UserName United Nations E/CN.15/2007/……

Economic and Social Council

Distr.: General
……. 2007

Original: English

Commission on Crime Prevention and Criminal Justice
Sixteenth session
Vienna, …….2007
Item …….. of the provisional agenda*

International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes
[Draft 1 Short Version]

Report of the Secretary-General

Results of the study on fraud and the criminal misuse and falsification of identity

Contents

6. The impact of fraud in countries under reconstruction or with economies in transition

V. International cooperation and jurisdiction

1. Mutual legal assistance and other investigative cooperation

2. Extradition

3. Jurisdiction

4. Cooperation in prevention

VI. Cooperation between the public and private sectors

VII. The prevention of economic fraud

Annex II: Results of the Study on Identity-related crime

VIII. Introduction: the nature of identity-related crime and use of terminology in the present Study

1. The nature of identity-related crime

2. Use of terminology in the present Study

IX. The basis of identity: means of identification used in Member States

1. Public and private identification systems

2. The concept of "identification information"

X. Identity-related crime

1. Types of crime encountered and legal responses

2. Means used to commit identity-related crime

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

1. Other crimes associated with identity-related crime

2. Relationship between identity-related crime and organized crime

3. Relationship between identity-related crime and terrorism

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

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

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

X I I . Rates and trends in identity-related crime

X I I I . Costs of identity related crime

XIV. Prevention of identity-related crime

L. The relationship between economic fraud and identity-related crime

I. Introduction: Substantive and procedural background

A. Legislative mandate

1. In its 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”, the Economic and Social Council requested the Secretary-General to convene, in consultation with regional groups and 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 reflecting the diversity of legal systems 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 that would deal, inter alia, with the following issues:

(a) The nature and extent of fraud and the criminal misuse and falsification of identity;

(b) Domestic and transnational trends in fraud and the criminal misuse and falsification of identity;

(c) The relationship between fraud, other forms of economic crime, the criminal misuse and falsification of identity and other illicit activities, including organized crime, money-laundering and terrorism;

(d) The prevention and control of fraud and the criminal misuse and falsification of identity using commercial and criminal law, criminal justice and other means, and how those could be harmonized;

(e) The particular problems posed by fraud and the criminal misuse and falsification of identity for developing countries and countries with economies in transition.

2. In the same resolution, the Economic and Social Council requested the Secretary-General to submit a progress report on the work of the intergovernmental expert group and the plan of work for the study to the Commission on Crime Prevention and Criminal Justice at its fourteenth session and to submit, in a timely manner, a substantive report containing the results of the study to the Commission at its fifteenth session or, if necessary, at its sixteenth session, for its consideration.

3. The Economic and Social Council also requested the intergovernmental expert group, in carrying out its work, 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.

B. First meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity (Vienna, 17-18 March 2005)

4. With the support of the Government of Canada, a first meeting of the open-ended Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity was held in Vienna on 17 and 18 March 2005. The report of that meeting was submitted to the Commission on Crime Prevention and Criminal Justice at its fourteenth session[1], in accordance with Economic and Social Council resolution 2004/26. It was a progress report that summarized the deliberations during the meeting and the recommendations made by the Expert Group with respect to the nature, scope and methodology of the study and the information that should be sought from Member States and other relevant entities to form the basis for it.

5. The meeting identified the following as priority areas for the scope of the study:

(a) The meaning of "fraud" and range of definitions presently in use, and the relationships between fraud and other forms of economic crime;

(b) The meaning of "identity fraud"[2], a much newer and still evolving concept, why this is seen as a problem by some States, and whether it poses the same challenges for developed and developing countries;

(c) Issues relating to transnationality in fraud and identity-fraud, including factors such as developments in legitimate commerce and information technologies, which are believed to influence transnational crime patterns, and the challenges posed by transnationality for policy-making, prevention, investigation and prosecution.

6. The meeting also agreed that it would be desirable to include in the study a general survey of the nature and scope of global fraud and identity fraud, and that some specific types of offending would be examined, to the extent possible within the limits of available time and resources. In this area, priority would be given to specific types of offending, either because they are of particular concern with respect to increases in volume, transnationality, or sophistication, or because they may be seen as exemplary of more general trends and developments.

C. Sources of information

7. At its first meeting, the intergovernmental expert group agreed that the study should consider information and materials provided by the experts themselves, data

---

[1] See E/CN.15/2005/11.

[2] There was agreement in the intergovernmental expert group that, for reasons of convenience, the term "identity fraud" would be used to refer to the problem described in ECOSOC resolution 2004/26 as "the criminal misuse and falsification of identity", on the understanding that such reference would be without prejudice to further discussions or the conclusion of the study. Subsequent analysis suggested that the terms "identity theft" and "identity fraud" were too specific to cover the full range of the subject matter. The terms "identity theft" and "identity fraud" are therefore used in the present report as sub-categories of identity-related crime. The meanings of these terms and related analysis are discussed at paragraph --- of the present Report.

available from governmental sources, including relevant and appropriate policy, legislative, research and other materials, and, where relevant and feasible, information from commercial (see below) and other intergovernmental or non-governmental sources. The expert group also agreed that a questionnaire should be prepared and disseminated by the Secretariat to Member States, in two parts, to obtain information on fraud and the criminal misuse and falsification of identity, based on outlines contained in the technical paper submitted by the delegation of Canada at the meeting, Economic and Social Council resolution 2004/26, and the views expressed during the meeting.

D. Questionnaire on Fraud and the Criminal Misuse and Falsification of Identity (Identity Fraud)

8. In view of the above, the Secretariat undertook to prepare a draft questionnaire in collaboration with the Expert Group. For that purpose, there was also preliminary consultation with experts attending the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 18 to 25 April 2005. It should be recalled that issues related to the scope of the study and the types of criminality that might be covered therein had a prominent place in the proceedings of the Eleventh Congress, as they were discussed in the Workshop on Measures to Combat Economic Crime, including Money-Laundering and the Workshop on Measures to Combat Computer-related Crime. In addition, in the Bangkok Declaration on Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice,[3] which was adopted at the high-level segment of the Eleventh Congress, Member States were called upon to strengthen policies, measures and institutions for national action and international cooperation in the prevention, investigation and prosecution of economic and financial crimes and such crimes conducted via, or facilitated by, information technologies. The Bangkok Declaration also included specific reference to the crucial importance of tackling document and identity fraud in order to curb organized crime and terrorism. Furthermore, Member States committed themselves to improving international cooperation, including through technical assistance, to combat document and identity fraud, in particular the fraudulent use of travel documents, through improved security measures, and encourage the adoption of appropriate national legislation.[4]

9. A first draft of the questionnaire elaborated for the purposes of the study was submitted as a conference room paper[5] to the Commission on Crime Prevention and Criminal Justice at its fourteenth session for consideration and review. The draft questionnaire was further updated prior to its dissemination to take into account, to the extent possible, comments and remarks received from Member States.

10. The questionnaire, as amended and finalized, was attached to a *note verbale* dated 15 September 2005 (CU 2005/144) and disseminated to Member States with a view to obtaining the necessary information for the elaboration of the study.

---

[3] A/CONF.203/18, chap. I, resolution 1.
[4] Ibid., paras. 26 and 27.
[5] E/CN.15/2005/CRP.5.

Member States were asked to respond to the questionnaire as fully as possible at their earliest convenience, but not later than 10 January 2006. The questionnaire was also sent to the experts who had attended the meeting of the expert group for their consideration, with a view to their submitting to the group data, observations or conclusions in specific subject areas of the study.

11. An additional information circular (CU 2006/65 of 7 April 2006) was also sent to Member States recalling the request addressed to them to respond to the questionnaire with a view to receiving more comprehensive data and that would allow a wide-ranging overview of the subject areas of the study. A similar reminder was sent to the participants of the meeting of the expert group.

E. Information from commercial and other private-sector sources

12. In furtherance of the relevant recommendation of the meeting of the Expert Group, joint action with the UNCITRAL secretariat was undertaken with a view to collecting information from commercial and other private-sector sources. Such action was deemed necessary also in view of the fact that the Commission on Crime Prevention and Criminal Justice, while discussing the problem of fraud at its thirteenth session, in 2004, and considering the recommendation of a resolution for adoption by the Economic and Social Council, had taken into account the earlier work of UNCITRAL bodies.[6] Furthermore, it had considered the problem from a criminal and public law perspective and in a broader context, including private law aspects and commercial and other types of fraud.

13. A joint letter from the UNCITRAL and UNODC secretariats, to which the above-mentioned questionnaire on fraud and identity fraud was attached, was sent to a selection of appropriate private-sector companies in October 2005 seeking information on issues falling within the scope of the study. 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. Both letters emphasized the vital importance of such information for capturing the complete picture of the problems to be addressed in the study, as well as its usefulness in pursuing a fair and balanced outcome in terms of not only the material that would form the basis of the study, but also its findings and recommendations. It was further pointed out that, as the questionnaire was designed to ensure the submission of information on both criminal and commercial aspects, it was not expected that private-sector entities would respond to all the questions therein, and therefore partial responses focusing mainly on the commercial aspects were encouraged. Finally, it was stressed that any data received from the private sector would remain confidential and, if published, anonymous.

F. Interim report of the Secretary-General before the Commission on Crime Prevention and Criminal Justice at its 15th session (Vienna, 24-28 April 2006)

[6] A/CN.9/540, A/CN.9/555.

14. At its first meeting, the expert group also considered the timeframe for the completion of the study, noting that the mandate given by the Economic and Social Council it its resolution 2004/26 called for completion of its work in time for the 15th session or "if necessary" the 16th session of the Commission on Crime Prevention and Criminal Justice. The view was expressed that, while it would be important to make every effort to complete the work as quickly as possible, the timing would also be governed by the length of time it would take to gather the information required. The group was also of the view that, should sufficient information not be received in time to permit completion of the present Report to the 15th session, it would be appropriate for the Secretary General to bring to the attention of the Commission an interim procedural report to the attention of the Commission at its fifteenth session. That interim report[7] presented an overview of the action taken by the Secretariat in conformity with the recommendations of the first meeting of the expert group, a brief presentation of the methodology of the study, and information on the timeframe for completion of the study and its submission to the Commission at its 16th session for consideration.

[Paragraphs 14 and 15 were merged]

G. Responses from Member States

16. As at 31 December 2006, the Secretariat had received responses to the questionnaire on fraud and identity fraud from the following 46 Member States: 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, 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 had also provided copies of their relevant legislation.

H. Private sector responses

17. The UNCITRAL secretariat received many expressions of interest and support for the present study from the private sector companies and organizations contacted, and a number completed and submitted relevant portions of the questionnaire. Other private sector entities preferred to leave the response in the hands of the States in which they were based. All information provided was taken into account in preparing this Report, while carefully maintaining confidentiality. Appropriate public reports of private companies and industry associations concerned about economic fraud and identity-related crime issues were also reviewed.

---

[7] E/CN.15/2006/11 and Corr. 1

I. Second meeting of the Intergovernmental Expert Group Meeting to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity (Vienna, 16-20 January, 2007)

18. With the support of the Governments of Canada and the United Kingdom, a second meeting of the open-ended Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity was held in Vienna from 16-20 January 2007. In preparation for the meeting a first draft of the present report was circulated to the experts, and comments from experts representing Canada, Germany, the United Kingdom and the United States of America, as well as materials and comments from the United Nations Office on Drugs and Crime and the secretariat for the United Nations Commission on International Trade Law were received and taken into consideration. A second draft was prepared on the basis of these comments and additional responses received from Member States, and was reviewed by the second meeting of the Expert Group.

……..

[Paragraphs 18-25]

J. Use of terminology in the study

26. 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",[8] and a forensic definition was not seen as essential to the work of the present study. For purposes of clarity and context, however, 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 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.

27. 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. by deception is described as recruitment by fraud.[9] 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 present study.

---

[8] *Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice*, A/CONF.203/18, paragraphs 173-189 at paragraph 181.

[9] *Protocol to Prevent, Suppress and Punish Trafficking in Persons*, A/RES/55/25, Annex II, Article 2, subparagraph (a).

28. 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 do not fully encompass the scope of the identity-related problems covered by the present study. In the present Report, scenarios in which genuine identity information or documents are actually taken or misappropriated are 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. Accordingly, in the present report, the term "identity-related crime" is used as a general reference, and the more specific terms "identity theft" or "identity fraud" are used where contextually appropriate.

29. 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.[10]

Conclusions and Recommendations

A. Further work on the gathering, analysis and dissemination of information about fraud and identity-related crime

30. 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 do 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 under-reported and underestimated. Data that would permit the quantification of fraud by occurrence or offence rates are not available in many States, almost no official data quantifying proceeds exists. Data gathered by national financial intelligence units and the Financial Action Task Force are not of a statistical nature and not linked to fraud or other specific predicate offences. Some data is gathered by the private sector, but only for specific commercial applications. There is growing awareness of and concern about identity-related crime, but it 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

[10] Commission on International Trade Law, *Report of the UNCITRAL on its thirty-sixth session*, 30 June – 11 July 2003, A/58/17, paragraph 237 and "Possible future work relating to commercial fraud", A/CN.9/540, 9 April 2003, paragraphs 12-26.

the primary focus of offenders, identity-related crimes appear 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 group of experts therefore makes the following recommendations:

a. That further general research into economic fraud as a global issue be conducted, based on information from the Member States and other entities engaged in work on fraud or other areas of economic crime, where appropriate.

b. That the subject-areas of economic fraud and identity-related crime be divided into sub-categories to support effective priority-setting and focused research and follow up work by the Commission, UNODC, other relevant international organizations, and the Member States. Some priority areas could include the following:

(i) In the case of economic fraud, most States had clear legislative definitions and offences, but these were not detailed enough to support research and analysis of many of the specific types, trends and patterns which raise concerns, including mass-frauds and factors such as the involvement of transnationality, organised criminal groups and information and communications technologies. The development of global research-oriented definitions and typologies and support for States in using these to carry our 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 by the present 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 entails further elaboration and dissemination of basic definitions and typologies. This would support not only research and analysis, but also criminalisation, as few States have adopted specific offences in this area.

c. That the setting of priorities and the conduct of further work take into account the need to avoid overlap or duplication of effort and 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. That systematic and structured processes for gathering and analysing data in each Member State be developed, and that the United Nations Office on Drugs and Crime be asked to encourage and assist in this process and to encourage and support standardisation among Member States where possible and appropriate and subject to the availability of extra-budgetary 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, but also alternative sources less likely to be influenced by under-reporting.

(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 taken by offenders, the indirect economic costs, and the non-economic

costs of fraud. To ensure consistency, avoid duplication and ensure that 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. The United Nations Office on Drugs and Crime and other appropriate entities could also be asked to examine the relationships between economic fraud, identity-related crime and money laundering to support coordination between work done in these subject areas.

f. The Financial Action Task Force (FATF/GAFI) 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.

B. International cooperation

31. 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 *Convention against Transnational Organized Crime*, the *Council of Europe Cybercrime Convention*,[11] 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.

32. 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" within the meaning of Article 2, subparagraph (a) of the 2000 *Convention against Transnational Organized Crime*. Further, only 5 of the 46 responding States reported maximum possible sentences shorter than the 4 years required by the definition of "serious crime" in Article 2, subparagraph (b), which means that the *Convention* will apply if the States affected are Parties. Whether the *Convention* will also apply to transnational cases of identity-related crime is less clear, as few States have adopted domestic crimes to-date, but still seems likely. Identity crimes which are transnational in nature tend to involve falsification or

[11] E.T.S No. 185, Budapest, 23 November 2001. See, in particular Articles 7 (computer forgery) and 8 (computer fraud). The *Convention* provides for the criminalisation of a series of common forms of computer-related crime, the establishment of appropriate investigative and procedural measures and international cooperation. Countries outside of the Council of Europe may become Parties by accession.

tampering with identification systems and documents which 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.

33. For these reasons, the 2000 *Convention against Transnational Organized Crime*, and where applicable the 2001 *Council of Europe Convention against Cybercrime*, and 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 group of experts sees no need for any further international legal instruments in this area. It does, however, recommend that careful consideration be given to the most effective possible application of the two Conventions in fraud cases, including by the following:

a. Member States which have not yet done so should ratify or accede to and fully implement the *Convention against Transnational Organized Crime.*

a *bis*. Member States should consider acceding to the *Convention against Cybercrime*, which is open to non-European States..

b. Most States reported punishments which would make their more serious offences "serious crimes" within the meaning of Article 2, subparagraph (b) of the *Convention against Transnational Organized Crime*. However, many had offences that would not be covered by the *Convention*, and a few did not report any fraud offences that would be covered. Member States are encouraged to review applicable legislation with a view to ensuring that all appropriate fraud and related offences fall within the scope of "serious crimes" under the *Convention*.

c. Few States have criminalised identity-related crime *per se*, but most had related offences such as document forgery and impersonation, and the more serious of these would also be covered by the *Convention against Transnational Organized Crime* where the requirements of Articles 2 and 3 of the *Convention* were met. It is recommended that States review existing criminal offences with a view to ensuring that the *Convention* can be applied in appropriate cases.

c *bis*. It is also recommended that the scope of application and appropriate definitions contained in Articles 2 and 3 of the *Convention against Transnational Organized Crime* be taken into consideration by Member States engaged in the development of new offences relating to identity-related crime.

d. 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 *Convention* and its domestic implementing legislation in appropriate cases.

e. States should ensure that law enforcement and other relevant agencies are trained in the investigation of cybercrime, including where appropriate, the use of the *Convention against Cybercrime.*

C. Domestic powers to investigate, prosecute and punish fraud and identity-related crime

1. Criminalisation of fraud and identity-related crime

34. Most States reported a range of criminal fraud offences ranging from small deprivations to complex schemes involving major economic disruption and collateral forms of harm. These appeared to criminalise fraud adequately for purposes of suppressing domestic fraud and supporting international cooperation. Most States also indicated that fraud was considered a predicate offence for purposes of anti-money laundering regimes. While the vast majority of criminalisation issues appear to have been addressed, the evidence suggests that some specific enhancements 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 anti-money laundering measures. Criminal offences which cover only individual transactions could also be augmented to reflect the expansion of transnational and mass-frauds by criminalising fraud schemes and mass frauds specifically. 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 frauds against individual victims. It is therefore recommended that States consider the following enhancements, where appropriate.

(a) States which have not done so may wish to consider the modernization of fraud offences and investigative powers to deal effectively with domestic and transnational frauds committed using telephone, e-mail, the Internet and other telecommunications technologies.

(b) In view of the substantial proceeds generated by major frauds, States which apply anti-money laundering measures only to designated predicate offences should consider including fraud and similar offences as such.

(c) States which criminalise fraud only on the basis of individual fraudulent transactions may wish to consider criminalising conduct such as the operation of fraud schemes and the perpetration of mass-frauds.

35. 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. Law-makers need to develop appropriate concepts, definitions and approaches to the criminalisation of a range of conduct, including identity theft, identity fraud, and other identity-related crimes. Also critical for most States will be to ensure consistency with each State's 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 which provide a good basis for international cooperation are desirable. It is therefore recommended that States consider the adoption of new identity-based criminal offences. It is also recommended that, in developing new offences, common approaches to criminalisation be taken, to the greatest extent possible.

2. Jurisdiction

36. *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 evolution. 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 these in the context of the range of fraud offences and options for territorial jurisdiction covered by 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 to ensure that cases are prosecuted, where possible, by the State which 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 the United Nations Office on Drugs and Crime and other appropriate bodies, to help ensure that States which have jurisdiction but lack capacity are able to investigate and prosecute complex transnational frauds effectively.

(d) States should ensure that they have sufficient investigative jurisdiction and powers to provide necessary assistance to another State which prosecutes a fraud case which involves or affects their interests and which they are unable to prosecute for jurisdictional or practical reasons, or in which jurisdiction is ceded.

37. *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 *Convention against Transnational Organized Crime*, 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. The nature of transnational fraud makes early identification of the States concerned and early investigative coordination and cooperation particularly important. Concerned States which are not the prosecuting State should assist the prosecuting State in any way possible.

38. *Extraterritorial jurisdiction*. Articles 15 and 16 of the *Convention against Transnational Organized Crime* require States Parties which cannot extradite their own nationals to ensure that they have sufficient jurisdiction to prosecute offences covered by the *Convention* where one of their nationals commits such an offence outside of their territorial jurisdiction. It also encourages States Parties to establish

sufficient jurisdiction to prosecute cases where an offender found in their jurisdiction is not extradited for other reasons (Article 15, paragraph 4). In view of the large numbers of fraud cases which are transnational or multi-national 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 which has territorial jurisdiction to prosecute the offence, assuming that the conduct in question is within the scope of domestic offences and is a "serious crime" within Article 2, subparagraph (b) of the *Convention*. More general forms of extraterritorial jurisdiction were not raised in the general context of economic fraud, but the group of experts noted that some States have extraterritorial jurisdiction in cases where their fundamental interests are affected, such as offences relating to the forgery of passports or counterfeiting of currency.

3. Limitation periods and amnesty powers.

39. Limitation periods are an integral part of the criminal justice practices of some States, but these may raise particular concerns in major and transnational fraud cases which tend to be complex, costly and time-consuming to investigate and prosecute successfully. 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.[12]

a. It is therefore recommended that States take into consideration the nature of such frauds when establishing limitation periods to ensure that these are not unduly restrictive, and that longer periods be considered for specific types of fraud which are seen as likely to require more time, such as offences relating to corporate, commercial or other complex forms of fraud, offences which are transnational in nature or offences which involve organized criminal groups, where these are specific offences in national law.

a *bis*. It is also recommended that States consider allowing for the possibility of extensions to time limits on a case by case basis where this is appropriate due to factors such as complexity, transnationality, the involvement of organized criminal groups, links to other criminal activities or attempts by offenders to evade justice or delay proceedings.

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.

b *bis*. 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

[12] Note that some actions taken pursuant to recommendations in this segment may also implement some requirements of Article 11, paragraph 5 of the *United Nations Convention against Transnational Organized Crime*, A/RES/55/25, Annex I, and Article 29 of the *United Nations Convention against Corruption* A/RES/58/4, Annex.

under concurrent or exclusive territorial jurisdiction and *aut dedere aut judicare* provisions as are applied to purely domestic prosecutions in their domestic laws.

c. 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 which involve identity-related crime in the context of criminal offences or activities with transnational aspects.

4. Law enforcement and investigative capacity

[The former paragraphs 40 and 42 were merged]

40. Most serious economic fraud and identity-related crime involve a degree of sophistication which 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 re-training of officials.

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 throughout law enforcement in each country in 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 come to 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 crimes.

41. Several States and some commercial entities noted the usefulness of screening of mass telecommunications and financial or commercial transactions to look for patterns suggestive of fraud so that timely investigative and other measures could be applied. This raises several concerns, including possible infringements 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.

a. It is recommended that Member States, individually, collectively and where appropriate in consultation with commercial entities, undertake research to identify any characteristics which might be used to distinguish between normal legitimate and fraudulent transactions or activities, such as unusual patterns in telecommunications activity or commercial transactions, specific commercial practices, markets or commodities representing a high risk of fraud.

b. It is also recommended that useful substantive criteria and procedural practices for the screening and identification of activities suspected of involving fraud be developed and shared among States and appropriate commercial entities, and that States and the private sector collaborate and assist one another in ensuring that these criteria and practices are kept up to date and that appropriate officials are trained in their use.

c. It is recommended that 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 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, it is recommended that there be coordination and sharing of information between officials involved in anti-fraud and anti-money laundering activities, where appropriate.

[Former paragraph 42 was merged with paragraph 40]

5. Cooperation between criminal justice systems and the private sector

43. 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 is crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes. Both of these have a substantial impact on private interests as well as public ones. Fraud affects both individual commerce and commerce as a whole: large scale frauds 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, and in countries where private documents are used for public purposes and *vice versa*, crimes against any form of identification affect both areas. This makes it critical 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.

44. To prevent fraud and identity related crime, it is important that security countermeasures be developed and incorporated into commercial technologies and practices when they are first developed. This in turn requires consultation between public entities such as standard-setting bodies and private interests, including companies which produce and sell new technologies and those who will use them.

Important issues will include ensuring that preventive measures will be effective as such and will 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, and not less so.

45. A number of States mentioned the relationships between State and commercial identification systems, and 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, 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 have already been ongoing for some time in some *fora*, especially with respect to key issues such as the preservation of data.

46. A key element of prevention is the education and training of persons in a position to identify and report economic fraud or identity related crime, ranging from commercial customers or communication subscribers to employees who handle business transactions. Such training and education requires frequent updating, to ensure that information reflects 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 in support of effective education and training, including by sharing appropriate information, and ensuring that it reaches audiences to which they have access.

6. Economic fraud and identity-related crime in the context of development, reconstruction and economic transition

47. Countries with economies in transition, whether in the course of reconstruction, development or simple economic reform, are particularly vulnerable to economic fraud. Confusion between old and new rules or practices creates opportunities for offenders, and the harm caused by offences is greater: direct economic losses are harder to absorb and confidence in new economic and legal structures is eroded. Further harm may result from corruption, organized crime and other problems fuelled by the proceeds of economic fraud. The ability to identify citizens is also important as a stabilising element and in support of measures against major crime, but developing and transitional States often lack the basic infrastructure needed, such infrastructure as exists may be affected by corruption, and citizens may have concerns that identification systems may be used for repression.

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 effort 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 infrastructures be included as an element when assessing needs 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

[The former sections 7 and 8 were merged]

[The former paragraphs 48 and 51 were merged]

48. Given the links between economic fraud and some forms of identity related crime, many measures which prevent or deter one will also have the same effect for the other. This 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 frauds require advance, often extensive and careful preparation by offenders, and some form of vulnerability to deception on the part of victims, and both of these elements create opportunities for effective crime-prevention. Most of the options for preventing identity-related crime are more technical, focusing on means intended to make identification documents harder to tamper with, identification systems harder to subvert or corrupt, and identification data harder to obtain. As previously noted, close collaboration between relevant public and private sector entities in developing and implementing preventive measures will also be important for success and to the advantage of both, 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 will also be important.

(a) It is therefore recommended that Member States develop and implement effective fraud-prevention measures, at the national, regional and global levels, and in cooperation with the private sector. These prevention efforts could include the following.

(i) The dissemination of information about fraud to potential victims so they are less likely to be deceived. This could include both general information to

raise awareness of the threat, and timely information about specific forms of fraud based on accurate and up-to-date monitoring of fraudulent activities by appropriate entities in both the public and private sectors. Information campaigns could be directed at general populations, and at specific groups seen as particularly vulnerable to particular frauds or at increased risk of being targeted by particular offenders.

(ii) The dissemination of information about fraud to others who may be in a position to identify, report and prevent frauds when they occur. Many commercial entities already train key employees in areas such as banking, credit card transactions and other specialised areas where specific frauds may be encountered.

(iii) The rapid and accurate gathering and analysis of information to support effective and timely prevention measures. As noted, this should include the gathering of relevant information among law enforcement, commercial and other entities at the domestic level and where appropriate at the international level.

(iv) The rapid sharing of information among appropriate law-enforcement and private sector entities at both the domestic and international levels. Such sharing must be subject to appropriate and applicable privacy and security considerations, but generally, information needed to prevent fraud should not require the sharing of types of information, such as personal or investigative information, which would raise or invoke such considerations.

(v) The development of commercial practices and systems in ways which recognize the specific and general threat and costs associated with fraud 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, inter-operability and fair competition.

(b) It is also recommended that Member States develop and implement effective measures for the prevention of identity-related crime, at the national, regional and global levels, and in cooperation with the private sector. These prevention efforts could include the following.

(i) Law enforcement and relevant commercial entities should work together to develop and maintain an accurate picture of the methods used by offenders, and to disseminate information to educate potential victims about the risks of identity related crime and precautions that can be taken to prevent it. As with fraud, precautions taken by persons whose identities are taken are a key preventive element.

(ii) Appropriate education and training should also be developed and made available to key private employees and public officials who are in a position to detect and prevent identity related crime.

(iii) Information about identity-related crime should be shared among appropriate law-enforcement and private sector entities at both the domestic and international levels, to ensure that information disseminated for prevention is accurate and up to date.

[The former paragraphs 49 and 52 were merged]

49. A number of responses mentioned a range of technical means of prevention, both for economic fraud and identity related crime. These included 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 by governments. Costs of research, development and implementation are 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 crimes such as economic fraud, immigration or travel-related crimes such as trafficking in persons, and in general security.

(a) It is therefore recommended that technical information be shared with developing countries where feasible, and that they be assisted in using such information to establish robust domestic identification infrastructures in support of both public and commercial functions.

(b) It is also recommended that government and commercial entities cooperate to ensure that identification systems are robust and inter-operable to the extent that this is feasible.

50. 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 crimes, which are by their nature pre-planned and commonly involve some element of cost-benefit analysis on the part of offenders. In addition to incarceration, the economic nature of fraud suggests that fines, confiscation and anti-money laundering measures may be viable deterrents. Further study and consideration of deterrence measures is therefore recommended. In addition to offences and punishments, this could include measures such as focused and specialised law enforcement units trained to deal with fraud cases, where these are seen as increasing the probability of detection, prosecution and punishment.

9. Training

[Paragraphs 53-57 were merged]

53. One issue raised by some of the responses is the need for training investigators and prosecutors, and the need for technical assistance for developing countries in this area. In the case of economic fraud, training must address the extremely wide range of variations 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, it must address the fact that this is a new and still-evolving concept which encompasses both new, high-technology forms of crime as well as long-established crimes 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. . Experts noted that

such training will often require a multidisciplinary approach in the development and implementation of training programmes, including a range of disciplines from both government and private-sector entities. 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 knowledge not only of crimes such as impersonation and forgery, but also a knowledge of the identification infrastructures and systems which support both government and commercial forms of identification.

(a) Generally, it is recommended that action be taken to develop and disseminate appropriate materials and information, and that it be used to train investigators, prosecutors and other public officials, and where appropriate, persons in private sector positions where there is the potential to prevent fraud or identity-related crime or assist in its investigation and prosecution.

(b) It is also recommended that Member States cooperate collectively in sharing information relevant to the development of training programmes and materials. This is important not only to ensure that useful practices are transferred from one State to another, but also to help ensure that national anti-fraud officials are able to cooperate effectively against a growing tide of transnational fraud cases.

(c) It is further recommended that materials and training programmes incorporate a general overview of fraud, but otherwise be directed at specific forms or types of offending.

(d) It is further recommended that there be effective collaboration among anti-fraud, anti-money laundering, anti-corruption, anti-terrorism anti-cybercrime and similar training efforts, including those in the private sector, with a view to exploiting synergies, ensuring consistency and avoiding unnecessary duplication.

(e) It is further recommended that anti-fraud recommendations and training materials be disseminated to other United Nations and other intergovernmental bodies so that they will be available for inclusion in training and other materials developed by those bodies.

List of States which responded to the questionnaire

Algeria	Nicaragua
Belarus	Norway
Canada	Oman
Costa Rica	Panama
Croatia	Peru
Egypt	Romania
Finland	Russian Federation
Germany	Saudi Arabia
Greece	Slovak Republic
Hungary	Slovenia
Italy	South Africa
Japan	Spain

Jordan	Sudan
Republic of Korea	Sweden
Latvia	Switzerland
Lebanon	Syria
Former Yugoslav Republic of Macedonia	Trinidad and Tobago
Madagascar	Turkey
Malta	United Arab Emirates
Mauritius	United Kingdom
Mexico	United States of America
Monaco	Zambia
Morocco	
Netherlands	

Annex I: Results of the study on economic fraud

I. Commercial context of economic fraud

1. Commercial law

60. Most States provided information about laws which regulated commercial activities, ranging from highly-regulated to largely unregulated Most have contract law or law of obligations based on the freedom to contract and circumscribed by additional rules intended to provide protection in situations of inequality, dishonesty or inadequate disclosure. Some also have more general consumer protections such as limits on advertising and standards for the quality of goods or services. Rules appeared designed to increase the stability and predictability of commercial dealings and to protect vulnerable parties. Many States had specific rules for specific types of commerce, and some had established specific agencies to administer these. Some also reported legislative or regulatory powers governing technical aspects of commerce, such as elements of the infrastructure of electronic commerce contracts and identification.[13] A number of States also mentioned the possibility of civil lawsuits as a means of recovery, either as an exclusively civil option, or a hybrid option in which civil claims could be based on a criminal conviction, and some mentioned other civil remedies, such as the voiding of contracts. Many also have additional requirements for commercial areas seen as vulnerable to fraud, such as corporate governance and breach of trust issues and areas such as telephone or Internet sales. One State observed that everyday commercial practice might not necessarily correspond with legislative ideals, noting that even where equality of bargaining power might be enacted in law, this did not necessarily mean that it would exist in practice.

2. Commercial technologies

61. Generally the experts considered commercial technologies to include technological systems which had been developed or adapted or were commonly used to support elements of commerce. These could also be broken down into mass consumer technologies and other commercial technologies used by banks and financial institutions for smaller numbers of larger transactions. Many commercial technologies depend on the availability of supporting information and communication technologies. There appear to be differences in the availability and use of technologies within countries. A number of States reported greater access and use in urban areas than rural ones, and this was more pronounced in developing countries. The use of information, communications and commercial technologies has expanded substantially in recent decades. Telephone access has increased from fewer than 100 million in 1950 to about 1 billion in 2000. Mobile telephone use has

---

[13] Regarding electronic commerce legislation see *UNCITRAL Model Law on Electronic Commerce*¸ A/RES/51/162, Annex, and *Guide to Enactment*, United Nations, 1999, Sales No. E.99.V.4. Regarding electronic means of identification, see *UNCITRAL Model Law on Electronic Signatures*, A/RES/56/80, Annex, and *Guide to Enactment*, United Nations, 2002, Sales No. E.02.V.8.

also rapidly expanded, especially in developing countries. Internet access has gone from zero in 1969 to 395,000,000 in 2006, and is expected to exceed 500,000,000 before the end of the present decade.[14] Use of consumer commercial technologies such as payment (debit and credit) cards varied widely. Generally, developing countries estimated relatively low usage, while the most technologically developed countries reported a range between approximately 25-50% of transactions and a shift from cash to the use of cards and other electronic means of payment. Most developing countries have no data on commercial technologies and a number of countries reported that only the companies involved would have such data. Developing countries reported higher usage of barter, but one developed country also noted increases in barter supported by the Internet. The ways technologies are used are also expanding. Electronic commerce, in which technologies are used for the advertising and sale of goods or services as well as payment, is expanding in countries where it is technologically viable, but is still a small fraction of overall commerce.

II. National experiences of economic fraud and legislative responses

1. Meaning of economic fraud and scope and elements of fraud offences

62. In most States, the legislative definition of fraud is exclusively economic, but practical use of the term sometimes includes other forms of crime which involve elements such as dishonesty or deception, but not necessarily any economic element. Most of the legal definitions of fraud were considered criminal law and contained economic elements. Some States 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 UNCITRAL, which suggests that commercial concepts of fraud include some conduct that some States would not necessarily see as criminal.[15] Some States indicated that they considered fraud as including non-economic crime, but reported fraud offences based on economic losses, and non-economic offences, such as forgery or impersonation, which were not legally defined as “fraud”. Common-law definitions are based on the original English concepts of fraud or false pretences, which include economic elements, but are defined in case law, and some common law States reported statutory offences supported by non-statutory definitions.

63. There was a high degree of consistency in the elements of the fraud offences provided or described by States. 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 or losses, including tangible property, financial

---

[14] Sources: (telephone access) International Telecommunication Union (ITU) *World Telecommunication Development Report 2002*, ITU, March 2002. Executive Summary available on-line at: http://www.itu.int/ITU-D/ict/publications/wtdr_02/material/WTDR02-Sum_E.pdf (Internet access) Internet Systems Consortium, Internet Domain Survey, http://www.isc.org/index.pl.

[15] UNCITRAL, Note by the Secretariat: “Possible future work relating to commercial fraud”, A/CN.9/540, Part III, “The nature of commercial fraud”, paragraph 12 *et seq*.

or other interests, and less-tangible losses such as exposure to risk or loss of expectation value, even if these did not materialise. The elements of dishonesty or deception were also consistently present. Some States required active conduct intended to mislead, while others included also deception 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, but most systems appear to have dealt with this issue in some way, treating machine-related variants as types of fraud. Similar issues arise with respect to cases where legal persons are deceived, and these too, are generally seen as forms of fraud. Some States appear to have offences only for individual transactions, while others also have offences of defrauding the public as a whole, perpetrating mass frauds or operating fraudulent schemes, which may simplify prosecution, evidentiary and jurisdictional issues in some cases.

64. Most fraud succeeds by imitating legitimate commerce, 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 contracts, advertising, and remedies for defective or misrepresented goods were reported, as were regulatory regimes establishing such elements as minimum standards for 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 provisions were directed at specific commerce such as stock markets, insurance or real property transfers, or key areas of professional practice such as law or accounting.

2. Approaches to classifying economic fraud

65. States were asked about the legal basis on which they classified fraud. The responses disclosed two strategies for criminalisation, depending on whether fraud was classified in detail or not. Some States reported only a very small number of general fraud offences, while other States reported larger numbers of more narrowly-framed, specific offences. Definitions based on *modus operandi*, types of infrastructure attacked or involved and victim status or characteristics were the most common. It was also clear that while national legislation sometimes followed the typology suggested by the questionnaire, the suggested categories overlapped. Descriptions such as “mass-market fraud”, “advance fee fraud” and “pyramid” or “Ponzi” fraud schemes are all used primarily as non-legislative terms, although several States did report specific offences or other legal provisions. Some States have criminalised frauds based on devices, passwords or access codes or the use of telephones or telecommunications, 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 attacking of public structures such as social benefits or tax systems, and private commercial structures such as insurance, credit card, banking or other financial operations. Fewer States reported fraud offences based on the type of victim or type of offender, but a number did consider these factors as the basis for aggravated offences or sentences. Specific groups of potential victims accorded additional

protection included the elderly, minors, the mentally disabled, legal persons and the estates of deceased persons. Some States also apply additional measures 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

66. States reported a wide range of specific offences of fraud and related or preparatory conduct. Many States have found it necessary to expand established offences or adopt new ones to deal with recent innovations by offenders, especially in the area of computer-related frauds. Computer fraud offences are required by Article 8 of the *Council of Europe Convention on Cybercrime*[16], and a number of States reported offences of computer fraud or more general computer-related crime offences that could apply in fraud cases. These included possession, trafficking in or use of instrumentalities for computer-related fraud and offences relating to computer "hacking" or the unauthorized access to or use of computer or telecommunications systems.

67. Other types of fraud which were the subject of specific offences included: 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 counterfeiting private intellectual property. Some States also have specific offences covering frauds against the State itself, which may include corruption offences, and the European Union requires its Member States to criminalise frauds which affect the EU's financial interests or funds covered by its budget.[17] Other frauds against the State included frauds against public procurement systems or public benefits 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. Some forms of tax evasion and the counterfeiting of currency or stamps are also seen as types of fraud in some States. Smuggling offences may be treated in some States as frauds if the purpose is to avoid excise taxes on commodities which are legal in that State, such as tobacco, as opposed to trafficking in illegal commodities such as narcotic drugs. A number of related or preparatory offences were also reported, including: identity-related crimes such as impersonation and misuse of identification documents or identity information; abuses related to documents other than identity documents; the falsification, destruction or tampering with electronic data; some corruption offences; arson and other forms of property damage 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.

---

[16] E.T.S No. 185, Budapest, 23 November 2001.

[17] *Convention on the Protection of the European Union's Financial Interests*, 26 July 1993, 93/C316/03, [1995] OJ C 316/49 of 27.11.1995, Article 1.

4. Types of fraud encountered by States

68. 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. 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.

69. While there are some superficial variables attributable to differences in language, culture or commercial practice, the underlying problem of economic 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.

70. Specific types of fraud raised by States included types defined by method, such as “advance fee” frauds, pyramid or “Ponzi” schemes, computer frauds and frauds using paper documents; frauds defined by the system or interests affected, including frauds relating to bankruptcy, loans, real estate transactions, charitable appeals, maritime transport, stock markets, insurance, or commercial frauds in general; mass frauds defined by the large numbers of victims; telemarketing and telecommunications frauds, in which telecommunications were either the medium used or the proceeds generated; the counterfeiting of goods or currency; and frauds against government or public interests, including immigration systems or documents, procurement systems, tax systems and public benefits systems. 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. Corruption offences such as bribery are seen by some States as a form of fraud against government, and are also often encountered as an element of larger fraud schemes, when officials are bribed to ensure the success of the primary fraud.

5. Liability of legal persons

71. 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. Most States indicated that they applied criminal liability to legal persons, and one extended it to both legally and factually-established bodies. Several other States indicated that they did not extend criminal liability but did provide for administrative liability and appropriate punishments. All of the States which had criminal or administrative liability provided for fines, and some included other measures, such as confiscation. Some also had specific judicial powers such as barring specified natural persons from involvement in a company, and ordering that a legal person be supervised or refrain from certain specified business activities. 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

72. Punishments generally 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. Cases 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, affected many victims, caused major bankruptcies, and in some cases proved serious enough to de-stabilise governments or cause damage to national economies. 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 of the fraud in terms of the numbers of victims affected or proceeds generated. Other common aggravating factors included repeat offending, mass-frauds, breach of trust or other abuse of power or inequality between offenders and victims, the involvement or organized criminal groups or money-laundering, and frauds which targeted or affected government or public interests. As noted, underlying policies generally reflected the need for additional deterrence to protect particularly vulnerable victims such as the elderly or to deter persons in positions where fraud was seen as exceptionally likely or damaging, or to protect the integrity of key commercial systems or documents.

72*bis*. Almost all States 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*,[18] or provided descriptions of offences that appear to meet those requirements. 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 provided for fines or confiscation, both as a punishment for less-serious cases and as a sanction for

[18] A/RES/55/25/Annex I. Note that Article 11, paragraph 2 of the Convention requires, *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.

legal persons, especially where the legislative framework only extends full criminal liability to natural persons.[19] Specific sentencing conditions are also imposed on a case by case basis in many systems. Non criminal penalties such as loss of professional status or licenses were also mentioned. 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, especially in legal systems where the trier of fact is a jury or magistrate. 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 travel. This problem may be addressed in some cases by mutual legal assistance in the form of video-link testimony under the *United Nations Convention against Transnational Organized Crime*,[20] where applicable.

III. Assessing the scope and extent of fraud

1. The reporting and recording of fraud

73. 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. There is widespread agreement among experts on fraud that it is systematically under-reported. 22 of the 24 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 UNCITRAL.[21] Some States noted that 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. In some States, the availability of multiple public and commercial entities to which frauds could be reported was a concern, as was the fact that data collected by commercial sources was not always available to or compatible with criminal justice statistics.

74. Many reasons were given for under-reporting, and most were consistent among States. The most commonly cited reason was the fact that victims, including both natural and legal persons, are embarrassed or humiliated and seek to avoid the publicity inherent in criminal proceedings or what one State described as "reputational damage". 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.[22] Frauds deceive victims and often contain elements intended to persuade

---

[19] See also *Convention on the Protection of the European Union's Financial Interests*, 26 July 1993, 93/C316/03, [1995] OJ C 316/49 of 27.11.1995, Article 4

[20] A/RES/55/25, Annex I, Article 18, paragraph 18.

[21] UNCITRAL, Possible future work relating to commercial fraud, A/CN.9/540, 9 April 2003, paragraph 6, subparagraph (c).

[22] *Canada-United States Cooperation Against Cross-Border Telemarketing Fraud: Report of the Canada-United States Working Group*, Governments of Canada and the United States (joint publication), November 1997, chapter 4.1, available on-line at: http://www.justice.gc.ca/en/dept/pub/wgtf/headings.html (English) and

victims not to report, including the fear of self-incrimination or loss of proceeds, or by persuading them that they have made a bad commercial bargain and were not victims of a crime. Victims also often believe that claims will not be taken seriously, that the costs of recovery or prosecution would be greater than any benefits, or that reporting losses to their banks or credit-card issuers is more likely to lead to recovery than reports to criminal justice agencies. Commercial entities which encounter fraud tend to rely more on their own internal investigative and other processes than criminal justice measures. Victims also see only their own individual case and may under-estimate the seriousness of the crime or importance of reporting, especially in some forms of mass fraud or commercial fraud.

75. 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. 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. 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.

2. The quantification of fraud

76. The counting of fraud cases can produce substantially different results depending on how cases are reported and recorded. Mass-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. A third picture may emerge if the amount of losses or proceeds of fraud are counted, because areas such as commercial fraud tend to involve small numbers of offences with very large losses, while mass marketing frauds often 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. There are also substantial differences between information gathered by criminal justice systems for policy purposes and by private businesses for commercial purposes, and commercial data may not be shared for business reasons.

---

http://www.justice.gc.ca/fr/dept/pub/wgtf/headings.html (French).

3. Rates and trends in fraud

77. Most States did not provide concrete statistics, but 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 inconclusive results. This was consistent with the views of the experts, as well as earlier work by UNCITRAL on commercial fraud.[23] A number of States expressed the view that there was a connection between overall increases, increases in transnational fraud and the expansion of access to information, communications and commercial technologies. Only five States provided statistical data. Of these, two found increases, one reported inconclusive data and one reported decreases, but noted that these might be attributable to changes in reporting or recording. 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. 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. 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.

78. Several critical questions arise for national and global statistical analysis. Under-reporting makes it difficult to assess real occurrence levels and may distort information about the relative prevalence of different types of fraud. Legal definitions vary, and the same fraud may be counted as one occurrence or many in different systems. Population trends may also have an effect: several States reported that commercial practices and access to and use of relevant technologies were more prevalent in urban areas than rural ones, 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 also noted that data reported were divided among criminal justice agencies, other agencies, and private sector entities, raising a need to identify gaps and compensate for multiple reporting.

IV. Relationship between economic fraud and other problems

1. Fraud and the involvement of organised criminal groups

---

[23] Report of the Commission on International Trade Law at its thirty-sixth session, A/58/17, paragraph 235 and "Possible future work relating to commercial fraud", A/CN.9/540, 9 April 2003, paragraph 5,

79. Fraud can be committed by individuals, but expert opinion and the information provided by States suggest that most serious frauds involve "organised criminal groups" within the meaning of the *Convention against Transnational Organized Crime.*[24] 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 also complementarities with other criminal activities in which they are engaged. Smaller, more flexible groups are formed to commit 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 third scenario is raised when frauds are committed by or on behalf of legal persons, and a company or group of employees may become "organised criminal group" when they commit or become involved in the fraud. Some States reported some types of fraud as more likely to involve organised groups than others, and many saw frauds by organized criminal groups 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.[25] A number of States have more serious offences or harsher punishments for cases where organised crime is involved. 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. The involvement of organized crime 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. 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

80. States did not have statistical information concerning transnational fraud *per se*, but it is common and many national experts have had extensive experiences with it. Many States indicated that they had encountered cases, and others expressed concern about the possibility. The major concerns were that transnational fraud appears to be increasing, and that transnational offences are easy to commit, but costly, difficult and complex to investigate. 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.[26] Other States reported

---

[24] A/RES/55/25/Annex I, Articles 2 and 3.

[25] See also Commission on International Trade Law, "Possible future work relating to commercial fraud", A/CN.9/540, paragraphs 3, 8 and 9.

[26] *Canada-United States Cooperation Against Cross-Border Telemarketing Fraud: Report of the Canada-United States Working Group*, Governments of Canada and the United States (joint publication), November 1997, pages 5-6, available on-line at: http://www.justice.gc.ca/en/dept/pub/wgtf/headings.html (English) and

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.

81. A number of States noted a relationship between the availability and use of information, communication and commercial technologies and transnational fraud cases. They 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 that media such as fax machines, e-mail, telephones and the Internet can be used to establish contact between offenders and victims, but there are also other links. One State noted that technologies make it possible for offenders to cooperate effectively with one another from different jurisdictions.[27] Others noted that information used in frauds itself becomes an illicit commodity, with lists of potential victims, and credit card data obtained by "skimming" or cybercrime bought and sold by offenders and often transferred by e-mail. Technologies and transnationality are also linked when offenders use call-forwarding, anonymous re-mailers and similar means in an effort to conceal their identities and locations and avoid tracing by law enforcement.

82. Several States also described frauds which are inherently transnational in nature. Examples included the smuggling of goods to avoid paying customs fees, a range of maritime-transport frauds, immigration, passport or visa frauds and frauds involving vacation travel or accommodations such as "time share" arrangements.. 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

83. Most States do not have records or specific offences that link the misuse of technologies to fraud, although many have found it necessary to ensure that existing fraud offences cover new technological variations as these are taken up by offenders. States Parties to the *Council of Europe Convention on Cybercrime* are required to criminalise computer fraud and forgery.[28] There are clear links between information and communications technologies and commercial technologies such as payment cards and electronic commerce, clear links between commercial technologies and many types of fraud, and many different ways in which technologies can be used to commit or support frauds. States which reported data generally described patterns which suggest a significant increase in information technologies, accompanied by a more gradual shift to the corresponding commercial

---

http://www.justice.gc.ca/fr/dept/pub/wgtf/headings.html (French). See also *Mass-Marketing Fraud: Report to the Attorney General of the United States and Solicitor General of Canada*, May 2003, pp.11-12, available on-line at: http://www.usdoj.gov/opa/pr/2003/May/remmffinal.pdf.

[27] See, for example, *Libman v. the Queen* [1985] 2 SCR 178 (Supreme Court of Canada) and *Secretary of State for Trade v. Markus* [1976] A.C. 37 (United Kingdom House of Lords).

[28] *Council of Europe Convention on Cybercrime*, E.T.S. No.185, 23 November 2001, Articles 7 and 8.

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. Other 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. Transitions to new technologies and commercial practice, new forms of offender behaviour and law enforcement and legislative responses can all produce rapid and unpredictable changes in offending rates some such changes were described by States. Other variables include the fact that crime statistics are also evolving, and that technologies are sometimes used to encourage reporting, which can generate increases in apparent offending that do not correspond to changes in actual offending.

84. Technologies affect fraud in a variety of ways. While they provide opportunities and reduced risks for offenders, they can also be very effective in preventing, controlling or deterring fraud, and several States noted that their impact was by no means one-sided or completely to the advantage of offenders. The most common offender use was for basic contact with victims, including initial identification, selection and contact of victims; 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. In many frauds, different technologies are used for each stage. After initial contact by mass communication, persuasion might involve more personal contact through telephone calls for example. Similarly, funds transfers from victims are done using fast, irrevocable means to which victims have access, such as credit cards or wire-transfer, while subsequent transfers between offenders may use other means less likely to attract the attention of anti-money laundering measures. Technologies were also used to link offenders together and to transfer information such as credit card data, to conceal offenders' true identities and locations, and to make the tracing of communications as difficult as possible. Other roles included the use of scanners and printers to produce high-quality document forgeries, offender research to make fraud schemes plausible and credible, and the dissemination of false information as part of wider fraud schemes such as auction frauds or stock frauds.

85. A number of specific examples or suggestions for the use of technologies for the prevention, investigation and prosecution of fraud were raised, both by States and private commercial sources, and some States noted this was a key area for effective cooperation between public and private entities. Generally, technical investigative measures offer benefits for law enforcement and criminal justice, but sometimes confront commercial entities with conflicting pressures of supporting criminal justice, while at the same time protecting customers and ensuring that operations remain competitive and commercially viable. The control of cybercrime is a major commercial activity in its own right, with companies producing security advice, training and technologies as a commodity for sale to other companies in need of them to protect customers and prevent monetary and other losses. Some States noted the need for close collaboration at all stages, including the development of new commercial and crime-control technologies, the need for a wide range of expertise, and the need for resources and commitment to what most saw as a rapidly and constantly-evolving problem. Specific technological applications raised included security and prevention elements such as firewalls and encryption, and

investigative methods such as interception of communications and the use of "traffic data" to trace offender communications.[29] One State noted that, in addition to locating offenders, proceeds and evidence, tracing communications was also used in mass-fraud cases to identify additional victims who had not complained about the fraud. One issue raised was the desire of law enforcement to preserve such data for as long as possible, while commercial entities generally have concerns about storage costs and the implications for customer or subscriber privacy. The use of technologies to prevent fraud by quickly publicising known schemes and new developments to alert law enforcement, private company officials and potential victims was also raised by a number of States. Commercial research also shows that most commercial fraud, including frauds using technologies, involve inside employees, highlighting the need for training in both the recognition and prevention of fraud and the importance of protecting the interests of companies and customers.

4. Fraud, the proceeds of fraud and money-laundering

86. 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. From a procedural standpoint, 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. Most States consider fraud to be a predicate offence for purposes of anti-money laundering measures: 30 States identified one or more serious fraud offences as predicate offences, 12 did not provide information and only 4 did not consider fraud as a predicate offence. 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.

87. Only a few States provided information about total losses or proceeds, but it is clear that these can be substantial, with frauds as high as hundreds of millions of dollars, and total losses in some States in the billions of dollars.[30] Commercial

---

[29] See, for example, *Council of Europe 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."

[30] See Commission on International Trade Law, "Possible future work on commercial fraud", A/CN.9/540, paragraphs 5-11.

sources were limited to specific sectors, such as the insurance or credit card industries but were consistent with this. The Financial Action Task Force (FATF/GAFI) does not report detailed statistics or estimates, but 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.[31] Obtaining accurate information about overall proceeds of fraud and other offences appears to pose a formidable challenge. National financial intelligence units operate on the basis of financial transactions which are reported as suspicious or falling under other criteria, such as large cash transfers, but the information is then used for investigative and not statistical purposes. At the investigative stage, it is usually not apparent whether funds are being laundered at all, or if so, which predicate offences may be linked to the funds. National crime statistics also tend to be based on numbers of occurrences, prosecutions, convictions and sentences, with proceeds, if known at all, generally estimated or representing only known transactions or victims which is only part of the total in most cases. The best information is in the hands of private companies, which track losses for business purposes, but these are limited to each company's specific areas of business, and in some cases are seen as commercially sensitive. Actual fraud losses are also much greater than actual proceeds taken by offenders. Not all proceeds are reported, detected or counted, and loss calculations may include indirect costs or what one commercial source described as "collateral damage" from frauds.[32]

88. Fraud and money laundering are conceptually different, but may resemble one another in practice.[33] The major difference is that fraud essentially converts legal funds into illicit proceeds, whereas criminal money-laundering involves the subsequent transfer and concealment of those proceeds, although neither fraud nor money-laundering are usually that simple in practice. Apparently-laundered money from one victim may be paid to others as "investment" proceeds to lure them into the scheme or even to the same victim to encourage further participation or discourage complaints to authorities, for example. The major similarity is that the means of deception and conduct of covert or unobtrusive transactions are often common to both. The inherent deception and resemblance of the two crimes sometimes poses a challenge for law enforcement, but may also represent 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 frauds, and some banks, telecommunications providers and other commercial or financial institutions already screen mass transaction data to look for unusual patterns suggestive of fraud for follow up. As with other predicate offences, fraud cases may from time to time generate money-laundering investigations and prosecutions and *vice versa*, suggesting the usefulness of cooperation between appropriate public and commercial entities.

---

[31] See FATF, Report on Money Laundering Typologies, 28 June 1996, paragraph 10-11, and Report on Money Laundering Typologies (2000-2001), paragraphs 52-53, available on-line at : http://www.fatf-gafi.org/pages/0,2966,en_32250379_32237235_1_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)

[32] PriceWaterhouseCoopers' Global Economic Crime Survey 2005, section 3.3.

[33] 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_1,00.html (English), http://www.fatf-gafi.org/pages/0,2966,fr_32250379_32237235_33631745_1_1_1_1,00.html (French)

89. 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, *in rem* proceedings, hybrid processes in which types of civil forfeiture or recovery could be based on criminal proceedings, and completely civil recovery schemes initiated by victims and in at least one State, by government. One State referred to a scheme under which some compensation could be claimed from the State itself where it could not be recovered from offenders. The recovery and return of proceeds can present major practical challenges, especially in major commercial frauds and mass frauds. In commercial frauds victims are often legal persons, and indirectly, investors, shareholders or customers whose rights can be difficult to identify. In mass frauds, very large numbers of small, competing claims in multiple jurisdictions may be so complex that the costs of assessment, adjudication and return exceed losses or available proceeds. Civil claims also face major obstacles, including the fact that criminal powers and remedies relating to tracing, freezing, seizure and forfeiture are usually not available.

5. Fraud and terrorism[34]

90. 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.[35] A similar range of crimes has been reported by the Financial Action Task Force in its work on the financing of terrorism.[36] Cases are rare, but several States indicated that they had encountered fraud cases linked or believed to be linked to terrorist activities, and additional States indicated that they had concerns about the problem. Small, local frauds and credit-card fraud were used or 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 more substantial and ongoing revenues for other purposes.[37] Sources suggest that there may be a trend towards smaller, more locally-based frauds and other crimes as a source of funds due to the

---

[34] While there is no consensus on the 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. The question of the meaning or scope of terrorism itself was left to the Member States, and it is not clear whether responses were based on the *Convention* or on definitions or descriptions used by the States themselves.

[35] See S/RES/1267 (1999), 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, paragraphs 69-70, and Fourth 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/2006/154, paragraphs 63-66.

[36] See Financial Action Task Force (FATF/GAFI), Report on Money Laundering Typologies, 2001-2002, http://www.fatf-gafi.org/dataoecd/29/35/34038006.pdf, chapter 1 paragraphs 10-12.

[37] See Financial Action Task Force (FATF/GAFI), Report on Money Laundering Typologies, 2001-2002, http://www.fatf-gafi.org/dataoecd/29/35/34038006.pdf, paragraph 11, Example 1.

low costs of many terrorist activities, the vulnerability of large, transnational activities to surveillance and the fragmentation of Al Qaida. [38]

91. Major economic frauds encountered by States included insurance fraud, smuggling and excise tax frauds, frauds relating to currency exchange, frauds against public benefit schemes, and business or commercial frauds. Benefit frauds and credit-card frauds have been encountered both as individual direct sources for small, local terrorist operations and as the basis of large-scale, organised schemes. Several States also voiced concerns about the use of frauds against telecommunications providers where the real motive was not obtaining free services, but gaining access to anonymous, untraceable Internet, e-mail or mobile telephone services. This type of fraud has been associated with cybercrime offenders and organized crime for some time, but has now been taken up by terrorist organizations for the same reasons. [39]

92. 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,[40] and by academic and journalistic sources.[41] 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.[42] 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.[43] 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.[44]

93. The two major scenarios of concern are the creation of sham charities to finance terrorism directly, which defrauds donors, and the infiltration of legitimate charities to divert donations to terrorism, which is either fraud or theft against the charity

---

[38] See 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, paragraphs 67-70 and "Why terror financing is so tough to track down", *Christian Science Monitor*, 8 March 2006, http://www.csmonitor.com/2006/0308/p04s01-woeu.html.

[39] See, for example, testimony of R.A, Rohde before the United States Senate Sub-Committee on Technology, Terrorism and Government Information, 24 February 1998, http://www.fas.org/irp/congress/1998_hr/s980224r.htm, and Alan Sipress, A., "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace: In Sign of New Threat, Militant Offers Tips on Credit Card Fraud", *Washington Post*, 14 December 2004, p. A-19, http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.

[40] See Financial Action Task Force, Special Recommendations on Terrorist Financing, 22 October 2004, Special Recommendation VIII, 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", http://www.fatf-gafi.org/dataoecd/12/63/34328318.PDF.

[41] See, e.g., Rudner, M., "Using Financial Intelligence against the Funding of Terrorism", *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" http://news.bbc.co.uk/2/hi/business/4692941.stm.

[42] Rudner, *supra*, at pp.43-44.

[43] 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.

[44] 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.

itself. Legitimate charities also have concerns. Strict accounting requirements are difficult for them to meet and raise administration costs, and even unfounded rumours of links to fraud or terrorism can have a major effect in deterring donors. 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.[45]

94. 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 proceeds may be diverted to terrorist groups and because accounting or oversight safeguards are particularly difficult to apply. It can be difficult to distinguish between fraud and other crimes in such cases. If donations are used for terrorism, it would generally be fraud if the donors were deceived and extortion if they not deceived but were intimidated. Where donors were aware of the true purpose and not coerced, 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*.[46] Aside from playing a role as a source of funds, charities may also be used as a conduit for funds generated by other crimes or legal sources, and in such cases financing or money-laundering offences may apply.

6. The impact of fraud in countries under reconstruction or with economies in transition

95. Economic fraud poses additional problems for countries under reconstruction, economies in transition and 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. 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 develop new laws and train officials is also a challenge because of the sophistication of offenders and complexity of many frauds. Fraud is also a crime of deception, and the potential for deception increases in transitional conditions, where new social or economic rules and practices are not well-understood. Major frauds can do great damage to economic development efforts by eroding essential popular and consumer confidence in the reforms. Fraud also has the potential to use resources from developed countries to fuel organized crime in developing countries in the same way as has been encountered with trafficking in narcotic drugs. Frauds against a number of reconstruction and transitional schemes were reported, including frauds against new taxation schemes, new procurement processes or privatization schemes. One State mentioned frauds against tax and privatisation schemes as a major source of funds for organized crime and another mentioned a fraud against its new value-added tax (VAT) refund scheme that was sufficiently serious to negatively affect the national budget. International charitable

---

[45] S/2005/572, above, at paragraphs 85-88.

[46] A/RES/54/109, Annex, adopted 9 December 1989, in force 10 April 2002.

and insurance-based efforts to rebuild after major natural disasters such as the 2004 Asian tsunami have also been exploited,[47] and in at least two cases, major "Ponzi" or pyramid-scheme frauds have been cited as a factor in de-stabilising countries in economic transition.[48]

96. The relationships between fraud and transition, reconstruction and rebuilding efforts have significant implications for governments and organizations involved. There is a clear need to ensure that participants are all aware of the high risk of fraud in these circumstances and the substantial harm it can cause, for the development of practices and procedures resistant to fraud and for close coordination to quickly identify and remedy problems. This may include 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.

VI. International cooperation and jurisdiction issues

97. 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 *Convention against Transnational Organized Crime*[49] and, for those countries which are States Parties to it, the *Council of Europe Convention on Cybercrime*[50] provide a sufficient legal basis for such cooperation, and that the focus should be on measures to ensure that the

---

[47] 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", http://www.ncis.co.uk/press/tsunami.asp and United States Federal Bureau of Investigation, "Tsunami disaster relief fraud alert: Don't be scammed", 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 http://www.usdoj.gov/katrina/Katrina_Fraud/index.html.

[48] See: Elbirt, Carlos, "Albania Under the Pyramid", World Bank 2001, available on-line at: http://www.worldbank.org/html/prddr/trans/so97/albania2.htm. 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, and some sources also cite the collapse of a government-sanctioned pyramid scheme as a factor in the fall of the Government of Haiti in late 2004.

[49] A/RES/55/25, Annex.

[50] E.T.S No. 185, Budapest, 23 November 2001

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

98. 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 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*.[51] 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

99. 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 refusing extradition requests, such as the absence of "dual criminality" *de minimus* limits and the fact that the offence was of a political character seem unlikely to raise concerns in fraud cases. Other reasons, however, 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

---

[51] See *Canada-United States Cooperation Against Cross-Border Telemarketing Fraud: Report of the Canada-United States Working Group*, Governments of Canada and the United States (joint publication), November 1997, and Article 18, paragraph 18 of the *United Nations Convention against Transnational Organized Crime*, which calls for the use of video-link evidence. Similar provisions are found in the *Convention against Corruption* at Article 46, paragraph 18.

cases, especially in cases where justice was evaded, and much the same rationale exists for the more complex fraud cases.[52]

100. 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."[53] 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.[54] 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.[55] 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*[56] 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. The scope of offences which are extraditable are narrower, being limited to offences of fraud and forgery which 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

101. Transnational fraud is one of the most common forms of criminal case raising challenges to conventional territorial jurisdiction.[57] 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.

---

[52] *United Nations Convention against Transnational Organized Crime*, A/RES/55/25, Annex I, Article 11, paragraph 5.

[53] See *Convention*, A/RES/55/25, Annex I, Article 2, subparagraphs (a) and (b), and Article 3, paragraph 2.

[54] See *Convention*, A/RES/55/25, Annex I, Articles 15-16, and in particular Article 15, paragraphs 3 and 4, Article 16, paragraphs 1 and 10 and Article 17. See also *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto*, U.N., 2004, Sales No. E.05.V.2.

[55] See *Convention*, A/RES/55/25, Annex I, Article 15, paragraph 4,

[56] E.T.S No. 185, Budapest, 23 November 2001, Articles 3 and 4 (criminalisation), and 24 (extradition).

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.[58] 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.[59] 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.[60] 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.

101*bis*. 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 lies 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.

---

[57] See, for example, Hirst, M., *Jurisdiction and the Ambit of the Criminal Law*, Oxford, 2003, pp.158-180.

[58] Seguin, J. "The Case for Transferring Territorial Jurisdiction in the European Union" (2001) *Criminal Law Forum*. Vol.12, pp.247-65 at 249.

[59] See, for example the United Kingdom *Criminal Justice Act, 1993*, c.33, Part I, http://www.opsi.gov.uk/ACTS/acts1993/Ukpga_19930036_en_1.htm and http://www.unodc.org/unodc/legal_library/gb/legal_library_1994-11-22_1994-58.html. For commentary, see Hirst, M., *Jurisdiction and the Ambit of the Criminal Law*, Oxford, 2003, p.163 *et seq*.

[60] 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

101*ter*.. 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 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.

101 *quartes.* 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.

102 *quinques*. 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) and Article 21 of the Convention against Transnational Organized Crime (2000).[61] Where two or more States have jurisdiction and want to prosecute, the following criteria could be considered.

---

[61] A/RES/45/118 of 14 December 1990, Annex, and A/RES/55/25 of 15 November 2000, Annex I, Article 21. See also Seguin, J. "The Case for Transferring Territorial Jurisdiction in the European Union" (2001) *Criminal Law Forum*. Vol.12, pp.247-65 at 249

(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.

(e) 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.

(f) 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.

(g) 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.

(h) 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

102. While concepts of territorial jurisdiction have expanded to keep pace with the evolution of fraud and other common transnational crimes, the application of extraterritorial jurisdiction in fraud cases is less common. Some States do apply extraterritorial jurisdiction in cases where crimes are committed abroad by their nationals or persons with domicile or other connections, especially if they have

constitutional bars to the extradition of their own nationals.[62] 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. Cooperation in prevention

103. 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. Transnational fraud consists of activities which are undertaken within individual States, and which can usually be prevented by measures taken at the domestic level if appropriate officials have the necessary information in time to act on it. International cooperation to prevent fraud includes general and specific elements. At a general level, assistance in developing and refining preventive techniques, sharing lessons learned and best practices and in sharing the information needed to develop such techniques and to make them work are all important. At the specific level information may be shared regarding specific cases, methods or fraud operations, and this need not necessarily include the types of personal or investigative information that would require a formal mutual legal assistance process.

VII. Cooperation between the public and private sectors

104. Economic fraud is a crime of commerce. This means that there is both a need and motivation for collaboration between commercial and criminal justice interests. In its Annual Report for 2003, UNCITRAL noted the need for such collaboration, calling for action by the Commission on Crime Prevention and Criminal Justice as well as continuing its own work, a call which led, in part, to the present study.[63] Criminal justice and commercial practices and objectives do not always coincide however. Some forms of commercial fraud may not be recognized as offences in criminal law, and where criminal justice interests tend to favour investigation,

---

[62] 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.

[63] Report of the UNCITRAL at its thirty-sixth session, A/58/17, paragraphs 238-41 see also E/RES/2006/24, paragraph 6 and E/2004/30, paragraph 82..

prosecution and punishments, commercial interests tend to favour dispute-settlement mechanisms and the recovery of losses. What is shared is an immediate interest in acting quickly against ongoing frauds, and an overarching strategic interest in prevention and suppression of both fraud and the organized criminal groups which appear to be responsible for a large portion of cases.

104 *bis*. Public and private interests diverge, in other areas, however. Where private interests are governed by commerce, the marketplace and fiduciary obligations to shareholders, public interests are more broadly accountable, and non-commercial considerations such as human rights, environmental concerns and the public interest as a whole are more dominant. The rule of law and maintenance of effective judicial and criminal justice institutions requires that key functions, particularly prosecutorial and judicial functions, remain independent of extrinsic influences. While effective cooperation is important, it is essential that adequate safeguards ensure that commercial interests do not compromise judicial or prosecutorial independence. In a broad strategic sense, this is also an interest shared between the public and private sectors: effective criminal justice systems and rule of law values and institutions are essential to the governance and regulation of commerce and the establishment and maintenance of the stable social and economic environments which are needed for commercial enterprises to prosper.

105. 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 indicated 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,[64] 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.

106. 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

---

64 *Public Company Accounting Reform And Corporate Responsibility Act*, Pub. L. 107-204, July 30, 2002, 116 Stat. 745, 15 U.S.C., Chapter 19, paragraph 7201 *et seq* (*Sarbanes-Oxley Act*).

course of business, and many companies could also face civil liability, should they disclose confidential information without being 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. The area of collaboration most commonly raised was the sharing of information by commercial entities. Such entities are often the first to become aware of a developing fraud case, either because their customers report it or unusual patterns of activity or commercial practice are observed, and the need to alert law enforcement quickly to allow both effective investigative measures and steps to halt ongoing frauds was seen as important. The other major area of potential collaboration is prevention. Prevention will be discussed in more detail in the following segment, but in the case of fraud can be broadly divided into measures which are addressed at potential victims to make them harder to deceive, and measures which are directed at the commercial structures which are targeted and exploited or victimised, to make them more difficult for offenders to attack or exploit.

VIII The prevention of economic fraud

107. 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. 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 also cited the utility of anti-money laundering and anti-corruption methods in preventing or mitigating fraud. 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.

108. A number of States also suggested that technical security measures were important preventive elements. The creation and use of modern cryptographic systems, for example, is widely credited with making modern payment-card technologies feasible, and the international commercial community has led the way in the use of digital signatures and other adaptations to reduce fraud in larger commercial transactions.[65] Technical measures were seen as necessary at almost every element of a commercial system, including elements in the hands of individual users, communications between system elements, and system elements

[65] *UNCITRAL Model Law on Electronic Signatures*, A/RES/56/80, Annex, and *Guide to Enactment*, United Nations, 2002, Sales No. E.02.V.8.

which process or store data. It was also noted that the global nature of commerce and identification made the global application of most technical measures necessary. Without this, security measures applied in one country would either be ineffective in others or could prevent the legitimate use of a card or other technology altogether. Another challenge faced by those developing new security technologies is the constant evolution of technologies, commercial applications and offender techniques. This makes it essential that both public and private entities maintain constant vigilance and the necessary commitment and resources to develop and disseminate new preventive measures as soon as existing ones become obsolete.

109. For commercial interests, issues of cost and competitiveness also arise when technical prevention measures are developed and implemented. There is sometimes controversy over whether crime-control elements, especially those which support investigation and prosecution, should be paid for by governments or by the companies and users of the technologies. Commercial interests also tend to weigh their options in cost-benefit terms and have concerns that incorporating some security elements may make them less competitive in a global market where competitors based in other jurisdictions do not face the same requirements. While the development and use of technical prevention measures may best be left to the marketplace, there are some roles which may involve governments. Many States indicated that they set minimum standards to protect consumers from fraud and related practices such as deceptive or misleading advertising, and some also set minimum standards to ensure the protection of customer information. States can also play a useful role, both individually and collectively, in ensuring that the marketplace encourages effective prevention and security and that the competitive positions or interests of companies which implement effective anti-fraud measures are not prejudiced by it.

Annex II: Results of the study on identity-related crime

I. Introduction: the nature of identity-related crime and use of terminology in the present Study

1. The nature of identity-related crime

110. The ability to identify both natural and legal persons as unique individuals is a critical element of virtually every aspect of human social, political, and economic activity. Identity must be created and linked to the specific entity being 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 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.

111. The present state of legislation and policy-making in most States is limited to dealing with identity problems primarily in terms of the other crimes which can be committed using identity abuses, but some States have recently 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 and various forms of tampering with identity systems should be treated as a new and distinct form of criminal offence. This is consistent with other recent developments, including the *Convention against Transnational Organized Crime* and the *Council of Europe Convention on Cybercrime*.[66] Identity-based criminal offences recognize that a primary abuse of identity can lead to a range of secondary crimes and allow the criminal justice system to intervene at an earlier stage. This approach 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

[66] See, for example Article 5 of the *Convention against Transnational Organized Crime* (participation in an organized criminal group) and Article 8 of the *Convention on Cybercrime*, which requires criminalization of computer-related conduct if there was intent to commit a fraud whether the fraud was completed or not.

112. The convening resolution for the present study uses the general description "…criminal misuse and falsification of identity and related crimes…" and early deliberations of the experts and the survey questionnaire used to gather information did not consider specific meanings or seek to distinguish between identity fraud and identity theft. Only one State provided a legislative definition, and most just indicated that the description proposed by the questionnaire[67] 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 is apparent that some misconduct reported was analogous to theft, other misconduct was more closely analogous to fraud, and some had elements of both or neither, and might best be considered as "related crime".

113. The general term *identity crime* is used to cover all forms of illicit conduct involving identity, including identity-theft and identity fraud. This is, of necessity, forward-looking, as most States have not established crimes. Generally, identity crimes would include preparatory or constituent offences such as forgery or impersonation. One definitional problem raised is that identity abuses may be directed at either identity information itself or the other information to which it is linked. The latter might not be considered "identity crime", although the effects of the crime would usually be the same. For purposes of the present study, the broader term *identity-related crime* has been used to include such scenarios. In some contexts the term *identity abuse* is also used. It has a similar meaning without any implicit assumption about whether certain conduct is already a criminal offence or should be criminalised. The concept of a *false identity* or *falsification* of identity or identity documents may include three 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.[68]

114. *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 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. *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.

---

[67] E/CN.15/2005/CRP.5, question 33.

[68] See *Interpretive Notes for the Official records (Travaux Préparatoires)* 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).

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

1. Public and private identification systems

115. 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 centralised national identification schemes, but, most appear to rely primarily on identification established for specific applications, such as drivers' licenses, passports, birth certificates, citizenship certificates and identification used for public taxation or benefit schemes. Within the private sector, identification tends to be issued for specific commercial purposes, such as banking or credit, although there may be a trend to more generalised forms established by companies who specialise in this. Some countries combine both approaches, and States with federal systems may have identity schemes run by states or provinces, raising the need for common standards for verification nationally and internationally. Where there is no national identification system, specific forms of identification tended to be used for purposes beyond what was originally intended, both out of necessity, and where redundancy was used for additional reliability. Several States mentioned corporate registries or similar systems to establish the identities of legal persons. The most common form of private commercial identification was the credit card. Views on national identification schemes appear to vary. In some countries national identification requirements are widely accepted, but in others proposals have been controversial and opposed on civil liberties grounds. One State noted that its national identification system was increasingly being used in support of commercial applications, and questions whether commercial interests might be asked to share the high costs of maintaining a centralised system.

2. The concept of "identification information"

116. The concept of "identification information" was novel to most States. Few recognized it in legal or legislative terms, although those examining identity-related crime had begun to consider it. Most States referred instead to identification documents or personal information. Personal information 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. Many States reported the establishment of offences and other measures to protect personal information which would include 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 element of the concept of identification information is that, while elements may be necessary to establish identity, they are usually not sufficient when used in isolation. 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 it identifies. Approaches to what constitutes identity information may depend to some degree on cultural elements or local traditions. Some cultures incorporate names of fathers or mothers, places of family origin or profession or

occupation into individual names. Another factor was degree to which traditional face-to-face recognition has been gradually replaced, first by paper documents, and more recently by electronic identification, as new forms of identification information are created.

117. 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 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 easy to use and common. Other biometric identifiers generate a high degree of security, but are expensive and raise privacy concerns, making them common only in areas where the costs are justified by the need for security or other factors, such as criminal records. 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, and the other reported a definition of the term "means of identification" used as an element of an offence relating 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

1. Types of crime encountered and legal responses

118. 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. Most States have some offences that include identity-related crimes within more general offences, but only six States reported that they had criminalised, in whole or part, the transfer, possession or use of another person's identification or identity information or of a false identity in connection with another crime, and only one of these, the United States of America, had criminalized identity theft *per se*. That offence 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 indicated that it had criminalised at least some of the specific forms of conduct covered by the proposed description of identity fraud 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 or unauthorised access to or tampering with computer systems. Some States also described offences which

were specific to types of identification or identity regarded as particularly critical, such as passports or government identification States which are Parties to the *Council of Europe Convention on Cybercrime*[69] are required to ensure that their forgery offences cover computer or data-related forgery. 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.

119. Another means of subverting identity systems is to attempt to deceive or corrupt the issuance process to issue valid identification to a person not entitled to have it, and several States reported offences of this nature, including general offences of bribery and corruption and more specific ones relating to the use of false or misleading information for the purposes of obtaining licenses or other identity documents. Some means of illicitly obtaining identity information were covered by existing theft offences, but these may not always apply. Intangible information may not be seen as property, and theft may not apply 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 has value. A few States also reported other offences, including illicit possession, transfer of or trafficking in identification, or information, such as computer passwords or 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 both assuming the identity of another person, and fabricating and assuming the identity of a non-existent person.

2. Means used to commit identity-related crime

120. To some degree, means used for identity-related crime depended on the nature and purpose of identification structures involved and means available to offenders. For most such 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 included the theft or copying of complete documents and various means of obtaining partial information used to build identities and obtain genuine documents. Some States noted that they had seen 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 to gradually build a comprehensive identity. A substantial number of States reported concerns about identity-related crime which targets victims based on their use of information technologies. 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. Victims are targeted by e-mail messages or web sites claiming to represent service providers or other authorities and asked for the information. Sites are often hosted in countries distant from both offenders and victims, one State noting that it had traced such sites to at least 10 different countries. Other forms of cybercrime have also been encountered, including malicious software infecting

[69] E.T.S No. 185, Budapest, 23 November 2001, Article 7 (computer forgery).

individual victim computers to capture personal information and transmit it to offenders and the invasion of commercial web sites by "hacking" to obtain credit card data and other customer identification information. Identification information, especially in large quantities, has become a form of illicit commodity, sold to other offenders. Commercial entities concerned about customer confidence have been the victims of extortion offences, in which offenders take the information and threaten to publicise it if not paid.

121. 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, whereas in the case of physical identity documents, further steps were often needed. Physical identification documents have become more sophisticated, requiring greater expertise, resources and equipment to forge, suggesting the involvement or support of organized criminal groups when this is encountered, although information and communications technologies have also brought some means of forgery within the reach of large numbers of individual offenders, triggering an evolution of both document safeguards and offender techniques. 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.

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

1. Other crimes associated with identity-related crime

122. Links between identity-related crime and other crimes 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 to avoid detection, interference and criminal justice consequences. Third, in the case of economic fraud, it was also used as part of the central deception element of the fraud scheme. 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. The *Protocol to Prevent, Suppress and Punish Trafficking in Persons* does not require criminalisation of deprivation of identification as an element of trafficking, some States Parties have done so.[70] The *United Nations Convention on the Rights of the Child* also establishes the right to be

[70] See for example *Criminal Code of Canada*, section 279.03 (offence of destroying or withholding travel or identity documents) as enacted by S.C. 2005, chapt.43, http://www.parl.gc.ca/38/1/parlbus/chambus/house/bills/government/C-49/C-49_4/C-49-3E.html (English and French).

registered at birth as a means of establishing identity,[71] and the systematic deprivation of identity has been encountered as an element of cases of genocide or ethnic cleansing.[72]

123. The most common link appears 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. A number of States also referred to the role of identity crime in money-laundering, used to avoid mechanisms which identify funds or assets as proceeds of crime *ab initio*, and mechanisms which identify transactions which are suspicious, as well as to avoid criminal liability for money-laundering itself and related offences. Many States also expressed particular concern about identity crime involving passports and other travel or related identity documents. This was seen as both a crime and a security issue, as passport systems are essential to the exclusion of known terrorists, criminal offenders and illicit migrants. Passport abuses were also linked to organized crime, in particular through trafficking in persons and the smuggling of migrants and a number of the countries which drew attention to those links were those which have seen high levels of smuggling or trafficking for geographical reasons. Several States also reported the establishment of new passport documents incorporating additional security measures. A number of links to forms of cybercrime have also 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

124. 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 elsewhere in the present report. Aside from identity-related crimes linked to other 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. Organised criminal groups may use identity-related crime to protect their own members and operations both from surveillance of illicit activities and for routine, non-criminal activities such as international travel. There is also some evidence of the specialisation of groups and treatment of identity documents or information as a form of illicit commodity. Groups may develop the expertise needed to fabricate increasingly-sophisticated identity documents or to exploit weaknesses in issuance schemes to deceive or corrupt authorities in order to obtain genuine documents, which can then be sold to others for use in crime, terrorism, illicit travel or migration, or other purposes where legitimate identification would be prejudicial. Organized criminal groups are sometimes

---

[71] A/RES/44/25, Annex, Article 7, paragraph 1.

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

sophisticated enough to use 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.

3. Relationship between identity-related crime and terrorism

125. Only a few States raised the question of 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. Most of the concern was focused on travel-related identification the international movement of terrorist suspects,[73] but the same issues arise with respect to purely domestic identification and activities, both because terrorists need to avoid attracting attention in everyday activities such as driving or banking and because common forms of domestic identification form the basis of obtaining more secure identification such as passports and forms of employment and related identification needed to access secure locations such as airports.

126. Other official sources consulted by experts set out examples of terrorist suspects obtaining and using identity documents to avoid surveillance or scrutiny. 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 its use and then falsely claim them as lost or stolen, and suspects whose passports record suspicious travel patterns may dispose of them and falsely obtain replacements.[74] 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.

127. Absent clear evidence, identity-related crime associated with terrorism may be difficult to distinguish from other related crimes, and especially organized crime. Many of basic scenarios would be the same for organized criminal groups and terrorist groups, and there is the possibility that terrorist groups which lack their own expertise may simply purchase false identification documents from organised crime. Identity-related crimes may also be linked to the financing of terrorism in much the same ways as to money laundering.

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

---

[73] See, e.g., Report of the Secretary General, "Uniting against terrorism: recommendations for a global counter-terrorism strategy" A/60/825, 2006, paragraph 62.

[74] Sources include the official report of the Government of the United States on the attacks of September 2001. See *Report of the National Commission on Terrorist Attacks upon the United States*, chapter 5.3 at pp.168-69, http://www.9-11commission.gov/report/index.htm.

128. Many anti-money laundering measures depend heavily on identity or identification elements, and the means used by offenders to launder proceeds involve identity-related crime. 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.[75] 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 predicate offences.[76] Some States noted that methods used for money-laundering were linked to the use of information, communications and commercial technologies. These provided the means of generating false identification information, made possible remote transfers using such identification, and supported large volumes of legitimate transfers in which to conceal money-laundering. They also supported a dramatic expansion of international transfers and offshore banking, which complicate the regulatory environment and bring 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.

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

129. As with economic fraud, the role of information and communications technologies in identity-related crime is complex. In some case examples, technologies were central to the identity-related crime, and others they formed only one element of a larger offence. On one hand, the greater reliance on technologies as opposed to personal contact in identification 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. Precautions include physical elements to make documents harder to produce, such as the incorporation of

---

[75] 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.html#40recs

[76] See Schott, P.A., *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism*, World Bank, 2003, chapter VI, part A.

photographs, micro-printing, holograms, and computer chips, which still require relatively sophisticated equipment and knowledge to produce. Modern, secure telecommunications also make it possible to quickly verify identity documents 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 or personal identification (PIN) numbers; and elements that were biologically unique to the subject, or "biometric" elements.

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

130. A number of States reported that they have encountered cases of identity-related crimes with transnational aspects. The majority involved offences related to passports and other travel-related identification. These included offences related to identification documents specifically, such as forgery, alteration, misuse of genuine documents, abuses of issuance processes, and other offences committed in part though the misuse of these forms of identification, such as trafficking in persons, the smuggling of migrants and other offences related to illegal entry or illegal migration. 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.

131. 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. A with economic fraud, most States saw existing frameworks such as the *United Nations Convention against Transnational Organized Crime* and the *Council of Europe Convention on Cybercrime* as sufficient, and several also highlighted the practical utility of INTERPOL, EUROPOL and similar organizations as mechanisms for actually providing cooperation. Most saw the specific forms of cooperation needed as similar to those for transnational fraud or other forms of cybercrime. Most major offences 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*, 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, as with cybercrime, the speed with which both formal assistance and informal cooperation could be provided was sometimes critical. 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 measures to

repair identities would not fall within the ambit of most countries' criminal cooperation frameworks.

V. Rates and trends in identity-related crime

132. Most of the States which provided data or assessments 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. 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. 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 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. Some of the States which indicated that identity-related crime was increasing cited several reasons that might contribute to such increases, including official and commercial corruption, 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. The lack of clear national definitions of identity-fraud or similar crimes precludes statistical analysis and all but the most general comparisons between countries or regions.

VI. Costs of identity related crime

133. 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.

134. One State noted that a qualitative assessment can be made, however. It suggested that harm or damage would include: economic and non-economic losses are likely to be suffered by persons whose identities are taken or misused; costs and time and effort expended repair 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 are also policy questions as to how some of these costs should be allocated, both as between public and commercial entities, and as among the various victims or interests harmed by identity-related crime.

VII. Prevention of identity-related crime

135. Some States mentioned controls or 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 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. Information provided by States suggests a number of specific methods which 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 or diversion or corrupt issuance.[77] Document validation and verification practices can be strengthened, especially through the use of telecommunications and data bases 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 can be used to link identity to unique physical characteristics. Generally, security audits to assess overall system security should be conducted, and should examine all elements of the system, including: document issuance and revocation; the updating of documents and information; information security practices; the validity and renewal cycle for documents; and the global interoperability of systems and security measures.

D. The relationship between economic fraud and identity-related crime

136. The present Study distinguishes between economic fraud and identity-related crimes, but the evidence suggests that in practice, there are significant areas of overlap. 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,

---

[77] See Protocols to the *United Nations Convention against Transnational Organized Crime* , A/RES/55/25, Annexes II and III, Article 12, subparagraphs (a) and (b).

and is one of the reasons that the Commission decided to conduct the present Study on a joint basis. As noted, identity abuses perform much the same role in economic fraud as for other crimes, combined with the added role that identity abuses play in deceiving victims in many fraud schemes. Many examples were provided. 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.

137. 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".[78] 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. 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.[79] 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

[78] A/55/25, Annex I, Article 2, subparagraph (a) and Article 3, paragraph 1.

[79] A/55/383/Add.1, paragraph 3. See also A/AC.254/4/Rev.1, footnote 4, A/AC.254/4/Rev.2, footnote 16, and A/RES/254/4/Rev.7, footnote 22, summarising deliberations at the first, second and seventh session of the Ad Hoc Committee established by A/RES/55/25.

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.[80]

[80] 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.