the ISPAC proceedings have proven a valuable opportunity to raise awareness of the seriousness and scope of the problem. Identity-related crime is novel, and therefore an interesting topic for governments and criminologists, but so little is known of it that only the most general of recommendations can be supported by the available evidence. These proceedings have served to clarify what is known, and to suggest a future direction, both for research, and for the eventual development of a global strategy for responding to the problem. Based on the presentations and discussion, let me suggest some of the elements that are needed in such a strategy.

We need to allocate resources to deal with the problems of economic fraud and identity-related crime that are in proportion to the seriousness of the problems themselves. Resources are needed for every level of the strategy. The immediate mandates for further research and the development of materials, found in ECOSOC Resolutions 2004/26 and 2007/20, are subject to the availability of extrabudgetary resources, without which the work cannot proceed. Over the longer term, resources will be needed to disseminate materials and to implement elements of the strategy in each Member State. This is likely to include developing or modernising legislation, the provision of technical assistance and training, and some form of cooperation between law enforcement, commercial regulators, and relevant elements of the private commercial sector. Economic fraud and identity-related crime are also likely to emerge as technical assistance challenges for developing countries, and it will be important for donors to see the funding of such assistance as an investment in the stability and security of the global economy as well as the recipient States.

We need more information, especially about identity-related crime. Many of the interventions in the ISPAC proceedings have highlighted how little is known. In the absence of domestic legal definitions and criminal offences, there is virtually no statistical data. From the actual cases given as examples, we understand the nature of identity-related crime, but not the extent. We know what is happening, but not how often, to whom, or at what cost, and without such information, it is difficult to develop new offences at the domestic level, and difficult to build consensus at the international level that the establishment of new crimes based on identity abuses is necessary and justified. Some data do exist, but they are hard to access, isolate and analyze. Private companies have good data, but these are strictly limited to their individual commercial needs, and in many cases companies see them as sensitive from a commercial or competitive standpoint. Existing crimes such as document forgery and impersonation offences overlap with new concepts of identity crime, but the
corresponding data may be difficult to isolate for an identity-crime focus. The available data have been gathered from different sources, for different purposes, using different methods, and we will need to develop a means of analysis that takes into account these differences, and which can be used by national governments and intergovernmental bodies to assemble the best possible picture of identity-related crime at the national, regional, and global levels. We also need to identify and fill gaps in the available data and assemble the expertise and resources needed to fill those gaps.

*We need to emphasize links to technologies and transnationality.* The Crime Commission Study and the practical experiences of law enforcement and other experts on economic fraud clearly show that it has already become a major transnational crime issue, and there is evidence that increases in transnational fraud to some extent follow increases in access to e-mail, Internet and other information and communications technologies. This is to be expected: fraud requires contact between offenders and victims to deceive the victim and transfer the proceeds. Use of some technologies also reduces risk to offenders, and increases the numbers of victims who can be targeted. Early works on the problem of cybercrime tend to emphasize at the non-economic motives of hackers and virus-writers, and the relatively limited forms of fraud committed on internal company networks, often by employees or other insiders. This has changed radically, as telephones, fax machines, e-mail and the Internet itself have all brought a global class of offenders into contact with a global class of potential victims. Other forms of cybercrime, such as the use of viruses or other hostile software for economic extortion, do sometimes occur, but the majority of cases where the primary motive is economic gain now tend to involve either elements of economic fraud, identity-related crime or other conduct preparatory to one or both, such as the hacking of large volumes of identity information for purposes of illicit sale or extortion.

These facts have several important implications for a control and suppression strategy. First, to the extent that future patterns in the development and spread of new technologies can be predicted, it is likely that similar patterns in fraud and identity-related crime can also be predicted. Second, to the extent that anti-fraud measures can be incorporated into new technologies in a competitive and cost-effective

---

manner, it will be important to ensure that governments and companies which develop or use commercial technologies collaborate to ensure that this is done to the extent feasible. Global collaboration would ensure the maximum possible levels of crime prevention, while minimising commercial concerns that the cost or effects of prevention elements made the technologies into which they were incorporated less competitive.

Third, while offenders have managed to exploit the technologies, they can also be used effectively for prevention, investigation and prosecution. Security measures can be incorporated, and the technologies can be used to train key employees in how to identify and prevent schemes, and to educate potential victims so they are less likely to be deceived. Fourth, while the specific effects of technologies differ between developed and developing countries, they exert an influence in all countries. In developed countries, the major concern is with cybercrime offences committed to access identity information or interfere with identity infrastructure, in developing countries the concern is more with the use of technologies to forge paper documents, and in all countries, concerns with transnational crime, especially with passports and commercial documents such as credit cards are much the same.

We need to consider the issues which confront victims, especially of ID related crime. The ISPAC proceedings heard many speakers highlight the damage to reputations and other interests which are suffered both by legal and natural persons whose identities are taken and used to commit crimes. At the practical level, we need to consider how victims can search for and correct fraudulent information that affects them. This includes both commercial and government information, and it includes information systems in the victim’s own countries, other countries and international data bases. At the legal and moral level, the question was raised of whether a person’s identity and reputation are a human right. Identity is mentioned in the Universal Declaration of Human Rights and in the Convention on the Rights of the Child. Privacy and the protection of personal data have become human rights issues, and this includes identity information. At the global level, we must ask ourselves, what is the nature of the right to identity, and what are the implications for companies, governments and their obligations to those whose identities they are charged with protecting. At the national and regional level, similar issues may arise under national human rights protections and the European Convention on Human Rights.

Most of the discussion of victims has been on victims whose identities were taken and abused, or on those impoverished by fraud, but another class of victims was also raised. Victims of trafficking in persons represent a different picture. Experts on trafficking have noted that it is
common for traffickers to deprive victims of all *indicia* of their identity, which increases their control and greatly increases the harm to the victims. Victims of trafficking require different remedies, some of which are set out in the Protocol to the *Palermo* Convention, and while victims of conventional forms of identity-related crime face formidable challenges, most victims of trafficking are in an even more difficult predicament. Identity crime harms both victims and the ability of public and private sector systems to identify those with whom they deal, and finding solutions for all victims of identity crime is essential, not just for the victims themselves, but for the integrity of identity itself.

*We need to consider the concept of identity information and the broader context of identity infrastructures in criminalising identity abuses and preventing identity-related crime.* Many speakers pointed out that the question of identity-related criminal offences are closely linked to more general questions of identity infrastructure. This includes the ways in which governments and the private sector establish identity, and the ways in which they verify it. Some States have centralised identity systems, and others rely on a range of specific forms of identification for specific applications, and each State has to consider how proposed identity-related crimes fit within its own identity system. At the same time, it seems likely that the same basic identifying information, such as names, places and dates of birth, fingerprints, photographs and other “biometric” information, is used to establish identity in all systems, regardless of their nature. Thus, “identity information” is likely to become both the foundation of national identity crime measures, and the common ground on which future international cooperation will be based. Other requirements of identity infrastructures were discussed, and although some lie beyond the scope of crime prevention and criminal justice, all have important implications for the ways in which criminal offences, investigative powers and crime-prevention measures are formulated. Both legislation and prevention have to ensure that identity can be easily and accurately verified. This includes the need to ensure that verification systems are secure and not open to misuse, and the need to ensure that identity can be quickly and accurately verified, especially in high-volume systems such as passport controls. Many presentations also emphasized that every aspect of identity infrastructures has to be taken into consideration, so that there are no weak links that can be exploited by offenders. This includes strong documents, strong verification systems and the protection of institutions from corruption and other threats.

*We need to consider the utility of establishing new criminal offences, based on the abuse of identity per se, as opposed to other crimes*
committed using stolen, falsified or fabricated identities. The Report to the Crime Commission recommends the adoption of specific new identity-related criminal offences, but not all Member States are convinced. Some expressed the view that further offences would be redundant or an unnecessary extension of the criminal law. States should ask themselves how far they are prepared to extend the criminal law, and what the benefits are. The idea underlying identity crime offences is to criminalise abuses of identity, whether or not any other offences are committed using the fabricated or stolen identity. This will allow some offences to be prosecuted in which secondary offences such as fraud are not completed or where there is not sufficient evidence for a successful prosecution. But when extending the criminal law, it is also important to ensure that innocent or innocuous conduct is not made a crime, and this makes the question of exclusions or limits on the offences important. Ultimately, criminalisation is a policy decision for each Member State. What identity crime offences do is to punish conduct which causes harm to persons whose identity is taken. They also deter conduct which has become increasingly harmful as modern technologies are used for identification. What Member States have to decide is whether the harm to victims and the risk to society is sufficiently great to warrant the full application of criminal justice measures.

While differing views have been expressed on the basic question of whether to criminalise, there was general agreement that if a State does adopt new offences, they should be “serious crimes” within the meaning of the Palermo Convention. There also seemed to be agreement that, if criminal offences were to be established, then the critical underlying concept would be that of “identity information”, and that this is likely to become the common basis for international cooperation in the future. This, in turn, will require some further refinement of the concept of identity information, taking into account similarities and differences in national systems. One area where further work is needed is with respect to what constitutes “identity information” for legal persons, the extent to which corporate identities should also be protected by the criminal law, and if so, how the requisite provisions should be formulated.

We need cooperation between the public and private sectors at the national and international levels, in assessment, prevention, investigation and prosecution. There seems to be consensus that effective responses to both fraud and identity-related crime require collaboration between public and private sector, and that this collaboration has to include international cooperation in appropriate cases. This is true in all areas, but especially in data-gathering, prevention, investigation and prosecution. Effective cooperation raises difficult substantive and procedural issues, bearing in
mind the different functions of commercial companies and criminal justice systems, but these can be overcome by working in a creative and collaborative manner. Companies must operate in a global environment, and they need stability, predictability, global coherence of national laws and regulations, and assurance that they and their competitors will all have to meet the same standards, wherever they are located, and wherever they operate. Governments require the active support of companies, especially with respect to developing and disseminating preventive materials and in detecting and investigating crime, and must recognize that coercive methods usually entail economic and trade costs that can often be avoided by a more consultative process. In many areas, such consultations can develop “win-win” solutions in which everyone benefits, and where this is not possible, they may still lead to responses which minimise the overall economic and non-economic costs, and ensure that these are allocated in a way which is equitable, transparent, and avoids unfavourable consequences for international commerce.

We need to emphasize prevention. There was also widespread agreement among panellists and commentators that transnational cases of fraud and identity-related crime are expensive and time-consuming to investigate and prosecute, and that this makes prevention very important. Effective prevention not only reduces criminal justice costs, it also prevents harm to victims, which in many cases can be far more serious than mere economic losses. There was also agreement that prevention includes both strategic prevention, through means such as education and training and the development of secure identity systems, and situational prevention, through the rapid identification of ongoing fraud schemes so they can be stopped as quickly as possible. Prevention is also probably the most critical area for cooperation between the public and private sectors. While crime-prevention is fundamentally a public responsibility, private companies often have control of the commercial systems in which technical prevention measures are implemented, and they have the best access to employees and customers for purposes of training and education programmes.

We need to develop means of using existing international legal instruments effectively. In the case of economic fraud, there seems to be general agreement with the conclusions and recommendations of the Crime Commission expert panel, that most serious transnational fraud involves organized criminal groups and that the Palermo Convention is therefore a sufficient as a basis for international cooperation. In the case of ID-related crime, the Crime Commission experts felt that it was likely that the Convention would prove sufficient, at least until more was learned about the nature of identity-related crime and those who tend to commit it.
Should a further instrument be needed, much more would have to be learned before the issues would be ripe for negotiation. A further Palermo Protocol would only be needed if the evidence suggests that most identity-related crime involved organized criminal groups, but that specific forms of investigative or other cooperation not found in the present Convention were needed, as was the case with firearm tracing or the maritime provisions of the existing Protocols.

A separate international legal instrument would be needed only if the evidence suggests that a significant part of the problem involves individual offenders or arrangements which were not organized criminal groups. It is likely to be some time before there will be answers to these questions, but should a further treaty be needed, it seems likely that a Palermo Protocol would be the most likely option. It was also suggested that further changes to the Council of Europe Convention on Cybercrime might be used to address ID-related crime. This might address part of the problem, but given the scope of that Convention, it could not address the many forms of identity-related crimes in developing countries which still use paper-based identification, including those which may be considering acceding to the Convention.

We need to identify more experts. One of the challenges, as work proceeds, will be to identify more experts who can represent the various interests that will need to be taken into account. The most obvious need is for experts from developing countries, who may not necessarily be experts on identity-related crime per se, but are needed to consider the national identity and other infrastructure conditions in which crimes are committed and preventive and reactive responses must be implemented. The other significant requirement will be for experts who can bridge the gap between the public and private sector. One factor that has emerged in the discussions is the fact that the private sector itself is by no means monolithic, and that a range of specific commercial sectors and interests will require representation.

We need to raise awareness in developing countries. The evidence suggests that both economic fraud and identity-related crime have become global problems to the extent where a global effort will be needed to control them. There is a need to persuade developing countries that the proceeds of fraud are harmful to their interests, fuelling organised crime, corruption, money-laundering, and other illicit activities. It is also likely that fraud poses a greater threat to developing countries in other ways. Developing economies are sometimes even more vulnerable to fraud than developed ones. Weaker financial controls and law enforcement increases risks of fraud, and the negative effects of frauds are more serious in weaker
economies than strong ones. This includes large commercial frauds, frauds against the State, which are often seen as corruption, and mass-frauds, which can effect large numbers of victims. There is a need for more information about how fraud and ID crimes are committed in developing countries, what their interests are, and what their needs are for technical assistance.
ANNEX I
RESULTS OF THE STUDY ON FRAUD AND THE CRIMINAL MISUSE AND FALSIFICATION OF IDENTITY (IDENTITY-RELATED CRIME)\footnote{The present text has been prepared by the Rapporteur based on the initial draft texts prepared and circulated to the expert panel, and the views of the panel expressed before and during its second meeting, held in Vienna from 16-19 January, 2007. The Report formally submitted to the Commission (E/CN.15/2007/8, E/CN.15/2007/8/Add.1 and E/CN.15/2007/8/Add.2) is a much shorter version of the initial draft texts, abridged to meet ECOSOC requirements for the length of documents. The present text therefore contains a more detailed and extensive summary and analysis of the evidence actually considered by the panel. It is a Rapporteur’s text, has not been edited, and is not an official document of the United Nations. The Conclusions and Recommendations were developed based on consultations within the group during and between its sessions, and were not prepared as part of the initial, full-length draft. These are incorporated verbatim from the final Report.}

Substantive and procedural background

Concern about economic fraud and identity-related crime as an emerging domestic and transnational crime problem has been growing for some time. Transnational fraud is an old problem which has been significantly expanded in scope and volume by the economic globalisation and the technologies which support it. These tend to support illicit economic activities in much the same ways as legitimate commerce, a fact which has been rapidly exploited by offenders. Identity-related crime has followed what is in many ways a parallel pattern. Commercial technologies incorporate and rely on digital means of identification which can be subverted for purposes of committing both economic and other forms of crime, and in a globalised environment, both States and commercial interests rely heavily on transnational identity documents and infrastructures, in which documents such as passports and credit cards are established in national systems but must be recognised and used globally. The incentives to commit economic fraud and identity-related crime are
substantial. Fraud is believed to be a leading global source of proceeds of crime, and the reduced risks and greater proceeds associated with transnational and mass-fraud schemes committed using information and communications technologies has attracted organised criminal groups in many parts of the world. Identity-related crime is a significant factor in fraud and other economic crimes, but is also commonly-associated with passport and travel-related crimes such as illegal migration and trafficking in persons, and with avoiding surveillance in support of organised crime and terrorist activities.

The problem of fraud first came to the attention of the UN Commission on Crime Prevention and Criminal Justice through the Commission on International Trade Law (UNCITRAL), which was asked by the Member States to look into the problems of “commercial fraud” in 2002\(^2\). The resulting process, which ran from 2002-2007 developed a set of indicators describing common types of commercial fraud, intended to support national policymakers and commercial interests in developing and using preventive measures. These were taken up at the 2007 session and are now in use.\(^3\) In accordance with its mandates, the UNCITRAL process focused on the commercial aspects of the problem, but both crime-prevention and criminal law aspects were frequently raised\(^4\). In taking up the first report of its expert panel, the 2003 UNCITRAL session noted that criminal aspects of the problem were beyond its mandates, expertise and resources, and “…appealed to the Commission on Crime Prevention and Criminal Justice for assistance in conducting a study on commercial fraud as the basis for possible future work in that area”\(^5\).


\(^3\) Note of the Secretary General to the 36\(^{th}\) UNCITRAL session “Possible future work on commercial fraud”, E/CN.9/540, 2003. See also Report of UNCITRAL to the UNGA, A/58/17, paragraphs 231-241, and report on the April 2004 Colloquium on commercial fraud, A/CN.9/555. The finished indicators were formally submitted to UNCITRAL at its 2007 session (A/CN.9/624, Annex, and A/CN.9/624/Add.1 and A/CN.9/624/Add.2). Comments were solicited from Member States and these were submitted to the 2008 session (A/CN.9/659, A/CN.9/659/Add.1 and A/CN.9/659/Add.2).

\(^4\) See, for example “Possible future work on commercial fraud”, E/CN.9/540, 2003 paragraphs 55-60 (cybercrime) and 68 (possible use of the 2000 Palermo Convention).

The Delegation of Canada, with the support of others, proposed a study which would include the subject matter raised by UNCITRAL, at the April 2004 session of the Crime Commission. Given the Commission’s mandates to address all forms of crime, it was felt that a broader scope than that applied by UNCITRAL would be appropriate. The proposed study would examine fraud in general, as opposed only to “commercial fraud”, and it was decided to propose a combined study which would also examine the related problem of identity crime. During the 2004 session, lacking a definition of “identity crime”, the Commission decided instead to use the descriptive term “criminal misuse and falsification of identity”, leaving questions of scope and terminology to its experts. The expert panel which conducted the study considered terms such as “identity theft” and “identity fraud”, but ultimately decided to employ new terminology. As a result, the Report refers to “economic fraud” to exclude the many non-economic uses of the term “fraud”, and to “identity-related crime” in order to include not only the emerging concepts of identity theft and identity fraud, but also other related illicit conduct, such as trafficking in identity documents and identity information.

In the resulting resolution, the Economic and Social Council requested the Secretary-General to convene, subject to the availability of extrabudgetary resources, an intergovernmental expert group, with representation based on the regional composition of the Commission on Crime Prevention and Criminal Justice, and open to any Member State wishing to participate as an observer, in order to prepare a study on fraud and the criminal misuse and falsification of identity. In addition to conducting the Study itself and reporting the results back to the Commission, the group was also requested to use the information gained by the study for the purpose of developing useful practices, guidelines or other materials in the prevention, investigation and prosecution of fraud and the criminal misuse and falsification of identity. In carrying out its work, the Group was asked to take into consideration the relevant work of the United Nations Commission on International Trade Law (UNCITRAL) and other bodies where relevant and appropriate, bearing in mind the need to avoid duplication.

---

6 Resolution 2004/26 of 21 July 2004, entitled “International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes”.

7 E/RES/2004/26, paragraphs 4, 5 and 6.
The first part of the mandate, completion and transmission of the study results, was completed at the 2007 session of the Commission, but the second part, the development of other materials based on the results of the Study, remains open. The 2007 session accordingly adopted a further resolution, renewing the original call for the development of further materials, and requesting the UN Office on Drugs and Crime to develop and deliver appropriate technical assistance, subject to the availability of extrabudgetary resources. At the time of writing (June 2008), a second, non-intergovernmental advisory “core group” of experts has been convened to advise UNODC on how best to implement the remaining mandates, taking into account the need to maintain the involvement of the UNCITRAL secretariat and to engage private sector elements in both the development of materials and delivery of assistance. That Group reports to the UNODC itself, but its reports are expected to be transmitted to both the Crime Commission and the Conference of States Parties to the Palermo Convention, as a number of the issues considered relate to how best to use the Convention against economic fraud and identity-related crime.

Conduct of the study

With the support of the Governments of Canada and the United Kingdom, two sessions of the open-ended Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity were held in Vienna, the first on 17 and 18 March 2005 and the second from 16-19 January 2007. At the first meeting of its first session, the group of experts elected Pedro David (Argentina) as Chairman and Christopher Ram (Canada) as Rapporteur. In the absence of the Chairman,

---

9 E/RES/2007/20, paragraphs 14 (technical assistance) and 18 (reference to E/RES/2004/26, para.5).
10 In addition to serving as Rapporteur to the intergovernmental expert group established by E/RES/2004/26, the Author serves as Rapporteur for the non-intergovernmental “core group” as well.
the second session was chaired by H.E. Eugenio Maria Curia, Argentina’s Ambassador to the international organizations in Vienna.

The first session considered the scope of the study, adopted a methodology and decided to include in the Study information from the Member States, the private sector, and the experts themselves. It requested the secretariat to prepare and disseminate a questionnaire, in two parts, to obtain information on economic fraud and the criminal misuse and falsification of identity. A progress report based on the meeting was submitted to the Commission on Crime Prevention and Criminal Justice at its fourteenth session\(^1\), in accordance with ECOSOC resolution 2004/26.

The questionnaire was submitted to the Commission at its fourteenth session\(^2\), revised to take into account, to the extent possible, comments and remarks received from Member States, and then disseminated to all Member States in December 2005. There was not a sufficient number of responses to conclude the work in time for the 15\(^{th}\) session of the Commission\(^3\), but at the completion of the study on 31 December 2006, 46 States had provided responses. The experts themselves were also invited to contribute data, and the questionnaire was sent with a joint letter from UNCITRAL and UNODC secretariats, to a selection of appropriate private-sector companies seeking their views and information. The UNCITRAL secretariat also sent the questionnaire to a broad array of international governmental and non-governmental organizations that participate regularly in UNCITRAL’s work, requesting that the questionnaire be circulated among their members for response, where appropriate. Input was received from the private sector through several channels. Some companies sent information via the UNCITRAL secretariat, others were reflected through the responses of the Member States in which some of the companies were domiciled, and the experts themselves reviewed a number of open information sources generated by individual companies or groups representing key sectors such as the insurance or telecommunications industries.

Responses to the survey questionnaire were received from 46 Member States by 31 December 2006: Algeria, Belarus, Canada, Costa Rica, Croatia, Egypt, Finland, Germany, Greece, Hungary, Italy, Japan, Jordan, Republic of Korea, Latvia, Lebanon, Former Yugoslav Republic of Macedonia, Madagascar, Malta, Mauritius, Mexico, Monaco, Morocco,

\(^1\) See E/CN.15/2005/11.
\(^2\) E/CN.15/2005/CRP.5.
\(^3\) See E/CN.15/2006/11.
Netherlands, Nicaragua, Norway, Oman, Panama, Peru, Romania, Russian Federation, Saudi Arabia, Slovakia, Slovenia, South Africa, Spain, Sudan, Sweden, Switzerland, Syrian Arab Republic, Trinidad and Tobago, Turkey, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, and Zambia. Many of them also provided copies of relevant legislation.

A long version of the Report was prepared and circulated to the experts in September 2006. A second draft was revised to take account of comments received and then abridged to reduce its length to meet ECOSOC requirements, and this text was taken up by the second session of the intergovernmental expert group, held in Vienna from 16-19 January 2007. Based on those deliberations, the Report was then finalised and submitted to the Commission at its 16th session, in April 2007.

**Conclusions and recommendations**

A. The relationship between fraud and identity-related crime and its effect on further work

The study established that there were not only significant links between economic fraud and identity-related crime, but also substantive and procedural differences between the two that will have an influence on future work in both areas. A substantial amount of identity-related crime is associated with economic fraud, as a means of avoiding fraud prevention measures and avoiding criminal liability and, in many cases, as a means of deception central to the fraud offence itself. However, not all forms of fraud involve identity-related crime, and many identity offences are committed for undetermined reasons or for reasons with no direct link to any financial or other material benefit. From a procedural standpoint, the responses also showed that although most States have well-developed legislative and other measures directed at economic fraud, most had no measures whatsoever against identity-related crime per se, although many had criminalized related conduct such as document forgery or impersonation. The complexity of the relationship and the substantive and procedural differences suggest that the most efficient and effective way to proceed would be to follow separate processes of developing materials to

---

14 E-CN.15-2007-8, paragraphs 16-37. The original paragraph numbers have been retained in this segment for ease of reference and citation.
assist Member States pursuant to paragraph 5 of Economic and Social Council resolution 2004/26. At the same time, the connections between the two suggest the need for close coordination to exploit synergies and avoid duplication of work in both areas. A separate but coordinated approach to such work is therefore recommended.

B. Further work on the gathering, analysis and dissemination of information

The available evidence clearly suggests that economic fraud is a serious problem and is increasing, both globally and in a number of Member States. However, many States reported that they did not have accurate information or a systematic framework for gathering and analysing such information. The evidence also suggests that the seriousness of the problem and the extent to which it is transnational in nature are often underreported and underestimated. Data that would permit the quantification of fraud by occurrence or offence rates are not available in many States, and there are almost no official data quantifying proceeds. Data gathered by national financial intelligence units and the Financial Action Task Force on Money Laundering are not of a statistical nature and are not linked to fraud or other specific predicate offences. Some data are gathered by the private sector, but only for specific commercial applications. Awareness of and concern about identity-related crime are growing, but such crime represents a novel concept for law enforcement and criminal justice experts in many States. There are few legislative definitions and many basic concepts remain fluid at this early stage. Unlike fraud, which is often the primary focus of offenders, identity-related crime appears to be most commonly found as a constituent element of larger criminal offences or operations, but there appears to be little research or information available about its nature, scope or relationship to other criminal activities. The Intergovernmental Expert Group therefore made the following recommendations:

a. Further general research into economic fraud and identity-related crime as global issues should be conducted, based on information from the Member States and entities engaged in work on fraud or other areas of economic crime, where appropriate. Such research should take into account the relationship between economic fraud and identity-related crime;

b. The subjects of economic fraud and identity-related crime should be divided into categories to support effective priority-setting and focused research and follow-up work by the Commission on Crime
Prevention and Criminal Justice, UNODC, other relevant international organizations and Member States. Some priority areas could include the following:

(i.) in the case of economic fraud, most States have clear legislative definitions and offences, but those are not detailed enough to support research and analysis of many of the specific types, trends and patterns that raise concerns, including mass fraud and factors such as the involvement of transnationality, organized criminal groups and information and communication technology. The development of global research-oriented definitions and typologies and support for States in using those to carry out research and analysis at the national level could be considered;

(ii.) in the case of identity-related crime, much less is known and more general research could be carried out based on the concepts developed in the study, with a view to better understanding the nature and scope of identity-related crime and how it relates to other forms of criminal activity. This would entail further elaboration and dissemination of basic definitions and typologies. This would support not only research and analysis, but also criminalization, as few States have adopted specific offences in this area;

c. the setting of priorities and the conducting of further work should take into account the need to avoid overlap or duplication of efforts and to maintain close coordination with the work of other bodies, particularly in the areas of money-laundering, the financing of terrorism, cybercrime and commercial fraud;

d. systematic and structured processes for gathering and analysing data in each Member State should be developed, and UNODC should be asked to assist in this process and to encourage and support standardization among Member States, where possible and appropriate and subject to the availability of extrabudgetary resources. Generally, such processes should include:

(i.) a standard typology or classification framework of offences or activities;

(ii.) the gathering of qualitative and quantitative information from multiple sources, including official offence reports or complaints and other sources, and also from alternative sources that are less likely to be influenced by underreporting;

(iii.) to the extent feasible, the gathering and analysis of information about the costs of fraud: this would include
assessments of the overall proceeds of fraud accumulated by offenders, the indirect economic costs, and the non-economic costs of fraud. To ensure consistency, avoid duplication and ensure that the analysis was based on the best information possible, national experts on money-laundering and other areas and appropriate industrial or commercial associations or representatives could be consulted;

(iv.) the gathering and analysis of information about identity-related crime, both in the context of related criminal activities and as a distinct crime problem in its own right;

e. UNODC and other appropriate entities could also be asked to examine the relationships between economic fraud, identity-related crime, corruption and money-laundering in order to support coordination between work done in those subject areas;

f. The Financial Action Task Force on Money Laundering could be asked to examine the means used to launder the proceeds of fraud with a view to developing materials [typologies] to assist Member States.

C. International cooperation

A number of States reported substantial increases in transnational fraud, which appear to be associated with the increased opportunities provided by the expansion of global trade and commerce and the increasing availability of information, communication and commercial technologies. Not enough information was available to support similar conclusions about identity-related crime, but States had concerns about transnational activities, in particular problems with passports and other travel documents and transnational credit card fraud. Accordingly, a number of States referred to the need for international cooperation. Those States which addressed the issue also felt that the existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, annex I), the Council of Europe Convention on Cybercrime15, and other regional and bilateral

---

15 Council of Europe, European Treaty Series, No. 185; see, in particular articles 7 (computer-related forgery) and article 8 (computer-related fraud). Experts noted that the Convention on Cybercrime was the only international instrument specifically addressing cybercrime. It contains three parts: substantive criminalization; procedural mechanisms for the investigation of computer crimes
instruments, were sufficient as a legal basis for cooperation, and that the focus should be on finding and disseminating ways to use the available tools effectively as opposed to creating new ones. Experts also noted the usefulness of the United Nations Convention against Corruption (General Assembly resolution 58/4, annex) in this regard.

The evidence also suggests that this is a viable approach. In the case of transnational economic fraud, new technologies make offences by individuals possible, but the vast majority of serious cases appear to involve “organized criminal groups” as defined in article 2, subparagraph (a), of the United Nations Convention against Transnational Organized Crime. Further, only 5 of the 46 responding States reported maximum possible sentences shorter than the four years required by the definition of “serious crime” in article 2, subparagraph (b), which means that the Organized Crime Convention will apply if the States affected are parties to the Convention. It is less clear whether the Organized Crime Convention will also apply to transnational cases of identity-related crime, as few States have established domestic crimes to date, but that seems likely. Identity crimes that are transnational in nature tend to involve falsification or tampering with identification systems and documents that are increasingly beyond the means of individual offenders and likely to require a degree of expertise and resources associated with organized criminal groups or terrorist groups.

For the above-mentioned reasons, the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and, where applicable, the Council of Europe Convention on Cybercrime, as well as the 13 universal legal instruments against terrorism, appear to provide a more than adequate framework and legal basis for the types of mutual legal assistance, extradition and other forms of international cooperation that are needed to deal with transnational cases of economic fraud and identity-related crime. As a result, the Intergovernmental Expert Group saw no need for any further international legal instruments in that area. It did, however, recommend that careful consideration be given to the most effective possible application of the conventions in fraud cases, including by the following:

---

and cases that involve electronic evidence; and international assistance for obtaining evidence or the extradition of offenders. The Convention covers only criminal (not civil) matters. States not members of the Council of Europe may become parties to the Convention by acceding to it.
a. member States that have not yet done so should ratify or accede to and fully implement the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption;

b. member States should consider acceding to the Convention on Cybercrime, which is open to States that are not members of the Council of Europe;

c. most States reported types of punishment that would make their more serious offences “serious crimes”, as defined in article 2, subparagraph (b), of the United Nations Convention against Transnational Organized Crime. However, many had offences that would not be covered by the Organized Crime Convention, and a few did not report any fraud offences that would be covered. Member States should ensure that all appropriate fraud and related offences fall within the scope of “serious crimes” as defined in the Organized Crime Convention;

d. few States have criminalized identity-related crime per se, but most had criminalized related offences such as document forgery and impersonation, and the more serious of those offences would also be covered by the United Nations Convention against Transnational Organized Crime where the requirements of articles 2 and 3 of that Convention were met. Document forgery and fraud involving electronic networks may also be covered by the Convention on Cybercrime. It is recommended that States review existing criminal offences with a view to ensuring that both conventions can be applied in appropriate cases;

e. it is also recommended that the scope of application and appropriate definitions contained in articles 2 and 3 of the United Nations Convention against Transnational Organized Crime be taken into consideration by Member States engaged in the development of new offences relating to identity-related crime;

f. national law enforcement and other agencies responsible for organized crime should be encouraged to consider major cases of economic fraud and identity-related crime as a form of organized crime and be trained in the effective use of the Organized Crime Convention and its implementing legislation in appropriate cases;

g. States should ensure that law enforcement and other relevant agencies are trained in the investigation of cybercrime, including where appropriate and applicable, the use of the Convention on Cybercrime and its domestic implementing legislation;
h. States should ensure that law enforcement and other relevant agencies cooperate more effectively in fighting economic fraud and identity-related crime, in particular through mutual legal assistance and the extradition of offenders, taking into account the transnational nature of those crimes.

D. Domestic powers to investigate, prosecute and punish fraud and identity-related crime

1. Legislative measures against fraud and identity-related crime

   Most States reported legislative measures against a variety of criminal fraud offences, ranging from small deprivations to complex schemes involving major economic disruption and collateral forms of harm. Those measures appeared to criminalize fraud adequately for the purposes of suppressing domestic fraud and supporting international cooperation. Most States also indicated that fraud was considered a predicate offence for purposes of regimes against money-laundering. While the vast majority of criminalization issues appear to have been addressed, the evidence suggests that some specific modifications could be considered to improve and modernize legislation. Fraud offences and investigative powers may not have kept pace with new variations of fraud committed using modern technologies, and not all States indicated that fraud was a predicate offence for measures against money-laundering. Criminal offences covering only individual transactions could also be augmented to reflect the expansion of transnational and mass fraud by specifically criminalizing fraud schemes and mass fraud. In transnational cases, this simplifies jurisdiction, as territorial jurisdiction would apply to the entire scheme and not just to specific transactions, evidence of the entire scheme and its effects could be used and it may not be necessary to prove the completion of fraud against individual victims. It is therefore recommended that States consider the following enhancements, where appropriate:

   a. States that have not done so should consider the modernization of fraud offences and investigative powers to deal effectively with domestic and transnational fraud committed using telephone, electronic mail (e-mail), the Internet and other types of telecommunication technology;

   b. in view of the substantial proceeds generated by major frauds, States that apply measures against money-laundering only to designated predicate offences should consider including fraud and similar offences as such;
c. States that criminalize fraud only on the basis of individual fraudulent transactions should consider criminalizing conduct such as the operation of fraud schemes and the perpetration of mass fraud;

d. States should assist one another in developing legislation and training legislative drafters in matters related to economic fraud and identity-related crime. In the case of identity-related crime, basing offences on abuses of identity represents a fresh approach for most States, and extensive work is needed. Lawmakers need to develop appropriate concepts, definitions and approaches to the criminalization of a range of conduct, including identity theft, identity fraud and other identity-related crimes. It is also critical for most States to ensure consistency with their respective private and public identity systems and with established crimes such as forgery and impersonation. Given the concerns expressed about the links between domestic means of identification, international and travel-related identification and transnational forms of identity-related crime, criminal offences that provide a good basis for international cooperation are desirable. It is therefore recommended that States consider the establishment of new identity-based criminal offences. It is also recommended that, in developing new offences, common approaches to criminalization be taken, to the greatest extent possible, to facilitate future transborder evidence-sharing, extradition of offenders and other forms of international cooperation.

2. Jurisdiction

Territorial jurisdiction. Modern transnational fraud tends to take place in many places at the same time and therefore may not be well addressed by traditional territorial jurisdiction unless laws have been updated to take into account recent developments. Narrow approaches can lead to cases where no State with the ability to prosecute effectively also has sufficient jurisdiction to do so, while overly broad approaches can result in conflicts of jurisdiction, ne bis in idem and other problems. It is therefore recommended that:

a. States whose laws follow relatively narrow approaches should review those approaches in the context of the range of fraud offences and options for territorial jurisdiction covered in the present report, and all States should ensure that their jurisdictional rules keep pace with the ongoing evolution of fraud offences;

b. when several States have jurisdiction, they should consult and collaborate with each other to ensure that cases are prosecuted, where possible, by the State that is in the best position to do so,
taking into account factors such as the availability of witnesses and evidence, the rights of accused persons, the capacity of the State to mount a fair and successful prosecution and the ability of other interested States to provide cooperation in support of the prosecution;

\(c\). States should consider technical assistance, both as a form of international cooperation in support of specific prosecutions, and more generally through UNODC and other appropriate bodies, to help ensure that States that have jurisdiction but lack capacity are able to effectively investigate and prosecute complex cases involving transnational fraud;

\(d\). States should ensure that they have sufficient investigative jurisdiction and powers to provide necessary assistance to a State prosecuting a fraud case that involves or affects their interests and that they are unable to prosecute for jurisdictional or practical reasons, or in which jurisdiction is ceded.

**Concurrent jurisdiction and cooperation.** Broad approaches to territorial jurisdiction will often result in several States having concurrent jurisdiction in major transnational fraud cases. In such cases it is recommended that the relevant States cooperate, under the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption, the Council of Europe Convention on Cybercrime and other relevant international legal instruments, where applicable, to ensure that the offences are thoroughly and comprehensively investigated in all relevant jurisdictions and that the offenders are prosecuted in the most appropriate jurisdictions, taking into consideration factors such as the locations of accused offenders, victims and evidence and the availability of the resources and expertise needed to prosecute effectively. Because of the nature of transnational fraud, early identification of the States concerned and early investigative coordination and cooperation are particularly important. The States concerned that are not the prosecuting State should assist the prosecuting State in every possible way. An approach similar to the criminalization, investigation and prosecution of transnational cases of identity-related crime is recommended.

**Extraterritorial jurisdiction.** Articles 15 and 16 of the United Nations Convention against Transnational Organized Crime and articles 42 and 43 of the United Nations Convention against Corruption require States parties that cannot extradite their own nationals to ensure that they have sufficient jurisdiction to prosecute offences covered by those conventions.
where one of their nationals commits such an offence outside of their
territorial jurisdiction. In the Organized Crime Convention, States parties
are also encouraged to establish sufficient jurisdiction to prosecute cases
where an offender found in their jurisdiction is not extradited for other
reasons (art. 15, para. 4). In view of the large number of fraud cases that are
transnational or multinational in nature, it is recommended that all Member
States consider establishing jurisdiction to prosecute fraud in any case
where the accused offender is found in their territory and they cannot
extradite for any reason to another State that has territorial jurisdiction to
prosecute the offence, assuming that the conduct in question is within the
scope of domestic offences and is defined as a “serious crime” in article 2,
subparagraph (b), of the Organized Crime Convention. In addition, articles
22 and 24 of the Convention on Cybercrime provide for extradition in such
cases if the crime is document forgery or fraud involving electronic
networks. More general forms of extraterritorial jurisdiction were not raised
in the general context of economic fraud, but the Intergovernmental Expert
Group noted that some States had extraterritorial jurisdiction in cases where
their fundamental interests were affected, such as offences relating to the
forgery of passports or counterfeiting of currency.

3. Limitation periods and amnesty powers

Limitation periods are an integral part of the criminal justice
practices of some States, but they may raise particular concerns in major
and transnational fraud cases, where successful investigation and
prosecution tend to be complex, costly and time-consuming. Approaches to
time limits and amnesties vary widely, but where limits exist, they should
take into account the time needed for effective investigations and
prosecutions in major fraud cases, bearing in mind the basic concepts of
each country’s legal and criminal justice system.16

a. it is therefore recommended that States take into consideration the
nature of such frauds when establishing limitation periods, to ensure
that they are not unduly restrictive, and that longer periods be
considered for specific types of fraud that are seen as likely to
require more time, such as offences relating to corporate, commercial
or other complex forms of fraud, offences that are transnational in

16 Some actions called for in the recommendations in this segment may also be
taken pursuant to the implementation of provisions of article 11, paragraph 5, of
the United Nations Convention against Transnational Organized Crime and article
29 of the United Nations Convention against Corruption.
nature or offences that involve organized criminal groups, where these are specific offences in national law;

b. in view of the length of time needed once investigative, prosecutorial proceedings have commenced in such cases, it is also recommended that limitation periods be suspended, cease to run or recommenced from the beginning once such proceedings have commenced;

c. it is further recommended that States apply the same provisions for longer time limits, extensions, suspensions and recommencement of limitation periods to proceedings relating to mutual legal assistance, extradition, domestic prosecutions under concurrent or exclusive territorial jurisdiction and aut dedere aut judicare provisions as are applied to purely domestic prosecutions in their domestic laws;

d. some States also reported the application of amnesties in cases of economic fraud. While amnesties are a matter for each State, it is recommended that, in cases involving transnational elements, the implications for transnational or foreign investigations and prosecutions be considered before the use of amnesty powers in fraud cases. A similar policy could be considered with respect to the use of amnesty powers in cases that involve identity-related crime in the context of criminal offences or activities with transnational aspects.

4. Law enforcement and investigative capacity

Most serious cases of economic fraud and identity-related crime involve a degree of sophistication that challenges even the most developed and well-equipped States and poses an even more serious challenge for developing countries and for international cooperation. The misuse of information, communications and commercial technologies makes the forensic expertise needed to investigate and gather and preserve evidence of cybercrime critical. Substantive knowledge of legitimate financial and economic systems, accounting, and money-laundering techniques and identity systems is also important, and in transnational cases expertise and capacity are needed to support international cooperation. A further factor is the rapid evolution of both legitimate technologies and commercial practices and the resulting evolution of criminal techniques, which require regular updating of training materials and retraining of officials. Some progress has also been made in developing effective countermeasures, including a “24/7” (24 hours a day, 7 days a week) emergency contact network for use in transborder cybercrime cases. Established in 1992, the emergency contact network included more than 45 countries in January
2007. Each country makes available specialists in computer investigations to receive emergency requests for assistance at any time:

a. it is therefore recommended that States develop and maintain adequate research capacity to keep abreast of new developments in the use of information, communication and commercial technologies in economic fraud and identity-related crime;

b. it is also recommended that the product of research be shared and disseminated to law enforcement agencies in each country through domestic training and, where feasible and appropriate, with other States through appropriate technical assistance and training and with relevant commercial entities;

c. it is further recommended that Governments and commercial entities collaborate on matters of research and development, recognizing, within the limits of commercial feasibility, the importance of incorporating crime control into new technologies and the social and commercial importance of ensuring appropriate law enforcement capacity as new technologies and products enter the market;

d. it is further recommended that States support and make use of the “24/7” emergency contact network in transborder cybercrime matters, both for emergency and non-emergency cases involving electronic fraud or identity-related crime.

Several States and some commercial entities noted the usefulness of screening mass telecommunications and financial or commercial transactions to look for patterns suggestive of fraud so that timely investigative and other measures could be applied. That raises several concerns, including the possible infringement of privacy and other human rights and, in the case of commercial systems, concerns about proprietary technologies and customer privacy, which need to be considered and addressed. It is therefore recommended that:

a. member States, individually, collectively and where appropriate in consultation with commercial entities, should undertake research to identify any characteristics that might be used to distinguish between normal legitimate and fraudulent transactions or activities, such as unusual patterns in telecommunication activity or commercial transactions, specific commercial practices, markets or commodities representing a high risk of fraud;

b. useful substantive criteria and procedural practices for the screening and identification of activities suspected of involving fraud should be developed and shared among States and appropriate commercial entities, and States and the private sector should collaborate and
assist one another in ensuring that those criteria and practices are kept up to date and that appropriate officials are trained in their use;

c. appropriate safeguards regarding the use of screening activities and the sharing of information generated from such activities, as well as the sharing of information about useful screening techniques and best practices, should be developed and taken into consideration;

d. while the criteria for identifying transactions suspected of fraud and those suspected of money-laundering will not necessarily be the same, there should be coordination and sharing of information between officials involved in activities aimed at countering fraud and money-laundering, where appropriate.

5. Cooperation between criminal justice systems and the private sector

Economic fraud is an inherently commercial crime and can be seen as a distortion or perversion of legitimate commercial dealings: victims are generally deceived when offenders succeed in imitating legitimate commerce of some kind. Identity-related crime either targets identification documents, systems or data or exploits them in the course of committing other types of crime. Both economic fraud and identity-related crime have a substantial impact on private interests, as well as on public interests. Fraud affects both individual commerce and commerce as a whole: large-scale fraud can bankrupt companies and erode confidence in markets. Identity-related crime affects both public identification, such as passports, and private credit cards and similar documents. In countries where private documents are used for public purposes and public identification is used for private purposes, crimes against any form of identification affect both areas. It is therefore essential that criminal justice and commercial entities cooperate effectively, both to develop an accurate and complete picture of the problems and to develop and implement preventive and reactive measures. Cooperation in investigation and prosecution is also essential, bearing in mind the need for appropriate safeguards to ensure the independence of investigative, prosecution and judicial functions.

To prevent fraud and identity-related crime, it is important that security countermeasures be developed and then incorporated into commercial technologies and practices. That, in turn, requires consultation between public entities, such as standard-setting bodies, and private interests, including those companies which produce and sell new technologies and those which will use them. Important issues include ensuring that preventive measures are effective and do not unduly impede normal commercial activities and ensuring that, where costs or competitive factors are affected, the same requirements apply globally, so that a normal
competitive environment is maintained. Generally, security measures should make products more competitive, not less competitive.

A number of States mentioned the relationships between State and commercial identification systems. Several also noted the importance of cooperation between law enforcement and commercial entities in detecting, investigating and prosecuting crimes such as economic fraud and related abuses of commercial identification. It was noted that commercial entities were often in the best position to monitor commercial traffic and identify suspicious or suggestive patterns and that, in many cases, victims were more likely to report specific crimes to companies than to law enforcement agencies, in the hopes of recovering losses. Commercial entities also noted, however, that proactive cooperation with law enforcement could affect competitive interests or customer privacy, or result in civil liability. It is therefore recommended that representatives of law enforcement and commercial entities consult with a view to developing useful practices for key areas such as the reporting of crimes and investigative cooperation. In this context, the experts noted that such activities had already been taking place for some time in some forums, especially with respect to key issues such as the preservation of data.

A key element of prevention is the education and training of persons who are in a position to identify and report economic fraud or identity-related crime: such persons range from commercial customers or communication subscribers to employees who handle business transactions. Such training and education require frequent updating, to reflect the latest developments in criminal methods and techniques, law enforcement measures and commercial practices. It is therefore recommended that criminal justice and commercial entities cooperate, to the greatest extent possible, to support effective education and training, including by sharing appropriate information and ensuring that the information reaches the right persons.

6. Economic fraud and identity-related crime in the context of development, reconstruction and economic transition

In countries with economies in transition, whether in the course of reconstruction, development, rebuilding after conflict or natural disasters or major economic reform, confusion between old and new rules or practices creates a risk of economic fraud; the harm caused by such offences could be great: direct economic losses are hard to absorb, and confidence in new economic and legal structures is eroded. Further harm may result from organized crime and other problems fuelled by the proceeds of economic fraud. That is an area where fraud and corruption are closely linked: fraud
is often the means of illicitly diverting resources, while bribery and other forms of corruption are used to ensure that the diversion will be successful or undetected. The role of identity-related crime is less clear, but the basic ability to establish and verify identity is important as it is a stabilizing element and it supports measures against crime. However, most developing countries and countries with economies in transition lack the basic identification and related infrastructure. There is a need to ensure that all participants are aware of the high risk of fraud in such circumstances and the substantial harm such fraud can cause:

a. it is therefore recommended that basic anti-fraud elements and expertise be included when planning and implementing technical assistance in the development or reconstruction of basic economic and commercial structures and that such elements be considered by appropriate authorities in the course of planning and implementation at the national level, whether international assistance is involved or not;

b. it was noted that there are substantial areas of overlap between fraud and corruption offences in many legal systems, particularly where fraud schemes target public officials, public institutions or public funds. It is therefore recommended that there be appropriate coordination between anti-fraud and anti-corruption experts and materials and that the need to coordinate work, exploit synergies and reduce unnecessary duplication of efforts be taken into consideration in developing and implementing specific projects;

c. it is recommended that the existence and efficacy or reliability of identification documents and infrastructure be included as elements when assessing the need for development and reconstruction projects and that projects to establish or strengthen identification be incorporated into development and reconstruction efforts where needed.

7. Recommendations for the prevention and deterrence of economic fraud and identity-related crime

Given the links between economic fraud and some forms of identity-related crime, many measures that prevent or deter the one will also have the same effect on the other. That is particularly true for the prevention of identity-related crime, which can also prevent many of the fraud and money-laundering offences committed using false identities. The elements of deception and economic loss generally mean that economic fraud requires advance and often extensive and careful preparation on the part of the perpetrators and some form of vulnerability to deception on the
part of the victims, and both of those elements create opportunities for effective crime prevention. Most of the options for preventing identity-related crime are rather technical, focusing on means intended to make it more difficult to tamper with identification documents, to subvert or corrupt identification systems and/or to obtain identification data. As previously noted, close collaboration between relevant entities in the public sector and the private sector in developing and implementing preventive measures are also important for success, bearing in mind the need to exploit synergies while ensuring consistency and avoiding unnecessary duplication. Collaboration with experts engaged in the prevention of related forms of crime, including organized crime, corruption and money-laundering, is also important. It is therefore recommended that Member States develop and implement effective measures for the prevention of fraud and identity-related crime at the national level and, where appropriate, the international level, as well as in cooperation with the private sector. Such prevention efforts could include the following:

a. the dissemination of information about fraud and identity-related crime to potential victims: such information could include both general information to raise awareness of the threat and timely information about specific forms of fraud and identity-related crime based on accurate and up-to-date monitoring of criminal activities by appropriate entities in both the public and private sectors. Information campaigns could be directed at the general population and at specific groups considered to be particularly vulnerable or at increased risk of being targeted;

b. the dissemination of information about fraud and identity-related crime to others who may be in a position to identify, report or prevent such offences when they occur;

c. the rapid and accurate gathering and analysis of information to support effective and timely prevention measures: this should include the gathering of relevant information among law enforcement, commercial and other entities at the national level and, where appropriate, at the international level;

d. the rapid sharing of information among appropriate law enforcement and private sector entities at the national and international levels: such sharing must be subject to appropriate and applicable privacy and security considerations; generally, however, information needed to prevent fraud should not require the sharing of types of information, such as personal or investigative information, that would raise or invoke such considerations;
e. the development of commercial and other practices and systems in ways which recognize the specific and general threat and costs associated with fraud and identity-related crime and the need to incorporate effective security and other preventive methods: effective collaboration between Governments and the private sector are essential to ensuring that effective measures to prevent fraud are incorporated and used, while avoiding excessive costs or other problems related to efficiency, interoperability and fair competition.

A number of responses mentioned a range of technical means of prevention, both for economic fraud and identity-related crime, including measures to make documents such as passports or credit cards more reliable as a means of identifying individuals and more difficult to alter or falsify and measures to make the supporting information systems more difficult to subvert and more reliable as a means of rapid identification when cards or documents are used. The evolution of technical means of prevention is already well established and ongoing, both in appropriate commercial sectors and the public sector. The experts noted in particular the efforts of Interpol and the International Civil Aviation Organization (ICAO) to enhance the security of passports and other travel-related identity documents, as well as the work of the OSCE Action against Terrorism Unit in promoting the implementation and use of the programmes of ICAO and Interpol and other assistance in relation to the security of travel and identity document security. The experts also noted that the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (General Assembly resolution 55/25, annex II), and the Protocol against the Smuggling of Migrants by Land, Sea and Air (Assembly resolution 55/25, annex III), supplementing the United Nations Convention against Transnational Organized Crime, contain provisions on travel documents that are secure against falsification or tampering, enhanced security and systems for production, issuance, validation and verification and measures to implement machine-readable document forms to facilitate the rapid checking of passports. The experts further noted that the costs of research, development and implementation were a significant factor, however, especially for developing countries and for commercial entities concerned about cost-effectiveness and competitive advantages. The establishment of stronger identification systems in every State would bring collective benefits for the international community in controlling, for example, economic fraud and immigration or travel-related crime (such as trafficking in persons) and in general security. It is therefore recommended that:
a. States should develop and implement measures to enhance the security of passports and other travel-related identification documents and the processes and systems used to produce, issue, validate and verify them, taking into consideration the measures called for in relation to passports and other travel-related identity documents in the United Nations Convention against Transnational Organized Crime and the Protocols thereto\(^{17}\) and in ICAO document 9303\(^{18}\), on machine-readable travel documents;

b. technical information should be shared with developing countries, where feasible, and should be assisted in using such information to establish robust domestic identification infrastructures in support of both public and commercial functions;

c. government and commercial entities should cooperate to ensure that identification systems are robust and interoperable to the extent that that is feasible.

Criminological studies of the effectiveness of deterrence have shown mixed results for many offences. There are, however, some reasons why deterrence may be more effective in cases of fraud and similar types of crime, which are by their nature pre-planned and commonly involve some element of cost-benefit analysis on the part of the offenders. In addition to incarceration, the economic nature of fraud suggests that fines, confiscation and measures against money-laundering may be viable deterrents. Further study and consideration of deterrence measures are therefore recommended. In addition to introducing offences and punishments, there could be measures such as the introduction of specialized law enforcement units trained to deal with fraud cases, where such a measure is seen as increasing the probability of the offenders being detected, prosecuted and punished.

8. *Training*

One issue raised in some of the responses is the need to train investigators and prosecutors and to provide technical assistance for developing countries in that area. In the case of economic fraud, training


\(^{18}\) The experts noted that the member States of ICAO had committed themselves to the implementation of the relevant portions of document 9303 by April 2010.
must address the extremely diverse forms of fraud, the sophisticated nature of many of the offences, the involvement of elements of transnationality and organized crime and the criminal-commercial duality of fraud. In the case of identity-related crime, training must address the fact that such crime is a new and evolving concept that encompasses both new, high-technology forms of crime and long-established forms of crime such as document forgery. In both cases, training must also be regularly updated to keep pace with the rapid evolution of techniques used by offenders. The experts noted that such training often requires a multidisciplinary approach in the development and implementation of training programmes, including a range of disciplines from entities in both the public sector and the private sector. Modern fraud investigators, for example, require knowledge in areas such as accounting and the operation of commercial and financial systems and the investigation, preservation and presentation of evidence in cybercrime cases. Those investigating identity-related crime require not only knowledge of crimes such as impersonation and forgery, but also knowledge of the identification infrastructure and systems that support both government and commercial forms of identification. It is therefore recommended that:

a. generally, action should be taken to develop and disseminate appropriate material and information to be used to train investigators, prosecutors and other public officials and, where appropriate, persons in positions in the private sector where there is the potential to prevent fraud or identity-related crime or assist in its investigation and prosecution;

b. member States should cooperate collectively in sharing information relevant to the development of training programmes and materials. That is important not only to ensure that useful practices are transferred from one State to another, but also to help ensure that officials responsible for fighting fraud at the national level are able to cooperate effectively to counter the growing number of transnational fraud cases;

c. materials and training programmes should incorporate a general overview of fraud, but should also be directed at specific forms or types of offending;

d. there should be effective collaboration among those involved in providing training to counter fraud, money-laundering, corruption, terrorism and cybercrime and similar types of training, including in the private sector, with a view to exploiting synergies, ensuring consistency and avoiding duplication;
e. recommendations and materials for training on countering fraud should be disseminated to United Nations and other intergovernmental bodies so that they may be included in training and other material developed by those bodies;

f. member States should exchange information regarding the availability of existing training programmes on the investigation of computer crime and computer-related fraud and should increase and further systematize such training. A great deal of training is already available in those and related areas. Such training is given by and for many States, organizations and private companies and is available worldwide in many languages and for many levels of expertise. It has proved highly valuable in providing criminal investigators with the technical skills and knowledge necessary to investigate computer fraud and computer-related crime effectively;

g. the United Nations Manual on the Prevention and Control of Computer-related Crime\(^{19}\) should be updated by incorporating material dealing with computer-related forms of fraud and identity-related crime.

Substantive analysis and assessment of the information received

Use of terminology in the study

The subject matter of economic and financial crime has been discussed in several fora, including at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, but there is no clear and comprehensive definition of the terms “economic crime” and “financial crime”\(^{20}\). A forensic definition was not seen as essential but for purposes of clarity and context, the term “financial crime” was taken to include crimes committed using major financial systems or against those systems themselves. This may include money-laundering, some forms of corruption affecting financial structures, and most major economic crimes in which financial structures were used or victimised. The term “economic crime” was taken as a more focused concept, referring only to crimes in which the

\(^{19}\) International Review of Criminal Policy, Nos. 43-44 (United Nations publication, Sales No. E.94.IV.5).

motive was some form of economic gain or financial or other material benefit. This includes all economic fraud, and most but not all identity-related crime. Some States reported identity-related crimes, particularly the falsification or misuse of passports and visas for travel purposes, which did not necessarily contain an economic element or motive.

The term “fraud” had two meanings. In legislation, almost all States limited “fraud” to cases where there was economic loss to victims, but the terms “fraud” or “fraudulent” are also commonly used as terms of art by officials, academics and others to describe conduct which involves the use of dishonesty or deception, but not necessarily any financial or other material loss or benefit. For example, the means of recruitment of victims of trafficking may include non-economic fraud, and fraud on the part of a negotiating state may invalidate a treaty. For clarity, and without prejudice to any future work, it was decided to use the terms “fraud” and “economic fraud” as appropriate when referring to fraud in the established economic sense, and the term “identity fraud” for other cases within the scope of the study.

Initially the experts decided to use the term “identity fraud” when discussing the criminal misuse and falsification of identity, but in reviewing the evidence, it was apparent that the terms “identity theft” and “identity fraud” are not used consistently and that they did not fully encompass the scope of the identity-related problems covered by the study. In the Report, scenarios in which genuine identity information or documents are actually taken or misappropriated were described as “identity theft”, while scenarios in which identities were used to deceive others are referred to as “identity fraud.” Cases in which identities or related information were simply fabricated are not analogous to either fraud or theft, although some States considered these to be identity fraud based on subsequent misuse of the identities, and some related activities, including the trafficking in identity documents or information as a new form of illicit commodity also needed to be included. Accordingly, the term “identity-related crime” was used as a general reference, and the more specific terms “identity theft” or “identity fraud” were used where contextually appropriate.

The terms “commerce”, “commercial crime” and “commercial fraud” also have a range of meanings. Commerce and commercial practice take many forms in different countries and regions, and the term commerce,
in the broadest sense, includes any form of monetary or barter transaction, ranging from very large commercial dealings to the smallest bargain made in the marketplace. In that sense virtually all forms of economic fraud can be considered as crimes of commerce. Most experts, however, consider commercial crime or commercial frauds as more limited in scope, including only fraudulent conduct which involves, affects or targets major commercial systems and which is a significant departure from legitimate commercial practice. The present Study uses the term in the narrower sense, as does UNCITRAL in its work on commercial fraud.22

Results of the study on economic fraud

I. Commercial context of economic fraud

1. Commercial law

The commercial law frameworks of responding States ranged from complex and highly-regulated to largely unregulated. Three of 46 countries described federal structures, with commercial laws sufficiently broad in scope that elements were regulated in part by the elements of commercial law established at both federal and regional levels, such that specific controls and protections might vary from one part of the country to another. Most systems appeared to include contract law or law of obligations based on the freedom to contract and circumscribed in some cases by additional rules intended to provide protection in situations of inequality, dishonesty or inadequate disclosure. Rules appeared designed to increase the stability and predictability of commercial dealings, and many were also intended to protect vulnerable parties and ensure a measure of equality in transactions.

Approaches to protection were based in some cases on legislative limits on contract law, such as requirements or limits on how contracts were made and enforced, and in other cases on more general consumer protections, such as standards for advertising or the quality of goods bought and sold. In many cases, specific rules have been developed to address specific types of commerce, commodity or transaction, such as transfers of real property, banking services, and legal, medical and other professional

services. In addition to offences, regulatory elements and other legislative provisions, several States reported that they had specific agencies or entities, some of them independent from government, to oversee, regulate or enforce specific areas of commercial activity. Typically, mandates included not only preventing and suppressing fraud and other unfair or abusive practices, but also maintaining credibility and confidence in commerce and in some cases the regulation of the commodities involved for public safety, environmental or similar concerns. Some States also reported legislative or regulatory powers governing technical aspects of commerce, such as elements of the infrastructure of electronic commerce and questions relating to identification and the formation and enforcement of commercial contracts using information and communications technologies.

A number of States also mentioned the possibility of civil lawsuits, mostly in the nature of breach of contract actions, as a means of recovering losses, either as an exclusively civil option, or a hybrid option in which a civil recovery or restitution claim could be based on a criminal conviction. Some described legal obligations such as debt as a form of property interest which could be transferred. Some mentioned other remedies, including the voiding or recission of contracts where there was inequality, misrepresentation or outright fraud, and safeguards such as time delays to give contracting parties time to reconsider before a contract became binding. Some also indicated that they had additional measures or protections in place with respect to specific types of transactions sometimes seen as correlative with fraud, including door-to-door sales, telephone or telemarketing sales, and chain sales or schemes in which profits were earned by recruiting new vendors as opposed to profits from the sale of merchandise, also known as “Ponzi” or “pyramid” schemes.

Another area of commercial law raised by some responses was law regarding legal persons or companies, governing areas such as the identification, certification and licensing of companies, measures that could be taken to prevent or punish fraud in companies and the relationships between legal and natural persons in criminal cases. Aside from the criminal liability of legal persons, which in most countries appears to be

---

seen as a matter of criminal law and not company law, there were provisions about legal relationships such as agency or trust relationships, in which one legal or natural person was authorised and obliged to act on behalf of, and in the best interests of another. These often arise in fraud cases, and for some countries, breach-of-trust was seen as either a separate offence or an aggravating condition when imposing criminal sentences for fraud and similar offences. Breach of trust issues often arise in cases of frauds against companies by employees or others in positions of trust, but can also occur where victims of fraud are children or lacking in capacity for other reasons.

Generally, commercial law can be seen as an exercise in striking a balance between ensuring fairness and stability in commerce and avoiding excessive interference with the marketplace, and in this context one State observed that commercial structures in everyday practice might not necessarily correspond with legislative ideals. While equality of bargaining power might be enacted in law, for example, this did not necessarily mean that it would exist in practice. In examining economic fraud therefore, as with any legitimate commercial activity, it is necessary to consider economic realities, the social and cultural environment and other relevant factors to get a full and realistic impression.

2. Commercial technologies

There is no definition or clear category of commercial technologies, but generally the experts took these to include technological systems which had been developed or adapted or were commonly used to support elements of commerce, including functions such as advertising, negotiation, sale and transfer of payment. As with commerce itself, these could also be broken down into consumer technologies, such as debit and credit cards, which were widely available and used for large volumes of small transactions, and other commercial technologies such as the electronic funds transfer systems used by banks and financial institutions, which are more limited in scope and handle smaller numbers of larger transactions. Users of commercial systems include both the card-holders who use the system to access funds or credit, and the merchants who use them to accept payment.

Since many commercial technologies depend on the availability of appropriate telecommunications services, there is a direct link between information and communication technologies and commercial ones. Most States did not have official statistics, and those which did provide data tended to be the most developed countries, which also tended to report relatively high rates of accessibility. There appear to be differences in the
availability and use of technologies within countries. A number reported
greater access and use in urban areas than rural ones, and this differential
appeared to be more pronounced in developing countries. Some countries
also reported substantial recent increases in accessibility, which is
consistent with data from other sources which indicate that access to
technologies, and in particular Internet and mobile telephone services, is
rapidly expanding on a global basis. The trend is clear over several
decades. The number of persons with access to conventional telephones
increased from fewer than 100 million in 1950 to about 1 billion in 2000,
and a similar increase occurred in mobile telephone use between 1990-
2000. The transition has been particularly prominent in developing
countries, where wireless mobile technologies are often cheaper and easier
to install than wire-based ones. The number of individual computers with
access to the Internet, which did not exist at all until 1969, stood at
395,000,000 as of January 2006 and is expected to exceed 500,000,000
before the end of the present decade\textsuperscript{24}.

While numbers of computers on-line can be counted, there is no
reliable means of counting the total numbers of persons who use those
collectors or who have access to the Internet or other information,
telecommunication or commercial technologies that may be associated with
fraud or identity-related crime, but numbers are probably much larger,
given the number of scenarios in which multiple users share the same
access channels or devices. With both wireless telephones and Internet
access, ratios of users: devices are also likely to be substantially larger in
developing countries, where the high costs of devices make shared access
such as rental of telephones and use of public Internet facilities much more
common. The identification of “users” also becomes complex, especially
for commercial technologies, in which the same transaction often involves
different uses by various parties. A single credit-card transaction usually
involves “use” of the technology by the card-holder, the vendor of goods or

\textsuperscript{24} Sources: (telephone access) International Telecommunication Union (ITU)
Executive Summary available on-line at: http://www.itu.int/ITU-
D/ict/publications/wtldr_02/material/WTDR02-Sum_E.pdf (Internet access) Internet
Numbers of computers have already passed the 500 million mark: as of 1 January
2008, the Internet Domain Survey listed Internet hosts as totalling 541.6 million.
services purchased with the card, the card-issuer, and possibly banks or other financial institutions.

Use of consumer commercial technologies such as payment (debit and credit) cards varied widely among the responding States, influenced by factors such as the availability of supporting information and communications technologies, patterns of commerce and the overall degree of development in each country. Generally, developing countries estimated relatively low usage, while the most technologically developed countries reported a range between approximately 25-50% of transactions using some form or payment card system or direct electronic transfer of funds. The information provided suggests that, at least in those countries, there is an ongoing shift in practice away from cash and paper-based means in favour of the use of payment cards and other means of electronically transferring both ownership and payment. No information was provided, but it is likely that there are also differences between developed and developing countries depending on the type of use, given the extensive use of payment cards in travel. In many developing countries, relatively few residents may use such technologies as customers, but businesses accept those of foreigners, especially in tourism and related sectors. There is also an expansion in the ways technologies are used. Electronic commerce, in which the advertising and sale of goods or services as well as payment use commercial technologies, is expanding in countries where it is technologically viable, although even in the countries with the highest usage of electronic commerce, it was still only a small portion of overall commerce.

One State noted that more extensive use of technologies for electronic commerce, where goods are chosen, ordered, paid for and in some cases even delivered electronically depended to some extent on the type of goods involved, and whether participants in transactions had sufficient confidence in electronic commerce.

The developing countries which responded reported higher usage of barter than did more developed countries, but there was one exception. One developed country reported that it saw significant levels of barter transaction, supported by companies set up for this purpose. This may be attributable in part to the use of computer networks effectively creating a new form of electronic marketplace for barter.

II. National experiences of economic fraud and legislative responses

1. Meaning of economic fraud and scope and elements of fraud offences

In most countries, the legislative definition of fraud was exclusively economic, but in everyday practice, the term is often applied to
any form of dishonesty or deception. Most of the States which provided
information about their legal definitions of fraud indicated that the
definitions were considered criminal law and contained economic elements.
Some also reported elements of their commercial law which addressed
fraud and related problems using non-criminal measures such as controls
on advertising. These were seen as anti-fraud measures, but generally
addressed a broader range of conduct not limited to criminal fraud. This is
consistent with earlier work undertaken by the Commission on
International Trade Law which suggests that commercial concepts of fraud
include some forms of conduct that some States would not necessarily see
as criminal conduct. Some States indicated that they considered fraud as
including non-economic crime, but their fraud offences were exclusively
based on material loss or risk of loss, and the other offences cited, such as
forgery or impersonation, were not legally defined as “fraud”. In common-
law countries, statutory definitions tend to be based on the original English
concepts of fraud or false pretences, which include economic elements, and
are defined primarily by case law, and several common law countries
reported fraud offences in which the term “fraud” was not fully defined by
legislation.

There was a high degree of consistency in the elements of the fraud
offences provided or described by States in their responses. The vast
majority include some form of dishonesty or deception, some form of
economic loss or transfer, and the need for a causal connection between the
two. The economic element covered a wide range of financial or other
material benefits, with various statutes mentioning property, financial or
other advantages. At least one included the illicit acquisition of ownership
or title to property or failure to register some title transfers as elements or
indicia of fraud. While a few required proof of enrichment of the offender,
most required only the element of some form of loss to the victim. This
would be easier to prove in most cases and would include cases where the
fraud was incomplete in the sense that the proceeds never reached the
offender or could not be proved to have done so. In addition to concrete
losses or benefits such as transfers of cash or property, for many States, the
concept of loss or benefit extended to less direct forms. Losses could
include exposure to risk or loss of expectation value, for example, even if
these remained intangible and did not materialise. For a few States, the

25 UNCITRAL, Note by the Secretariat: “Possible future work relating to
paragraph 12 et seq.
The element of loss was framed in terms of more general prejudice to the victim, which might in some cases include non-economic forms of prejudice.

The element of deception was also consistently present, but details varied. Some States required some form of active conduct which was intended to mislead or deceive, while others included also cases where the deception was accomplished through the withholding of information, failing to provide information or taking advantage of the fact that the victim did not have relevant information. One issue which has arisen in States where automated commercial forms of identification are used is whether a machine or system can be deceived. Generally, the presentation of false commercial identification for economic gain appears to be treated as fraud whether the identification is presented to a human being or a machine, which implies either that it is possible in law to deceive a machine or that the machine is being used by offenders as a means of deceiving its owners or operators. Similar issues arise with respect to cases where legal persons are victimised. In such cases, there is usually either deception of an employee or agent of the victim, or collaboration of an employee, in which the legal person itself and other individuals are deceived. Some States also noted that a causal link between the elements of deception and benefit or loss was required, although this tends to become more tenuous in cases where the loss is less tangible. One State indicated that the causation requirement had become sufficiently attenuated that there could be a conviction for fraud even where the deception was unsuccessful, while other legal systems would deal with such cases as attempts.26

One issue raised by many of the responses of both States and commercial interests was the dual nature of economic fraud as both a criminal and commercial issue. Most fraud succeeds by imitating legitimate commerce, in large and small transactions, raising the need for commerce-based initiatives in response, and almost all States indicated that they dealt with fraud as both a commercial and a criminal matter. Laws regulating the making of contracts, advertising, and remedies for defective or misrepresented goods were reported by a number of States, as were regulatory regimes establishing such elements as minimum standards for

---

26 South Africa includes as fraud cases where there was no direct causation because misrepresentations were made but not successfully transmitted to victims. See Francis [1981] 1 SA 230 (ZA). In Canada, similar cases would result in criminal liability for an unsuccessful attempt. See Detering v. The Queen [1982] 2 S.C.R. 583 (Supreme Court of Canada).
commercial practice, criminal or administrative prohibitions and offences, inspection powers and bodies empowered to monitor laws and practices, consider disputes and apply remedies. More specific regulatory requirements and offences were directed at specific forms of commerce such as transactions in stocks, insurance or real property, or key areas of professional practice such as law or accounting that were seen as particularly vulnerable to fraud. In some cases these included offences identified as fraud, often against specific regulated structures such as stock exchanges or the insurance, banking or financial industries, but the overall picture is one of more general measures which address criminal fraud as part of a broader problem. As noted, legislative regimes have sought to ensure a degree of fairness, stability and predictability in commercial dealings with relatively broad legislative frameworks, reserving the definition of fraud and the application of criminal offences and criminal justice measures for those activities which are seen either as the greatest threat to economic or commercial integrity or as having particularly harsh consequences for identifiable victims.

2. Approaches to classifying economic fraud

States were asked about the legal basis on which they classified fraud, including: fraud defined by type of structure attacked, fraud defined by offender modus operandi, fraud defined by type of victim, fraud defined by type of offender, fraud defined by type of infrastructure involved, but not attacked, and any other categories. The responses disclosed two general strategies for criminalisation, depending on whether fraud was classified in detail or not. Some States reported only a very small number of fraud and related offences, framed in a very general way so as to encompass a comprehensive range of frauds. These States generally did not provide information about legal classification or typology, nor did their legislation suggest any. Other States reported larger numbers of more narrowly-framed, specific fraud offences, intended to punish and deter specific conduct, and these reflected some of the classifications suggested by the survey questionnaire. Of the States which described classifications definitions based on modus operandi, types of infrastructure involved or attacked and victim status or characteristics were the most common, and it was clear from some responses that there were significant areas of overlap between the categories. Most responses made it clear that, while national legislation sometimes followed the typology suggested by the questionnaire, the suggested categories overlapped, and different States might well classify the same fraud in different categories. Offences such as credit-card fraud, for example, might be seen as frauds against the credit...
card system or frauds against card-holders using the system as a means, depending on how the costs or losses were allocated.

Fraud definitions based on *modus operandi* were probably more commonly used by investigators and prosecutors than in legal definitions. Descriptions such as “mass-market fraud”, “advance fee fraud” and “pyramid” or “Ponzi” fraud schemes are all used primarily as terms of art, although several States did report offences or other provisions specifically directed at these problems. In legislation, some States have criminalised frauds which involve the use of devices, passwords or access codes or frauds or other offences using telephones or telecommunications media, and several have adopted offences which criminalise preparatory steps, such as the theft of, possession of, or trafficking in computer passwords, credit card information or devices used to “skim” and copy the data from credit or debit cards. Many States reported fraud offences based on the type of structure attacked. A number reported frauds against government or specific public structures such as social benefits or tax systems, for example, and some consider the counterfeiting of currency or stamps to be a form of fraud against those structures. A number of States also had specific offences of committing frauds against private commercial structures, the most commonly reported being insurance frauds credit card frauds, and frauds against banks or other financial institutions. Some offences in this category were even more specific, addressing frauds using specific documents such as wills or real estate documents or misrepresentations or other abusive practices within specific regulated commercial activities, such as stock markets.

Fewer States reported fraud offences based on the type of victim or type of offender, but a number did consider this as the basis for either more serious offences or aggravating circumstances for sentencing. The apparent policy objective for many was to enhance deterrence for frauds where there was a great imbalance between offender and victim, either because the offender was in a position of power, trust or influence, or because the victim was in some way exceptionally vulnerable. An overlapping objective, especially with commercial frauds, was the need to protect the integrity of specific activities such as stock markets. Specific groups of potential victims accorded additional protection included the elderly, minors, the mentally disabled, legal persons and the estates of deceased persons. Only some States reported specific legislative provisions, but it is likely that in additional States, these same factors would be taken into account by courts in exercising discretion when sentencing offenders. Some States also apply additional preventive or deterrence measures or specific legal requirements to those in positions of trust, such as lawyers,
accountants or corporate officers, and in some countries these are further supported by regulatory and disciplinary requirements imposed by governing bodies for key professions.

3. Types of fraud criminalised by States

States reported a wide range of specific offences of fraud and related or preparatory conduct. As noted, some had a few broad, general offences. While others had more specific offences. Many States have found it necessary to expand established offences or adopt new ones to deal with recent innovations by offenders. For example, Article 8 of the European Convention on Cybercrime requires the criminalisation of specified actions in respect of computer systems or data, if done with “fraudulent or dishonest intent”, and “…for the economic benefit of oneself or another person”, and several States Parties to that Convention reported specialised computer-fraud offences. A number of other States also reported offences that apply to computer-related crime in general as effective in prosecuting computer-related fraud cases. These included offences relating to the possession, trafficking in or use of instrumentalities for computer-related fraud, such as passwords, credit-card data, and some types of hostile software programs, and offences relating to computer “hacking” or the unauthorized access to or use of computer or telecommunications systems.

Other types of fraud which were the subject of specific offences included: frauds against tax or public benefits systems; the counterfeiting of currency, stamps and in some cases private intellectual property; frauds using specific types of documents, including testamentary instruments, real estate documents and financial instruments; frauds against specific types of commercial activity, including bankruptcy proceedings, insurance frauds, frauds involving financial markets; bank frauds and credit-card frauds; frauds involving gambling or lottery schemes; and frauds against the State itself, including some corruption offences. Some States also reported offences intended to protect the integrity of specific mechanisms or processes. These included frauds against public procurement systems, military fraud offences, frauds in municipal codes, fraud offences in laws governing professions and trades unions, and frauds affecting political parties or similar organizations.

A number of related or preparatory offences were also reported, including: identity-related crimes such as impersonation and the

falsification, forgery and use of falsified identification documents or electronic identity information; abuses related to other types of document, such as forgery and the use of forged documents, suppression of genuine documents, and illicit possession of or trafficking in certain genuine or forged documents; the falsification, destruction or tampering with electronic data; some corruption offences, such as the bribery of public or private officials in support of fraud schemes; arson and other forms of property damage or destruction in support of fraudulent insurance claims; and depending on the fundamental principles of each State’s domestic law, conduct such as organizing, directing, aiding or abetting, attempting and conspiracy to commit fraud.

4. Types of fraud encountered by States

States have encountered a wide range of different types of fraud, and even within individual States, no single typological framework exists for classifying it. A further complication is that many frauds are effectively hybrid or compound, using more than one medium or message for different stages of the fraud, and the same victims can be targeted more than once by offenders using different messages. Victims might be initially contacted by soliciting responses to an Internet web-site, for example, with subsequent contact by offenders using postal mail and printed documents, e-mail or telephone calls, depending on the nature of the solicitation, and wire-transfers or some other means used to transfer the proceeds. Once victimised successfully, they are often targeted again by the same offenders or others who have purchased their names with fresh fraud messages, including offers of assistance, for an advance fee, in recovering the losses from the earlier frauds. All of this makes classification difficult, and approaches to classification in each State may differ depending on who does it and why. Different approaches apply to offences and other legislative provisions which must support legal proceedings, working classifications used by law enforcement and other investigators for practical and training purposes, and criminological classifications intended to support research and policy development. Further categories are added by private sector interests, often based on the commercial sector involved, such as all types of bank, insurance or credit card fraud, and in accordance with needs such as loss prevention, audit requirements and civil litigation to recover proceeds.

While there are some superficial variables attributable to differences in language, culture or commercial practice, the underlying problem of fraud appears to be fairly universal, described in similar terms by countries from different regions and at different levels of development.
To a large extent, reported differences appear to relate more closely to difference in underlying commerce than any other situational factors. Frauds involving credit cards, real property, financial markets, and the counterfeiting of currency were widely reported, for example, whereas frauds involving subject matter such as the mining and trading in valuable minerals and maritime frauds were reported only by States with substantial legitimate commerce in those areas. Similarly, most of the transnational fraud concerns related either to frauds involving transnational technologies or to travel documents such as passports. Some specific types of fraud raised by States included the following:

a. **Advance fee fraud.** This is primarily used as a descriptive term by experts and law-enforcement and not as a legislative offence or definition. Generally it describes a wide range of frauds in which fees are solicited in advance for goods or services which are not delivered as promised. Some of the types commonly encountered by responding States included a range of schemes employing postal mail, electronic mail, telephone and Internet solicitations, including West-African “419” solicitations, Internet auction frauds, loan frauds, lottery frauds, investment or stock frauds and “affinity” frauds directed at victims based on appeals to religious, cultural or ethnic values.

b. **Bankruptcy fraud.** Several States mentioned fraudulent conduct in the context of the bankruptcy process. Specific occurrences range from comprehensive schemes in which businesses are established and stripped of assets by offenders who then seek to avoid liability through bankruptcy, to schemes in which fraudulent conduct such as the diversion of assets or fraudulent preference of some creditors over others occur incidentally to legitimate bankruptcy proceedings. Victims may include the companies themselves, their owners, investors or shareholders, and cases may involve both civil and criminal aspects.

c. **Charitable frauds.** Charitable frauds consist of schemes in which victims are either donors or charitable causes. Donors are victimised by offenders soliciting contributions for causes which may or may not exist, but which do not receive the contributions. Charitable causes or organizations are victimised when offenders divert funds originally contributed to legitimate appeals for legitimate causes. In both cases, indirect harm is caused, both to the legitimate causes which do not receive contributions, and to charitable work in general, as donors may be deterred from contributing in future. These frauds can be difficult to detect and investigate because unlike other frauds,
charitable donors will often never be aware that donations were not used for the purpose for which they are solicited. Some charitable frauds have been encountered in ethnic expatriate communities, based on the sympathy of community members for promoted causes in their countries of origin or ancestry, and a number of States expressed concern about their potential role as a source of financing for terrorist groups for this reason. One State noted a pattern in which charitable frauds tended to cluster around mass-appeals for legitimate charitable causes such as relief efforts for major natural disasters such as the December 2004 Asian tsunami. Charitable frauds may be linked to tax frauds in jurisdictions where claims of charitable donations may be used to reduce tax liability.

d. **Computer, E-mail, wire, or Internet frauds.** This is a difficult classification because a number of different types of fraud can be committed using computer systems and the technologies themselves can be used by offenders in different ways. The most common scenarios appear to be frauds in which goods or services, often high-value items, are advertised and offered for sale electronically, but never delivered. Computer network systems are also used to run fraudulent on-line auctions, or to manipulate legitimate auctions. Computer frauds have also targeted stock-trading, ranging from the establishment of completely-fraudulent Internet brokerage web sites to the use of the Internet to disseminate false information in order to improperly manipulate stock prices to the offenders’ advantage. Computer systems can also be used as one element of a larger fraud scheme. Mass-advertising on the Internet can be used to identify those who respond as having specific interests which make them potential victims of frauds committed by telephone or other methods, for example. Roles played by computer systems in fraud are discussed in more detail below, but generally States saw the involvement of computer technologies as a major factor in increases in mass-frauds and transnational frauds, and the versatility of the technologies reflected in the wide range of specific roles reported.

e. **Telemarketing, Internet or Mass-marketing frauds (mass frauds).** These employ a range of different appeals and deceptions, but have in common the media used, which can target large numbers of victims simultaneously at long distances and across international borders. Early forms of mass fraud used postal mail and whatever mass-media advertising is available to offenders and victims. More recent forms have taken advantage of the opportunities afforded by the Internet and mass electronic mail, or “spam”. Specific appeals
are most commonly advance fee solicitations, but can also include others, such as fraudulent charitable appeals or the sale of overvalued or non-existent goods. Geographical patterns are influenced by the need for access to the technologies both to solicit and deceive victims and to transfer funds, which are sometimes different. *Modus operandi* are also influenced by the nature of the technologies to some degree. Mass electronic mail messages can target millions of victims simultaneously, for example, but have lower success rates than telephone-based frauds, which use one-on-one conversations. These target smaller, although still substantial, numbers of victims, but offer potentially stronger means of persuasion through verbal contact, and therefore higher success rates. Telephone frauds also require a higher degree of skill and proficiency in the language spoken by victims than do Internet or e-mail based schemes. Internet-based schemes often use fraudulent but official-looking websites to establish credibility. As noted, in some cases offenders use different media for different stages of the same fraud to maximise overall advantage and minimise risk.

*f.* *Telecommunications fraud.* This is distinct from the previous category in that telecommunications services or fees are the proceeds of the fraud, rather than the means of committing the offence. Several variants were reported, including cases where fraudsters use hacking or passwords taken from legitimate users to gain access to telecommunications services to which they are not entitled, which could then be used or sold. A more lucrative variant exploits the use of automated billing systems. In these cases, victims’ calls or Internet access are routed to or through systems which charge inflated fees, which are paid to the fraudsters, victimising either the subscriber or the telecommunications provider, or both, depending on how the ultimate losses are assigned. Some States noted that, while telecommunications fraud was economic fraud in the sense that the value of telecommunications services was involved, in a significant number of cases the primary motive was not the economic value of the telecommunications services, but obtaining the use of untraceable communications for use in the commission of other crimes, particularly some forms of cybercrime, organized crime and terrorism. Several reported links to credit-card fraud and forms of identity-related crime in which offenders first faked identities and then used these to obtain and pay for telecommunications, which even if intercepted could not be traced.
g. **Counterfeit goods and intellectual property offences.** Several States reported the sale of counterfeit goods or intellectual property to purchasers as frauds. Whether they would be considered as forms of economic fraud within the scope of the present study depends to some degree on the facts of each case. The simple taking of intellectual property or creation of counterfeit items may victimise the owners of the intellectual property rights, but there is no deception, and therefore no fraud. However, several States noted that the subsequent sale of such goods at prices based on the value of genuine items was a fraud against the purchasers if they were deceived about the origin, quality or true value of the merchandise.

h. **Stock, securities or capital markets fraud.** The ways in which stock markets and similar structures operate offer some specific opportunities for economic fraud, and their legitimacy or credibility is of sufficient importance that many States provide additional protection in the form of specific offences, regulatory and institutional regimes. Fair markets require assurances and confidence that all investors are able to assess stock values on the basis of accurate and equal information, and actions which provide some with an improper advantage over others are generally treated as frauds against disadvantaged investors, other criminal or regulatory offences, or in some cases subject to sanctions such as loss of trading privileges. Two specific types of conduct were mentioned by States. One involves the use of false or misleading information to artificially manipulate the values of stocks in ways which only the offenders could predict. Many States have offences of “insider trading”, and several indicated that they saw these as a form of fraud against investors.

i. **Frauds using paper documents.** Frauds involving document abuses tend to mimic the legitimate use of paper documents in a particular region or type of commerce. Some developed countries reported that paper instruments are now being gradually replaced by credit cards, debit cards and electronic funds transfers, and that fraud patterns are also shifting from the old medium to the new. Paper-based frauds still frequently occur where the commercial context makes them plausible, or provides some advantage for offenders, however, including most commerce in developing countries and specific areas of commerce which rely on paper documents out of custom, a need for security, or because they involve economies or commercial sectors which are still largely paper-based. Some States reported transnational cheque frauds originating from regions where paper is
more common, such as West Africa, and forged instruments are still seen in a range of major commercial frauds where formal paper instruments are still used for legal reasons. Offenders also sometimes use high-quality forged documents, often prepared using modern document scanners and computer printers, for types of fraud or types of victim where these will have more credibility than other media. Forged paper instruments may be used to fraudulently corroborate offences perpetrated on computer networks, for example.

Paper-based frauds have been detected in respect of virtually any type of instrument or document which can be exchanged for value. The most basic forms of document frauds involve simply exchanging worthless false documents for money or valuable assets. Other frauds rely on the fact that paper-based systems take some time to establish whether a document is authentic or not, allowing offenders time to exchange them for cash and then transfer the cash out of reach before the fact that the document is false or worthless can be discovered. As a preventive measure, banks commonly block any further transfer of deposited funds until value and authenticity can be established, and large commercial systems which rely on paper contracts or instruments now commonly back them up with either similar delays, effectively holding back both transfers of goods and transfers of funds until both sides of the transaction can be authenticated. Some such frauds may never be discovered. Several States reported specific offences relating fraud-related document abuses, such as the forgery of testamentary documents or titles to land.

Immigration-related fraud. Several States mentioned passport or visa frauds which may or may not have economic elements and one State mentioned economic frauds committed in the context of its immigration processes. In the economic frauds, victims were targeted by misrepresentation to the effect that the offenders could advise or assist them in obtaining immigration documents, status or preferential consideration, in exchange for proceeds represented as either fees or funds for bribing immigration officials. The non-economic variations were forms of identity theft or fraud, in which false passports, visas or other documents were obtained or provided, or genuine documents are used by persons not entitled to do so. These may be economic forms of identity-related crime, especially if identity information was purchased or sold, but would not be economic fraud, as there is no direct link between the elements of deception and economic loss. Immigration-related frauds are similar in most respects to other forms of economic or identity fraud, with

248
two important differences. First, in addition to the direct harm and losses to potential migrants, harm was also caused to State immigration systems in the form of additional costs and procedural issues raised by undocumented migrants, and in some cases security risks posed by persons not fully screened for domestic or international criminality, terrorism risks or other factors that would make them unacceptable as immigrants. Second, these frauds are also inherently transnational in nature, because the harm usually accrues in a jurisdiction other than where the fraud itself was committed, and some States have extended adjudicative jurisdiction, either on the basis that the effects of the offences were felt in their territory or that the need to protect the integrity of the immigration process was an essential interest of the State concerned.

k. **Insurance fraud.** A number of States reported frauds against insurers as a distinct offence or type of fraud frequently encountered. Most of the cases mentioned involved claims against insurance contracts that were based on non-existent or exaggerated losses, including property losses and in some cases false claims of death against life-insurance policies. Cases also involve publicly-operated health, motor-vehicle and other insurance schemes where these are operated by the State. Some States also reported the adoption of preparatory or related offences such as arson or destruction of property, which are seen as part of frauds when the property is insured for more than its actual value and then destroyed. Another form mentioned was the use of fraudulent insurance contracts, in which insurance premiums are collected but no insurance is obtained. These are difficult to detect in most cases because they are not apparent to the victims unless an insured loss occurs, and they can be difficult to quantify for purposes of prosecution, sentencing and civil or administrative litigation because the foreseeable loss could be either the amount of the insurance premiums actually taken from victims or the amount of insurance that would have been paid if an insured loss had occurred.

l. **Loan or credit-related frauds.** A number of countries reported frauds related to loans or loan guarantees. The most common appear to be variants in which money is loaned based on fraudulent misrepresentations as to the credit-worthiness of the debtor or the existence or value of security or collateral property, and then not repaid. Another commonly-reported variant is cases in which advance fees are paid by victims seeking loans in exchange for a favourable credit-rating or guarantee that the loan will be received and/or insured. The advance fee is paid and the loan does not
materialize. One country reported a further variant in which the fraud consisted of lending the victim’s money to others, a scenario also common in some major commercial frauds, where corporate funds are improperly loaned to unsecured creditors. The deprivation and enrichment elements can also be difficult to quantify in loan frauds: offenders are generally enriched by fraudulent fees or commissions, but losses can include, in addition to the fees, other costs of reliance on credit that does not materialise. Where fraudulent loans are actually made to offenders they gain the use of the funds, and if not repaid, the funds themselves, and victims suffer similar losses. Aside from direct economic losses, in corporate frauds the costs include loss of customer or investor confidence in the company and in some cases, bankruptcy.

m. *Procurement frauds and sale of defective or substandard materials.* Procurement frauds can target either public or private procurement processes, and generally rely on the fact that officials who specialise in procurement, especially for governments or large companies, are often unfamiliar with the nature of the goods or services involved or their true value and therefore not in a position to detect exorbitant bids or the delivery of inferior goods or services. One State noted that fraud offenders in this area sometimes target exceptional procurement efforts, such as schemes for recovery after natural disasters, on the basis that large volumes must be procured quickly and that contract scrutiny and other safeguards are likely to be weakened. In such cases, the victims can include governments, public and private insurers and those attempting to rebuild after the disaster. A related problem is the sale of substandard or defective materials, which victimise not only the purchaser, but also others, especially if the materials are used in critical functions such as construction, transportation systems, food supplies or health care, where failures can lead to catastrophic loss of life. This is one form of fraud in which indirect and non-economic losses, such the effects of delays in rebuilding housing and essential infrastructure, can be much higher than the actual proceeds taken by offenders.

n. *Pyramid or “Ponzi” scheme frauds.* These are schemes in which profits are generated for offenders through fees generated from the recruitment of additional participants by each initial recruit, in a geometric progression. Each recruit pays fees to others who were recruited earlier and are at higher levels in the scheme, and the geometric progression ensures very large numbers of recruits are quickly taken into the scheme. The fraud lies in the fact that numbers
of possible participants are quickly exhausted by the progression, deceptively depriving later recruits of their contributions and enriching earlier recruits. A scheme in which each recruit is asked to recruit five further participants, for example, requires almost 2 million participants at the eighth level of the “pyramid”, and more than 6 billion participants at the 13th level. Schemes of this nature are often disguised or presented as sales schemes in which profits are generated by the recruitment of further sales persons as opposed to the actual sale of merchandise, or investment schemes, and several States reported laws specifically prohibiting such schemes. Total losses can be very large and difficult to both quantify and recover, because they can accrue to a number of persons at or near the top of the pyramid. Effectively each person becomes a perpetrator of fraud on those he or she recruits into the scheme, but the intention to commit the offence can be difficult to prove against those who simply pass on a scheme devised by others.

o. Real estate or mortgage fraud. Some States identified specific forms of fraud in relation to transactions involving real property interests. Given the values involved, occurrences may be less frequent than some other forms of fraud but losses in each case tend to be larger, and may be suffered by individual victims on whom they have a disproportionate effect. Common variations include mortgage fraud, in which mortgage lenders are defrauded using false or misleading information about property to obtain mortgages, and title fraud, in which offenders impersonate title-holders, assume title to property and fraudulently sell or mortgage it. A further variant occurs when fraudsters may actually own property, but conduct a series of sham transfers, at increasing prices, to make it appear that the property is more valuable than is actually the case. Some schemes combine all of these elements.

p. Transportation or maritime frauds. Generally these depend on some element of deception relating to the movement of goods or accompanying documents or information, or to the means of transport itself\(^\text{28}\). Thus the proceeds of a fraud could be the cargo of a ship, for example, the ship itself, and in some cases, both. The frauds

themselves consisted of the use of false or deceptive information either to cause the shippers of goods to deliver them without proper payment, or to cause the recipients to pay for goods that had not been delivered or were not as ordered, and most rely on contextual elements such as the length of time needed to deliver physical goods, especially by sea, the time needed to obtain customs and other clearances, and uncertainties created by the fact that shippers may be unfamiliar with commercial laws and practices in recipients’ jurisdictions, and vice-versa. Some States noted connections with other types of crime and others suggested that the sophistication needed to perpetrate these types of fraud generally required the involvement of organized criminal groups. In addition to frauds targeting the value of vessels or cargoes, States reported other crimes related to maritime transport fraud. These included frauds related to the identification of vessels and in some cases possession or control of the vessels themselves used to procure the services of the vessels for trafficking in narcotic drugs or other contraband. Maritime piracy has been used to obtain documents or information, and in some cases actual vessels which were later used for frauds involving cargoes or fees. A number of cybercrime offences have been used in support of transport fraud, ranging from the taking over of computer systems in order to falsely order goods or indicate delivery and claim payment, to lesser intrusions used to gather information about documents or practices needed to make later fraud schemes plausible. Computer scanners and printers have also been used to produce document forgeries.

q. Frauds against government. A number of frauds against government were reported. Some States had separate offences for cases where government or public interests are defrauded, while others relied on more general offences, in some cases linked to aggravated punishments. There were substantial areas of overlap with some corruption offences. Specific types of frauds against government or the State included the following.

i. Benefits fraud, subsidy fraud or subvention fraud. States which have schemes which pay social benefits to persons in need reported the making of false benefit claims as a common form of fraud. These ranged from single individuals claiming or accepting benefits to which they were not entitled to elaborate schemes creating large numbers of completely fictional claimants or using genuine identity information to make false claims en masse. These overlap with insurance
frauds when the benefit schemes themselves are insurance-based, such as subsidised public health or unemployment insurance schemes in some States. The European Union operates a common or standard benefits system, and a number of European counties reported benefits-fraud offences adopted as part of that scheme.

**ii. Corruption offences.** A number of corruption-related crimes, including some of the offences covered by the *United Nations Convention against Corruption*\(^ {29} \) could also be considered as forms of fraud, and at least one of the responding State treats them as such\(^ {30} \). The bribery of a public official or sale of influence by such an official, for example, can be seen as the sale by that official of some form of preference or benefit which rightfully belongs to the government and not the official. The improper decisions or actions which flow from bribery deprive the public interest of something of value and illicitly transfer that value to the person who paid the bribe. Bribery can also be used in support of other frauds against the State by inducing officials who would normally be expected to prevent or detect fraud not to do so. Embezzlement offences may also be considered as variations of either fraud or theft, depending on domestic law and how the offence was actually committed in each case.

**iii. Economic fraud.** Government entities can be defrauded in much the same ways as other victims, and some States treat this as either a separate offence or a circumstance which aggravates punishment. Many also have either breach of trust offences or further aggravating conditions for cases where the economic fraud was committed by public servants or inside employees in a position of trust which was breached by the fraud. One of the types of economic fraud against government cited by a number of States was frauds against public procurement systems.

**iv. Immigration, passport and visa frauds.** As described above, these can be seen as frauds against persons wishing to migrate, or governments, or both, depending on the facts of each case.

---

\(^{29}\) A/RES/58/4, Annex, Articles 16-18.

v. **Insurance fraud.** The majority of insurance frauds target private insurance schemes, but government-operated or publicly-funded insurance schemes covering health, motor vehicles or social benefits are also targeted in countries where they exist.

vi. **Tax frauds.** Every State raises revenues from some form of taxation, and the reports suggest that most of those who responded consider at least some forms of tax evasion as frauds against the State or relevant tax systems. Specific types of tax fraud were as varied as the underlying tax systems they targeted. The more commonly reported were frauds which involved either withholding information or providing false information in order to reduce taxes otherwise payable, and the making of fraudulent claims against tax-refund schemes. These forms of fraudulent tax evasion are probably universal, but were identified as a particular problem by some States in varying degrees of economic transition, suggesting that it may be a specific challenge for those in the process of establishing new governance structures and tax systems, who must persuade the population to pay taxes. Several European States made similar references to fraudulent refund claims against their common VAT (value-added-tax) system. Several also reported the involvement of organised criminal groups in these frauds, and one reported a scheme so large that it caused significant harm to the national economy. A further category reported by some States was smuggling, which was in some cases seen as a fraud against excise tax systems. Smuggling offences may or may not fall within the scope of economic fraud for the purposes of the present study. The smuggling of contraband which is legal but taxed, such as alcohol or tobacco in many States, could be seen as defrauding the State of excise taxes, but the smuggling of prohibited contraband such as narcotic drugs would not be economic fraud, as there is no economic loss to the tax system, and any gain for offenders derives from the illicit sale of the contraband and not the evasion of tax or deception of a victim.

vii. **Counterfeiting stamps and currency.** Some States reported that they consider currency counterfeiting as a form of fraud. This could be considered as economic fraud against the State, in the sense that currency values are eroded. It may also be a fraud
against any person who suffers a loss when given counterfeit currency which is not redeemed by the State.

5. Liability of legal persons

Criminal liability entails moral culpability, high standards of proof, elements of intent and relatively severe punishments, which in some legal systems can only be applied to natural persons. Of the 27 States which provided information on this question, 16 indicated that they applied full criminal liability to legal persons, and a further 5 indicated that they did not extend criminal liability but did provide for administrative liability and appropriate punishments. One State which has full criminal liability also extends this liability to a wider category of organization wider than only legal persons, including both legally and factually-established bodies. All of the States which had criminal or administrative liability provided for fines and some included other measures, such as confiscation of proceeds or other assets, and specific remedies or punishments, such as orders barring specified natural persons from involvement in a company, and orders that the legal person be supervised or refrain from certain specified business activities.

A number of responses referred to the relationship between legal and natural persons in such cases and indicated that both could be convicted in the same case. At least one State noted that it also has administrative offences relating to theft and fraud which require direct intent as an element, and that as a result, these offences, even though administrative in nature, could not be committed by a legal person. Some States also mentioned civil liability, imposed not by the State, but by the courts in response to a private action brought by another party. This was usually the victim, although some systems now allow the State to bring a civil action and some have made provision for the recovery of civil damages based on a criminal conviction.

6. Punishments for economic fraud

Generally, punishments in most countries reflected the fact that economic fraud is not a violent offence, and that there is a very broad range of ways fraud can be committed and a broad range of degrees of harm it can cause. Example cases considered by the experts ranged from single offences with relatively minor harm to a single victim, to major corporate or commercial frauds and mass-frauds which have generated losses in the hundreds of millions of dollars and have caused large numbers of victims substantial harm. Several cases were serious enough to de-stabilise governments or cause damage to national economies, and the harm was not
necessarily limited to economic damages or proportional to the proceeds taken by offenders. Indeed, with serious frauds, indirect harm such as political instability or loss of consumer or shareholder confidence in a company can often far exceed the direct economic losses.

To cover the full range of frauds with appropriate deterrents and punishments, many States reported either a series of fraud offences of escalating seriousness or single offences with lists of aggravating factors which affected potential sentences that could be imposed by their courts. The most commonly-cited factor was the size or scope of the fraud, usually measured in terms of amount of proceeds. Most States also apply harsher punishments if there is evidence of repeat offending, and in some cases schemes which entail ongoing mass-fraud operations as a form of repeat offending subsumed within a single criminal charge or prosecution. Another common aggravating factor was the element of breach of trust or some kind of abuse of power or inequality between offenders and victims, reflecting both a need for added deterrence and the added damage such frauds can cause to institutions. Examples in this area included frauds by trustees, corporate insiders or public officials, and frauds against vulnerable victims such as legal persons, minors, the elderly, the mentally handicapped, and estates of deceased persons. One State indicated that the subjective impact of the fraud on victims could also be an aggravating factor. Additional deterrence was also used in some systems to extend added protection to certain documents or processes where the risk or threat posed by fraud was seen as particularly high, such as frauds involving real estate documents or transactions, frauds involving stock markets and related activities, and frauds exploiting religious belief.

Several States also reported additional sentencing powers where fraud was associated with other predicate offences, money-laundering or involved organised crime, and most either reported that some or all of their serious fraud offences fell within the meaning of “serious crime” in Article 2, subparagraph (b) of the Convention against Transnational Organized Crime, or provided descriptions of offences that appear to meet those requirements.

\[A/RES/55/25/Annex I\]. Note that Article 11, paragraph 2 of the Convention requires, \textit{inter alia}, that any discretionary legal powers be exercised to maximise the effectiveness of deterrence in respect of offences covered by the Convention, which would include serious frauds. The requirement in Article 11, paragraph 1 to apply sanctions that take account of the gravity of the offence only applies to the offences actually established by the Convention and Protocols, however, and would not apply in fraud cases.
requirements. Many States also had less-serious offences to deal expeditiously with relatively minor frauds and a range of related practices considered as commercially abusive but short of full criminal fraud, such as the use of deceptive or abusive practices in the course of advertising, bargaining or forming a contract.

Punishments which could be imposed ranged from 0-3 months for minor offences up to maximums of 30 years for more serious cases, and one State mentioned that mandatory minimum punishments applied to some types of fraud. Most countries also reported that fines or confiscation could be imposed in addition to imprisonment, and several also noted that specific conditions could be imposed, such as orders that the person convicted not be involved in certain types of commercial or other activity or not seek or hold political office. Depending on a country’s regulatory regime, this could also involve loss of licenses or the right to practice in critical professions or positions, such as law or accounting. Most of the States which responded extended either criminal or administrative liability to legal persons convicted of fraud, and in such cases had sentencing powers to impose fines confiscation orders and specific conditions.

Within the framework of legal sentencing powers, there is also the more practical question of how they are applied by the courts and the ability of prosecutors to produce evidence of the severity or seriousness of the impact of frauds. In sophisticated commercial frauds, the evidence may be complicated and difficult to understand, and this has caused some concerns for prosecutors, especially in legal systems where the trier of fact is a jury or magistrate without legal training. In mass-fraud cases, large numbers of victims cannot all be called into court, and it will usually be necessary to produce secondary or expert evidence of the true extent of harm and numbers of victims affected. In transnational fraud cases it may be difficult to have expert opinions or summaries admitted as evidence and some individual victims may not be able to travel32.

32 The last problem may be addressed in some cases by mutual legal assistance in the form of video-link testimony under Article 18, paragraph 18 of the United Nations Convention against Transnational Organized Crime, where applicable.
III. Assessing the scope and extent of fraud

1. The reporting and recording of fraud

Reporting and recording problems make it difficult to obtain accurate data from original sources, and difficult to assess the degree of accuracy of such data that are obtained. In addition, when comparing States or developing an international picture of the problem, approaches to the reporting and recording of offences and the need to avoid under or over reporting of transnational cases becomes a factor. Further, differences in national definitions must be taken into consideration. There appears to be substantial consistency with respect to core definitions, but there may be differences in areas where offences considered as criminal fraud in one State are dealt with in commercial law in others, and in the treatment of mass-frauds, which produce different results depending on whether victims or fraud schemes are counted.

There is widespread agreement among experts that fraud is systematically under-reported. 16 of the 17 States that expressed an opinion or provided evidence on this question expressed a similar view, as does earlier work on the subject of commercial fraud undertaken by the Commission on International Trade Law.33 Some States noted that, in addition to a general underestimation of the total extent or prevalence of fraud, under-reporting could also produce distortions in information about the relative prevalence of specific types of fraud because some specific types may be affected by under-reporting to a greater or lesser degree than other types. It was also noted that, in some countries, frauds may be reported to a range of different agencies, making the assembly of data into a comprehensive package a challenge. Aside from law-enforcement and other criminal-justice agencies, frauds in particular settings could be reported to commercial regulators, professional governing bodies and similar entities, as well as a range of private sector entities, and in federal systems, to both levels of government. While fraud is generally under-reported, taking account of the extent of duplicated or overlapping reports was also a concern for some States.

Many reasons were given for under-reporting, and most were consistent among States. The most commonly cited reason was the fact that victims are embarrassed or humiliated and seek to avoid the publicity inherent in criminal proceedings. One State, speaking of both natural and

33 UNCITRAL, Possible future work relating to commercial fraud, A/CN.9/540, 9 April 2003, paragraph 6, subparagraph (c).
legal persons, described this as fear of “reputational damage”. This appears widespread across different cultures, and may be most acute in cultures where bargaining is a part of every day life and skills and sophistication are the norm. It also extends in some degree to legal persons who are victimised and reluctant to report for fear of loss of confidence on the part of investors or customers, or that weaknesses in security or audit protections will be exposed. Some States noted that fraud could be seen as an appeal by offenders to the greed of victims, a fact which increases embarrassment. The perception by victims and others that victims are partly responsible for their own misfortune has been identified not only as an impediment to reporting, but also to an effective response by law enforcement and society in general. Many victims also fear self-incrimination. A number of States mentioned frauds in which offenders intentionally led victims to believe that they were accomplices in crime, making them reluctant to report, and law-enforcement less than sympathetic if they did report, the crime. The classic “419”, “Nigerian” or “West African” fraud is an example: victims are usually led to believe they are accomplices in a scheme to launder the proceeds of crime or corruption. Victims are deterred by the fear of self-incrimination or the threat that proceeds will be confiscated before they obtain them.

Some States and commercial entities also noted that victims often believe that claims will not be taken seriously or given priority by law enforcement, and at least one pointed out that apparent fraud rates tended to increase after public education campaigns which counter this effect by depicting fraud as a serious crime. Some commercial companies were reluctant to report offences due to what they saw as unsatisfactory responses from criminal justice systems in the past, and companies in areas where fraud is common tend to rely more on their own internal investigative and other processes than criminal justice measures to respond and recover losses. Several States noted that credit card issuers and other major companies tended to see fraud as a form of manageable business loss and that commercial data was gathered for commercial rather than criminal justice purposes and was not always made available to public authorities. Several States also noted that indicated that private sector entities such as

---

banks, insurance companies and credit-card issuers often had better information in specific areas, being more familiar with the technologies and practices involved and because victims had a financial incentive to report occurrences. In some areas companies had concerns that release of data about fraud might be sensitive in commercial or competition terms, and in others there may be concern about release of data that could weaken security or assist offenders. One State indicated that its laws made it an offence for banking or public officials not to report crimes of which they became aware.

Fraud is also a crime of deception, and offenders often incorporate elements intended to reduce the likelihood that victims will complain when developing schemes. In some frauds, victims may not realise that they are victims of crime and not just a bad bargain. In others, such as charitable fraud, losses are suffered by others or are indirect or intangible and victims may never become aware of them. A related factor may be the fact that the same fraud can appear differently to victims and criminal justice officials, especially in areas such as commercial fraud and mass-market fraud. Where law enforcement may be aware of an ongoing, large-scale fraud operation and engage substantial investigative resources, the individual victims may see only their own losses and conclude that these will be seen as not worthy of a major investigation. As noted above, another factor in some cases is that victims are more concerned with recovering their losses than engaging the criminal justice system and are thus more likely to complain to banks and credit-card issuers than law enforcement. Fear of retaliation was not reported, but is a possible further explanation, particularly with respect to locations and types of fraud reported as being associated with organised criminal groups.

To confirm the degree of under-reporting and estimate the true extent of the problem, it is necessary to compare reported rates of victimisation with actual rates, usually obtained by extrapolating mass-surveys of population samples. This must be done in some detail, as the factors which produce under-reporting do not apply equally to all types of fraud and could also vary depending on the characteristics of victims or other factors, producing distortions as well as general under-reporting. Only one State indicated that it had gathered such information, although several others indicated that they saw a need for it and that projects to

obtain it were under consideration or development. Several States expressed concern about the quality of available data and indicated that measures were already under consideration to obtain a more accurate and complete picture. Aside from the need for basic information about rates and trends of fraud occurrences in general, some States saw a need for more detailed information that would show how frauds were committed and identify changing patterns to support both policy and legislative development and education and prevention programmes. In the State which did report data, approximately 30% of persons who told the mass-survey they had been victimised had also reported this to official sources, but 67% had reported it to appropriate private sources, such as credit-card issuers or banks. This supports the conclusion that only a small fraction of overall fraud is reported, and that victims are more concerned with recovering their losses than with criminal justice measures.

Some States also discussed practical concerns with respect to reporting and recording of data. Several mentioned the need to obtain as much of the available data as possible for commercial sources and the need for these to be compatible with public practices for gathering and analyzing statistics. One noted that it had a range of commercial, criminal and other legal or regulatory frameworks and agencies to which specific types of fraud could be reported, raising the need to coordinate data from all sources and eliminate any duplication in order to get an accurate picture. Similar issues are likely to arise in federal systems where there could be duplication between federal and regional reporting and in respect of frauds occurring in or reported to more than one region.

2. The quantification of fraud

Even with accurate statistical data, fraud can be difficult to quantify or compare within and among States because a different picture can present itself depending on what aspect of fraud is counted and how types of fraud are classified. The counting of fraud cases can produce substantially different results depending on how cases are reported and recorded. Statistical practices vary, but generally mass-marketing fraud schemes tend to produce large numbers of cases if occurrences are based on counting numbers of victims or complaints but lower rates if numbers of offenders fraud schemes or prosecutions are counted. For practical reasons prosecutions tend to focus on offenders and treat mass-victimisation by the same offender or group as a single large fraud rather than many small ones.

This is further complicated in the area of transnational frauds, where some States may be counting victims while others count offenders in the same cases.
A third picture may well emerge if the standard for quantification is the amount of losses or proceeds of fraud, because areas such as commercial fraud tend to involve small numbers of offences with very large losses, while mass marketing frauds involve very large numbers of smaller offences, but can still generate very substantial proceeds. Also, quantification of losses to victims and proceeds in the hands of offenders can provide different results. In simple frauds there is often a direct link between losses and proceeds, but in the case of some complex fraud schemes, corporate frauds and pyramid or “Ponzi” schemes, the indirect losses and non-monetary damages can far exceed any proceeds realized by offenders or recovered by authorities or victims.

Few countries had statistics that allowed for detailed reporting of fraud losses. Some specific areas of the private sector, such as the insurance industry and credit card issuers do maintain records or estimates of losses, although some of these are seen as sensitive proprietary information. Conceptually, fraud losses include not only the direct economic losses to victims, but also indirect losses to victims and commercial structures, as well as additional costs associated with prevention, detection, prosecution and the civil or criminal recovery of losses. Further damage may occur when the often-substantial proceeds of fraud are made available to organised criminal groups or terrorist groups to fund their other operations. The allocation of losses also varies, especially in commercial contexts.

3. Rates and trends in fraud

Most of the States which provided information about rates and trends in fraud did not provide concrete statistics, but expressed the view that fraud in general has been increasing. Of 28 responses, 24 reported either general increases in fraud or the belief that such increases existed, with two States reporting declines and two reporting information they saw as either inconclusive or suggesting increases or decreases too small to estimate or measure. Most of the experts also saw increases based on their own evidence and experiences, and experts involved in earlier UNCITRAL work on commercial fraud had the same conclusion36. A number of States expressed the view that there was a connection between overall increases in fraud, increases in some specific categories of fraud, including

---

transnational cases, and the expansion of access to information, communications and commercial technologies and systems, both by offenders and potential victims.

Only five States were able to provide statistical data, and of these two found increases in numbers of victims or total proceeds of fraud. One reported data which were inconclusive and the fourth reported decreases, but noted that these might be attributable to changes in the reporting and recording of crime rates. One State reported very large increases, of up to 1,400% in the seven-year period from 1999-2005, and another described “dramatic” increases in the use of information and communications technologies by offenders both to defraud victims and to transfer and conceal proceeds. One State provided long-term data that suggested that increases in frauds involving credit and debit cards and decreases in frauds using cheques and other paper documents corresponded to a similar shift in consumer and commercial practice from the early 1990s to the present time.

Many States indicated that within the overall scope of fraud, occurrences involving transnational fraud were increasing as well, and a number of these States reported either evidence or the belief that increases in overall fraud, and in particular transnational fraud, were strongly linked to the increasing use of the Internet and other information and communications technologies, and related commercial technologies by offenders and victims. This is also consistent with earlier assessments by the Commission on International Trade Law and concerns expressed by the U.N. Legal Advisers37. One State noted that its officials have seen steady increases in overall fraud, and that within the scope of overall fraud complaints, transnational fraud appeared to be increasing at a greater rate than fraud in general. One State also noted that fraud was more commonly encountered in transnational transactions than in transactions in general.

Generally, the States which expressed strong concerns about the role of information technologies reported either high rates of access to and use of the technologies, or rapid expansions in such access, both of which would be expected to lead to high and increasing rates of fraud occurrences. However, one State which did provide statistical information noted that the basic increases in transnational fraud continued even in years where the sub-category of Internet fraud was decreasing or stable, suggesting that either overall fraud may be increasing in part due to factors other than

---

technologies, or that possibly the increases might be due at least in part to
technologies other than the Internet, such as telephones.

The convergence of technologies raises methodological and policy
issues in this area. It is becoming increasingly difficult to distinguish
between technologies in the context of Internet-based telephone, e-mail, fax
and other services, which makes it difficult to analyze and compare
statistical data and complicates the regulatory environment in many States.
Analysis is further complicated by the fact that many frauds involve the use
of several technologies or use of the technologies in different ways. Aside
from basic use of the Internet to contact and defraud victims, for example,
it has also been used in preparatory and supportive roles such as to
download false documents or e-mail stolen credit card data, which might or
might not be considered as Internet fraud for statistical purposes. In some
cases the growing concern has also led to public-education efforts and
mechanisms such as Internet websites and dedicated telephone lines to
assist victims or others in reporting fraud, which also tends to increase
reporting rates independent of occurrence rates. However, the available
evidence strongly suggests that much of the apparent increases reflects real
and substantial increases in actual offending rates.

Information provided by States generally did not address the
question of whether the substantive scope of fraud is increasing, but the
examples provided and other evidence suggest that the range and diversity
of offences has also expanded significantly, especially in those areas
influenced by factors such as economic transition and the expansion of
information technologies, which change the environment in which offences
are committed. New variations are in some cases entirely new types of
fraud, but more commonly can be seen as variations on long-established
schemes with modifications to take account of new opportunities or risks
associated with technologies or current events in order to keep the frauds
plausible. Frauds which appear new to the authorities of one State are in
some cases variants of long established schemes found elsewhere which
have moved from place to place, as local conditions have made them
possible to commit and the necessary expertise has been transferred,
offenders commit them from abroad, targeting new regions, or the
offenders themselves have moved. Whether there is real expansion or not,
the scope of fraud offences encountered by States and the commercial
community is clearly very broad, reflecting the full diversity of legitimate
commercial activity within and among the Member States.

Several critical questions arise for the gathering of data on fraud
levels and for global comparative statistical analysis. As noted, under-
reporting makes it difficult to assess real occurrence levels and may distort
information about the relative prevalence of different types of fraud. Another consideration is whether each country’s legal system treats the targeting of many victims in a single scheme by a single group of offenders as one occurrence or many. Population trends may also have an effect: several States reported that access to and use of information, communications and commercial technologies was more prevalent in urban areas than rural ones, and noted regional differences in commercial practices for example, and others reported data suggesting that specific forms of fraud and criminal techniques may migrate from one place to another with offenders. Fraud imitates legitimate commerce, making variations of commercial practice likely to produce parallel variations in fraud over time, between countries or regions, and with respect to specific areas of commerce. Conditions such as post-conflict reconstruction and major economic development or transitions can also have a substantial impact on fraud, as the confusion between old and new economic principles and specific activities such as major reconstruction efforts and the privatisation of State-owned operations provide opportunities for fraud offenders. Several States noted that data reported were divided among general criminal justice agencies, specialised regulatory agencies, in federal States among agencies at different levels of government, and in the private sector among a range of commercial companies gathering specific data for specific commercial purposes, and that assembling and comparing this data required a substantial effort both to identify gaps and to assess and compensate for double or multiple reporting.

IV. Relationship between economic fraud and other problems

1. Fraud and the involvement of organised criminal groups

Serious frauds can be committed by individuals, but both the views of the experts and the responses of States suggest that the great majority of serious frauds involve “organised criminal groups” of three or more persons within the meaning of Article 2, subparagraph (a) of the Convention against Transnational Organized Crime. States described both frauds committed by or on behalf of long-established organized criminal groups, and the establishment or organization of new groups specifically for the purpose of fraud and related crimes. Established groups are attracted by the large potential proceeds, relatively low risks and possibly

38 A/RES/55/25/Annex I, see in particular Articles 2 and 3.
also complementarities with other criminal activities in which they are engaged. Two joint studies of transnational mass fraud by the United States of America and Canada, and made available to the expert group, expressed concerns about the attraction of traditional organized crime elements into this type of fraud\(^\text{39}\). A number of States also reported the involvement of smaller, more flexible groups in some forms of fraud such as debit-card or credit-card fraud, sometimes moving from place to place in order to avoid law enforcement and target fresh victims. A further possible scenario is raised when frauds are committed by or on behalf of legal persons. In some cases companies have been established expressly to perpetrate or conceal frauds. Large corporations have also been implicated in frauds against the general public or investors, and in some cases companies are defrauded by groups of employees acting from within. Where a group of employees or the company itself becomes involved in fraud, they or it may become an “organised criminal group”. The Convention definition excludes purely *ad hoc* cooperation between offenders by requiring that the group must have acted in concert and over a period of time, but given the extensive planning and preparation needed to successfully perpetrate a major fraud or mass fraud, few such fraud cases would be excluded by this requirement.

Most of the States which responded to the survey reported some degree of involvement or suspected involvement of organized crime in fraud occurrences, and many reported some types of fraud as more likely to involve organised groups than others. A further concern noted by some States was that frauds by organized criminal groups were seen as more harmful because there was not only the question of losses to victims, but the fact that the proceeds were used for corruption or to otherwise strengthen the activities or influence of organized crime itself. This is a particular concern in countries or regions with economies in transition, where institutions are weaker and well-financed organized criminal groups

were therefore a much greater threat. Of the States which reported a range of fraud offences and punishments, several reported that proof of the involvement of organised crime was a triggering condition either for more serious offences or harsher punishments. Several also mentioned their anti-organised crime legislation as measures that were or could be useful against serious fraud cases, especially in areas such as investigative powers, sentencing, and the tracing and confiscation of proceeds.

Two patterns of organised criminal involvement in fraud could be seen in the examples provided. In some cases, reports described sophisticated and complex frauds, which would be consistent with the gradual development and evolution of such schemes by established organized criminal groups rather than individuals, and with the transfer of the more successful fraud expertise as individuals form new groups or move from one group to another. At least one respondent suggested such an evolutionary process. This pattern was typified by some forms of large-scale commercial fraud, and some forms of mass-market consumer fraud in which established “boiler-room” operations targeted large numbers of victims over long periods. The other pattern in the reports suggests a substantial amount of fraud committed by smaller, less-sophisticated groups. A number of States reported offences such as payment-card fraud and frauds against public subsidy or benefit systems by smaller organized groups, often moving from place to place to avoid law enforcement and target fresh victims. One State had accumulated sufficient numbers of cases linked to organised crime to conclude that there were also links between the type of transnational fraud encountered and the specific organized criminal groups committing them or the regions in which those groups were based. In some cases this might be attributable to factors such as the availability of technical media needed to commit the fraud, and in many it is also likely that it is due to the regional spread of specific expertise or skills needed to commit a particular type of fraud.

As noted, most States have a range of fraud offences and punishments, and the majority either stated that their more serious offences fell within the definition of “serious crime” in Article 2, subparagraph (b) of the Convention, or provided sentencing provisions that would appear to meet the principal requirement, liability to maximum possible punishments of four years or more. 21 States appear to meet this standard, 3 do not, and the remainder did not provide sufficient information to make an

40 See also Commission on International Trade Law, “Possible future work relating to commercial fraud”, A/CN.9/540, paragraphs 3, 8 and 9.
assessment. This means that in most cases, the *Convention* could be applied for mutual legal assistance, extradition and other forms of cooperation where the fraud alleged was also transnational in nature and involved the requisite “organized criminal group”. A number of States expressed the view that its existing provisions were sufficient to deal with the problem, and several emphasized the need for work in areas such as technical assistance and training to ensure that the *Convention* could be used as effectively as possible.

2. *Fraud and the element of transnationality*

None of the responding States had statistical information based on transnationality, but transnational fraud is common and many national experts have had extensive experiences with it. Many States indicated that they had seen at least some cases, while others did not mention cases, but were aware of and concerned about the possibilities. The major concern expressed was that transnational frauds appear to be increasing in volume, and that while they can be relatively easy for offenders to commit, they are much more costly, difficult and complex to investigate than domestic frauds. Some States have seen evidence that offenders intentionally exploit this difficulty by targeting only victims well away from the jurisdiction of their own local law enforcement\(^41\). Other States reported examples of frauds perpetrated by small groups of offenders who travel within and among countries as a means of targeting fresh victims and avoiding prosecution.

A number of States noted a relationship between transnationality and information, communication and commercial technologies. They tended to attribute both general increases in fraud and increases in the portion of all fraud cases which involve some element of transnationality to the increasing availability of technologies to offenders and potential victims. The most obvious relationship between technologies and transnationality is the simple fact that any modern communications

medium, including fax machines, e-mail, telephones and the Internet can be used to establish contact between offenders and victims and transmit the deceptive information which lies at the heart of economic fraud, and many States described examples of the use of all of these media in fraud cases.

A number also noted other ways in which fraud, transnationality and technologies are linked. One State noted that information and communications technologies make it possible for offenders to cooperate effectively with one another while working from several different jurisdictions. Cases of this kind often involve offenders with the nationality of one State, operating from another State, targeting victims in one or more additional States, and concealing proceeds in a further different State. Others noted that information used in frauds itself becomes an illicit commodity which can be purchased, sold and transferred electronically, and at least two examples were provided. Lists of victims or persons likely to be vulnerable have been transferred from one criminal group to another, and credit card data obtained by “skimming” and copying legitimate cards or gaining unauthorised access to commercial credit card files is often quickly e-mailed to other countries so it can be used to create duplicate cards before the originals are cancelled. Technologies and transnationality are also used by offenders in an effort to complicate and frustrate criminal investigations or conceal the true nature and origins of the operation from potential victims. At least one State has seen the use of telephone call-forwarding technologies to make it seem to respondents that calls from abroad are of local origin, and the use of e-mail forwarding, anonymous re-mailers and similar technologies is a well-known technique for concealing a range of cyber-crime offences from detection and tracing back to the offenders.

In addition to the role of technologies in committing conventional forms of fraud across national borders, several States described frauds which are inherently transnational in nature or some form of cross-border activity was a central part of the fraud. Examples included the smuggling of goods to avoid paying customs fees, a range of maritime-transport frauds, and immigration, passport or visa frauds. Generally, these frauds depend on either the uncertainties created by the application of different legal rules or commercial practices or the delays inherent in some forms of transnational movement of goods. Immigration-based frauds depend on the

\[42\] See, for example, Libman v. the Queen [1995] 2 SCR 178 (Supreme Court of Canada) and Secretary of State for Trade v. Markus [1976] A.C. 37 (United Kingdom House of Lords).
desire of victims to migrate from one country to another, for example, and on their lack of understanding of the immigration laws in the State to which they wish to move. Many maritime and other transport frauds exploit the time needed to physically deliver goods and clear national customs procedures to allow offenders to make off with the payments or divert the goods. Use of third countries was encountered as an element of money-laundering schemes and some tax frauds, where records, other evidence, or assets were concealed out of the reach of investigators, or as an element of some Internet frauds where multiple jurisdictions were used to make the tracing of e-mail or other communications difficult.

3. The role of information, communications and commercial technologies in fraud

(i) Assessing the role of information and communications technologies

Most States do not keep records or have offences dealing specifically with the misuse of technologies in the course of fraud offences: fraud offences may or may not involve technologies, and cybercrime offences include conduct other than fraud. However, there are clear links between the availability of information and communications technologies and the use of commercial technologies such as payment cards and electronic commerce, and clear links between commercial technologies and many types of fraud, and as noted above, a range of different ways in which technologies can be used to commit or support the commission of frauds. States which reported data on trends in information and commercial technologies generally described patterns which suggest a significant increase in information technologies, accompanied by a more gradual shift to the corresponding commercial technologies, and a corresponding shift by offenders to frauds which target or exploit commercial technologies and which take advantage of information technologies to reduce risks and increase potential proceeds and numbers of victims. States which did not have concrete data either reported similar observations on the part of their experts, or indicated that they expected or were concerned about such a relationship under the circumstances.

The limited statistical information which is available should be treated with caution, for several reasons. First, the implementation of basic information and communications infrastructure and the commercial technologies it supports, as well as related technologies such as security measures for commercial transactions are still very much a work in progress in many States. They are still in the process of being deployed by service providers and commercial interests, and patterns of use by both
legitimate users and offenders are still evolving. In this environment, rapid and unpredictable changes in offending rates are possible as new crime techniques and new crime-prevention techniques suddenly come into use, and some such changes were described by States. Second, the responses of States in criminal and commercial legislation, law enforcement and other areas is also still evolving, and frameworks for gathering and analysing statistics may not have kept pace with this evolution. Third, the ways in which technologies are converging and the variety of ways in which they can be used to commit fraud make consistent statistical analysis over time difficult and complicate efforts to compare data from different sources or different countries. For example, classifications such as “computer fraud” could include the use of the Internet, e-mail or telephones to defraud, as well as less-direct involvement such as the use of computers and printers to produce fraudulent documents.

Fourth, technologies are also being increasingly used both by commercial and State entities as a means of educating and warning potential victims and as a means of collecting complaints or reports from victims. Several States drew attention to dedicated telephone services or Internet web-sites where victims could easily, and in some cases anonymously, report frauds. In general, these tend to increase apparent occurrence rates without any increase in actual occurrence rates, as a greater proportion of frauds are reported, and they may also increase sampling biases, if certain types of victim become more likely to report cases or have easier access to the reporting mechanisms. Internet reporting sites, for example, would be expected to produce a more accurate reflection of Internet-based frauds, where victims by definition have Internet access, than document or telephone-based frauds, where victims may not necessarily have Internet access. Finally, data on fraud are often reported through multiple channels, raising the possibility of gaps, double-counting of occurrences or other problems.

(ii) Use of information and communications technologies by offenders

The most common offender use of technologies was as the basic link to contact and defraud victims. Specific methods vary from one type of fraud to another, but generally, the process involved initial identification or selection of victims and contact, the making of a deceptive solicitation, a response by the victim and the transfer of funds, first from victim to offender, and then onward by the offender for purposes of laundering and concealment. Technologies were used to link offenders together and to transfer information such as credit card data, lists of potential victims, or
general expertise from one offender or group to another, or to enable attenuated groups or clusters of offenders to collaborate in large multinational fraud schemes. Technologies were also used by offenders to conceal their true identities and locations, both to avoid making victims suspicious and to avoid investigation and prosecution. The automatic forwarding of e-mail or telephone calls, postal “drop boxes” and similar means were used as a way to make the tracing of communications as difficult as possible.

Technologies were also used in other supporting roles. These included the use of scanners and printers to produce high-quality document forgeries, which then became either the primary means of fraud or were used to support the credibility of other means being used. False financial instruments might be sold directly for example, or false letters of introduction generated for use by offenders. Another potential role, especially for the Internet, is research by offenders, who gain access to background information needed to make fraud schemes plausible and credible. The Internet has also been used to disseminate false information as part of wider fraud schemes to bolster the credibility of a particular fraud or to manipulate markets to give offenders an unfair advantage. Such market manipulation ranges from making false bids on individual auction sales to attempting to affect the values of the stocks of large corporations.

Technologies are also used to launder proceeds, but there are some differences between their use in fraud and in money-laundering in general. Unlike other predicate offences, funds are usually transferred at two stages with fraud, and these often exploit different technologies. Offenders must first induce victims to transfer funds to the offenders themselves, for which speed, ease of access by victims and irrevocability are selection criteria. Some States noted that credit card payments are often selected by offenders because victims have and will use them, but that wire-transfers are chosen where possible because they are fast, irrevocable if the victim later reconsiders, and can be made difficult to trace. Funds are then transferred onward in the course of money-laundering in essentially the same ways and for the same reasons as funds from any other predicate offence. In money-laundering, offenders generally seek concealment and security for and access to their proceeds, and in some cases, ways to transfer funds which will not attract the scrutiny of anti-money-laundering mechanisms. This may be easier with mass frauds, as they may be arranged so as to take the form of large numbers of smaller transactions as offenders pass on the funds from each victim separately.

Many examples of specific uses of technologies were cited. The most commonly cited occurrences for basic offender-victim contact were
frauds in Internet auctions and a range of what some States describe as telemarketing or mass-marketing frauds. A number of States also reported the use of e-mail to quickly transfer payment card data from one country to another. The digital data would be obtained by “skimming” with card-readers, combined with identification information from the face of the card in an e-mail, and transmitted to cooperating offenders in other countries, who would be able to produce accurate duplicate cards quickly enough to use them before any alerts were circulated by law enforcement or card-issuers. Several respondents noted the need for very rapid information-sharing, both among countries and among private sector companies, to address these problems. Several States also described varieties of compound fraud in which technologies played multiple roles. For example, in a single fraud, the Internet might be used for mass-advertising, generating lists of contact information for those whose responses suggest interests that make them likely victims. That information is then used to target victims individually using e-mail, postal mail or telephone solicitations, with funds transferred using credit cards or wire-transfers.

Some States which did not have separate statistical information for frauds involving such technologies had nevertheless adopted specific offences of computer fraud. Many States also have specific offences dealing with credit card fraud, and others have cybercrime offences such as gaining unauthorized access to computer systems or the illicit possession or use of passwords or hostile software programs that would apply to preparatory conduct in many fraud cases. Regarding the types of technology most likely to be involved, most countries focused on the Internet, although telephone fraud is also a serious problem in regions where the conditions (e.g. common language) are favourable. Some States noted that they have seen evidence of offenders modifying their methods to keep pace with technological change. Long-term evidence of this can be seen, as noted above, in the development of various forms of payment card fraud. One example of this provided by a number of States was the use of card readers and miniature video cameras to generate fraudulent debit cards and PIN numbers. Another example was the use of automatic systems to forward e-mails and telephone calls to conceal the foreign location of

---

43 Some of these States were Parties to the European Convention on Cybercrime, ETS No.185, 23 November 2001. Article 7 of the Convention requires criminalisation of computer forgery, and Article 8 requires criminalisation of computer fraud.
offenders from law enforcement agencies and from potential victims who had been alerted to the risks of foreign solicitations.

(iii) Use of technologies to prevent and control fraud

While technologies provide opportunities and reduced risks for offenders, several States noted that they can also be very effective in preventing, controlling or deterring fraud, and a number of specific examples or suggestions were raised. The use of technologies against fraud and similar crimes is also a critical issue for the private sector, and was raised by some States as a key area where effective cooperation between public and private entities was needed. Cooperative investigative measures offer benefits for law enforcement, but also tend to confront commercial entities with the pressures of protecting privacy and other customer interests and ensuring that operations remain competitive and commercially viable. Preventing fraud and cybercrime is also a major commercial issue in its own right. Companies whose operations are vulnerable to crime represent a substantial market for countermeasures. This makes security and crime-prevention elements an important part of the research, development and marketing of information and communications technologies, especially those intended for use in commercial or financial applications. A number of companies specialise in security products and training, and most of the major hardware, software and telecommunications providers have substantial in-house capacity.

A number of States mentioned the importance of ensuring that innovation in crime-control kept pace with the development of new technologies, and cited this as an area of particular importance for cooperation between the public and private sectors. Aside from the general participation of representatives of public and private interests, some of the issues raised suggest that fairly broad-ranging expertise on both sides would be needed. On the public side, this could include not only technical law enforcement, but also interests such as privacy and industrial development, legislative policy, and international relations. On the private side, expertise on the engineering development of new technologies, their use in foreseeable commercial applications and in security and loss-prevention would all be important. A number of countries noted concerns about frauds being committed using computer network media, especially e-mail and the Internet itself, and one noted that on the public sector side coordination between investigators trained in cybercrime and fraud techniques was important. One response also noted that in a global environment for information, communication and commercial technologies, ensuring balance between crime-control, commercial and other elements at
the global level was essential to the support of effective international cooperation.

Technologies support the prevention, investigation and prosecution of fraud in a number of different ways. Electronic communications among offenders and between offenders and victims are vulnerable to interception, and if intercepted can be recorded for use as evidence. Unlike more ephemeral means of offender-victim communication, information technologies also create records, if not of the content of communications, then usually of “traffic data” which establish when and where a communication took place, and between which devices. This can be used to great advantage for both investigative leads and as evidence in criminal or civil litigation if properly obtained and preserved\(^4^4\). In some cases, computer technologies used to support large volumes of commercial transactions can be configured to monitor these for any aspects seen as suspicious or characteristic of fraud and to alert authorities for purposes of investigative follow up. One State also noted that communications data could be used to trace and identify victims, especially in mass frauds, if recovered during an investigation.

Many telecommunications and computer security applications also help to prevent fraud. Electronic commercial communications and stored data are usually protected from unauthorised access by firewalls, encryption and similar applications. Security experts generally recommend that these be accompanied by the establishment of security practices and training of staff in how to use applications effectively and the avoidance of practices which might render systems vulnerable to outside attack. Private sector sources indicated that a significant proportion of corporate and commercial fraud was perpetrated by or with the assistance of employees with inside access to systems or information, and that both technologies and practices should allow for this with redundancy elements, effective auditing and surveillance, and most important, policies to inspire employee loyalty and vigilance. Telecommunications technologies can also be used in a preventive capacity, to identify, contact and educate or warn potential

\(^4^4\) See, for example, European Convention on Cybercrime, ETS #185, 23 November 2001, Article 1, subparagraph (d): “traffic data’ means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service”.

275
victims. This usually involves using the same techniques as offenders to select victims and the same means of establishing contact, such as telephone calls or mass e-mail circulations. Many Internet and telecommunications service providers also monitor developments in fraud and alert their customers to new developments before they can be targeted by offenders.

States mentioned a wide range of specific crime-control innovations, some appropriate for the operators or users of commercial systems and others more in the domain of State law-enforcement authorities. These included the use of video-cameras to record images at cash-dispensing machines, computer chips or other security measures to make debit and credit cards harder to forge and easier to verify, more sophisticated access codes for customers and system users, such as the use of both Personal Identification (PIN) Numbers and Transaction (TAN) Numbers, and the use of digital signatures and other encryption applications. One State noted that a global approach was needed for some measures, such as those incorporated into credit or debit cards used by travellers. If all countries did not implement such measures, the result in places where they were not implemented would either be cards which could not be used at all or cards that could be used, but without the protection of the added security elements. Innovations more appropriate for investigative and other law enforcement purposes included “honey-pot” accounts maintained by law enforcement to attract and trap offenders and secure web sites and networks on which information about new cases or other developments could be posted and shared.

Other technologies are used by service-providers and law enforcement to locate, identify and gather evidence against offenders. Viruses, Trojans and other hostile software programs may be analysed to obtain information about who created them, for example, and other software can be used to locate evidence or screen large commercial systems for suspicious transactions or patterns that might suggest fraud. General or targeted messages about frauds can also be used by private companies to alert law enforcement or potential victims to new or ongoing frauds and vice versa. Some States noted that security technologies are also in use by offenders. Encryption is used by offenders to shield communications and data from surveillance and avoid anti-money laundering measures; devices such as card-readers and miniature cameras are used to copy payment cards; up-to-date wireless devices are used to communicate in ways which are difficult to intercept; electronic cash cards and other devices may be used to launder proceeds; and flash-memory and other compact memory devices are used to conceal electronic evidence.
The question of the retention of traffic data has been under discussion for some time, and was raised by several States. Retrieval of such data is needed to trace communications, linking offenders, victims and proceeds both for investigative and evidentiary purposes, and law enforcement would prefer that such data be kept indefinitely. Service providers tend to erase it once billing and other commercial uses are completed, both to protect customer privacy and limit the costs of storing the vast amounts of data involved. Requirements which target specific information can only be imposed once it becomes apparent that it is needed for a criminal investigation, and by this time the data may already have been lost. Retention is a particular concern in major transnational fraud cases because of the added importance of tracing communications and identifying and locating offenders, the use of multiple jurisdictions and technical elements by offenders to conceal their true locations, and the complexity and length of time needed to conduct successful investigations. Compromise requirements for retention for limited periods have been discussed, but the major focus of States which have dealt with the issue at all has been to develop requirements that support rapid retention requirements targeted at specific information once it can be identified and rapid responses to mutual legal assistance requests that ensure data will be preserved while formal proceedings are completed. Several States raised the importance of relatively rapid information sharing and other cooperation in such cases. A related issue is the need for laws and technical systems which ensure that both traffic data and substantive content resulting from all types of electronic communications meet basic standards of reliability both as investigative information and for eventual use as evidence in criminal and other legal proceedings.

(iv) Use of commercial systems and technologies

Given that many forms of fraud involve the manipulation or exploitation of common commercial technologies, substantial relationships between technologies and fraud are to be expected, but most States had only anecdotal information or expert assessments of these relationships. There are links between the use of commercial systems such as automated bank teller (ATM) machines and the information and communication technologies needed to support them, and where technologies are available, there are also likely to be significant differences in how they are used by

different types of commercial enterprise and in different regions. For this reason much of the data is more likely to be found in a wide range of commercial sources than in centralised State criminal justice statistics.

Several States noted in their responses that there was a complex relationship between information technologies and commercial systems, which was likely to vary depending on availability and the commercial practice that offenders needed to imitate with particular frauds. In the case of transnational frauds, commercial systems in both offender and victim jurisdictions would likely exert an influence. Given a choice, offenders may be expected to exploit whichever commercial systems best support the specific fraud at hand and reduce the probability of detection, identification and prosecution. As noted, that choice also often leads to the use of different technologies at different stages of the same fraud.

Offenders must find ways to transfer funds, not only for purposes of laundering after the offence, but in order to obtain them from victims during it. Offenders have the same need for secure and reliable structures as does legitimate commerce, to ensure reliable access to their proceeds, but their selection of commercial payment systems also takes into account the fact that their intended victims must have ready access to them, which tends to favour credit cards and direct deposit or other electronic transfers where available. Some States noted that fast and irrevocable transfers are also preferred by offenders as a means of completing the fraud before victims could seek advice or have second thoughts about the merits of the transaction, and some noted that their laws required commercial systems and practices to include mandatory delays or periods in which transactions could be reversed or contracts rescinded.

Some States also noted that commercial systems also have a dual aspect, with some elements supportive of criminal opportunities or activities, while others were more supportive of crime-prevention or control. Commercial or technological change could produce both positive and negative displacement, shifting criminal behaviour into more or less harmful patterns, both by creating new opportunities for offenders to obtain greater proceeds and by creating new risks of criminal liability. A further concern in the context of transnational fraud is that the application of new controls in developed countries might displace offending into developing countries less able to deter or prevent them, and also less able to withstand the costs.

The most widely recognized links between fraud and specific commercial systems are to payment (credit and debit) card systems, and it could be said that the establishment and proliferation of payment cards and the related technologies has virtually created some of the more common
forms of contemporary fraud. One State noted that commercial systems could be seen as both targets and instrumentalities for fraud offenders in some types of fraud, such as credit card fraud. Of those countries which did report statistical information, the long term statistics of some did show a gradual shift from paper-based cheque frauds to credit cards that roughly corresponds with the uptake of the technologies in general commerce. Conversely, some countries which reported that information, communication and commercial technologies were less accessible, especially in rural areas, also indicated that fraud and identity frauds involving these technologies were relatively uncommon, although some expressed concerns about problems such as Internet fraud as their technological infrastructures expanded. Some of those States indicated that commercial systems still tended to be paper-based, and that fraud patterns reflected this, and in such States, there was greater concern about the use of computer technologies to produce high-quality document forgeries than frauds which attack or exploit electronic commerce or communications aspects of these technologies.

Some States also raised the human element in commercial systems, and the need to incorporate anti-fraud elements in training materials and everyday practices. These included elements such as vetting, screening and surveillance for employees, especially those in positions to commit major forms of fraud, training in how to recognize and prevent appropriate forms of fraud, and specific practices such as customer-identification, accounting practices, and appropriate scrutiny for loans and other transactions to ensure the parties were protected. One State noted that some of these were already requirements as precautions against money-laundering. Commercial sources noted that controlling and preventing fraud required a comprehensive approach, but that as about half of all frauds against legal persons involved inside employees, measures intended to instil values, ethics and employee loyalty were the most important measures, having the potential to convert employees from potential offenders to a source of prevention, reporting and deterrence⁴⁶.

4. Fraud, the proceeds of fraud and money-laundering

Fraud and money-laundering are linked, but were seen as distinct issues by most States. Fraud was seen as an economic crime in the sense that its purpose or motive was to generate a financial or other material

benefit for the offenders, whereas money-laundering occurred in an economic environment, but was not seen as a form of economic crime because its purpose was to conceal and transfer proceeds only after they were already generated by other crimes. Aside from providing relevant legislation, most responding States did not comment extensively on anti-money laundering measures. Some noted that, while fraud and money-laundering were connected and there was a need for coordination in developing responses, money-laundering was already the subject of extensive work in other bodies and that future work on fraud should avoid any unnecessary duplication of effort. From a substantive standpoint, most States either indicated that fraud is considered as a predicate offence for purposes anti-money laundering measures, or provided provisions in which this appeared to be the case. A wide range of civil, criminal and evidentiary provisions governing the freezing, seizure, confiscation and return of the proceeds of fraud were included in the responses. Key issues with respect to fraud proceeds include the need for assessment of the overall national and global costs and proceeds; its relative position with respect to other major predicate offences as a source of proceeds for laundering; and the ultimate destinations of fraud proceeds. In addition, commercial interests and some victim advocates have concerns about differences between criminal confiscation of proceeds and commercial recovery of losses.

Only a few States provided information about total losses or proceeds, but it is clear that these can be substantial. It is not unusual for individual frauds to generate losses in the hundreds of millions of dollars, and those countries which provided information suggest that total losses are in the billions of dollars\(^{47}\). The largest and most serious frauds described tended to be major commercial frauds or mass-frauds involving large numbers of victims, with one State reporting a very large fraud against its tax system. Commercial information sources tend to break down losses by specific commercial sectors, such as the insurance or credit card industries, but report losses of similar magnitude. The Financial Action Task Force (FATF/GAFI) does not report detailed statistics or estimates\(^{48}\), but


\(^{48}\) Several experts and some Member States noted that both FATF and the Financial Intelligence Units in individual States gather and use financial intelligence information about money-laundering, but are neither mandated nor equipped to gather criminal or economic statistics. Thus, for example, these bodies might be able to examine specific links between fraud and money-laundering or
generally considers fraud and related forms of financial crime to be among the top four crimes identified as single sources of illicit proceeds, the other three being trafficking in narcotic drugs, trafficking in weapons and the smuggling of migrants or trafficking in human beings. One State noted that the extreme range of magnitude in fraud cases was also a challenge in making comparisons or assessing trends, since some offences were so large that a few individual occurrences could significantly affect annual totals. Other obstacles to global statistical analysis include chronic under-reporting and the fact that while core fraud offences are generally consistent among States, many areas of commercial regulation involve approaches to offence structure, reporting complaints and assessing losses that differ from country to country. In most sources losses generated by fraud are much greater than actual proceeds taken by offenders. Not all proceeds are detected and counted, and loss calculations may include indirect costs or what one commercial source described as “collateral damage” from frauds.

While fraud and money laundering are seen as separate legal and conceptual matters by most States, there is some overlap in the techniques used by offenders, and actual crimes can be difficult to distinguish at the investigative and practical levels. The major difference is that fraud essentially converts legal funds in the hands of victims into illicit proceeds in the hands of offenders, whereas criminal money-laundering involves the subsequent transfer and concealment of funds which were illicit proceeds from the outset. The major similarity is that the means of deception and conduct of covert or unobtrusive transactions are often common to both.

---


51 See FATF, Report on Money Laundering Typologies (2000-2001), paragraphs 13-15 and 58, available on-line at: http://www.fatf-gafi.org/pages/0,2966,en_32250379_32237235_1_1_1_1,00.html (English), http://www.fatf-gafi.org/pages/0,2966,fr_32250379_32237235_33631745_1_1_1_1,00.html(French).
This represents a challenge for law enforcement and criminal justice officials, but it may also represent something of an opportunity. Several States pointed out that anti-money laundering mechanisms such as requirements that suspicious transactions be reported might also be used or adapted for use to identify transactions that might be fraudulent, although the substantive criteria used might not necessarily be the same. Some banks, telecommunications providers and other commercial or financial institutions already screen mass transaction data to look for unusual patterns that suggest frauds against themselves or their customers. More generally, as with other predicate offences, measures against fraud may from time to time generate money-laundering investigations and prosecutions and *vice versa*. This suggests the usefulness of effective cooperation between financial intelligence units and other anti-money-laundering bodies, those charged with preventing, investigating and prosecuting fraud, and appropriate private-sector interests.

Most States indicated that they had in place legislative provisions dealing with the confiscation of proceeds of fraud and other crimes. These included schemes based on the criminal conviction of offenders, and in some cases on proof of the offence and tracing or identification of the proceeds even where there was no conviction. Many also indicated that confiscation schemes included or extended to property which was not proceeds but was derived from proceeds, or to the confiscation or imposition of equivalent fines when actual proceeds or derivative assets could not be located. In cases where assets could not be proven to be proceeds or derived from proceeds, one State also noted that they could still be taxed as income, and that offences relating to tax evasion would apply in appropriate cases.

Some States indicated that they had specific powers to seize, freeze or prevent the transfer of assets pending criminal proceedings, and as the point was not specifically addressed in the questionnaire, it is possible that additional States have such provisions and did not refer to them. A number of States also indicated that proceeds are effectively seized or immobilised as evidence from the time they are identified until any criminal proceedings are concluded. Several States indicated that they had powers to confiscate the proceeds of fraud even though fraud itself was not treated as a predicate offence for purposes of anti-money-laundering measures. One State also referred to the burden of proof in confiscation proceedings, indicating that when an offender had been convicted, if its prosecutors proved that the individual had a criminal lifestyle, all of that person’s assets and any assets that had been in the possession of the person within a set period prior to
conviction were presumed to be proceeds of crime and liable to confiscation.

Several States also indicated that there was provision for the return of proceeds to victims, either after confiscation by the State or through proceedings in which victims could claim compensation or restitution in criminal proceedings. The return of proceeds to victims may pose several challenges in major fraud cases. As with other forms of economic crime, there may be practical difficulties with establishing the identity or status of victims as such, and quantifying claims. Victims of individual frauds may be easy to identify, but many forms of commercial fraud victimise legal persons, raising the question of whether compensation should go to the natural persons affected, such as shareholders or creditors in a bankruptcy process. While return-based schemes would only return actual proceeds traced to and recovered from offenders, compensation or restitution-based schemes might also include claims for compensation for indirect losses. In many commercial and mass frauds, competing claims to the proceeds could also arise. Regarding competing claims as between victims and governments, some States indicated that claims by victims were given priority or that government confiscation proceedings could not be concluded until victims’ claims were dealt with.

States indicated a range of measures in place for civil recovery, including both criminal justice or hybrid systems, in which crime victims could have claims adjudicated and enforced in the context of criminal proceedings, and civil litigation, in which victims were responsible for bringing their own claims to court on a private basis. Others noted the limitations of civil litigation as a remedy for fraud, including the fact that proceeds were often transferred or dispersed beyond the reach of civil proceedings, and the fact that aside from major commercial victims, most victims had limited abilities to conduct their own litigation. One State noted that its own agencies could bring civil claims on behalf of victims, and another referred to a scheme under which some compensation could be claimed from the State itself where it could not be recovered from offenders.
5. Fraud and terrorism

Unlike identity fraud, which can include non-economic motives such as concealment, economic fraud is committed for material gain, which makes it useful to terrorists primarily as a means of financing terrorist organizations or operations. Reports of the team responsible for monitoring sanctions against Al Qaida and the Taliban to the Security Council identify fraud, along with other offences such as kidnapping, extortion, robbery and narcotics trafficking as potential sources of funds for terrorism. A similar range of crimes has been reported by the Financial Action Task Force in its work on the financing of terrorism. Occurrences of terrorism-related fraud appear to be too infrequent to support any national or comparative analysis of rates or trends, but individual cases were taken very seriously. In their responses, several States indicated that they had encountered fraud cases linked or believed to be linked to terrorist activities, but most indicated that these were relatively rare or identified only individual incidents or cases. Some additional States did not indicate that they had actually encountered the problem but that their officials were concerned about the potential use of fraud in support of terrorism.

A range of different frauds were raised. Small, local frauds, frauds against public benefits schemes, and credit-card fraud have been used or are suspected of being used to sustain individuals or small groups and finance small operations, and more extensive and sophisticated credit-card fraud schemes can also be used to finance larger operations or generate

52 While there is no consensus on the scope or meaning of “terrorism” in general, the term is clarified for the purposes of financing offences by the International Convention for the Suppression of the Financing of Terrorism. See A/RES/54/109, Annex, Article 2. In the present study, the question of the meaning or scope of terrorism itself was left to the Member States, and responses may therefore reflect the Convention or definitions or descriptions used by the States themselves.


more substantial and ongoing revenues for other purposes.\(^{55}\) It has been suggested that the relatively low costs of acts of terrorism, the fragmentation of groups such as Al Qaida, and the implementation of measures against large-scale financing operations and international funds transfers in Security Council resolutions such as Resolutions 1267, 1373 and 1526 will likely produce a trend towards smaller, more locally-based terrorist operations supported by smaller, more localised crimes, including smaller frauds.\(^{56}\) These are more difficult to detect and link to terrorism and more likely to avoid the surveillance risks inherent in larger and more international transfers. Assuming that sophisticated terrorists would seek to avoid the attention of local law enforcement, the use of minor frauds may suggest either a lack of sophistication on the part of local operatives, or a calculated assessment that the probability or risk to offenders of triggering an investigation and prosecution for minor fraud offences is lower than that for more centralised financing structures. Only a few examples of major frauds intended for use in financing terrorist groups were provided, including insurance fraud, smuggling and excise tax frauds, frauds relating to currency exchange, frauds against public benefit schemes and business or commercial frauds.

Several States expressed concern about the use by terrorists of frauds against telecommunications providers where the underlying purpose was not economic advantage, but obtaining anonymous and untraceable telecommunications, and some have encountered this. The same *modus operandi* is often used by cybercrime offenders and organized criminal groups for the same reasons. Typically, false identities and stolen or copied credit cards are used to open mobile telephone or Internet accounts, which are used for a short time and abandoned before the fraud becomes apparent. If the content or destination of messages attracts suspicion, they cannot be traced back to the sender, especially if the account has already been abandoned. A number of public reports refer to the development,


Several responses voiced particular concern about the potential use of charitable fraud to finance terrorism, and some States had encountered cases where this was detected or suspected. The abuse of charities and other non-profit organizations by terrorist organizations has also been identified as a matter of concern by FATF\footnote{See Financial Action Task Force, Special Recommendations on Terrorist Financing, 22 October 2004, Special Recommendation VIII, \url{http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf}, and FATF Annual Report, 2002-2003, Annex B, “Combating the Abuse of Non-Profit Organisations”, \url{http://www.fatf-gafi.org/dataoecd/12/63/34328318.PDF}.}, and by academic and journalistic sources.\footnote{See, e.g., RUDNER, M., “Using Financial Intelligence against the Funding of Terrorism”, \textit{International Journal of Intelligence and Counter Intelligence}, Vol. 19(1), 2006, pp.32-58 at 42-43 and sources there cited, and BBC News, “Warning Signs for the Funding of Terrorism” \url{http://news.bbc.co.uk/2/hi/business/4692941.stm}.} Aside from fraud and the diversion of charitable donations as a source of funds, charities have also been used as a means of laundering or covertly transferring funds from other sources.\footnote{Rudner, supra, at pp.43-44.}

The Security Council Counter-Terrorism Committee has noted the particular difficulties encountered by States in suppressing the abuse of non-profit organizations as a source or conduit for funds for terrorism pursuant to Resolution 1373\footnote{See Report by the Chair of the Counter-Terrorism Committee on the problems encountered in the implementation of Security Council resolution 1373 (2001), S/2004/70, Annex, section II, subsection A.}. In 2004, the list of entities identified and listed as the subject of measures against the financing of Al Qaida and the Taliban pursuant to Security Council Resolution 1267 (1999) included 17 charitable or non-profit organizations with 75 operations active in 37 States.\footnote{Third Report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al Qaida and the Taliban and associated individuals and entities, S/2005/572, paragraph 84.}
At least two major scenarios for charitable fraud exist. Sham charities may be set up to finance terrorism directly, both by soliciting funds from charitable donors and using the cover of charitable work as a means of transferring them without attracting attention. Legitimate charities may also be infiltrated and exploited to divert donations to terrorism. In the former case, under the legislation of most reporting States, the donors themselves would be defrauded, and in the latter, the charity itself would be the victim of either fraud or theft, depending on applicable domestic law and the facts of each case. This also poses serious problems for charities. Any links to either fraud or terrorism are a major concern because even unfounded rumours of links can have a major effect in deterring the donors on which they rely. Also, non-profit organizations may have more difficulty screening employees and volunteers than commercial ones, and strict accounting requirements are more difficult to meet because the results of charitable work are often remote, intangible and not directly linked back to donors. Additional monitoring and accounting costs also reduce funds available for charitable work. A lack of State and charitable capacity to combat infiltration and diversion has been identified as a serious concern, both for charities and for the States in which most of the work using charitable funds is carried out. As with money-laundering, it has been suggested that certain specific activities in the course of charitable work should be cause for suspicion that a charity may be involved in the financing or terrorism, and many of these are also suggestive of charitable frauds in general. These include: the solicitation and use of informal or undocumented donations; the absence of normal accounting and audit information tracing funds from donor to recipient or final expenditure; the use of multiple or unusual financial transactions; abnormal ratios between fund-raising costs, contributions and expenditures; overlapping functions or a lack of clear separation between different charities or between charities and other entities; and the transfer of funds to other organizations rather than direct use for charitable causes.

A further concern arises with charitable organizations that address specific religious, ethnic or cultural communities or causes linked to regions where there is conflict because charitable proceeds may be diverted to terrorist or insurgent groups and because accounting or oversight safeguards are particularly difficult to apply in conflict or post-conflict regions. Recent political, academic and journalistic discussion has focused

---

64 S/2006/154, above, at paragraph 81.
on links between Islamic charities and associated terrorist or insurgent groups, but expatriate or other groups defined by religion, culture, national origin or other characteristics have also been associated with terrorist or insurgent activities in other locations, including the conflicts in Northern Ireland and Sri Lanka. Political discussions of whether particular groups or activities should be considered as “terrorism” or not aside, it can be difficult to distinguish between fraud and other crimes in such cases. Where charitable donations are ultimately used for terrorism, it will generally be considered as fraud if the donors were deceived as to the true purpose, and extortion if they were aware of the purpose but were intimidated in some way. Where donors were aware of the true purpose and not coerced, no fraud, theft or extortion offence would apply, but both the donors and the recipient charity may be committing domestic offences relating to the financing of terrorism, including those which implement the International Convention for the Suppression of the Financing of Terrorism\(^6\). Charities are also sometimes used as a conduit for funds generated by other licit or illicit means, and in such cases financing or money-laundering offences may also apply.

6. The impact of fraud in countries under reconstruction or with economies in transition

Economic fraud may pose additional problems for countries under reconstruction or with economies in transition, as well as for both donors and recipients engaged in major reconstruction projects following conflict or natural disasters. Many deterrent and control factors are weaker in such environments, opportunities for fraud may be greater, and the effects of economic and non-economic damage can be magnified by the weakened state of key governance, criminal justice, economic and other structures. Urgent major reconstruction efforts are a particularly tempting target for fraud offenders, because large amounts of funding must often be spent quickly, limiting the effectiveness of safeguards, and in environments where applying conventional accounting and other safeguards may be difficult or impossible. Losses from major frauds may be large enough to harm economies already weakened or de-stabilised by other problems, and may considerably strengthen organised criminal groups already facing weakened criminal justice systems, fuelling corruption and other problems. The need to quickly develop criminal law, establish effective law

enforcement and criminal justice institutions and train large numbers of officials confronts all reconstruction and transition projects, but can be particular problem where fraud and corruption are concerned. Economic fraud can be a complex and sophisticated crime, requiring high levels of skill and education on the part of investigators, and as a non-violent crime it is often accorded a relatively low priority, even in highly developed countries. Development agencies and local officials often face difficult choices between work that supports the human security of individuals and work that protects the viability and integrity of reconstruction efforts themselves.

Fraud is also a crime of deception, and the potential for this increases in transitional conditions, where new social or economic rules and practices are not well-understood and may be taken up by different population groups at different rates. Offenders may be in a position to take advantage of both victims and law-enforcement officials who do not fully understand the new economic environment, and victims may also be induced to cooperate with offenders due to unrealistic expectations for economic transition or liberalisation. There may also be gaps in criminal or commercial law, as comprehensive new rules are implemented, but specific safeguards and criminal offences are only updated as offences are detected and the need for amendments becomes apparent. Frauds which do occur, especially major ones, can do great damage to the efforts of States to develop their economies and implement economic reforms, not only by direct economic damage, but also by eroding the popular and consumer confidence needed to make such reforms a success. As noted, major fraud schemes also tend to be carried out by organised criminal groups, and the substantial proceeds may make them a much more serious threat in environments where governance institutions are weakened. Unlike other problems arising from fraud, which tend to arise in jurisdictions where victims are located, the strengthening of organized crime is manifest in the places where offenders are located. In some transnational fraud cases this could develop as it has with trafficking in narcotic drugs, where organized crime in developing countries is strengthened by proceeds taken from other, more affluent countries.

Major frauds and associated problems (sometimes also identified as forms of corruption) have been seen in many countries or regions where major economic transitions have been implemented in recent decades, including the Russian Federation, Eastern Europe, China, and elsewhere. In some cases major financial structures or activities related to transition, such as new taxation schemes, new procurement processes or privatization schemes have been exploited or targeted, and in other cases more common
forms of fraud have simply taken advantage of a favourable environment for offenders. Several countries in the process of joining the European Union reported major sophisticated frauds against their value-added tax (VAT) refund schemes, one such country cited a lack of anti-fraud protections in its new scheme as a factor. One indicated that the impact of one fraud scheme was sufficiently serious to negatively affect its entire national budget. In China, the process of economic transformation and the need to maintain confidence has led to anti-corruption initiatives and other responses, including both criminal law measures (1997) and an ongoing process of developing commercial law controls which facilitate and regulate legitimate commerce while suppressing fraud and other illegitimate economic activities\textsuperscript{66}. The Russian Federation expressed concerns about the involvement of organized crime and mentioned frauds against its new tax system and the privatisation elements of its economic reform process. While not examples of transition or reconstruction, national and international charitable and insurance-based efforts to rebuild after major natural disasters such as the 2004 Asian tsunami have also been exploited by fraud offenders taking advantage of charitable donors and the fact that local law enforcement and other control factors are often overwhelmed by both the initial disaster and the rebuilding effort\textsuperscript{67}.

Major frauds in such cases can become a national and regional security issue in themselves or complicate efforts at domestic development, reform or reconstruction, or regional stability. In at least two cases, major “Ponzi” or pyramid-scheme frauds have been cited as a factor in de-


\textsuperscript{67} Several national law enforcement efforts were targeted specifically at frauds exploiting disaster relief efforts. See, for example, United Kingdom National Criminal Intelligence Service, “Tsunami fraud threat: advice to the public”, \url{http://www.ncis.co.uk/press/tsunami.asp} and United States Federal Bureau of Investigation, “Tsunami disaster relief fraud alert: Don’t be scammed”, \url{http://www.fbi.gov/page2/jan05/tsunamiscam010505.htm}. The United States Justice Department established a special Task Force to deal with a range of frauds arising from the 2005 Katrina disaster, including charitable fraud, public and private-sector benefit fraud, identity theft, insurance fraud, procurement fraud, and public corruption. See \url{http://www.usdoj.gov/katrina/Katrina_Fraud/index.html}.
stabilising countries in economic transition. Albania encountered serious problems, including violence and the looting of small-arms from armouries, following the collapse of a pyramid investment scheme in 1996-97. This in turn contributed to small-arms trafficking and other transnational organized crime activities across the region, some of which remained a problem almost a decade later. The scheme, which may have affected as much as half of the population, also depleted the retirement savings of many Albanians, depriving the national economy of what would otherwise have been a factor contributing to long-term stability and economic security.

The relationships between fraud and transition, reconstruction and rebuilding efforts have several significant implications for governments and national and international organizations involved in such efforts. There is a clear need to ensure that international, national commercial and non-profit entities are all aware of the high risk of fraud in these circumstances and the substantial harm it can cause, both to the projects themselves and those they are intended to assist. In international efforts, both donors and recipients share the objective and the responsibility of ensuring that funds are not diverted. In both domestic and international efforts, there is a need for close coordination among the entities which raise and transmit funds, those who spend them and those they are intended to benefit, to establish processes which are both resistant to fraud and which contain elements to quickly identify and remedy problems. In many cases this will include a broad coalition of intergovernmental organizations, national development agencies, charitable organisations, insurers, profit and non-profit entities which provide assistance goods, services and logistics, and appropriate law enforcement and other anti-fraud entities. This is one area where fraud and corruption are closely linked: fraud is often the means of illicitly diverting resources, while bribery and other forms of corruption are used to ensure that the diversion will be successful or undetected. This suggests that, in at least some areas and some projects, anti-fraud and anti-corruption elements should be coordinated or even integrated.

V. International cooperation and jurisdiction

Major transnational fraud cases pose a significant challenge for international cooperation. They tend to be large, complex, costly and multi-jurisdictional, involving many offenders, large numbers of victims, and investigative agencies and private sector institutions. Where cooperation rules and practices have evolved to deal with small numbers of major cases, some mass frauds can present themselves as large numbers of relatively small frauds. Successful frauds also generate substantial proceeds, which can be used to support organized criminal groups, protect ongoing fraud operations, conceal and launder proceeds, mount protracted legal challenges to mutual legal assistance and extradition. Many of the comments highlighted the need for cooperation, but the prevalent view appears to be that existing legal instruments, especially the UN Convention against Transnational Organized Crime\(^89\) and, for those countries which are States Parties to it, the Council of Europe Convention on Cybercrime\(^70\) provide a sufficient legal basis for such cooperation, and that the focus should be on measures to ensure that the available instruments can be and are used effectively rather than on developing new ones. It was also noted that no formal legal authority or basis of any kind was needed for some of important areas of cooperation against fraud, especially in areas such as prevention.

1. Mutual legal assistance and other investigative cooperation

The general need to deliver effective mutual legal assistance was highlighted by a number of States. Generally, investigators and prosecutors need information and evidence relating to communication between offenders and victims and the transfer of funds. That includes information to identify the sources and destinations of communications and offenders and victims, and the content of communications to prove elements such as deception. Also needed are financial records to prove the transfer of economic benefits. Tracing and identifying proceeds is important, and includes initial transfers from victims to offenders as well as subsequent money-laundering. Evidence of the harm caused by major transnational frauds is also important, and this may involve direct evidence from individual victims or expert forensic evidence. Expert evidence may also be needed to establish that offender conduct was not consistent with normal

\(^69\) A/RES/55/25, Annex I.
\(^70\) E.T.S No. 185, Budapest, 23 November 2001
commercial practice. Several States raised the question of transferring testimonial evidence efficiently, and experts drew attention to the use of video-link evidence under the Convention against Transnational Organized Crime. Effective cooperation in fraud cases does not always require formal mutual legal assistance, as some communications and evidence can be intercepted or accessed within the jurisdiction investigating the crime. The major challenges identified included the complexity of cases and length of time needed for cooperation. Several States highlighted the importance of fast and informal cooperation among investigators. Most forms of cooperation involve the sharing of information, which entails balancing investigative interests and appropriate safeguards. One State noted that while fast information sharing was often important in transnational fraud cases, there was also a need for balance and transparency to ensure that shared information was accurate and used within appropriate legal rules.

2. Extradition

Most countries indicated that they could extradite criminal suspects, and some indicated that they had authority to prosecute offences committed outside of their territorial jurisdiction in cases where they could not extradite. Some reasons for the refusal of extradition requests, such as bars on extradition of nationals, amnesty laws and limitation periods, could prove an obstacle in fraud cases. Experts noted that Article 11, paragraph 5 of the Convention against Transnational Organized Crime calls for long limitation periods in organized crime cases, especially in cases where justice was evaded, and much the same rationale exists for the more complex fraud cases.

The Convention against Transnational Organized Crime obliges States Parties to extradite offenders accused of most serious frauds or to prosecute them, subject to exclusions set out in Article 16 of the

---


Convention, but the obligation to prosecute applies only if the reason for refusal to extradite is the nationality of the offender. The basic requirements for extradition are that the type of fraud be a “serious crime” in the domestic law of both States Parties, that it involve an “organized criminal group,” and be “transnational in nature.”\(^{73}\) The Convention also requires States Parties to ensure that they have jurisdiction to prosecute extraterritorial offences if committed by one of their nationals and they cannot extradite by reason of nationality, and allows for the transfer of convicted offenders to serve sentences in their home countries.\(^{74}\)

States Parties are also encouraged to adopt sufficient extraterritorial jurisdiction to enable them to prosecute cases in which the accused are found in their jurisdiction and are not extradited for any other reason, but this is not mandatory.\(^{75}\) Within the framework of the Convention, gaps that could be addressed include ensuring that all States fully implement it, that they ensure that serious frauds meet the requirements for “serious crime”, and that States which do not extradite their nationals implement the aut dedere aut judicare requirements. A further potential gap exists with respect to two other scenarios. States should ensure that they are willing and able to prosecute fraud offenders not extradited for reasons other than nationality, thereby implementing the optional Article 15, paragraph 4. Finally, while most major frauds involve “organized criminal groups”, transnational offences by individuals are possible and could be provided for by responses such as case-specific agreements or arrangements. The Council of Europe Convention on Cybercrime\(^{76}\) also provides for extradition in cases where the countries concerned are Parties, and this is not limited to countries which are Members of the Council. However, extradition for the Convention offences of fraud and forgery is available

\(^{73}\) See *Convention*, A/RES/55/25, Annex I, Article 2, subparagraphs (a) and (b), and Article 3, paragraph 2.


\(^{75}\) See *Convention*, A/RES/55/25, Annex I, Article 15, paragraph 4.

\(^{76}\) *ETS No. 185*, Budapest, 23 November 2001, Articles 3 and 4 (criminalisation), and 24 (extradition).
only in certain circumstances, when the crimes involve the use of computers, computer systems or data. The Convention on Cybercrime, however, is not limited to cases where an “organized criminal group” is involved and could be used where computer fraud or forgery was committed by an individual.

3. Jurisdiction
   (a) Territorial jurisdiction

   Transnational fraud is one of the most common forms of criminal case raising challenges to conventional territorial jurisdiction. Offences may be planned in one country, committed by offenders based in a second country, victimizing persons in a third country, with proceeds accumulated and laundered in a fourth country. Victims are often in many countries and additional countries may be used for other purposes such as the location of “drop boxes” to transfer funds or as a base for fraudulent Internet sites. In sophisticated transnational fraud cases, offenders are aware of jurisdictional limits and are fully capable of structuring transactions so as to take maximum advantage of any gaps or weaknesses. In response, concepts of territorial jurisdiction have also evolved, extending territorial jurisdiction to include offences which take place in two or more countries at the same time, which continue from one country to another over time, or which take place in one country but have some tangible impact on another. Jurisdiction where an offence is commenced in the prosecuting State and completed elsewhere or where any essential element of the offence takes place in that State now seems common. Some States base territorial jurisdiction on the place where the offence was planned or where the last element, or any essential element, of the offence took place, or if the place where the offence was committed is uncertain. Whether jurisdiction could be based on the presence of non-essential elements in a State’s territory is less clear.

Only one State reported the possibility of going further. In that State a real and substantial link to its territory must be shown, and this may include the presence of non-essential elements such as planning, preparation or the presence of proceeds, but it is not clear whether jurisdiction could be based exclusively on these factors. National laws that require the presence of an essential element as the basis for territorial jurisdiction also depend to a substantial degree on how offences are formulated and what elements are included as essential. Conspiracy-type offences are usually broader, for example, and cybercrime or telecommunication offences may expressly include elements such as the sort of effect or impact which must arise within a State’s territory. Article 11 of the Convention on Cybercrime provides for criminalization of attempting, aiding, or abetting the substantive offences in the Convention, including computer-related fraud and forgery.

Often, the strongest incentive to prosecute lies in countries with victims or other adverse impacts. Many States have jurisdiction based on the fact that a result or effect of the offence occurred in their territory. Most limit this to effects which are essential or factual elements of the offence, which in fraud usually requires the presence of victims. Some may apply a broader version of the same principle, also including indirect losses. Frauds against companies may also affect shareholders or markets for example. The strongest disincentives to prosecute, especially in major fraud cases, often lie in the costs and complexity of the cases, ne bis in idem, and the fact that essential requirements such as witnesses and other evidence have to be imported and may not meet domestic evidentiary standards. Even where a State has legal jurisdiction, such obstacles may prevent it from exercising it or result in discussions with other States about which is the most convenient forum for a prosecution.

The nature of fraud itself and the fact that offenders can and do take jurisdictional gaps or limits into consideration when planning and carrying out fraud schemes poses significant challenges to existing concepts of territorial jurisdiction. On one hand, the need to ensure that offences can be prosecuted at all and the need to avoid jurisdictional gaps that offenders

---

80 In Canada the test is based on case law holding that the test is whether there is a “real and substantial link” to its territory. The case involves a fraud planned in Canada but involving victims and proceeds in other countries. Jurisdiction was based on the fact that the fraud was planned in Canada and that proceeds were returned there via other countries, but some essential elements also took place there. See: Libman v. the Queen [1985] 2 SCR 178
will exploit suggests relatively broad models. On the other hand, the potential for jurisdictional conflicts and the problems of prosecuting costly and complex transnational crimes sound a more cautionary note. The gradual trend toward the expansion of territorial jurisdiction is likely to continue, driven in part by the creativity of transnational fraud schemes and greater access to information technologies. A single straightforward formula for determining jurisdiction is unlikely to be viable or valid for all cases, and none of the existing models covers every possible case. The best approach is probably to ensure that as many States as possible have relatively broad territorial jurisdiction, that the various interested States collaborate effectively, and that the single State which is in the best or most convenient position to prosecute actually does so.

To ensure that transnational frauds can be prosecuted effectively, a number of legal and practical possibilities exist, depending on what measures are already available in each State. These include ensuring that sufficient jurisdiction exists, based on the various jurisdictional models discussed in the present Report, and where appropriate considering non-essential elements such as the presence of planning, preparation and proceeds, which may be more important in fraud cases than for some other crimes. The formulation of fraud offences is also important, especially where territorial jurisdiction is based on essential elements defined as part of the offence itself. In the case of fraud schemes based in or committed using countries which lack law enforcement or prosecutorial capacity, general technical assistance to build the necessary capacity could be offered, and assistance might also be tendered with respect to specific offences as part of international cooperation programmes.

Within applicable jurisdictional rules, there will often be several States which might claim jurisdiction, and consultations on which State should actually prosecute will be important. This may involve legal, diplomatic and practical issues, ranging from the relative jurisdictional and other legal strengths and weaknesses of each State’s case and whether offenders can be extradited to the State which wants to conduct the prosecution, to pragmatic considerations such as the costs and obstacles to transferring evidence from one State to another, ensuring its admission into proceedings and effective presentation before the courts. Where it is decided that one of several possible States should prosecute, the jurisdiction of other States can effectively be transferred. Provision for this is made in the United Nations Model Treaty on the Transfer of Proceedings in
Criminal Matters (1990), Article 21 of the UN Convention against Transnational Organized Crime (2000) and Article 47 of the UN Convention against Corruption (2003). Where two or more States have jurisdiction and want to prosecute, the following criteria could be considered.

a) Which State has suffered the greatest direct and indirect harm?
   Harm provides incentive and justification to prosecute, and usually means that evidence will be available.

b) In which State were most of the elements of the offence committed?

c) Which State has the greatest investment of investigative effort in the case? Aside from the commitment of resources, this will also usually mean that the State has the necessary evidence.

d) Where are witnesses and other evidence located? Transferring large volumes of evidence, especially in complex or mass fraud cases, raises costs significantly and may also have a bearing on legal admissibility and whether the evidence can be used effectively.

e) Which State has the strongest case? Taking into account the totality of evidence which can be assembled in or transferred to each State, the evidence laws of each State and similar criteria, it may be apparent that one State has a stronger possibility of a successful prosecution.

f) Which State has the best capacity? The complexity of major fraud cases can place substantial demands on investigators and prosecutors in terms of both costs and expertise. States with extensive experience and resources may consider either taking jurisdiction, if this is legally feasible, or of providing assistance to another State which has a stronger case or claim but less capacity.

g) What is the nationality of the offender and can he or she be extradited? States with what are otherwise weaker claims may have to prosecute their own nationals if they cannot be extradited.

h) What other offences may be involved or may be prosecuted? While jurisdiction is usually linked to specific offences, major fraud schemes often incorporate other crimes, including identity-related crimes and money-laundering, and in some cases it may be

---

advantageous to consider which State is in the best position to prosecute all of them so they can be tried together.

i) What other offenders may be involved or may be prosecuted? Similarly, there may be advantages in specific cases to determining the most convenient forum for some members of a criminal group and then extraditing others to try everyone together.

j) What are the respective sentencing regimes? Generally, States adopt punishments they see as appropriate and may be willing to cede jurisdiction to other States with similar punishments and are less likely to do so where the prospective sentences are seen as excessively harsh or lenient.

(b) Extraterritorial jurisdiction

While concepts of territorial jurisdiction have expanded, the application of extraterritorial jurisdiction in fraud cases is less common, apart from aut dedere aut judicare requirements and the extension of jurisdiction to their own nationals where there are constitutional bars to extradition. Jurisdiction based on the nationality of victims (passive personality) is also possible, although in economic fraud this may be difficult to distinguish from territorial jurisdiction based on effects or results. Some States also reported the adoption of extraterritorial offences to protect what they saw as vital interests against specific types of fraud, based on the protective principle. Examples include the counterfeiting of currency, passports or other essential documents, and frauds which affected national immigration systems. Another area which was not mentioned but which could invoke the protective principle would be major frauds against governments, which may also be corruption offences.

4. Limitation periods

The experts noted that limitation periods could be a problem in many fraud cases, due to the length of time needed to properly investigate and prosecute complex and transnational cases, and also noted provisions of the Convention against Transnational Organized Crime and Convention

82 States Parties to the 2000 Convention against Transnational Organized Crime and the 2003 Convention against Corruption which cannot extradite their nationals are obliged to provide for such jurisdiction. See A/RES/55/25, Annex I, Article 16, paragraph 10 and Article 15, paragraph 3 and A/RES/58/4, Annex, Article 44, paragraph 11 and Article 42, paragraph 3.
against Corruption calling for the establishment of appropriate periods taking into account offences covered by that Convention and cases where the offender has evaded the administration of justice. Several approaches to ensuring the application of appropriate limitation periods were considered, including the establishment of basic limits by statute that were appropriate for the fraud offences to which they applied, provisions for the suspension of limits in some circumstances, such as where the offender delayed proceedings or evaded the administration of justice, and the development of legislative provisions allowing for the judicial extension of a limitation period in appropriate circumstances prescribed by legislation. The option involving judicial extension was seen as inconsistent with the fundamental principle of *nullum crimen sine lege* by some experts and as a potential infringement of rights established by fundamental laws by others and was not seen as a viable option.

**VI. Cooperation between the public and private sectors**

Economic fraud is a crime of commerce. This means that there is both a need for collaboration between the commercial and criminal justice communities and substantial motivation, since neither can fully and effectively address the problem on its own. Within the United Nations, the need for effective collaboration between experts on crime and commerce has been recognized. The need to engage the Crime Commission was recognized by UNCITRAL in its initial work on commercial fraud, and close coordination, via the two Commission secretariats and the participation of several experts on both the commercial and criminal expert groups, has been a significant feature of the work from 2002 to the present.

While there is a clear need for collaboration, it is important to recognize that practices and objectives do not always coincide. Some forms of commercial fraud are defined in terms of deviance from established commercial practice, and may not be recognized as offences in criminal law. More fundamentally, where criminal justice interests tend to favour investigation, prosecution and punishments, and specific and general deterrence and the incapacitation of offenders, commercial interests tend to

---

83 See A/RES/55/25, Annex I, Article 12, paragraph (5) and A/RES/58/4, Annex, Article 29.

favour dispute-settlement mechanisms and the recovery of losses. State agencies will often prosecute cases that would be dropped as not being cost-effective to pursue in the private sector. What is shared between the two is an immediate interest in acting quickly against ongoing frauds, an overarching strategic interest in prevention and suppression of fraud, and a need to maintain public confidence in both the stability of commerce and the integrity and efficacy of criminal justice. What must remain separate are the interests of commercial profit, on the one hand, and the rule of law on the other. Where commercial entities have a primary obligation to generate profits for their owners and shareholders, criminal justice systems have obligations to the rule of law, human rights, independent decision-making on the part of prosecutors and judges, and to look beyond individual cases to the general deterrence of crime.

The responses of States suggest that there is both substantial need for the expansion of private-public cooperation and substantial potential for such an expansion. Most States did not provide much information about cooperation, but many of them did indicate that they saw a need for it. A number of responses described only coercive measures, such as legal requirements to report offences or disclose information where legal persons or their employees were involved in fraud. Some States did mention regulatory or legislative standards. The United States of America described its 2002 legislation establishing a range of standards intended to address fraud and corporate governance issues, and several other States mentioned laws in the area of commercial regulation which were intended to encourage standards and practices which would deter and prevent fraud. These include elements intended to promote more transparent reporting and auditing of companies and encourage individuals who may be aware of wrongdoing to report it or cooperate with authorities as well as elements requiring senior officials to take responsibility for the accuracy of accounting and financial information. A few States reported national strategies for commercial or industrial development which included issues relating to fraud and other crime problems of mutual interest. These included consultations or meetings in which commercial and criminal justice experts could meet to identify new issues and develop either common or coordinated approaches. Some States also indicated that joint

---

consultative bodies had been established to deal with specific problems such as fraud or money-laundering.

The presence of coercive measures is not necessarily indicative of the overall public-private relationship. A number of States reported legal requirements that private companies protect privacy and personal information given to them in the course of business, and in such systems companies are often prohibited from disclosing information, even to law enforcement officials, unless compelled to do so by a judicial order or similar directive. In many States, companies are also under contractual obligations to their customers to protect privacy and could be sued civilly for disclosing information unless compelled by law to do so. Nevertheless, there appears to be significant opportunity in many countries for the development of regulatory standards and collaborative, rather than coercive commercial and criminal justice practices against fraud, based on joint consultations between appropriate public and private sector entities.

Such dialog is important as a means of identifying and discussing issues and options, and collaboration is possible in a number of different areas, ranging from general cooperation on research and the development or harmonization of public policy and private commercial infrastructure, to highly specific cooperation in dealing with specific individual cases of fraud. Many States identified the need for fast information-sharing as a high priority, but there was relatively little discussion of what sorts of apparatus or framework would be needed for this, and what sorts of information could be shared with or without legal or other safeguards. Some also noted that cooperation was important in developing and setting up new technologies, to make them as resistant to crime and as supportive of crime control as possible. Several also discussed the importance of prevention by educating and training both employees in a position to prevent and detect fraud and customers who might be targeted by fraudulent solicitations. All of these represent fertile areas for policy development based on public-private consultations and collaboration, and several States reported successful efforts in this area.

One State noted that, while some general principles of cooperation could be identified, the specific ways in which private and public entities could and should cooperate varied depending on the types of commerce and fraud at hand, and the roles played by various different companies. It identified some key sectors as industries which operate commercial systems, such as the credit card, insurance, banking and financial sectors, and increasingly companies which specialise in areas such as auditing, security and loss-prevention, that control fraud and other economic crime. Another key sector was companies which develop and market information
and communication technologies and which provide telecommunications and other services to commercial enterprises and their customers. Several other States mentioned consultations or policy efforts that were focused on specific commercial sectors. This suggests also the need for coordination based on subject-matter. Having successfully developed a joint overall strategy against fraud, public-private bodies could then turn to the adaptation of general strategic elements to the specific circumstances of businesses such as banking and financial services, and also play a role in ensuring that new initiatives developed at the specific level were coordinated with developments in other commercial sectors.

Concerning specific forms of cooperation, most of the States which commented highlighted the need for information-sharing, and several noted that rapid and accurate sharing was critical to be able to intervene in time to limit victimisation or minimise losses. One State divided its own experience into the areas of collaboration in receiving and dealing with specific complaints; collaboration in analysing other evidence or information, and collaboration in public education and prevention. Most of the comments concerned the sharing of information concerning specific frauds and investigations, but more general consultations around issues such as the coordination of overall anti-fraud strategies have taken place and should be encouraged. Many large companies also employ persons with law enforcement or other official expertise in security and loss-prevention capacities, which helps ensure consistency of approach and maintain channels of communication.

Information-sharing about ongoing cases or new offender developments is particularly important with many modern mass-frauds, in which many different victims, jurisdictions and public and private-sector entities may be affected, each having only limited information. Relatively fast reactions are critical both to limit victimisations and launch coordinated investigations before important evidence is lost, especially when the frauds employ telecommunications media. Such frauds may first become apparent only when unusual patterns of reporting are noticed by law enforcement or patterns of commercial activity become apparent to private entities such as financial institutions or telecommunications service providers. Within the applicable legal limits, the sooner all of the commercial entities and investigative agencies in all of the jurisdictions affected can be alerted, the better. Companies can often take action to limit the damage, such as delaying funds transfers, and if they are not permitted to alert law enforcement, they may be able to encourage their customers to do so directly or authorise disclosure of their information. Law enforcement agencies, if alerted early, can work more quickly both to take action to halt
illicit transactions and to build cases for eventual prosecution. Several States indicated that they supported the successful use of dedicated websites as a form of “clearing-house” where information could be shared quickly and some commercial industries also maintain facilities where individual companies can exchange information.

Some States also noted that there are some legal and policy constraints on information-sharing, however. Information about customers is protected from disclosure by privacy laws in many countries, and commercial entities also have common concerns about the potential for civil liability if they disclose such information. Some information may also be sensitive for proprietary or competitive reasons, and most major commercial entities believe that publicly disclosing the fact that they have been successfully defrauded may cause them as much or more harm in indirect or non-economic areas such as loss of confidence of customers or investors than the direct economic damage caused by the fraud itself.86 Information security is also an issue in this area. Both companies and law enforcement share an interest in ensuring that information about fraud developments does not fall into the hands of offenders who can use it to avoid security measures or investigative scrutiny or modify their schemes to reduce the effectiveness of warnings or other preventive measures. Anti-fraud messages have in the past been exploited by offenders, especially in recovery schemes in which the deceptive element consists of promising those already victimised that the new offenders will assist in recovering the earlier losses. Law enforcement agencies also have concerns and restrictions on their ability to share information with the private sector. Case-related information can be sensitive for investigative, evidentiary and legal or human rights reasons.

The possibility of private financial or other support for prevention, investigation, prosecution or other public sector functions was considered. Private support may offer substantial advantages to both public and private interests, but there are some concerns about ensuring that this does not affect the independence of law enforcement, prosecutorial or judicial functions. Commercial interests affected by fraud may derive substantial benefits from any enhancement of public enforcement capacity and deterrence, and may well view financial or other support as a form of investment in loss-reduction. Provided independence is not compromised, public sector interests may derive benefits in terms of training, better

information about both legitimate and fraudulent commerce, and general investigative capacity. The extent to which private resources can safely be mobilised may vary, depending on the nature of the assistance provided and the system in which it is provided. Assistance with training, prevention and other general matters is likely to be less problematic than support which might influence independent decision making on specific cases, or financial contributions which might have conditions attached, and the viability of any form of assistance may be greater in States where there are comprehensive and well-established rule of law safeguards to protect the independence of the judicial, prosecutorial and law enforcement processes.

VII. The prevention of economic fraud

A range of possible preventive measures were raised. Fraud involves the deception of victims, and some responses discussed information campaigns to warn and educate potential victims. Other measures raised focused on technical means of prevention involving the use of technologies and practices to make fraud more difficult to commit and to increase the likelihood of early detection and disruption before a major fraud can be completed or before large numbers of people can be victimised in a mass fraud. Several States noted the importance of fast and accurate information-sharing to permit timely and successful education and disruption efforts. One respondent noted that a side-effect of public information campaigns could be apparent increases in offending rates, as disincentives to report cases were reduced and more cases were reported, but this did not affect the usefulness of education as a preventive measure. Some States also mentioned the education of persons other than victims, particularly employees of banks or financial institutions which were likely to encounter frauds. Some compared such efforts to measures against money-laundering, suggesting that workers being trained to identify suspicious transactions for purposes of detecting money-laundering could also be trained with respect to characteristics that could raise suspicion that a transaction was fraudulent. Some also cited the utility of some anti-corruption methods in preventing fraud, especially frauds against governments noting that measures to make procurement and similar systems more resistant to corruption also made fraud more difficult. One also noted that the use of orders banning those convicted of offences from future participation in commercial business (e.g., by license-denial) might be of some use with repeat fraud offenders. Another noted that simple precautions, such as safeguards on processes for changing postal addresses
and re-directing mail, undertaken by businesses and customers, had substantial preventive potential.

A number of States and commercial sources indicated the importance of technical security measures. In some cases, commercial technologies were not seen as viable at all without technical security elements, such as the asymmetrical cryptographic systems employed in all modern payment-card technologies. Technical measures were seen as necessary at almost every element of a commercial system, including elements in the hands of individual users, such as payment cards, communications between system elements, and system elements which process or store data. Payment cards or documents must be resistant to copying, communications must be protected from interception, reading or alteration, and stored or processed information must be protected from unauthorized access or tampering. The means of protection raised included measures such as the use of computer chips to make payment cards harder to “skim” and copy; the use of PIN-TAN access codes, in which both a permanent Personal Identification Number and a further one-time transaction number (TAN) are required; the use of digital chips or other devices in cards to deter copying and expedite reliable verification; the use of encryption, anti-virus and firewall software to make systems resistant to cybercrime attacks; and the use of physical security and electronic and video-surveillance to monitor employees with access to sensitive data and in some circumstances to document the activities of customers.

Several key technical security challenges were raised. The global nature of commerce and communications requires global standards for security and interoperability. Without this, offenders can easily target a global system in places where security is weak or absent, and customers from some places could not access or use systems in other places where security measures were not interoperable. Another challenge is the constant evolution of commerce and the ways in which most technologies are used, and the corresponding evolution of criminal techniques as offenders adapt. This generates pressures on business to develop and deploy new measures, on law enforcement to develop new prevention and investigation methods, and on both companies and States which have extensive capacity to transfer knowledge to companies and States which do not to avoid weak security areas which offenders can exploit. For commercial interests, issues of cost and competitiveness also arise. There is sometimes controversy over how the cost of prevention and investigation should be allocated among State and commercial interests. Companies also compete domestically and globally, which makes it essential that prevention and security measures be presented as attractive to customers,
and in some cases that legislative or regulatory standards be established to ensure that all companies are competing fairly under the same conditions.

Much of the focus in international cooperation against fraud is on reactive measures such as the investigation and prosecution of fraud when cases are ongoing or have already occurred, and most States did not discuss prevention when they provided information about international cooperation. However, there are areas where international cooperation can play an important role in prevention, and the costs and complexities associated with investigating and prosecuting major transnational fraud cases suggest that the benefits of cooperative prevention efforts may be substantial. Many States noted that a substantial amount of major and transnational fraud cases involve organised criminal groups, which suggests that the prevention and cooperation provisions of the 2000 Convention against Transnational Organized Crime may be applied in some areas. In particular, Article 31 of the Convention sets out a range of possibilities for the prevention of transnational organized crime, based primarily on measures taken within each State Party, and Article 31, paragraph 7 calls on States Parties to cooperate with one another in developing and promoting these preventive measures. International cooperation in prevention requires sharing information, but the nature of the information is such that this will not usually raise the security, sovereignty, human rights and other concerns that underlie mutual legal assistance proceedings. Information will usually consist of general information about trends, patterns and emerging offender techniques, and if case-specific information is shared, it need only be sufficient to alert appropriate officials to the fact that a new fraud pattern is suspected and provide them with enough information to identify it. Such information may be sensitive from a commercial or investigative security standpoint, but could probably be shared informally in many cases.

C. Results of the Study on Identity-related crime

I. Introduction

1. The nature of identity-related crime

The ability to establish and verify unique identity is often so fundamental as to pass virtually unnoticed unless it is being actively used or misused. Identity itself is composed of information, which must be created and linked to the specific entity being identified. Identification information must be transmitted, stored and retrieved, and it is usually linked to other information about the individual it identifies, such as
nationality or citizenship status, financial or banking records, criminal records and similar personal or commercial information. The fundamental role it plays in so many different systems opens a vast range of opportunities for crime if basic identification information can be altered or falsified, or if the systems by which it is created, altered, retrieved and used to verify identity and access other information can be subverted. For this reason, virtually every State has applied its criminal law and criminal justice systems to identity-related issues in some way. Illicit conduct carried out using stolen or fabricated identity information, such as economic fraud, illegal entry into a State and impersonating public officials are already crimes in most States, and many have additional offences to protect key identity documents, such as the forging or illegally obtaining of documents such as passports and the possession of stolen or falsified identity documents.

Identity-related crime itself is not new, and these offences have existed for many years, but many of the same factors which have influenced economic fraud and cybercrime have also led to substantial changes in the nature and extent of such crime, as offenders have adapted to new technological opportunities. In recent years, some States have begun to consider the problem from the perspective of identity itself. In addition to criminalising the actual misuse of identity, it is suggested that underlying, preparatory or supporting conduct such as taking, copying or fabricating identity, tampering with identity systems, and trafficking in identity documents or information should be treated as a new and distinct form of criminal offence. This recognises that a primary abuse of identity can lead to a range of secondary crimes and allows the criminal justice system to intervene at an earlier stage. It also recognizes that, where a genuine identity is used to commit other crimes, the person identified by the genuine identity and those targeted by the subsequent crimes both suffer harm and should be considered to be victims of crime. It further recognizes that, especially in cases where organized criminal groups are involved, identification information or documents have become an illicit commodity, transferred from the offenders who commit identity-related crimes to other offenders who commit other crimes using that information or falsified identities based on it.

2. Use of terminology in the present Study

In the absence of a generally-agreed label or definition, the convening resolution for the study used the general description “...criminal misuse and falsification of identity and related crimes...”, leaving definitional questions to the expert panel. The experts themselves decided
on a preliminary and non-prejudicial basis to use the term “identity fraud”, but as results accumulated, it became apparent that other experts and the States themselves were not using the labels “identity theft” and “identity fraud” consistently. In the case of identity fraud, some included conduct where a genuine identity was taken by fraudulent or deceptive means, such as on-line “phishing” schemes, whereas others included only conduct where the false identity, however obtained, was used in a fraudulent manner. Other conduct, including the fabrication of entirely fictional identities and illicit trafficking in identification documents or information, did not seem to fit within any of the definitions. Some countries have begun to consider terminology more specifically, but only one provided a legislative definition, and most just indicated that the description proposed by the questionnaire was an accurate reflection of problems that they had encountered.

As a result, the experts decided to use the general term identity crime to cover all forms of illicit conduct involving identity, including the new concepts of identity-theft, identity fraud and trafficking in identity information, as well as existing ones such as impersonation and forgery of identity documents. This was, of necessity, forward-looking, as most States have not yet specifically criminalised most of these abuses. One problem of scope is that identity seldom exists in isolation and in many cases much the same illicit results could be accomplished by tampering either with identity information itself or with other information to which it was linked. A person seeking to avoid the consequences of a criminal record, for example, could do so either by assuming a new identity, or by maintaining the existing identity but using means such as bribery or corruption to remove prejudicial information from the records. One State noted that a substantial amount of migration-related crime was not identity-theft or identity fraud because it involved the real identities of migrants but concealment of other information or legal status. For purposes of the study, which was mandated to also look at the relationships between identity crime and other crimes such as fraud, money laundering and terrorism, an inclusive approach was taken, and in most cases the broader term identity-related crime was used to include such scenarios. A further issue is that identity crime involves the misuse of genuine identities, the fabrication of fictitious ones and other related conduct. For this reason, the terms false identity or falsification of identity or identity documents included three

---

87 E/CN.15/2005/CRP.5, question 33.
types of misconduct: the invention or fabrication of a wholly-fictitious identity; the alteration of a genuine identity or use of parts of a genuine identity; and the use of a genuine identity by a person other than the genuine individual or in the case of documents, lawful holder of the document.\textsuperscript{88}

Identity theft generally refers to occurrences in which information related to genuine identity is actually taken in some manner analogous to theft or fraud. This includes conduct ranging from the physical theft of documents (e.g., by pickpockets), the taking of other documents, even if discarded or abandoned, and various means of taking information on computer systems, including conduct such as “phishing” or “hacking” in which information is taken without authorisation or system users are deceived into surrendering it voluntarily. Identity fraud generally refers to the use of identification or identity information to commit other crimes or avoid detection and prosecution in some way. In this sense, the element of deception, and hence the term “fraud” lies not in the use of deception to obtain the information, but in the subsequent use of the information to deceive others. As with economic fraud, this element of deception includes the deception of technical systems as well as human beings. Thus the taking or copying of credit card information would be identity theft, and the subsequent use of a (genuine or forged) credit card to deceive a person or machine would be identity fraud. If the deception generated illicit economic losses to victims and/or enrichment of the offender, it would also be economic fraud.

II. The basis of identity: means of identification used in Member States

1. Public and private identification systems

Identity-related crime is linked to the means used to establish identity, which can vary substantially from State to State and depending on the reasons why identity or identification are needed. Most States indicated or referred to both public and private sector infrastructures, and most described a range of application-specific forms of identification. Within the public sector, some States described national identification schemes, in

\textsuperscript{88} See Interpretive Notes for the Official records (Travaux Précis) for the Convention against Transnational Organized Crime, commentaries on common Article 12 of the Protocols dealing with trafficking in persons and the smuggling of migrants (Security and Control of Travel or Identity Documents), A/55/383/Add.1, paragraphs 82 (trafficking) and 105 (smuggling).
which the government created and maintained a centralised system whose only purpose was to establish identity. However, most States appear to rely primarily on forms of identification which are established for specific applications, such as drivers’ licenses for the operation of motor vehicles and passports for international travel. Birth certificates and citizenship certificates are also common. Within the private sector, identification tends to be issued for specific commercial purposes, such as gaining access to bank accounts or credit, although there may be some recent trend to the establishment of more generalised forms of commercial identification by companies who specialise in this. The most commonly cited means of commercial identification was the credit card.

Views on national identification schemes appear to vary. States were not asked to provide information, but in some countries national identification requirements seem well established and widely accepted, both as a public security measure and as a form of support structure for commercial and other private activities. However, similar measures are often seen as controversial and raising privacy and other concerns when they are proposed in countries where they have not been seen before. One country which has a centralised identification system referred to its dual use. It had originally been established as a means of locating and identifying residents for public purposes ranging from domestic security and crime control to maintaining accurate population and determining eligibility for voting, but was now increasingly being relied upon as a form of support-structure for a range of private commercial applications. That country noted that, to the extent that commercial and other private interests relied on public identification systems, those interests might be asked to share the high costs of maintaining a centralised system.

2. The concept of “identification information”

States were asked to comment on the concept of “identification information”, which was described in the questionnaire as information which can be used alone or in combination with other information to establish identity. Almost all of the States which discussed this issue did not recognize the concept in legal or legislative terms, although several which were examining identity-related crime as such had begun to consider it. Most of the other States who responded referred instead to specific types of document considered as identification for various public and private purposes. Many also referred to terms such as personal information, which generally included identification information, but also other information about status or activities of persons identified which was of a personal or private nature, but might not necessarily be necessary or sufficient to
identify an individual. This is a key concept underlying European laws on privacy, and most European countries referred to it. In the case of a bank account, for example, information such as names, account numbers and signatures or personal identification numbers would be both identity information and personal information, whereas information such as account balances or transaction records would be personal information only. Many States reported the establishment of offences and other measures to protect personal information which would apply to most or all identification information. Many also reported offences such as theft, forgery, trafficking and illicit possession or use that were specific to certain identification documents such as passports.

Identity information is necessary to establish identity, but it is not always sufficient, and most systems use multiple identifiers, such as name, gender, date of birth and other factors to ensure uniqueness. This means that, unless legally defined, what constitutes “identification information” might vary from one case or context to another. In addition, many systems may require knowledge of other personal information which is not itself “identification information”, such as knowing the names of relatives, to corroborate or verify identity. Most common identity documents contain several elements of identification information for this reason, and automated modern commercial identification such as debit and credit cards tend to require at least two elements, one from the card or document, and one from the individual it identifies. Increasingly, in modern identification systems, identity information is fragmented, with identity based on several elements in different places on the underlying assumption that it will be harder for offenders to falsify such information or subvert the systems which accumulate, store and transmit it when identity is to be verified. Offenders, for their part, have focused on finding new ways to accomplish one or the other. A successful debit-card fraud, for example, requires that offenders obtain both a card with digital information identifying the holder and the location of his or her bank account, and the personal identification (PIN) number needed to access the accounts.

Approaches to what constitutes identity information may depend to some degree on cultural elements or local traditions. Arabic-speaking countries sometimes link an individual’s name with a town or village of family origin, for example, while several cultures incorporate names of fathers or mothers. Many common names in European countries originated with the profession or occupation of the holder, although they are now standardised as surnames and passed on by inheritance or marriage. Approaches to the concept of identification information also varied to some degree depending on the extent to which traditional face-to-face recognition
has been gradually replaced, first by photographs and information on paper documents, and more recently by electronic means which can receive information and verify it by comparing the individual, information stored on documents or cards in the individual’s possession and information stored elsewhere.

The most commonly-cited information for paper-based documents included various names, including common or given names, family names, names of parents, date and place of birth, and current places of residence or business. For electronic systems, information included either full names or abbreviated “usernames”, passwords, personal identification (PIN) numbers, transaction-identification (TAN) numbers, and digital signatures and other cryptographic applications. A number of application-specific identifiers, such as numbers used for identification in public benefits or taxation systems, bank account and credit card numbers were also mentioned. A new area of development where the technological support is present is a range of physical or “biometric” identifiers, including DNA information, fingerprints, photographs, voice prints, images of iris or retinal tissue. Photographs are relatively easy to use and are common. Other biometric identifiers generate a high degree of security, but raise privacy concerns and tend to be expensive, making them common only in areas where the costs are justified by the need for security or other factors. For example, fingerprints, and more recently DNA radiogram profiles, are commonly used in criminal justice systems because they offer a high degree of certainty, because suspicion of criminality or a criminal conviction justifies the privacy infringement involved, and because both fingerprints and DNA evidence are commonly left by offenders at crime scenes. They are very reliable and unique, but also require expensive equipment and individual skill to record, transmit and verify.

Two States reported relevant legislative or other provisions. One used the term “identification data” to refer to electronic information which is a constituent element of identification in its automated systems. A second reported a definition of the term “means of identification” used as an element of an offence relating to identity theft. Reflecting the need to capture a range of fragmented identity information, its legislature defined “means of identification” as “…any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual…”. The provision then continues with an indicative list of common elements used on paper identity documents, electronic or computer systems and biometric information, effectively ensuring that key types of identification will not be left out and providing interpretive guidelines to assist its courts in applying the general definition.
III. Identity-related crime

1. Types of crime encountered and legal responses

As noted, only one State reported that it presently has an offence and legal definition, which it labels as “identity theft”. Its legislation defines “means of identification”, and then criminalises the knowing possession, transfer and use of such information without lawful authority. Several other States indicated that they were examining the underlying concepts of crimes based specifically on identity abuses, including the taking, fabrication and improper uses of identity information, including its use to commit other criminal offences. Almost every State which provided information indicated that at least some of the specific forms of conduct covered by the proposed description of identity fraud or some closely-related conduct was criminalised in its system in some form. There seems to be fairly broad consensus that some forms of identity abuses should be the subject of criminal offences and punishments, but some variations with respect to the exact types of conduct that should be criminalised. The established or traditional approach of governments has been to focus on the abuse of identity only in the context of other crimes, either as a form of preparation or constituent element of crimes such as economic fraud, migration-related offences, and other crimes where false identities are used either to commit the crime or as a means of avoiding prosecution and punishment.

The most commonly described offences were those related to forgery, including the forgery of identification documents, and forms of impersonation, including the misuse of identification documents or information. A number of specific identity abuses were also subsumed within broader crimes where the underlying conduct was criminalised in general and not just in the context of identity. Examples include forgery offences which included the forgery of identity documents and cybercrime offences such as theft of data or unauthorised access to or tampering with computer systems, which would include data or systems used for identification purposes. Some States also described offences which were specific to types of identification or identity regarded as particularly critical. Many States have specific offences such as forgery or unauthorized use of passports or government identification, or offences such as impersonating law-enforcement officials or other public officials, for

89 This was the situation as of 31 December 2006, when the last survey instruments were collected.
example. States which are Parties to the *European Convention on Cybercrime*⁹⁰ are required to ensure either that their existing forgery offences cover computer or data-related forgery or to adopt new ones which do so, and a number of computer-forgery and computer-fraud offences were reported. Several States reported offences dealing with computer “phishing” and similar conduct, and in other States this may also be covered by more general cybercrime offences, such as those covering the theft or illicit possession of passwords.

Another means of subverting identity systems is to attempt to deceive or corrupt the issuance process into issuing valid identification to a person not entitled to have it. Several States reported general offences of bribery and corruption and more specific ones relating to the use of false or misleading information for the purposes of obtaining passports, licenses or other identity documents. Some States also noted that some means of illicitly obtaining identity information were covered by existing theft offences, such as the taking of identity documents. These may not apply, however, in places and circumstances where intangible information is involved and is not seen as property for purposes of theft offences or where it is taken from open sources such as discarded documents. Existing offences of economic fraud may also apply to conduct such as “phishing” if it can be established that the identity information taken by deception meets legal requirements for economic value. A few States also reported offences relating to the illicit or unauthorised possession of identification, and several described offences of illicit transfer of or trafficking in either identity documents or identification information, such as computer passwords or credit card information. Some of those who reported offences of this type noted that criminalising simple possession or transfers was over-broad and it was necessary to have additional limits in their legislation to distinguish between legitimate and illicit activities.

Several States reported experiences with or concerns about the potential for offenders to obtain identity information about large numbers of individuals through computer hacking and similar crimes. General offences adopted by countries implementing the European Convention on Cybercrime would also apply to the unauthorised access to or taking of any information, including identity information, from computer systems⁹¹. A

---

⁹⁰ ETS No. 185, Budapest, 23 November 2001, Article 7 (computer forgery).
⁹¹ States Parties are required to criminalise, *inter alia*, unauthorised access with the intent of obtaining data, interception of data, and interference with data or
few States also mentioned offences in the nature of the possession of or trafficking in instrumentalities or elements of identity documents, such as blank document forms, identity stamps, or the hardware or software needed to read and copy debit or credit cards. Some also have more general offences such as the possession of computer-hacking software, which would also apply to software designed or used for accessing identity information or identity systems.

Responses suggest many specific offences are based on policies of providing additional protection or deterrence for specific documents where misuse is either seen as likely or particularly problematic, such as passports, national identity documents, some forms of government identity documents and in the private sector, credit cards. A number of States mentioned offences of impersonation or substitution of personality, and some of these indicated that such offences included both assuming the identity of another person, and fabricating and assuming the identity of a non-existent person. Some countries also identified gaps or challenges under existing laws in this area. One mentioned the fact that, while forgery offences included the making of forged paper or electronic documents, the mere transfer or possession of identification information was not necessarily a crime. Several also noted that, unless the facts constituted theft, the simple taking or possession of identification information or documents was not necessarily a criminal offence, although some did report offences of possession for the purpose of committing other crimes.

2. Means used to commit identity-related crime

Most States have no formal or consolidated information about the means used to commit identity-related crime, which precludes any statistical analysis or comparisons. However, several States did describe offender methods that had been commonly encountered or were of particular concerns to their officials. To some degree, means used varied depending on the nature of the identification and supporting structures involved, the purpose for which they are used, and the means available to offenders. For example, computer hacking was not raised as a major concern by States in which identification is still based primarily on paper documents, but for both fraud and identity-related crime, these States did express concerns about the use of document scanners, computers and systems. See Convention on Cybercrime, ETS No. 185, Budapest, 23 November 2001, Articles 2-5.
printers to produce high-quality forgeries of a range of documents, including identification documents.

For most identity-related crime, identification information must be taken, copied or plausibly fabricated; rendered into some useable form; and then used. The means used by offenders to obtain identification information ranged from the theft or copying of complete documents to various means of obtaining partial information which was not itself sufficient to establish identity but was used as the basis of plausible applications used to obtain genuine identification documents. Often this could be done through open public sources such as registries for birth, death or other records. Some States noted that they had seen cases where the identity of a person who had died at a young age was effectively resurrected, so that legitimate birth records would be found, if searched. Once an appropriate name was obtained from a source such as a newspaper death notice, the offenders could file fraudulent applications for birth certificates and other basic identification, with each successive element used as the basis for further applications to gradually build a comprehensive identity. A number of States reported the physical theft of identity documents by “pickpocket” and other theft schemes, and the collection of information from personal correspondence or financial documents discarded as trash. Several States had also encountered cases in which postal mail was diverted by offenders pretending to be addressees. Aside from collecting any payments sent through the mail, sufficient information about banking, credit and other personal business affairs could be accumulated to permit offenders to assume the victims’ identity before the diversion was noticed.

As the use of information and communication technologies for basic public identification purposes as well as a range of commercial applications has increased, so have related criminal offences, and a substantial number of States reported experiences and concerns about identity-related crime which targets victims based on their use of these technologies or exploits related vulnerabilities. The most common related to “phishing” or “pharming”, in which users of computer networks are deceived into providing offenders with user names, passwords and other electronic identification information. In its most primitive form, victims are simply sent e-mail messages by offenders claiming to be service providers or other authorities and asked for the information, but these have rapidly evolved. Several States noted that the most common form now involved the use of web sites, which are often hosted in countries distant from both offenders and victims, accumulating information which could be periodically downloaded. These make communications harder to trace and enhance the credibility of solicitations. One State noted that it had traced
such sites to at least ten different countries and noted that the location of the computer servers hosting such sites were unlikely to be the same physical location of the offenders who had set them up.

Other forms of cybercrime have also been encountered, including malicious software infecting individual victim computers in the form of viruses, worms, spyware and adware designed to capture personal information and transmit it to a second location and the invasion of commercial web sites by “hacking” to obtain credit card data and other customer identification information. Identification information, especially if obtained in large quantities, has become a form of illicit commodity, being obtained by offenders specialising in identity-related crime and sold to other offenders for use in other crimes such as economic fraud, and a number of States had encountered cases where such information was taken in one country and used in others, having been quickly transferred by e-mail or similar means. The concerns of commercial entities about customer confidence have also led to stolen identity information being used as the basis of extortion offences, in which offenders take the information and threaten to publicise it or the fact of the theft if not paid.

A number of States reported methods used to gain identity information relating to debit and credit cards, primarily for subsequent use in forms of economic fraud. Digital information was gathered by “skimming”, or running the card through a data-reading device. In the case of debit cards, the devices were attached to automated teller (ATM) machines, along with miniature video cameras to record users’ personal identification (PIN) numbers. Other States had seen cases where identity information was obtained by officials with inside access to government or commercial systems or obtained by outside offenders by means of bribery or other corrupt means.

Once obtained, digital identification information can often be used immediately to impersonate the victim, and the need for fast responses to limit the harm caused in such cases was mentioned by several respondents as a challenge, both for public law-enforcement and the private sector. In the case of physical identity documents, further steps were often needed by offenders in order to convert stolen documents into a useable form or to use acquired information to obtain or produce new documents. One exception was credit cards, which if stolen must usually be used quickly by offenders before the theft becomes apparent and the cards are cancelled. Physical identification documents have become more sophisticated, requiring greater expertise, resources and equipment to modify or imitate, and some responses mentioned the use of equipment such as printing presses and forged official seals, which would suggest the involvement or support of
organized criminal groups. Many modern documents would also require either the theft of blank documents or sophisticated techniques to make or imitate papers and inks.

While information and communications technologies have in some cases made documents harder to tamper with and provided the means of fast, secure verification when documents are used, they have also brought some means of document forgery within the reach of large numbers of individual offenders, who may be able to use sophisticated scanners and printers to produce convincing imitations of such documents. To a large extent changes to both public identification documents such as passports and private documents such as credit – and debit – cards in recent years reflect a fairly rapid evolution in information, communication, printing and other technologies, but they also reflect a corresponding evolution in crime as offenders have found ways to use the new technologies.

Aside from tampering with physical documents, identity related crimes can also be committed by tampering with the underlying systems to which the documents are linked. This has become more important as modern systems have been developed which allow identification to be verified in real time when it is actually used. For example, major credit card issuers now require an independent validation exercise, usually by telephone, before activating new credit cards as a safeguard against physical interception or diversion of the cards themselves, and banks which rely extensively on ATM or cash-dispensing machines routinely caution customers against writing down personal identification numbers or allowing them to be seen by others when being entered into a machine.

Not much information was provided about how and why offenders choose methods, but some inferences can be made from the information available. Major factors include the nature of the identification information involved, the systems used for creating, altering and verifying identity, and the means which are available to offenders. As noted, paper-based identity systems cannot be attacked using computer hacking, but computers can be used to produce false documents, and computer hacking can be used to tamper with the information used to validate or verify paper identification documents. Identity-related crimes are most commonly committed in support of one or more specific secondary offences, such as illegal entry into a country or credit card fraud, and methods reported also appeared in some cases to be chosen with this in mind. For example, in countries where passports and visas are elaborate and difficult to forge, offenders may be more likely to build up false identities using other forms of identification and then obtain genuine passport documents using fraudulent applications.
based on those identities, offences described by one State as passport or visa frauds. Another use of false identities raised was simply to avoid detection or surveillance in the course of ongoing illicit schemes such as those of organised criminal or terrorist groups, and for such applications offenders would be more likely to choose documents and means for which the falsification would remain undetected for an extended period.

IV. The relationship between identity-related crime and other factors

1. Other crimes associated with identity-related crime

No States offered statistical information on links between identity crime and other offences, but a number offered opinions based on the views and experience of domestic law enforcement and other experts. Primary links fell into three groups, based on how false or assumed identity was used. First, it was used to gain access to physical places or electronic accounts so that other crimes could be committed. Second, it was used to shield the true identities of offenders before and during the crime to avoid detection, interference and criminal justice consequences. Third, in the case of economic fraud and similar offences, it was also used as part of the central deception, to enhance the credibility of offenders and the attractiveness and plausibility of the fraud scheme. Some States gave examples of offenders impersonating public officials or employees of banks, financial institutions, telecommunications providers and other key commercial enterprises for this purpose.

While the most common links between identity abuses and other crimes involve the identities of offenders, abuses of the identities of victims can also be an issue. Many country reports on trafficking in persons mention the confiscation of victims’ passports or identity documents by offenders as a means of controlling victims or preventing them from fleeing. While the Protocol to Prevent, Suppress and Punish Trafficking in Persons does not require States Parties to criminalise the deprivation of identification as an element of trafficking or related offence, some States have done so as an element of anti-trafficking legislation92. The United Nations Convention on the Rights of the Child also establishes the right to

be registered at birth as a means of establishing identity\(^\text{93}\), and the systematic deprivation of the *indicia* of identity in order to prevent expelled victims from returning or claiming status or property rights has been cited as an element of cases of genocide or ethnic cleansing\(^\text{94}\).

While no statistical information about the relative prevalence of identity-related crime and links to other offences was available, most experts appear to consider the most common link to be with economic fraud and similar crimes, in part because the crimes themselves are very common in most States, and in part because identity abuses are so central to the success of most frauds. There is some additional support for this assessment in the fact that many commercial entities link fraud and identity issues both generally and in patterns which are specific to frauds such as common forms of bank and credit-card fraud, and in the fact that many States apply the same experts in law enforcement and policy development to both economic fraud and identity-related crime.

A number of States also referred to the role of identity crime in money-laundering, although most did not provide much detail. Much of the effort against money-laundering consists of either mechanisms which identify funds or assets as proceeds of crime *ab initio* and then seek to trace them through various laundering transactions, or mechanisms which identify transactions which are suspicious or indicative of money laundering and then seek to trace the proceeds back to the original predicate offences and forward to their eventual destinations. Deception about the identities of the parties to a transaction can be used to elude or screening or surveillance of the transaction and avoid triggering anti-money laundering measures in the first place, and it can also be used to frustrate efforts to trace the proceeds. Also, as with other forms of crime, if assets are eventually proved to be proceeds and confiscated, false identities may still shield the offenders from criminal liability for money-laundering and related offences.

Many States expressed particular concern about identity crime involving travel or related identity documents. This was seen as both a

\(^{93}\) A/RES/44/25, Annex, Article 7, paragraph 1. See also *International Covenant on Civil and Political Rights* A/RES/2200 A (XXI), 16 December 1966, UNTS 14668, Article 24, paragraph 2 (right of child to registration and name at birth) and Article 16 (right to status as a person before the law).

crime and a security issue, as passports, visas and similar documents and
the relating infrastructures are essential to the control of national borders
and the exclusion of known terrorists, criminal offenders and illicit
migrants. It was also seen as being linked to organized crime through
offences in relation to trafficking in persons and the smuggling of migrants.
One State noted that it had seen some document-related crimes that tended
to involve false passports using migrants’ true identities rather than identity
fraud or identity theft, which involved the use of false or fabricated
identities. A further area mentioned was cybercrime, to which a number of
links have been encountered. Apart from the deception of victims to obtain
computer-related identity information, several States also mentioned the
use of fraudulent identities and credit cards to obtain untraceable
telecommunications services for use in other crimes, including terrorist
activities.

2. Relationship between identity-related crime and organized crime

A number of States reported that they had seen links between
organised criminal groups and identity-related crime. The most commonly
encountered scenarios involved organized economic fraud, money-
laundering, schemes involving trafficking in persons or the smuggling of
migrants, and the use of fraud to obtain untraceable telecommunications.
These are discussed separately. Aside from the misuse of identity
documents or information as part of specific crimes or criminal schemes
such as money-laundering, some organized criminal groups may be
sophisticated enough to engage in identity-related crimes as a distinct
criminal operation. The responses suggest two major scenarios. The first
involves the more general use of identity-related crime by organised
criminal groups in order to protect their own members and operations from
law enforcement. In addition to avoiding surveillance of illicit activities,
false identities may be needed for routine, non-criminal activities such as
international travel. The second involves the specialisation of groups and
treatment of identity documents or information as a commodity. A group
may develop skills in stealing or falsifying identities, which are then sold to
other individuals or groups for use in crime, illicit travel or migration,
terrorism or other conduct for which the use of legitimate and genuine
identification would be prejudicial.

As documents such as passports and identity cards have become
more sophisticated and resistant to alteration or falsification, forgery may
become only feasible where an organised criminal group with the necessary
resources, equipment and skills is involved. Alternatively, as documents
become more difficult to forge, the use of false applications to obtain
genuine documents becomes more attractive, and this also may require the sort of experience and sophistication normally associated with organised criminal groups. Aside from learning to identify and exploit any weaknesses in identification processes, organised criminal groups are more likely to be capable of multi-stage identity schemes, in which identity information from one source can be used to submit fraudulent applications for genuine documents in an effort to build and maintain more solid and elaborate fictitious identities. The genuine documents can then be used to avoid various forms of surveillance and travel anonymously, nationally and internationally.

3. Relationship between identity-related crime and terrorism

Only a few States raised links between identity-related crime and terrorism. Of those who did, the primary concern was essentially the same as for organised crime and other problems: that terrorist organizations could use identity-related crime to obtain identification information and documents that could in turn be used by terrorist operatives to operate without the surveillance or arrest that would occur if their true identities were known. In the case of terrorism, most of the concern appears focused on the need to increase the security of travel-related identification in order to curtail the international movement of terrorist suspects, but the same issues arise with respect to purely domestic identification and activities such as obtaining and driving motor vehicles, conducting banking and financial transactions, obtaining credit cards, and gaining access to public benefit schemes. Purely domestic identification security measures and international travel are also linked, as domestic identification is often used as the basis for obtaining passports, visas and other travel documents. As with organised criminal groups, terrorist groups may be sophisticated enough to carry out long-term and multi-stage identity-related crimes, in which false identities are gradually built up by obtaining routine domestic identity documents such as drivers’ licenses or credit cards, and then used to obtain more secure forms of identification such as passports or forms of employment-related identification needed to gain access to secure locations such as airports or government facilities.

Other official sources consulted by experts set out examples of terrorist suspects obtaining and using passports and other identity

---

documents intended to avoid surveillance or scrutiny they might otherwise attract. These include documents which are forged or altered or which are genuine but obtained using false names, such that key information such as names or birth dates will not correctly identify the user or be linked with incriminating records. Another pattern encountered involves false or misleading applications for new documents. Sympathizers may simply give documents to a terrorist organization for use in forgery and then falsely claim them as lost or stolen to obtain a genuine replacement. Suspects whose passports record travel to countries which would attract suspicion may also dispose of them and falsely obtain replacements without this information.\(^6\) Another concern raised by some States, as with economic fraud, was the use of basic frauds against telecommunications providers to obtain anonymous and untraceable mobile telephone, Internet or other telecommunications services.

Absent clear evidence of the direct involvement of terrorist individuals or groups, identity-related crime associated with terrorism may be difficult to distinguish from other related crimes, and especially organized crime. As noted, the many of basic uses of identity-related crime would be the same for organized criminal groups and terrorist groups, and as identity-related crime emerges as a new and distinct area of criminal expertise, there is the possibility that terrorist groups which lack their own expertise may simply purchase false identification documents from organised crime. Identity-related crimes are also often associated with elements of many money-laundering schemes, in which false identities are used to defeat the tracing of funds from their origin in a predicate offence to their destination when either seized or used, and these same concerns would arise with respect to elements of the financing of terrorism.

4. *Relationship between identity-related crime and money-laundering*

Most States considered the subject-matter of money-laundering to be beyond the scope of the Study and did not provide detailed information beyond their existing legislation. However, it is clear from the information provided as well as from other sources, that many anti-money laundering measures depend heavily on identity or identification elements, and that many of the means used by offenders to launder proceeds of crime involve

identity-related crime. In its essence, money-laundering consists of conduct
in which proceeds of crime are physically moved or transferred by any
means in order to conceal their source or origins as proceeds of a predicate
offence and their ultimate destination or form, in order to defeat any
attempts to trace them, establish that they are in fact proceeds and to
confiscate them. From the perspective of offenders, these efforts involve
concealment or deception with respect to identity for several reasons. At
the preliminary stages, many control measures depend on the identification
of transactions which are deemed suspicious for further investigative
scrutiny, and one basis for suspicion is that participants to a transaction are
identified as being associated in some way with organized criminal groups
or with some specific offence. Identity issues may also raise suspicion only
in association with other factors. A transaction which involved large
amounts of cash or unusual commercial aspects might trigger suspicion in
combination with an absence of verifiable identification information, for
example.

The ability to identify customers or parties of financial transactions,
sometimes described as the “know your customer” principle, is a
fundamental element of anti-money laundering regimes, along with the
keeping of financial records and the reporting of suspicious transactions. The
identification of parties to a transaction may assist in establishing that
the funds or assets are proceeds, or assist in the investigation of underlying
predicate offences. At later stages, the identification of all parties to a series
of laundering transfers will usually be essential to the prosecution of
offenders, forensic tracing of proceeds and derivative funds or assets, and
to establishing linkages or continuity between the predicate offences and
the ultimate form and location of the proceeds to a sufficient degree of
certainty to support criminal confiscation. Reliable identification processes
also serve as a form of control or deterrent for other forms of economic and
financial crime, including economic fraud, an important consideration for
commercial operations such as the banking and insurance industries where
both fraud and money-laundering are major concerns.

97 See, for example, Convention against Transnational Organized Crime,
A/RES/55/25, Annex I, Article 7, subparagraph 1(a) and Financial Action Task
Force, 40 Recommendations, Recommendation #5, at: http://www.fatf-
gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.htm
98 See SCHOTT, P.A., Reference Guide to Anti-Money Laundering and
Combatting the Financing of Terrorism, World Bank, 2003, chapter VI, part A.
Some States noted that methods used for money-laundering were linked to the use of information, communications and commercial technologies, especially those which allow for the transfers of funds or assets based on automated or electronic identification processes. In processes where there is no physical presence of the parties, false identities can be constructed and used by offenders to avoid attracting initial suspicion and to defeat later attempts at tracing the proceeds. Access to commercial transfer technologies assists in such subterfuge, first, by making possible remote electronic transfers and supporting large volumes of legitimate transfers in which money-laundering, fraud or other financial or economic crimes can be concealed, and second, by providing the technological means of generating false identification information.

A further problem for anti-money laundering authorities is the underlying fact that technologies have permitted a dramatic expansion of international transfers and offshore banking. This complicates the regulatory environment by raising jurisdictional issues and increases the number of money laundering cases where they arise by bringing offshore banking and concealment within the reach of a much broader range of offenders. As with other crimes, technologies also support corresponding developments in crime prevention, security and investigative support, and the evolution of these technologies can be seen as an ongoing process in which law enforcement and offenders constantly adapt to one another, and commercial interests seek countermeasures which are, if not attractive then at least not repugnant to customers and are viable from a technical and commercial standpoint. The development of accurate and verifiable means of identification of parties which are never in physical contact has been an integral element of this process, essential both for the commercial viability of many systems and for the investigation and prosecution of money laundering and other crimes. More generally, the need to incorporate technical measures which support effective tracing and other measures against money laundering, including identity-based measures, is a significant influence on the evolution of commercial technologies, and was mentioned by some States as one area where effective cooperation between governments and the private sector was needed, at both the domestic and international levels.

As with identification documents and information in general, the other types of information to which identity is linked is also critical in measures against money laundering. In financial transactions, information which uniquely identifies a natural or legal person is used primarily to link the individual to other information such as legal rights in respect of property, rights of access to bank accounts, and to establish that the same
individual is involved where there is a course of commerce and repeated or related transactions. This has many commercial applications, but is also critical to the ability to trace proceeds of crime, especially if multiple transfers and multiple identities are used in an attempt to make such tracing difficult. Identity information is also used by both commercial and government entities to link individuals to records of criminal behaviour or other suspicious activity, and as the basis for comparing and verifying other information.

5. Relationship between identity-related crime and information, communication and commercial technologies

As with economic fraud, the role of information and communications technologies in identity-related crime is complex. Case examples provided included cases where technologies were central to the identity-related crime, and cases where technologies only formed one element or aspect of a larger offence. Offences such as the use of “phishing” or hostile software to obtain electronic identification information, most forms of ATM or debit-card fraud, and the use of “skimming” to commit credit-card fraud are all examples of offences in which the identification itself consisted of digital or electronic information, it was taken or fabricated using other information taken and transmitted using technologies, and was used in crimes involving information, communication or commercial technologies. Other examples illustrate the use of specific technologies for specific purposes. The most common reference, from countries which still rely primarily on paper-based identification documents, was the use of computer scanners and printers to produce high-quality document forgeries. While no examples were given, it is also possible that, once documents are scanned, the resulting data can be transmitted and used to produce documents in other jurisdictions.

On one hand, the greater reliance on technologies as opposed to personal contact in identification, especially in private commercial applications, has created new criminal opportunities for impersonation in which knowledge of passwords and other identifiers is sufficient to deceive automatic systems regardless of the offender’s true identity. The spread of technologies has also brought some sophisticated means for the forgery of both physical and electronic documents within the range of large numbers of relatively unsophisticated criminal offenders. On the other hand, technological development has included elements which tend to prevent or suppress identity-related crime. Some of these are inherent in new technologies, some are specifically incorporated to prevent crime or facilitate detection and investigation, and some have been developed and
marketed specifically to deal with new crime problems as they have evolved and become apparent. As with fraud, applications such as encryption and physical security measures are used to protect identity information, for example, and key physical documents such as passports, national identification cards and credit cards and other forms of commercial identification have all shown a steady progression in which anti-forgery measures have been incorporated. These include physical elements to make documents harder to produce, such as the incorporation of photographs, micro-printing, holograms, and computer chips, which still require relatively sophisticated equipment and knowledge to produce.

Perhaps the most powerful technical aid on the side of crime-control, however, lies in the area of telecommunications. Multiple identity-checks, based on the assumption that several separate identification systems are much more difficult to subvert than one, have long been an established practice in establishing identification. Modern, secure telecommunications makes it possible to quickly conduct such checks against multiple secure databases, and information technologies make the process fast enough to be practical in applications such as passport checks at border crossings. One State noted that where feasible, the increasing trend was towards what has been described as multi-factor identification, in which several different identifiers are maintained separately and cross-checked whenever identity was to be established or verified. These included elements in 3 basic areas: elements that the subject could physically possess, such as a debit or credit card or a national identity card or passport; elements that only the subject would know, such as passwords, personal identification (PIN) numbers or other unique personal information; and elements that were biologically unique to the subject, or “biometric” elements. These include some well-established elements such as photographs and finger-prints, and more novel identifiers such as images of the irises or retinalae of subjects’ eyes and radiographs of DNA profiles. In principle, biometric identifiers have been in use for some time, but in practice they are becoming more feasible as technological developments permit them to be recorded, stored, transmitted and read when needed for purposes of verifying identity.

6. Transnational elements and the need for international cooperation against identity-related crime

Based on experiences with cybercrime and fraud, extensive transnational elements seem inevitable for identity-related crime, and a number of States reported that they have encountered transnational cases. The majority of these involved offences related to passports, visas and other travel-related forms of identification, all of which are inherently
transnational in nature. These included offences related to identification documents specifically, such as forgery, alteration, misuse of genuine documents, abuses of the processes whereby such documents were issued such as the use of false applications or corruption of officials, and other offences committed in part though the misuse of these forms of identification. A number of States referred to trafficking in persons, the smuggling of migrants and other offences related to illegal entry or illegal migration. One State had seen cases where identity-related crime was linked to forms of economic fraud related to its immigration process, with potential immigrants being defrauded by offenders representing themselves as immigration consultants or experts giving false advice on how to obtain the desired immigration status and documents.

Digital identification information can easily be transmitted internationally, and the other major category of identity-related crime commonly mentioned as having transnational aspects was cybercrime offences. One State reported research showing that the computer servers hosting “phishing” web sites and the addresses to which hostile software programs were transmitting personal information were in a number of different countries. It noted that, as with most forms of cybercrime, the apparent point of origin for criminal communications was not necessarily the actual location of the offenders, since many route their communications through a series of countries in order to mask their true identities and locations, but that all of this activity clearly had transnational aspects and required international cooperation to conduct effective investigations and prosecutions. As noted, several countries pointed out that the data accumulated by “phishing” web sites and “hacked” credit card information effectively became an illicit commodity in its own right, purchased and sold among offenders.

Several States highlighted the importance of international cooperation in the investigation and prosecution of transnational identity-related crime, but not much detail was provided with respect to the specific forms of cooperation needed in such cases. A with economic fraud, most States saw existing frameworks such as the United Nations Convention against Transnational Organized Crime and the European Convention on Cybercrime as sufficient, and several also highlighted the practical utility of INTERPOL, EUROPOL and similar organizations as mechanisms for actually providing cooperation when it was needed. Most saw the specific forms of cooperation needed in identity-related crime as similar to what was needed for transnational fraud or other forms of cybercrime. Major or serious fraud offences and most of the other offences likely to be committed using stolen or fabricated identities are likely to be “serious
crimes” within the ambit of Article 2, subparagraph (b) of the United Nations Convention, making it applicable where the requisite elements of the involvement of an organized criminal group and transnationality are present, but as States proceed to consider identity abuses as a distinct form of crime the question of whether any new, specialised offences will also fall within the scope of application of the Convention will arise.

Several States did note that for “phishing” and other forms of identity-related crime, as with cybercrime in general, the speed with which both formal assistance and informal cooperation could be provided was sometimes critical. Transnational crimes involving computer networks can be committed very quickly, and it is often necessary to obtain assistance from all of the countries involved either while the crime is actually occurring, or within a relatively short period afterward, while communications traffic data can still be recovered. One issue not raised by most States is the fact that, aside from any economic losses, the harm caused by identity-related crime also extends to the identities of any real natural or legal persons whose identities have been misused. Damage to reputation and the viability of basic identity for personal and commercial purposes can be considerable and can in many cases be transnational in nature, with victims wrongfully identified in foreign government and private systems as criminals, terrorists or credit-risks. Measures to purge false information and repair identities may well be needed but would not fall within the ambit of most countries’ cooperation frameworks, which are limited to criminal matters.

V. Rates and trends in identity-related crime

Most States expressed the view that identity-related crime was expanding, and several noted what appeared to be very rapid expansions. Some of these noted expansions not only in the overall rates or volumes of occurrences, but also in the range and diversity of offences. Only two States suggested that identity-related crime was decreasing, and several other States indicated that their information was either insufficient or inconclusive. In the absence of legislative definitions and offences, most were able to provide only expert opinion or assessment, and only one State provided statistical information. That State reported early statistical information that suggests that identity theft is a substantial problem and is increasing. Even where statistics exist, the concept is still so novel that any dramatic increases could be attributable in part to growing public awareness of the problem, enhanced government attention to it and the recent development of reporting facilities, but the available data clearly
show a substantial number of occurrences. Large economic losses are also reported, but it is not clear to what extent these would be losses from economic fraud and other secondary offences committed by means of identity theft or losses from other causes, such as damage to victims’ reputations or the costs of restoring identity. One State also reported research into the number of Internet web sites being used for “phishing”, and found that the number of such sites tripled from 2005-2006. Assuming these figures to be accurate, they may reflect a pattern in which novel offences increase dramatically over a short period as knowledge of the techniques spreads and then level off as public awareness increases and countermeasures are developed.

Identity-related crime is also commonly linked to other forms of crime, and rates of identity-related crime also probably have similar links. The related problems or offences most commonly mentioned involved were forms of economic fraud and trafficking in persons, illegal entry or immigration and other travel-related crimes, and overall identity crime rates may therefore be correlated to such things as economic, social, conflict-related or other factors which influence migration and trafficking and the balance of economic and crime-control factors which influence fraud rates. Major movements of large numbers of refugees or migrants pose a significant identification problem for governments and other organizations involved, not just for criminal justice purposes, but also for basic immigration, tracing, family reunification and other matters and could also exert anomalous influences on rates.

Some of the States which indicated that identity-related crime was increasing cited several reasons that might contribute to such increases. These included official corruption, which weakened the systems for issuing and verifying identification and increases in some specific offences such as trafficking in persons, which are commonly associated with identity crimes. Also cited were increases supported by opportunities generated by expanding use of computer technologies and difficulties in developing and deploying technical measures to verify identification and generally keep pace with the evolution of criminal techniques.

VI. Costs of identity related crime

None of the responding States provided detailed information about the actual costs of identity-related crime, and only a few had estimates of total losses. A number pointed out that, in the absence of specific legislative offences, no accurate gathering or analysis of statistical information could be attempted, and some also noted that, given the nature
of identity theft, it would be difficult to separate the costs or losses from identity crime *per se* from other crimes such as fraud, committed using false or assumed identities. Those who did provide overall loss figures did so by aggregating all of the losses from all of the primary offences linked to identity crimes, and some commercial sources took this approach as well. Given some of the examples provided, it would be difficult to quantify some of the forms of harm or damage caused, such as loss of reputation, in monetary terms, and given the sustained duration of the harm, to determine an appropriate point in time for measuring it.

One State noted that a qualitative assessment of costs can be made, even if these cannot be quantified. It noted that, in general, identity-related crime causes harm or losses to distinct groups of victims, those whose identities are taken and misused, and those victimized by crimes committed using stolen or fabricated identities. These losses could affect both natural and legal persons, but the actual harm caused and the means of repairing any damage might well be different in a personal or commercial context. It suggested that harm or damage in the following areas could be expected in many cases.

a. Economic and non-economic losses are likely to be suffered by persons whose identities are taken or misused. Examples of non-economic losses range from embarrassment to cases of mistaken arrest and detention for crimes committed by the impostor, and economic losses include consequences such as opportunities lost or credit costs increased when the victim’s creditworthiness is called into question.

b. Persons whose identities are taken or misused incur substantial costs and time and effort expended attempting to correct records and generally repair the damage to their identities and reputations. This often entails identifying and contacting a range of commercial entities, government agencies, and in some cases foreign governments or entities. One issue raised in relation to costs in this area for States with schemes for compensating victims of crime for losses is whether existing schemes are sufficiently broad to cover this sort of harm.

c. Economic and non-economic losses are suffered by persons or organizations who become the victims of other crimes committed using the fraudulent identity. These include economic losses from fraud and other crimes and non-economic losses which can be as wide ranging as the range of offences which may be committed or facilitated by the original identity theft. These can range from
relatively minor offences such as illegal immigration or entry to the staging of major crimes or terrorist incidents.

d. The need to be able to establish and verify identity both in the public and private sectors mean that systems find it necessary to incorporate appropriate and costly measures to prevent and detect identity abuses. These include increasingly complex and expensive anti-forgery elements on documents such as passports and credit cards; biometric identifiers; and security measures to protect transmitted and stored information from interception and unauthorized access. A number of States and commercial sources noted that this is an ongoing process in which offender techniques must be monitored and appropriate countermeasures developed and implemented, which entailed research, development and implementation costs.

e. A further related cost factor in this area is a general erosion of efficiency. In most cases, the security measures adopted by public and private sector entities entail a compromise which seeks adequate levels of security at acceptable costs in terms of efficiency, and involves some loss in both. For example, encryption is widely used to protect both stored and transmitted data, but such technologies often require greater computing power, more bandwidth and storage space, and slower speeds. A major concern for commercial entities, aside from the costs of security, is the extent to which security measures will increase costs or inconvenience to customers or system users.

f. Economic losses in the commercial sector also include costs associated with a general loss of consumer confidence. If consumers are not confident their personal information will be protected, they are less likely to use some commercial systems. This is particularly true of electronic, or “e-commerce”. While electronic forms of commerce have substantial economic potential, customers typically base decisions on whether to use e-commerce based on factors such as convenience on one hand and confidence that they will be protected on the other. Many potential customers are concerned about the potential for fraud (e.g., fear that goods will not be delivered or will not be as advertised) or disclosure of their credit card or other personal information. More generally, many are concerned about basic privacy issues (e.g., disclosure of web sites visited, purchasing patterns etc.). Incidents of identity theft, especially major incidents such as the hacking of commercial sites with large amounts of credit card or other personal information,
contribute to an overall loss of confidence and reduced rates of commerce.

Aside from questions of basic quantification, there are also policy questions as to how some of these costs should be allocated. One of the States which has a centralised national identification infrastructure noted that this could be seen as a form of commercial resource, in the sense that national identity cards were commonly used as a means of obtaining or validating credit cards or other forms of commercial identification, and that to the extent that it supported private commerce it might be funded to some extent by commerce and commercial users as opposed to the State itself. More generally, the State and commercial entities clearly share an interest in preventing and suppressing identity-related crime, which suggests some form of sharing or allocation of the costs involved. A related issue is the need for coordination between different countries and different governmental and commercial sectors, both to avoid security gaps or vulnerabilities and to assist commerce in ensuring that a competitive environment is preserved.

VII. Prevention of identity-related crime

As noted, identity-related crime is usually committed in association with other forms of crime, either directly, where offenders establish false identities in support of their own illicit schemes in areas such as fraud and money laundering, or indirectly, where specialised offenders commit identity crimes and traffic the stolen or fabricated identities to other offenders. Thus, measures which prevent identity crime also prevent the secondary crimes which result from it, and many of the examples provided were either intended as measures to prevent offences such as fraud, money laundering, illegal entry or trafficking in persons, or were largely parallel to such measures. For this reason, the experts decided to make one common set of conclusions and recommendations with respect to prevention, and this is reflected in the analysis and conclusions submitted to the Crime Commission. To more clearly reflect the responses of Member States, however, discussion of preventive measures for identity-related crime are set out separately in this paper.

Some States mentioned controls or precautions on identification documents, including limits on validity periods or renewal requirements and technical measures to make documents difficult to tamper with. A further factor in place in most States is the fact that there are de facto checks on validity each time an identity document is used. Some also raised the need for technical systems and training of officials, in order to make
such checks more effective in identifying illicit documents. The extent to which technologies were a factor in basic infrastructure reflected the availability and use of technologies in general. Developed countries have begun using electronic identification and information technologies for some forms of basic communication with government, such as the filing of income-tax returns, and digital and biometric information on documents and real-time verification against databases when identification is used, whereas most developing countries still rely on paper identification documents with printed anti-forgery elements and visual inspection by officials when the documents are used. Some of the developments reported related to the infrastructure supporting passports and other travel-related identification, which reflect efforts to control trafficking in persons, the smuggling of migrants and other forms of transnational organized crime, illicit migration, and transnational terrorism. Information provided by States suggests a number of methods which could be used to make identity-related crime more difficult to commit, thereby preventing offences, or easier to detect, investigate and prosecute, thereby increasing deterrence and reducing the losses or harm caused.

a. Document security precautions. Responses from both States and private-sector entities contained a number of proposals or precautions which had already been implemented. These include two basic types of measure: document-based measures intended to make the physical or electronic documents more difficult to imitate or tamper with; and system-based measures intended to protect authentic documents from losses due to problems such as theft, diversion or corrupt issuance.99

(i) Document based measures. In most countries, documents such as passports and national identification cards show a constant evolution to make them harder to imitate or alter, as offenders have gained access to technological means of forgery and developed means to subvert existing security precautions. As access to sophisticated printing technologies has become more open, other means, such as the inclusion of metal threads, holograms, and detectable inks have been used. For both public and private documents, the use of computer chips has been suggested, and at least one State is already

99 A similar approach is taken by the Protocols to the United Nations Convention against Transnational Organized Crime which deal with travel and identity documents. See A/RES/55/25, Annexes II and III, Article 12, subparagraphs (a) and (b).
using them in its passports. Difficult to fabricate or subvert, these either contain unique identifiers which identify the document, or information about the holder which can be accessed by machine and used to verify identity. Lost, stolen and expired identity documents are a major source of materials for forgery, and at least one State has adopted requirements or offences of failing to report losses or thefts. Offences of transfer or trafficking in identification might include cases where expired documents were sold by their original holders.

(ii) System based measures. Some States mentioned the need to restrict the issuance of important documents to a small number of locations which could be properly monitored. Also mentioned in connection with documents such as passports was the need to question claims that the document had been lost or stolen more rigorously to deter holders from trafficking in their own documents, and to record details of such cases to prevent alteration and re-use of those documents by others. Other possible measures are as varied as the national systems involved, and in many cases might already be covered by measures undertaken in the course of implementing either the first two Protocols to the United Nations Convention against Transnational Organized Crime or the United Nations Convention against Corruption. A brief outline of areas to be considered or issues that might arise is discussed in subparagraph (e) (security audits), below.

b. Document validation or verification. Increasingly, the ability of offenders to create documents which are difficult to identify as false at the point of use has led to the adoption of systems which involve the use of telecommunications to permit real-time comparison with the data on the document and physical presence of the user with information kept in a secure system. In the case of passports, for example, photographs and other information collected about the holder can be recorded when the document is issued, and then checked whenever it is presented at a border-crossing. If information on the document, stored in the record and obtained by the user do not all match, a probable offence has been detected. Both document security and the need for validation by cross-checking information were identified as important means of preventing and suppressing trafficking in persons and the smuggling of migrants in the Protocols
to the 2000 United Nations Convention against Transnational Organized Crime\(^{100}\).

c. **Use of “biometrics”**. Essentially, the term “biometrics” refers to physical characteristics of an individual which are unique to that individual and can be recorded in some way to permit comparison when a document purporting to identify the individual is used. They are sometimes seen as a new concept, as new technologies have made automated checking of characteristics such as fingerprints possible, but have in fact been in common use for many decades, the most common example being the attachment of photographs to identity documents.

d. **Data-security measures**. As identification systems rely more on information and communications technologies, the protection of data from unauthorized interception, retrieval or tampering, protection of electronic data assumes greater importance. At least one State highlighted the need for precautions against attacks on stored data, which could be used to obtain information and create or support false identities, and attacks on transmitted data, which were a threat to the integrity of processes where communications were used to verify or validate identification. A range of specific precautions could be applied, including physical protection of data-storage and any points from which data can be accessed, precautions against unauthorized remote access or the interception of transmitted data, and encryption and similar technologies which prevent reading or use of data even if it is obtained by offenders.

e. **Security audits**. Generally a specific identification system can be seen as a process or network, in which identification is created, updated, used, and verified, and all of these elements require periodic review to identify and address elements which could be subverted. These include the following:

(i) **Issuance**. Processes whereby identification is created and issued are vulnerable to both deception (e.g. by providing false information) and corruption.

(ii) **Updating**. Information added to the system can be used improperly if not subject to the same requirements as the creation of new information.

\(^{100}\) A/RES/55/25, Annexes II and III, Articles 12 and 13 (both Protocols).
(iii) Revocation. The processes whereby identity is revoked or cancelled also require protection. The failure of a system to record the fact that an individual has died, for example, may permit his or her identity to be used by others.

(iv) Security of information and data. Means used by the system to store and transmit data must be sufficiently secure to prevent tampering. This includes physical security, and increasingly, encryption and other means to protect the security of data.

(v) Validity and renewal cycle. Recognizing that regardless of other precautions, illicit identification will sometimes be created, most systems limit the validity of identity documents and periodically change forms or formats. This allows for the incorporation of the latest document security elements, automatically renders any older documents useless, and makes it difficult to alter older documents into the newer forms.

(vi) Global considerations. Where a particular type of document is used internationally, some State responses have noted that to be effective, and in many cases to be viable at all, precautions have to be implemented globally. This is true for both public documents such as passports and for private ones such as debit or credit cards. Depending on the specific precaution and the way it is implemented, it would either be ineffective as a security measure, or prevent the use of the document entirely in countries where it was not implemented. It is also true for both security measures incorporated into the physical documents, such as computer chips in credit cards, and for the means of verification when the document is used.

D. The relationship between economic fraud and identity-related crime

For purposes of the present Study, a fairly clear distinction between economic fraud and identity-related crimes was made, but the responses of States and legislative and other materials provided suggest that in practice, there are significant areas of overlap and overall relationship is more complex. This is also the view of some governments, whose own experts in economic fraud have taken up much of the work on the new area of identity crime, and is one of the reasons that the Commission decided to conduct the present Study on a joint basis. Generally, the reports confirm that identity abuses perform much the same role in economic fraud as for other crimes insofar as avoiding surveillance and preventive measures before and during offences and investigative measures afterward are concerned,
combined with the added role that identity abuses play in deceiving victims in many fraud schemes.

A number of States reported specific links with this dual aspect. Perpetrators of economic frauds have impersonated public officials to obtain information or as part of frauds in which the basis of the scheme was a false claim to pursue and recover the proceeds of a previous fraud, and the impersonation of officials of banks, credit card issuers and telecommunications providers was a common element of many economic frauds and telecommunications frauds. The use of false identities was also a significant element of many identity-thefts, especially “phishing”, in which the assumption of some kind of authority was used to deceive victims into providing computer passwords or other forms of identification information. Some States reported conduct which could form the basis of offences such as identity theft or identity fraud as elements of larger fraud schemes. Some frauds such as credit-card fraud could also be seen as identity-fraud, in the sense that the offender is using a copied or stolen card as a form of identification, effectively impersonating the legitimate card-holder. In most commercial schemes such as credit cards, the basis of identity is so specific to the commercial aspect that any attempt to distinguish identity fraud and economic fraud can be difficult if not moot.

One key difference between fraud and identity related crime is that, for almost all of the reporting States, legal definitions and offences of fraud were economic crimes, requiring some form of material loss to victims or gain to offenders, whereas most identity-related crimes are not necessarily economic in nature, and may be committed in support of other crimes which also may or may not be economic in nature. One possible implication of this difference lies in the application of the United Nations Convention against Transnational Organized Crime. The Convention applies only in cases where an “organized criminal group” is involved, and such groups only exist where at least one of their objectives is to generate a “financial or other material benefit”\(^\text{101}\). Thus an organized group which had exclusively non-economic objectives, such as a terrorist group, and any identity crimes it committed, would not be covered. Aside from terrorism, however, the vast majority of cases would be covered. First, the Convention makes it clear that it is the objectives of the group, and not any specific offences it may commit or be involved in, that must involve a financial or other material benefit.

\(^{101}\) A/55/25, Annex I, Article 2, subparagraph (a) and Article 3, paragraph 1.
This means that non-economic identity offences would be covered if linked to an organised criminal group that was also involved in economic crime. This would cover scenarios such as identity crimes used in support of trafficking in persons, the smuggling of migrants, money-laundering and other forms of smuggling or trafficking, even if there was no obvious link beyond the involvement of the group itself in the early investigative stages. Second, the meaning of “financial or other material benefit” is relatively broad, including, for example, trafficking in child pornography for reasons of sexual gratification. This would include identity crimes where stolen or fabricated identification or identity information was treated as a form of illicit commodity and bought, sold or exchanged, as well as scenarios where identification was misused for personal or organizational gains, even if these were not necessarily financial, such as securing entry into another country. Third, based on the reports received, the most common offences associated with identity crime are either economic offences such as fraud, or offences related to travel or identity documents covered by the Protocols against trafficking in persons and the smuggling of migrants. These are presumed to involve financial or other material benefits, with the exception of cases where migrants are smuggled for humanitarian or other non-criminal purposes.


103 The definition of “smuggling of migrants” also requires a link to “financial or other material benefit” in order to ensure that States Parties are not required to criminalise smuggling for non criminal purposes such as humanitarian purposes or the smuggling of close family members. See A/RES/55/25, Annex III, Article 2, subparagraph (a) and agreed Notes for the Travaux Préparatoires, A/55/383/Add.1, paragraph 88.