United Nations E/CN.15/2007/8/Add.3

Economic and Social Council

Distr.: General
31 January 2007

Original: English

Commission on Crime Prevention and Criminal Justice
Sixteenth session
Vienna, 23-27 April 2007
Item 4 of the provisional agenda*
World crime trends and responses: integration and coordination of efforts by the United Nations Office on Drugs and Crime and by Member States in the field of crime prevention and criminal justice

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

Addendum

Identity-related crime

Contents

* E/CN.15/2007/1.

V.07-80501 (E) 260207 270207

I. Introduction

A. Nature of identity-related crime

1. The ability to uniquely identify individuals[1] is a critical element of virtually every aspect of social, political and economic activity. An identity must be created and linked to the specific entity identified. Identification information must be created, transmitted, stored and retrieved, and it is usually linked to other information about the individual it identifies, such as nationality or citizenship status, financial and banking records, criminal records and similar personal and commercial information. The fundamental role identity plays in so many different systems creates a vast range of opportunities for crime if basic identification information can be altered or falsified or if the systems for creating, altering, retrieving and verifying identity and other information can be subverted. For that reason, the criminal law and criminal justice systems of almost all States have addressed identity-related issues in some way.

2. The present state of legislation and policymaking in most States is limited to dealing with identity problems primarily in terms of the further crimes that can be committed through identity abuses. However, recently, some States have begun to consider the problem from the perspective of identity itself. It is suggested that, in addition to criminalizing the misuse of identity, underlying, preparatory or supporting conduct such as taking, copying or fabricating identity and the various forms of tampering with identity systems should be treated as a new and distinct form of criminal offence. That is consistent with other recent developments, including the United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, annex I) and the Council of Europe Convention on Cybercrime.[2] The criminalization of identity-based offences reflects 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. That approach also reflects that, where a genuine identity is used to commit other crimes, the person identified by the genuine identity and those targeted by subsequent crimes both suffer harm and should be considered victims of crime. The criminalization of identity-related offences also reflects recognition of the fact that, especially in cases where organized criminal groups are involved, identification information and documents have become an illicit commodity that is transferred from the offenders that commit identity-related crimes to others who commit further crimes using that information or falsified identities based on it.

---

[1] States were provided with a description of identity fraud that included conduct involving the identity or identification information of both legal and natural persons, but were not asked specific questions regarding the identity of legal persons. In their replies, several mentioned corporate registries or similar systems to establish the identities of legal persons, but not enough information was provided to assess the specific problems associated with the identification of legal persons.

[2] See, for example, article 5 of the Organized Crime Convention on criminalization of participation in an organized criminal group, and article 8 of the Convention on Cybercrime (Council of Europe, *Treaty Series*, No. 185), which requires criminalization of computer-related conduct with the intent to commit fraud, whether the fraud was completed or not. Both conventions contain provisions that largely address the need to deal with underlying, preparatory and supporting conduct.

B. Use of terminology in the present study

3. In its resolution 2004/26, the Economic and Social Council requested the Secretary-General to convene an expert group to prepare a study on "fraud and the criminal misuse and falsification of identity" and related crimes. Early deliberations of the experts, as reflected in the survey questionnaire used to gather information, did not consider specific meanings of those terms or seek to distinguish between identity fraud and identity theft. Only one State provided a legislative definition, while most States simply indicated that the description proposed by the questionnaire (E/CN.15/2005/CRP.5, question 33) was an accurate reflection of problems that they had encountered. Experts decided on a preliminary and non-prejudicial basis to use the term "identity fraud", but in reviewing the responses of States and other materials, it became apparent that some misconduct reported was analogous to theft, that some was more closely analogous to fraud and that other misconduct had elements of both or neither and might best be considered "related crime".

4. The general term "identity crime" is used to cover all forms of illicit conduct involving identity, including identity theft and identity fraud. That is, of necessity, a forward-looking usage, because most States have not yet adopted legislation on such offences. Generally, identity crime includes preparatory or constituent offences such as forgery and impersonation. One definitional problem is that identity abuses may target identity information itself or other information to which it is linked. The latter case might not be considered identity crime, although the effects of such crime would usually be the same. For the purposes of the present study, the broader term "identity-related crime" has been used to include such situations. In some contexts, the term "identity abuse" is also used. It has a similar meaning but carries no implicit assumption about whether a given conduct is already a criminal offence or should be criminalized. 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.[3]

5. The term "identity theft" generally 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 a manner analogous to theft or fraud, including theft of tangible documents and intangible information, the taking of documents or information that have been abandoned or are freely available, and deceptively persuading individuals to surrender documents or information voluntarily. The term "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 using that term, the element of deception referred to is not the use of deception to obtain the information but subsequent use of the information to deceive

---

[3] *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations publication, Sales No. E.06.V.5), part two, art. 12, sect. C, interpretative note (b), and part three, art. 12, sect. C, interpretative note (b).

others. As with economic fraud, the element of deception includes the deception of technical systems as well as human beings.

II. The basis of identity: means of identification used by Member States

A. Public and private identification systems

6. Most States reported both public and private sector infrastructure for identification, and most described a range of application-specific forms of identification. With respect to public sector identification, some States reported on centralized national identification schemes, but most States appeared to rely primarily on identification established for specific applications, such as driver's licences, passports, birth certificates, citizenship certificates and identification used for public taxation or benefit schemes. Private sector identification tended to be issued for specific commercial purposes, such as banking or credit purposes, although there was a possible trend to more generalized forms of identification, established by companies specialized in that field. Some countries combined both approaches, and some States with federal systems had identity schemes run by individual states or provinces, giving rise to the need for common standards for verification at the national and international levels. Where no national identification system existed, specific forms of identification tended to be used for purposes beyond the original intent, both out of necessity and, where the principle of redundancy was exploited, for added reliability. The most common form of private commercial identification reported was the credit card. Views on national identification schemes varied. In some countries, national identification requirements were widely accepted. In others, proposals had been controversial and had been opposed on civil liberties grounds. One State noted that its national identification system was increasingly being used in support of commercial applications and questioned whether commercial interests should be asked to share the high costs of maintaining a centralized system.

B. The concept of identification information

7. The concept of identification information was novel for most States. Few recognized it in legal or legislative terms, although those States examining identity-related crime had begun to consider it. Most States referred instead to identification documents or personal information. Personal information included identification information as well as other information about the status or activities of the persons identified that was of a personal or private nature but not necessarily sufficient to identify an individual. Many States reported the establishment of criminal legislation and other measures to protect personal information including 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. An important aspect of the concept of identification information is that its elements, while necessary to establish identity, are not usually sufficient when used in isolation. The most common identity documents actually contain several elements of identification information, and automated 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 that it identifies. Approaches to what constitutes identity information may depend to some degree on cultural elements and local traditions. Some cultures incorporate names of parents, places of family origin or profession or occupation into individual names. Another factor was the degree to which traditional face-to-face recognition has gradually been replaced, first by paper documents and, more recently, by electronic identification as new forms of identification information are created.

8. 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 user names, passwords, personal identification numbers (PIN), transaction authentication numbers (TAN) and digital signatures and other cryptographic applications. A new area of development in technological support is the range of biometric identifiers, including DNA information, fingerprints, photographs, voice prints and images of iris and retinal tissue. Photographs, which are easy to use are common. Other biometric identifiers generate a high degree of security but are expensive and raise privacy concerns, making them common only in areas, such as criminal records, where the costs are justified by the need for security or other factors. Two States reported relevant legislative and other provisions. One used the term “identification data” to refer to electronic information that is a constituent element of identification in its automated systems. One State reported a definition of the term “means of identification” as used to describe an element of an offence related to identity theft. Its legislation 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”.

III. Identity-related crime

A. Types of crime encountered

9. States reported a range of crimes involving the criminal misuse or falsification of identity. Common crimes included the forgery of identity documents and various types of impersonation. In addition to offences involving identification documents, offences targeting the systems or processes used to create, establish or verify identity were reported. One way of subverting identity systems was to attempt to deceive or corrupt the issuance process to issue valid identification to a person not entitled to it. Several States reported offences of that nature, including the general offences of bribery and corruption and more specific offences related to the use of false or misleading information for the purpose of obtaining licences or other identity documents. Some ways of illicitly obtaining identity information were covered by existing legislation on theft, but that legislation might not always apply. Because intangible information might not be seen as property, theft legislation might not apply to cases where that information was taken from sources such as discarded documents. Existing legislation on economic fraud might apply to conduct such as “phishing” if it could be established that the identity information taken by deception had value. A few States reported legislation on other offences,

including the illicit possession, transfer of or trafficking in identification or information such as computer passwords and credit card information. Several States were concerned about the potential for offenders to obtain large amounts of identity information through computer hacking. A number of States mentioned offences of impersonation, including by assuming the identity of another person and by fabricating and assuming the identity of a non-existent person.

B. Means used to commit identity-related crime

10. Replies to the questionnaire revealed that, to some degree, the means used for identity-related crime depended on the nature and purpose of the identification structures involved and the means available to offenders. In most such crime, identification information was taken, copied or plausibly fabricated, rendered into some useable form and then used. Offenders obtained identification information through the theft or copying of complete documents or by obtaining, by various means, partial information to build identities and procure genuine documents. Some States reported cases where the identity of a person who had died at a young age was obtained and used to file fraudulent applications for birth certificates and other basic identification in order to gradually build a comprehensive identity. A substantial number of States reported concerns about identity-related crime targeting victims based on their use of information technologies. The most commonly used method was “phishing”, or “pharming”, in which users of computer networks were deceived into providing offenders with user names, passwords and other electronic identification information. Victims were reached through e-mail messages or websites claiming to represent service providers or other authorities and were asked for identification information. Websites were often hosted in countries distant from both offenders and victims, and one State noted that it had traced such websites to at least 10 different countries. Other forms of cybercrime had also been encountered, including malicious software that infected individual victim computers, captured personal information and transmitted it to offenders, and the hacking of commercial websites to obtain credit card data and other customer identification information. Identification information, especially in large quantities, had become an illicit commodity, sold to other offenders. Commercial entities concerned about customer confidence had been the victims of extortion offences in which offenders took the information and threatened to publicize it if they were not paid.

11. A number of States reported methods used to gain identity information relating to debit and credit cards, primarily for subsequent use in economic fraud. Some information was gathered by skimming (running the card through a data-reading device). In the case of debit cards, the devices were attached to automated teller machines (ATM), along with miniature video cameras to record users’ PIN numbers. Other States reported cases where identity information was obtained by officials with inside access to government or commercial systems or was obtained by outside offenders by means of bribery or other corrupt means. Obtained identification information could often be used immediately to impersonate the victim, whereas in the case of physical identity documents, further steps were often needed. Physical identification documents had become more sophisticated, requiring greater expertise, resources and equipment to forge. Thus, the presence of such documents suggested the involvement or support of organized criminal groups. However,

information and communications technologies had brought some means of forgery within the reach of a large number of individual offenders, triggering an evolution of both document safeguards and criminal techniques. In addition to tampering with physical documents, identity-related crimes were also committed through tampering with the underlying systems to which the documents were linked.

C. Legal responses

12. There seemed to be a fairly broad consensus that some forms of identity abuse should be made a criminal offence and be subject to punishment, but there were some differences of opinion with respect to the exact types of conduct that should be criminalized. Most States had established identity-related crimes within more general offences. But only six States reported that they had criminalized, in whole or in part, the transfer, possession or use of another person's identification or identity information or a false identity in connection with another crime, and only one of those, the United States of America, had criminalized identity theft per se. That relevant legislation of the United States defined "means of identification" and criminalized 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 all States indicated that they had criminalized at least some of the specific forms of conduct covered by the description of identity fraud proposed in the questionnaire or related conduct. The most commonly described offences were those related to forgery and impersonation. A number of specific identity abuses were also subsumed within broader crimes, such as forgery offences, which included the forgery of identity documents, and cybercrime offences such as theft of data and unauthorized access to or tampering with computer systems. Some States reported the criminalization of offences that were specific to types of identification or identity considered particularly critical, such as passports or government identification. States parties to the Convention on Cybercrime were required by article 7 of the Convention to ensure that their legislation on forgery covered computer- or data-related forgery. Several States reported offences related to computer "phishing" and similar conduct. In other States, that activity might also be covered by more general cybercrime legislation, such as that covering the theft or illicit possession of passwords.

IV. The relationship between identity-related crime and other factors

A. Relationship between identity-related crime and economic fraud

13. The present study distinguishes between economic fraud and identity-related crimes, but the evidence suggests that in practice, there are significant areas of overlap. That is also the view of some Governments, whose own experts in economic fraud have taken up much of the work in the new area of identity crime. That is one reason why the Commission on Crime Prevention and Criminal Justice decided to conduct the present study on a joint basis. As noted, 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. Many examples of that were provided. Perpetrators of economic fraud impersonated public officials to obtain information or as part of a fraud employing a false claim to recover the proceeds of a previous fraud. The impersonation of officials of banks, credit card issuers and telecommunications providers was a common element of many reported economic and telecommunications frauds. The use of false identities was also a significant element of many identity thefts, especially "phishing", in which offenders assumed the identity of authorities to deceive victims into providing computer passwords and other forms of identification information. Some States reported conduct that could form the basis of offences such as the use of identity theft and identity fraud as elements of larger fraud schemes. Frauds such as credit card fraud could also be considered identity fraud, because the offender was using a copied or stolen card as a form of identification, effectively impersonating the legitimate cardholder. In commercial schemes such as credit cards, the basis of identity was often so closely linked to the commercial aspect that attempting to distinguish between identity fraud and economic fraud was difficult if not impossible.

14. One key difference between fraud and identity-related crime was that, for almost all reporting States, legal definitions and legislation classified fraud as an economic crime. Accordingly, some form of material loss by victims or gain for offenders had to be demonstrated. In fact, identity-related crimes were not necessarily economic in nature and might be committed in support of further crimes that might or might not be economic in nature. One possible implication of that difference lay in the application of the Organized Crime Convention. The Convention applies only in cases where an organized criminal group is involved, and defines a group as such if one of its objectives is to generate a "financial or other material benefit".[4] Thus, an organized group that had exclusively non-economic objectives, such as a terrorist group, and any identity crimes that it committed, would not fall within the scope of the Convention. Aside from terrorism, however, the vast majority of cases would be covered. First, the Convention makes clear that it is the objectives of the group, not any specific offences it may commit or be involved in, that must involve a financial or other material benefit. That means that non-economic identity-related offences fall within the scope of the Convention if they are linked to an organized criminal group that is also involved in economic crime. The Convention would apply to situations in which identity crimes were used in support of trafficking in persons, the smuggling of migrants, money-laundering or other forms of smuggling or trafficking, even if, in the early investigative stages, there was no obvious link beyond involvement in the group itself. Secondly, 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 (A/55/383/Add.1, para. 3).[5] It encompasses 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 instances where

---

[4] See the Organized Crime Convention, art. 2, subpara. (a), and art. 3, para. 1.

[5] *Travaux Préparatoires*…, part one, art. 2, sect. C, interpretative note (d). See also A/AC.254/4/Rev.1, footnote 4, A/AC.254/4/Rev.2, footnote 16, and A/AC.254/4/Rev.7, footnote 22.

identification was misused for personal or organizational gains, including non-financial gains such as securing entry into another country. Thirdly, based on the reports received, it appears that the offences most commonly associated with identity-related crime are economic offences, such as fraud, and offences related to travel and identity documents that fall within the scope of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, and the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the Organized Crime Convention (General Assembly resolution 55/25, annexes II and III). Those were presumed to involve financial or other material benefits, with the exception of cases where migrants were smuggled for humanitarian or other non-criminal purposes.[6]

B. Other crimes associated with identity-related crime

15. Reported links between identity-related crimes and other crimes fell into three groups based on how false or assumed identities were used: first, to gain access to physical places or electronic accounts so that other crimes could be committed; secondly, to shield the real identities of offenders to avoid detection, interference and prosecution; and thirdly, in the case of economic fraud, it was used as part of the central deception element of a fraud scheme.

16. While the links between identity abuse and other crimes most commonly involve the identities of offenders, the abuse of the identities of victims can also be an issue. Many country reports on trafficking in persons noted that offenders confiscated victims' passports or identity documents as a means of controlling them or preventing them from fleeing. Although the Trafficking in Persons Protocol does not require the criminalization of deprivation of identification as an element of trafficking, some States parties have done so.[7] Article 7, paragraph 1, of the United Nations Convention on the Rights of the Child (General Assembly resolution 44/25, annex) establishes the right to registration at birth as a means of establishing identity, and the systematic deprivation of identity has been encountered as an element in cases of genocide and ethnic cleansing.[8]

17. Identity-related crimes are most commonly linked to economic fraud and similar crimes, in part because economic fraud is very common in most States and because identity abuse is so central to the successful execution of most frauds. A number of States noted that identity crime was used in money-laundering to defeat mechanisms for identifying the proceeds of crime and suspicious transactions. Many States expressed particular concern about identity crimes involving passports and other travel-related identity documents, considering them to be both a crime and a

---

[6] The definition of "smuggling of migrants" requires reference to the question of "financial or other material benefit" in order to ensure that States parties are not required to criminalize smuggling for non-criminal purposes such as humanitarian purposes or the smuggling of close family members (see the Migrants Protocol, art. 2, subpara. (a) and the *Travaux Préparatoires*…, part three, art. 3, sect. C, interpretative note (a)).

[7] See, for example, *Criminal Code of Canada*, section 279.03 on withholding or destroying travel and identity documents, as enacted by Statute of Canada 2005, chapter 43.

[8] See, for example, *Prosecutor of the International Criminal Tribunal for the former Yugoslavia v. Slobodan Milosevic et al*, Case No. IT-99-37-PT, Second Amended Indictment (29 October 2001), paragraph 61 (http://www.un.org/icty/indictment/english/mil-2ai011029e.htm).

security issue, because passport systems are essential to preventing the entry of known terrorists, criminal offenders and illegal migrants. Passport abuses were also linked to organized crime, in particular through trafficking in persons and the smuggling of migrants, and a number of States that drew attention to those links reported high levels of smuggling or trafficking due to the country's geographical location. Several States reported the establishment of new passport documents incorporating additional security measures. A number of links between identity-related crime and cybercrime were encountered. Several States reported, in addition to the deception of victims to obtain computer-related identity information, the use of fraudulent identities and credit cards to obtain untraceable telecommunications services for use in other crimes, including terrorist activities.

C. Relationship between identity-related crime and organized crime

18. A number of States reported links between identity-related crime and organized criminal groups. The most commonly encountered situations 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. Those issues are discussed elsewhere in the present report. Beyond carrying out identity-related crimes as part of other criminal activities such as money-laundering, some organized criminal groups may be sophisticated enough to engage in identity-related crimes as a distinct criminal operation. Responses from States suggested two key scenarios. Organized criminal groups might use identity-related crime to protect their members and operations from surveillance of illicit activities and to carry out routine, non-criminal activities such as international travel. There was also evidence of the specialization of groups and the treatment of identity documents and information as an illicit commodity. Such groups might develop the expertise to fabricate increasingly 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, migration or other activities in which legitimate identification would be prejudicial. Some organized criminal groups were sophisticated enough to use multistage identity schemes in which identity information from one source was used to submit fraudulent applications for genuine documents in an effort to build and maintain even more solid and elaborate fictitious identities.

D. Relationship between identity-related crime and terrorism

19. Only a few States raised the issue of links between identity-related crime and terrorism. Their primary concern in that respect was essentially the same as the concern about organized crime and other problems: terrorist organizations could use identity-related crime to obtain identification information and documents that could, in turn, be used by terrorist operatives to evade surveillance or arrest, which would be likely to occur if their true identities were known. Most of the concern of States focused on travel-related identification and the international movement of terrorist

suspects,[9] but the same issues arose with respect to purely domestic identification and activities, because terrorists had to avoid attracting attention in everyday activities such as driving or banking, and because common forms of domestic identification formed the basis for obtaining more secure identification such as passports and employment and related identification, which were needed to access secure locations such as airports.

20. Other official sources consulted by experts gave examples of terrorist suspects obtaining and using identity documents to avoid surveillance and scrutiny. Those included forged or altered documents and genuine documents, obtained using false names, whose key information, such as names and birth dates, would not correctly identify the user or be linked with incriminating records. Another pattern encountered involved the use of false or misleading applications for new documents. Sympathizers might simply give documents to a terrorist organization for its use and later falsely claim that they have been lost or stolen, and suspects whose passports record suspicious travel patterns might dispose of them and falsely obtain replacements.[10] Another concern raised in that connection by some States was, as with economic fraud, the use of basic fraud against telecommunications providers to obtain anonymous and untraceable mobile telephone, Internet or other telecommunication services.

21. Absent clear evidence, identity-related crime associated with terrorism can be difficult to distinguish from related crimes, especially organized crime. Many basic scenarios are common to organized criminal groups and terrorist groups, and terrorist groups that lack their own expertise might simply purchase false identification documents from organized criminal groups. Identity-related crimes can be employed for the financing of terrorism much the same way they can for money-laundering.

E. Relationship between identity-related crime and money-laundering

22. Many measures to counter money-laundering heavily depend on identity or identification elements, and the means used by offenders to launder proceeds involve identity-related crime. The ability to identify customers and parties of financial transactions, sometimes described as the “know-your-customer” principle, is, in addition to keeping financial records and reporting suspicious transactions, a fundamental element of regimes to counter money-laundering.[11] Identifying parties to a transaction can help establish that funds or assets are criminal proceeds or assist in the investigation of underlying and predicate offences. At later stages, the identification of all parties involved in a series of money-laundering transfers is usually essential to the prosecution of offenders, the forensic tracing of proceeds

---

[9] See, for example, the report of the Secretary-General entitled “Uniting against terrorism: recommendations for a global counter-terrorism strategy” (A/60/825, para. 62).

[10] See, for example, the *Report of the National Commission on Terrorist Attacks upon the United States*, chapter 5.3, pp.168-169 (http://www.9-11commission.gov/report/index.htm).

[11] See, for example, the *Organized Crime Convention*, article 7, paragraph 1 (a); *United Nations Convention against Corruption*, article 14; and recommendation 5 of the 40 recommendations of the Financial Action Task Force on Money Laundering (http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html#40recs).

and derivative funds or assets and the establishment of linkages or continuity between the predicate offences and the ultimate form and location of the proceeds with sufficient certainty to support criminal confiscation. Reliable identification processes also serve as a form of control or deterrent for predicate offences.[12] Some States noted that money-laundering methods made use of information, communication and commercial technologies, which provided a means of generating false identification information, enabled remote transfers through the use of that false identification and supported large volumes of legitimate transfers in which laundered assets could be concealed. Those technologies had 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. At the same time, new technologies supported corresponding developments in crime prevention, security and investigative support.

F. Relationship between identity-related crime and corruption

23. Member States were not asked to discuss links between identity-related crime and corruption, but experts considered some possible relationships. Identity-related crime could be used as a means of avoiding detection or criminal liability when committing corruption offences, as used in other crimes. For example, false identities might be used to frustrate the investigation of offences such as embezzlement. As with money-laundering offences, identity abuses could also be used to avoid the tracing and forfeiture of the proceeds of corruption. The other key aspect of the relationship was 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 could be used to alter or falsify information in systems used to validate or verify identity. That was seen as a new area, and experts were of the view that such situations would probably emerge as more experience was gained.

G. Relationship between identity-related crime and information, communication and commercial technologies

24. As with economic fraud, the role of information and communication technologies in identity-related crime is complex. In some cases examined, technologies were central to the identity-related crime, while in others, they formed only one element of a larger offence. The greater reliance on technologies, as opposed to personal contact, in identification had created new criminal opportunities for impersonation because knowledge of passwords and other identifiers was sufficient to deceive automatic systems, regardless of the offender's true identity. The spread of technologies had also brought sophisticated means of forging both physical and electronic documents within the reach of large numbers of relatively unsophisticated criminals. Further, new technologies had made it possible

---

[12] See P. A. Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (World Bank, 2003), chap. VI, part A.

to subvert issuance systems and obtain genuine documents. However, technological developments also had elements that tended to prevent or suppress identity-related crime. Some of those elements were inherent to new technologies, some were specifically incorporated to prevent crime or facilitate detection and investigation, and others had been developed and marketed specifically to deal with new crime problems as they had evolved and become apparent. Precautions included physical elements to make documents harder to produce, such as the incorporation of photographs, microprinting, holograms and computer chips, which still required relatively sophisticated equipment and knowledge to produce. In addition, modern, secure telecommunications made it possible to quickly verify identity documents against multiple secure databases, and information technologies made the process fast enough to be practical in applications such as passport checks at border crossings. One State noted that where feasible, there was a growing trend towards what has been described as multi-factor identification, in which several different identifiers were maintained separately and cross-checked whenever identity was to be established or verified. Those included elements in three basic areas: elements that the subject physically possessed, such as a debit or credit card, a national identity card or a passport; elements that only the subject would know, such as passwords and PIN numbers; and biometric elements (elements that were biologically unique to the subject).

H. Transnational elements and the need for international cooperation against identity-related crime

25. A number of States reported that they had encountered cases of identity-related crimes with transnational aspects. The majority of those cases involved offences related to passports and other travel-related identification. They included offences specifically related to identification documents, such as forgery, alteration, misuse of genuine documents and abuses of issuance processes, and other offences committed in part though the misuse of those forms of identification, such as trafficking in persons, smuggling of migrants and other offences related to illegal entry or illegal migration. Digital identification information was easily transmitted internationally. The other major category of identity-related crime commonly mentioned as having transnational aspects was cybercrime.

26. Several States highlighted the importance of international cooperation in the investigation and prosecution of transnational identity-related crime, but not many details were provided with respect to the specific forms of cooperation needed. As was the case with economic fraud, most States saw existing frameworks such as the Organized Crime Convention, the United Nations Convention against Corruption and the Convention on Cybercrime as sufficient. Several States also highlighted the practical utility of Interpol, the European Police Office (Europol) and similar organizations as mechanisms for cooperation. Most States believed that the specific forms of cooperation required in this area were similar to those required for transnational fraud and other forms of cybercrime. Most major offences committed using stolen and fabricated identities were likely to be considered “serious crimes” as defined by article 2, subparagraph (b), of the Organized Crime Convention, but as States proceed to consider identity abuses as a distinct form of crime, the question of whether new, specialized offences also fall within the scope of the Convention

will arise. Several States noted that, as with cybercrime, the speed with which both formal assistance and informal cooperation was provided was sometimes critical. In that connection, the 24/7 network could be of assistance with fraud cases involving electronic evidence, particularly when the case was urgent. One issue not raised by most States was the fact that, aside from economic losses, the harm caused by identity-related crime extended to the identities of real natural and legal persons whose identities had been misused. Damage to reputation and the viability of basic identity for personal and commercial purposes can be considerable, and measures to repair identities would not fall within the ambit of the criminal cooperation frameworks of most States.

V. Rates and trends in identity-related crime

27. Most States which provided data or assessments expressed the view that identity-related crime was growing, and several noted what appeared to be very rapid growth. Some of the growth observed concerned not only overall rates and volumes of occurrences but also the range and diversity of offences. Only two States suggested that identity-related crime was decreasing, and several States indicated that their information was either insufficient or inconclusive. Most were able to provide only expert opinions or assessments, and only one State provided statistical information. That State reported early statistical information that suggested that identity theft was a substantial, growing problem. The concept was so new that any dramatic increases observed could be attributed in part to growing public awareness of the problem, enhanced government attention and the recent establishment of reporting facilities, but the data clearly showed a substantial number of occurrences. Large economic losses were also reported, but it was not clear to what extent those were losses from economic fraud and other, secondary offences committed using identity theft and to what extent they were losses from other causes, such as damage to victims' reputations and the cost of restoring identity. One State reported research into the number of Internet websites being used for "phishing", which found that the number of such websites tripled from 2005 to 2006. Assuming those figures are accurate, they may reflect a pattern in which new forms of crime increase dramatically over a short period as knowledge of the techniques spreads and then level off as public awareness increases and countermeasures are developed. Some of the States that indicated that identity-related crime was increasing cited several possible reasons for such increases, including official and commercial corruption, opportunities generated by the 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. The lack of clear national definitions of identity fraud and similar crimes precludes statistical analysis and all but the most general comparisons between countries or regions.

VI. Cost of identity-related crime

28. None of the responding States provided detailed information about the actual cost of identity-related crime, and only a few had estimates of total losses. A number of States pointed out that, in the absence of specific legislation for offences, no accurate gathering or analysis of statistical information could be attempted. And

some States noted that, given the nature of identity theft, it would be difficult to separate the costs and losses from identity crime per se from the cost of further crimes, such as fraud, committed using false or assumed identities. Those States that provided overall loss calculations aggregated all losses from all primary offences linked to identity crimes, and some commercial sources also took that approach. Given some of the examples provided, it was recognized that it would be difficult to quantify in monetary terms some of the forms of harm and damage caused, such as loss of reputation, or, given the sustained duration of the harm, to determine an appropriate length of time for measuring it.

29. However, one State noted that a qualitative assessment could be made. It suggested that harm and damage would include: economic and non-economic losses that are likely to be suffered by persons whose identities are taken or misused; costs, time and effort expended to repair the damage to identities and reputations; economic and non-economic losses from other crimes committed using the fraudulent identity; public and commercial costs of prevention, investigation and prosecution; a general erosion of efficiency as a result of security measures; and costs associated with loss or lack of consumer confidence in commercial operations. Aside from questions of basic quantification, there were also policy questions about how some of those costs should be shared between public and commercial entities and how compensation should be distributed among the various victims or interests harmed by identity-related crime.

VII. Prevention of identity-related crime

30. Some States reported controls and precautions such as limits on validity periods, renewal requirements, technical measures to make documents difficult to tamper with and de facto checks on validity each time an identity document was used. Some States raised the need for technical systems and training of officials in order to make such checks more effective in identifying illicit documents. Information provided by States suggested a number of specific methods that could be used to prevent identity-related crime. Document security measures included both measures intended to make documents more difficult to forge and system-based measures intended to protect authentic documents and issuance systems from theft, diversion and corrupt issuance.[13] Document validation and verification practices could be strengthened, especially through the use of telecommunications and databases protected by encryption and similar measures, used to compare the document and holder with reference information at the time the document is used. Biometric elements could be used to link identity to unique physical characteristics. Generally, security audits to assess overall system security could be conducted, examining all elements of the system, including: document issuance and revocation; the updating of documents and information; information security practices; the validity and renewal cycle of documents; and the global interoperability of systems and security measures.

---

[13] See article 12, subparagraphs (a) and (b), of both the Trafficking in Persons Protocol and the Migrants Protocol.