United Nations E/CN.15/2007/8*

Economic and Social Council

Distr.: General
2 April 2007

Original: English

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

Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity

Report of the Secretary-General

Contents

* Reissued for technical reasons.
** E/CN.15/2007/1.

V.07-82033 (E) 040407 050407

I. Introduction

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, subject to the availability of extrabudgetary resources, an intergovernmental expert group, with representation based on the regional composition of the Commission on Crime Prevention and Criminal Justice and open to any Member State wishing to participate as an observer, to prepare a study on fraud and the criminal misuse and falsification of identity; and 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.

2. 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 Intergovernmental Expert Group considered the scope of the study, adopted a methodology and decided to include in the study information from Member States, the private sector and the experts themselves. It requested the secretariat to prepare and disseminate a questionnaire, in two parts, to obtain information on economic fraud and the criminal misuse and falsification of identity. A progress report was submitted to the Commission on Crime Prevention and Criminal Justice at its fourteenth session (E/CN.15/2005/11), in accordance with Economic and Social Council resolution 2004/26.

3. A first draft of the questionnaire was made available to the Commission on Crime Prevention and Criminal Justice at its fourteenth session as a conference room paper (E/CN.15/2005/CRP.5), 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. In December 2005 the finalized questionnaire was disseminated to Member States with a view to obtaining the necessary information for the study. There was not a sufficient number of responses to conclude the work in time for the fifteenth session of the Commission (E/CN.15/2006/11 and Corr.1), but by the time the study had been completed, on 31 December 2006, 46 States had provided responses.[1] The questionnaire was also sent to the experts who had attended the meeting of the Intergovernmental Expert Group for their consideration, with a view to their submitting to the Group data, observations or conclusions on specific subject areas covered in the study.

---

[1] Responses were received by 31 December 2006 from the following States: Algeria, Belarus, Canada, Costa Rica, Croatia, Egypt, Finland, Germany, Greece, Hungary, Italy, Japan, Jordan, Latvia, Lebanon, Madagascar, Malta, Mauritius, Mexico, Monaco, Morocco, Netherlands, Nicaragua, Norway, Oman, Panama, Peru, Republic of Korea, Romania, Russian Federation, Saudi Arabia, Slovakia, Slovenia, South Africa, Spain, Sudan, Sweden, Switzerland, Syrian Arab Republic, the former Yugoslav Republic of Macedonia, Trinidad and Tobago, Turkey, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America and Zambia. Many of those States also provided copies of relevant legislation.

4. At the request of the first meeting of the Intergovernmental Expert Group, a joint letter from the secretariat of UNCITRAL and the United Nations Office on Drugs and Crime (UNODC), to which the questionnaire on fraud and identity fraud was attached, was sent to a selection of appropriate private-sector companies 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 participated regularly in the work of UNCITRAL, requesting that the questionnaire be circulated among their members for response, where appropriate.

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

II. Second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity

6. With the support of the Governments of Canada and the United Kingdom of Great Britain and Northern Ireland, 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 to 19 January 2007. The Intergovernmental Expert Group held seven meetings and completed the study, including its report and recommendations, as well as annexes summarizing the evidence and its analysis of economic fraud and identity-related crime, in accordance with paragraphs 4 and 11 of Economic and Social Council resolution 2004/26. The Intergovernmental Expert Group also held some preliminary discussions pursuant to paragraph 5 of that resolution, in which it was requested to use the information gained by the study for the purpose of developing useful practices, guidelines or other materials; however, it did not finish that work.

7. In preparation for the second meeting, a first draft of the present report was circulated in September 2006 to the experts. Comments and remarks received from experts representing Canada, Germany, the United Kingdom and the United States of America, as well as additional responses received from Member States and materials and comments from UNODC and the UNCITRAL secretariat were taken into consideration for the preparation of a second draft of the report, which was completed and disseminated to the experts in December 2006. The second draft was the working paper considered during the second meeting of the Intergovernmental Expert Group.

8. A longer version had also been prepared in advance and circulated as background material to the experts. The longer version was not revised after the first time it was circulated, pending a decision on a potential publication. It would have

to be updated to reflect comments received since October 2006 and the deliberations of the Intergovernmental Expert Group and may probably be recirculated or brought to the attention of an expanded panel of experts for final review.

9. The second meeting of the Intergovernmental Expert Group was opened by the Chairman, Eugenio María Curia (Argentina).

10. The second meeting of the Intergovernmental Expert Group was attended by experts from 18 Member States. Also attending the meeting were observers for the secretariat of UNCITRAL and the Organization for Security and Cooperation in Europe (OSCE).

11. At its 7th meeting, on 19 January 2007, the Intergovernmental Expert Group adopted its report.

III. Use of terminology in the study

12. While the subject of economic and financial crime has been discussed in several forums, including the Eleventh United Nations Congress on Crime Prevention and Criminal Justice,[2] there is no clear and comprehensive definition of the terms "economic crime" and "financial crime",[3] and a forensic definition was not seen as essential to the study of the Intergovernmental Expert Group. For clarity, however, the term "financial crime" was taken by the Intergovernmental Expert Group to include crimes committed using major financial systems or against those systems themselves. That could include money-laundering, some forms of corruption affecting financial structures, and most major economic crimes in which financial structures were used or victimized. 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. That would include 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.

13. The term "fraud" has two meanings. In almost all countries, legislation limits "fraud" to cases where there was economic loss to victims, but the terms "fraud" and "fraudulent" are also commonly used as terms of art by officials, academics and others to describe conduct involving the use of dishonesty or deception, but not necessarily any financial or other material loss or benefit. For example, the means of recruitment of victims of trafficking may include non-economic fraud, and fraud on the part of a negotiating State may invalidate a treaty.[4] For clarity and without prejudice to any future work, it was decided to use the terms "fraud" and "economic

---

[2] *Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005: report prepared by the Secretariat* (United Nations publication, Sales No. E.05.IV.7), paras. 173-189.

[3] Ibid., para. 181.

[4] Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, annex II), art. 3, subpara. (a); and Vienna Convention on the Law of Treaties (United Nations, *Treaty Series*, vol. 1155, No. 18232), art. 49.

fraud" as appropriate when referring to fraud in the established economic sense and to use the term "identity fraud" for other cases within the scope of the study.

14. Initially, the experts decided to use the term "identity fraud" when discussing the criminal misuse and falsification of identity; however, in reviewing the evidence, it became apparent that the terms "identity theft" and "identity fraud" were not used consistently and that they did not fully encompass the scope of the identity-related problems covered by the 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 those 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.

15. 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 crimes of commerce. Most experts, however, consider commercial crime or commercial frauds to be more limited in scope, including only fraudulent conduct that involves, affects or targets major commercial systems and that is a significant departure from legitimate commercial practice. The study uses the term in the narrower sense, as does UNCITRAL in its work on commercial fraud.[5]

IV. Conclusions and recommendations

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

16. The study established that there were not only significant links between economic fraud and identity-related crime, but also substantive and procedural differences between the two that will have an influence on future work in both areas. A substantial amount of identity-related crime is associated with economic fraud, as a means of avoiding fraud prevention measures and avoiding criminal liability and, in many cases, as a means of deception central to the fraud offence itself. However, not all forms of fraud involve identity-related crime, and many identity offences are committed for undetermined reasons or for reasons with no direct link to any financial or other material benefit. From a procedural standpoint, the responses also showed that although most States have well-developed legislative and other measures directed at economic fraud, most had no measures whatsoever

[5] See the report of the United Nations Commission on International Trade Law on the work of its thirty-sixth session (*Official Records of the General Assembly, Fifty-eighth Session, Supplement No. 17* (A/58/17), para. 237); and the note by the Secretariat entitled "Possible future work relating to commercial fraud" (A/CN.9/540, paras. 12-26).

against identity-related crime per se, although many had criminalized related conduct such as document forgery or impersonation. The complexity of the relationship and the substantive and procedural differences suggest that the most efficient and effective way to proceed would be to follow separate processes of developing materials to assist Member States pursuant to paragraph 5 of Economic and Social Council resolution 2004/26. At the same time, the connections between the two suggest the need for close coordination to exploit synergies and avoid duplication of work in both areas. A separate but coordinated approach to such work is therefore recommended.

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

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

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

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

(i) In the case of economic fraud, most States have clear legislative definitions and offences, but those are not detailed enough to support research and analysis of many of the specific types, trends and patterns that raise concerns, including mass fraud and factors such as the involvement of

transnationality, organized criminal groups and information and communication technology. The development of global research-oriented definitions and typologies and support for States in using those to carry out research and analysis at the national level could be considered;

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

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

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

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

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

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

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

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

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

C. International cooperation

18. A number of States reported substantial increases in transnational fraud, which appear to be associated with the increased opportunities provided by the expansion of global trade and commerce and the increasing availability of information, communication and commercial technologies. Not enough information was available to support similar conclusions about identity-related crime, but States had concerns about transnational activities, in particular problems with passports and other travel documents and transnational credit card fraud. Accordingly, a number of States referred to the need for international cooperation. Those States which addressed the issue also felt that the existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, annex I), the Council of Europe Convention on Cybercrime,[6] 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. Experts also noted the usefulness of the United Nations Convention against Corruption (General Assembly resolution 58/4, annex) in this regard.

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

20. For the above-mentioned reasons, the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and, where applicable, the Council of Europe Convention on Cybercrime, as well as the 13 universal legal instruments against terrorism, appear to provide a more than adequate framework and legal basis for the types of mutual legal assistance, extradition and other forms of international cooperation that are needed to deal with transnational cases of economic fraud and identity-related crime. As a result, the

---

[6] Council of Europe, *European Treaty Series*, No. 185; see, in particular articles 7 (computer-related forgery) and article 8 (computer-related fraud). Experts noted that the Convention on Cybercrime was the only international instrument specifically addressing cybercrime. It contains three parts: substantive criminalization; procedural mechanisms for the investigation of computer crimes and cases that involve electronic evidence; and international assistance for obtaining evidence or the extradition of offenders. The Convention covers only criminal (not civil) matters. States not members of the Council of Europe may become parties to the Convention by acceding to it.

Intergovernmental Expert Group saw no need for any further international legal instruments in that area. It did, however, recommend that careful consideration be given to the most effective possible application of the conventions in fraud cases, including by the following:

(a) Member States that have not yet done so should ratify or accede to and fully implement the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption;

(b) Member States should consider acceding to the Convention on Cybercrime, which is open to States that are not members of the Council of Europe;

(c) Most States reported types of punishment that would make their more serious offences "serious crimes", as defined in article 2, subparagraph (b), of the United Nations Convention against Transnational Organized Crime. However, many had offences that would not be covered by the Organized Crime Convention, and a few did not report any fraud offences that would be covered. Member States should ensure that all appropriate fraud and related offences fall within the scope of "serious crimes" as defined in the Organized Crime Convention;

(d) Few States have criminalized identity-related crime per se, but most had criminalized related offences such as document forgery and impersonation, and the more serious of those offences would also be covered by the United Nations Convention against Transnational Organized Crime where the requirements of articles 2 and 3 of that Convention were met. Document forgery and fraud involving electronic networks may also be covered by the Convention on Cybercrime. It is recommended that States review existing criminal offences with a view to ensuring that both conventions can be applied in appropriate cases;

(e) It is also recommended that the scope of application and appropriate definitions contained in articles 2 and 3 of the United Nations Convention against Transnational Organized Crime be taken into consideration by Member States engaged in the development of new offences relating to identity-related crime;

(f) National law enforcement and other agencies responsible for organized crime should be encouraged to consider major cases of economic fraud and identity-related crime as a form of organized crime and be trained in the effective use of the Organized Crime Convention and its implementing legislation in appropriate cases;

(g) States should ensure that law enforcement and other relevant agencies are trained in the investigation of cybercrime, including where appropriate and applicable, the use of the Convention on Cybercrime and its domestic implementing legislation;

(h) States should ensure that law enforcement and other relevant agencies cooperate more effectively in fighting economic fraud and identity-related crime, in particular through mutual legal assistance and the extradition of offenders, taking into account the transnational nature of those crimes.

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

1. Legislative measures against fraud and identity-related crime

21. Most States reported legislative measures against a variety of criminal fraud offences, ranging from small deprivations to complex schemes involving major economic disruption and collateral forms of harm. Those measures appeared to criminalize fraud adequately for the purposes of suppressing domestic fraud and supporting international cooperation. Most States also indicated that fraud was considered a predicate offence for purposes of regimes against money-laundering. While the vast majority of criminalization issues appear to have been addressed, the evidence suggests that some specific modifications could be considered to improve and modernize legislation. Fraud offences and investigative powers may not have kept pace with new variations of fraud committed using modern technologies, and not all States indicated that fraud was a predicate offence for measures against money-laundering. Criminal offences covering only individual transactions could also be augmented to reflect the expansion of transnational and mass fraud by specifically criminalizing fraud schemes and mass fraud. In transnational cases, this simplifies jurisdiction, as territorial jurisdiction would apply to the entire scheme and not just to specific transactions, evidence of the entire scheme and its effects could be used and it may not be necessary to prove the completion of fraud against individual victims. It is therefore recommended that States consider the following enhancements, where appropriate:

(a) States that have not done so should consider the modernization of fraud offences and investigative powers to deal effectively with domestic and transnational fraud committed using telephone, electronic mail (e-mail), the Internet and other types of telecommunication technology;

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

(c) States that criminalize fraud only on the basis of individual fraudulent transactions should consider criminalizing conduct such as the operation of fraud schemes and the perpetration of mass fraud;

(d) States should assist one another in developing legislation and training legislative drafters in matters related to economic fraud and identity-related crime.

22. In the case of identity-related crime, basing offences on abuses of identity represents a fresh approach for most States, and extensive work is needed. Lawmakers need to develop appropriate concepts, definitions and approaches to the criminalization of a range of conduct, including identity theft, identity fraud and other identity-related crimes. It is also critical for most States to ensure consistency with their respective private and public identity systems and with established crimes such as forgery and impersonation. Given the concerns expressed about the links between domestic means of identification, international and travel-related identification and transnational forms of identity-related crime, criminal offences that provide a good basis for international cooperation are desirable. It is therefore recommended that States consider the establishment of new identity-based criminal

offences. It is also recommended that, in developing new offences, common approaches to criminalization be taken, to the greatest extent possible, to facilitate future transborder evidence-sharing, extradition of offenders and other forms of international cooperation.

2. Jurisdiction

23. *Territorial jurisdiction*. Modern transnational fraud tends to take place in many places at the same time and therefore may not be well addressed by traditional territorial jurisdiction unless laws have been updated to take into account recent developments. Narrow approaches can lead to cases where no State with the ability to prosecute effectively also has sufficient jurisdiction to do so, while overly broad approaches can result in conflicts of jurisdiction, *ne bis in idem* and other problems. It is therefore recommended that:

(a) States whose laws follow relatively narrow approaches should review those approaches in the context of the range of fraud offences and options for territorial jurisdiction covered in the present report, and all States should ensure that their jurisdictional rules keep pace with the ongoing evolution of fraud offences;

(b) When several States have jurisdiction, they should consult and collaborate with each other to ensure that cases are prosecuted, where possible, by the State that is in the best position to do so, taking into account factors such as the availability of witnesses and evidence, the rights of accused persons, the capacity of the State to mount a fair and successful prosecution and the ability of other interested States to provide cooperation in support of the prosecution;

(c) States should consider technical assistance, both as a form of international cooperation in support of specific prosecutions, and more generally through UNODC and other appropriate bodies, to help ensure that States that have jurisdiction but lack capacity are able to effectively investigate and prosecute complex cases involving transnational fraud;

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

24. *Concurrent jurisdiction and cooperation*. Broad approaches to territorial jurisdiction will often result in several States having concurrent jurisdiction in major transnational fraud cases. In such cases it is recommended that the relevant States cooperate, under the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption, the Council of Europe Convention on Cybercrime and other relevant international legal instruments, where applicable, to ensure that the offences are thoroughly and comprehensively investigated in all relevant jurisdictions and that the offenders are prosecuted in the most appropriate jurisdictions, taking into consideration factors such as the locations of accused offenders, victims and evidence and the availability of the resources and expertise needed to prosecute effectively. Because of the nature of transnational fraud, early identification of the States concerned and early investigative coordination and cooperation are particularly important. The States concerned that are not the prosecuting State should assist the prosecuting State in

every possible way. An approach similar to the criminalization, investigation and prosecution of transnational cases of identity-related crime is recommended.

25. *Extraterritorial jurisdiction*. Articles 15 and 16 of the United Nations Convention against Transnational Organized Crime and articles 42 and 43 of the United Nations Convention against Corruption require States parties that cannot extradite their own nationals to ensure that they have sufficient jurisdiction to prosecute offences covered by those conventions where one of their nationals commits such an offence outside of their territorial jurisdiction. In the Organized Crime Convention, States parties are also encouraged to establish sufficient jurisdiction to prosecute cases where an offender found in their jurisdiction is not extradited for other reasons (art. 15, para. 4). In view of the large number of fraud cases that are transnational or multinational in nature, it is recommended that all Member States consider establishing jurisdiction to prosecute fraud in any case where the accused offender is found in their territory and they cannot extradite for any reason to another State that has territorial jurisdiction to prosecute the offence, assuming that the conduct in question is within the scope of domestic offences and is defined as a "serious crime" in article 2, subparagraph (b), of the Organized Crime Convention. In addition, articles 22 and 24 of the Convention on Cybercrime provide for extradition in such cases if the crime is document forgery or fraud involving electronic networks. More general forms of extraterritorial jurisdiction were not raised in the general context of economic fraud, but the Intergovernmental Expert Group noted that some States had extraterritorial jurisdiction in cases where their fundamental interests were affected, such as offences relating to the forgery of passports or counterfeiting of currency.

3. Limitation periods and amnesty powers

26. Limitation periods are an integral part of the criminal justice practices of some States, but they may raise particular concerns in major and transnational fraud cases, where successful investigation and prosecution tend to be complex, costly and time-consuming. Approaches to time limits and amnesties vary widely, but where limits exist, they should take into account the time needed for effective investigations and prosecutions in major fraud cases, bearing in mind the basic concepts of each country's legal and criminal justice system:[7]

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

(b) In view of the length of time needed once investigative, prosecutorial proceedings have commenced in such cases, it is also recommended that limitation

[7] Some actions called for in the recommendations in this segment may also be taken pursuant to the implementation of provisions of article 11, paragraph 5, of the United Nations Convention against Transnational Organized Crime and article 29 of the United Nations Convention against Corruption.

periods be suspended, cease to run or recommenced from the beginning once such proceedings have commenced;

(c) It is further recommended that States apply the same provisions for longer time limits, extensions, suspensions and recommencement of limitation periods to proceedings relating to mutual legal assistance, extradition, domestic prosecutions under concurrent or exclusive territorial jurisdiction and *aut dedere aut judicare* provisions as are applied to purely domestic prosecutions in their domestic laws;

(d) Some States also reported the application of amnesties in cases of economic fraud. While amnesties are a matter for each State, it is recommended that, in cases involving transnational elements, the implications for transnational or foreign investigations and prosecutions be considered before the use of amnesty powers in fraud cases. A similar policy could be considered with respect to the use of amnesty powers in cases that involve identity-related crime in the context of criminal offences or activities with transnational aspects.

4. Law enforcement and investigative capacity

27. Most serious cases of economic fraud and identity-related crime involve a degree of sophistication that challenges even the most developed and well-equipped States and poses an even more serious challenge for developing countries and for international cooperation. The misuse of information, communications and commercial technologies makes the forensic expertise needed to investigate and gather and preserve evidence of cybercrime critical. Substantive knowledge of legitimate financial and economic systems, accounting, and money-laundering techniques and identity systems is also important, and in transnational cases expertise and capacity are needed to support international cooperation. A further factor is the rapid evolution of both legitimate technologies and commercial practices and the resulting evolution of criminal techniques, which require regular updating of training materials and retraining of officials. Some progress has also been made in developing effective countermeasures, including a "24/7" (24 hours a day, 7 days a week) emergency contact network for use in transborder cybercrime cases. Established in 1992, the emergency contact network included more than 45 countries in January 2007. Each country makes available specialists in computer investigations to receive emergency requests for assistance at any time:

(a) It is therefore recommended that States develop and maintain adequate research capacity to keep abreast of new developments in the use of information, communication and commercial technologies in economic fraud and identity-related crime;

(b) It is also recommended that the product of research be shared and disseminated to law enforcement agencies in each country through domestic training and, where feasible and appropriate, with other States through appropriate technical assistance and training and with relevant commercial entities;

(c) It is further recommended that Governments and commercial entities collaborate on matters of research and development, recognizing, within the limits of commercial feasibility, the importance of incorporating crime control into new technologies and the social and commercial importance of ensuring appropriate law enforcement capacity as new technologies and products enter the market;

(d) It is further recommended that States support and make use of the "24/7" emergency contact network in transborder cybercrime matters, both for emergency and non-emergency cases involving electronic fraud or identity-related crime.

28. Several States and some commercial entities noted the usefulness of screening mass telecommunications and financial or commercial transactions to look for patterns suggestive of fraud so that timely investigative and other measures could be applied. That raises several concerns, including the possible infringement of privacy and other human rights and, in the case of commercial systems, concerns about proprietary technologies and customer privacy, which need to be considered and addressed. It is therefore recommended that:

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

(b) Useful substantive criteria and procedural practices for the screening and identification of activities suspected of involving fraud should be developed and shared among States and appropriate commercial entities, and States and the private sector should collaborate and assist one another in ensuring that those criteria and practices are kept up to date and that appropriate officials are trained in their use;

(c) Appropriate safeguards regarding the use of screening activities and the sharing of information generated from such activities, as well as the sharing of information about useful screening techniques and best practices, should be developed and taken into consideration;

(d) While the criteria for identifying transactions suspected of fraud and those suspected of money-laundering will not necessarily be the same, there should be coordination and sharing of information between officials involved in activities aimed at countering fraud and money-laundering, where appropriate.

5. Cooperation between criminal justice systems and the private sector

29. Economic fraud is an inherently commercial crime and can be seen as a distortion or perversion of legitimate commercial dealings: victims are generally deceived when offenders succeed in imitating legitimate commerce of some kind. Identity-related crime either targets identification documents, systems or data or exploits them in the course of committing other types of crime. Both economic fraud and identity-related crime have a substantial impact on private interests, as well as on public interests. Fraud affects both individual commerce and commerce as a whole: large-scale fraud can bankrupt companies and erode confidence in markets. Identity-related crime affects both public identification, such as passports, and private credit cards and similar documents. In countries where private documents are used for public purposes and public identification is used for private purposes, crimes against any form of identification affect both areas. It is therefore essential that criminal justice and commercial entities cooperate effectively, both to develop an accurate and complete picture of the problems and to develop and implement preventive and reactive measures. Cooperation in investigation and

prosecution is also essential, bearing in mind the need for appropriate safeguards to ensure the independence of investigative, prosecution and judicial functions.

30. To prevent fraud and identity-related crime, it is important that security countermeasures be developed and then incorporated into commercial technologies and practices. That, in turn, requires consultation between public entities, such as standard-setting bodies, and private interests, including those companies which produce and sell new technologies and those which will use them. Important issues include ensuring that preventive measures are effective and do not unduly impede normal commercial activities and ensuring that, where costs or competitive factors are affected, the same requirements apply globally, so that a normal competitive environment is maintained. Generally, security measures should make products more competitive, not less competitive.

31. A number of States mentioned the relationships between State and commercial identification systems. Several also noted the importance of cooperation between law enforcement and commercial entities in detecting, investigating and prosecuting crimes such as economic fraud and related abuses of commercial identification. It was noted that commercial entities were often in the best position to monitor commercial traffic and identify suspicious or suggestive patterns and that, in many cases, victims were more likely to report specific crimes to companies than to law enforcement agencies, in the hopes of recovering losses. Commercial entities also noted, however, that proactive cooperation with law enforcement could affect competitive interests or customer privacy, or result in civil liability. It is therefore recommended that representatives of law enforcement and commercial entities consult with a view to developing useful practices for key areas such as the reporting of crimes and investigative cooperation. In this context, the experts noted that such activities had already been taking place for some time in some forums, especially with respect to key issues such as the preservation of data.

32. A key element of prevention is the education and training of persons who are in a position to identify and report economic fraud or identity-related crime: such persons range from commercial customers or communication subscribers to employees who handle business transactions. Such training and education require frequent updating, to reflect the latest developments in criminal methods and techniques, law enforcement measures and commercial practices. It is therefore recommended that criminal justice and commercial entities cooperate, to the greatest extent possible, to support effective education and training, including by sharing appropriate information and ensuring that the information reaches the right persons.

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

33. In countries with economies in transition, whether in the course of reconstruction, development, rebuilding after conflict or natural disasters or major economic reform, confusion between old and new rules or practices creates a risk of economic fraud; the harm caused by such offences could be great: direct economic losses are hard to absorb, and confidence in new economic and legal structures is eroded. Further harm may result from organized crime and other problems fuelled by the proceeds of economic fraud. That is an area where fraud and corruption are closely linked: fraud is often the means of illicitly diverting resources, while bribery

and other forms of corruption are used to ensure that the diversion will be successful or undetected. The role of identity-related crime is less clear, but the basic ability to establish and verify identity is important as it is a stabilizing element and it supports measures against crime. However, most developing countries and countries with economies in transition lack the basic identification and related infrastructure. There is a need to ensure that all participants are aware of the high risk of fraud in such circumstances and the substantial harm such fraud can cause:

(a) It is therefore recommended that basic anti-fraud elements and expertise be included when planning and implementing technical assistance in the development or reconstruction of basic economic and commercial structures and that such elements be considered by appropriate authorities in the course of planning and implementation at the national level, whether international assistance is involved or not;

(b) It was noted that there are substantial areas of overlap between fraud and corruption offences in many legal systems, particularly where fraud schemes target public officials, public institutions or public funds. It is therefore recommended that there be appropriate coordination between anti-fraud and anti-corruption experts and materials and that the need to coordinate work, exploit synergies and reduce unnecessary duplication of efforts be taken into consideration in developing and implementing specific projects;

(c) It is recommended that the existence and efficacy or reliability of identification documents and infrastructure be included as elements when assessing the need for development and reconstruction projects and that projects to establish or strengthen identification be incorporated into development and reconstruction efforts where needed.

7. Recommendations for the prevention and deterrence of economic fraud and identity-related crime

34. Given the links between economic fraud and some forms of identity-related crime, many measures that prevent or deter the one will also have the same effect on the other. That is particularly true for the prevention of identity-related crime, which can also prevent many of the fraud and money-laundering offences committed using false identities. The elements of deception and economic loss generally mean that economic fraud requires advance and often extensive and careful preparation on the part of the perpetrators and some form of vulnerability to deception on the part of the victims, and both of those elements create opportunities for effective crime prevention. Most of the options for preventing identity-related crime are rather technical, focusing on means intended to make it more difficult to tamper with identification documents, to subvert or corrupt identification systems and/or to obtain identification data. As previously noted, close collaboration between relevant entities in the public sector and the private sector in developing and implementing preventive measures are also important for success, bearing in mind the need to exploit synergies while ensuring consistency and avoiding unnecessary duplication. Collaboration with experts engaged in the prevention of related forms of crime, including organized crime, corruption and money-laundering, is also important. It is therefore recommended that Member States develop and implement effective measures for the prevention of fraud and identity-related crime at the national level

and, where appropriate, the international level, as well as in cooperation with the private sector. Such prevention efforts could include the following:

(a) The dissemination of information about fraud and identity-related crime to potential victims: such information could include both general information to raise awareness of the threat and timely information about specific forms of fraud and identity-related crime based on accurate and up-to-date monitoring of criminal activities by appropriate entities in both the public and private sectors. Information campaigns could be directed at the general population and at specific groups considered to be particularly vulnerable or at increased risk of being targeted;

(b) The dissemination of information about fraud and identity-related crime to others who may be in a position to identify, report or prevent such offences when they occur;

(c) The rapid and accurate gathering and analysis of information to support effective and timely prevention measures: this should include the gathering of relevant information among law enforcement, commercial and other entities at the national level and, where appropriate, at the international level;

(d) The rapid sharing of information among appropriate law enforcement and private sector entities at the national and international levels: such sharing must be subject to appropriate and applicable privacy and security considerations; generally, however, information needed to prevent fraud should not require the sharing of types of information, such as personal or investigative information, that would raise or invoke such considerations;

(e) The development of commercial and other practices and systems in ways which recognize the specific and general threat and costs associated with fraud and identity-related crime and the need to incorporate effective security and other preventive methods: effective collaboration between Governments and the private sector are essential to ensuring that effective measures to prevent fraud are incorporated and used, while avoiding excessive costs or other problems related to efficiency, interoperability and fair competition.

35. A number of responses mentioned a range of technical means of prevention, both for economic fraud and identity-related crime, including measures to make documents such as passports or credit cards more reliable as a means of identifying individuals and more difficult to alter or falsify and measures to make the supporting information systems more difficult to subvert and more reliable as a means of rapid identification when cards or documents are used. The evolution of technical means of prevention is already well established and ongoing, both in appropriate commercial sectors and the public sector. The experts noted in particular the efforts of Interpol and the International Civil Aviation Organization (ICAO) to enhance the security of passports and other travel-related identity documents, as well as the work of the OSCE Action against Terrorism Unit in promoting the implementation and use of the programmes of ICAO and Interpol and other assistance in relation to the security of travel and identity document security. The experts also noted that the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (General Assembly resolution 55/25, annex II), and the Protocol against the Smuggling of Migrants by Land, Sea and Air (Assembly resolution 55/25, annex III), supplementing the United Nations Convention against Transnational Organized Crime, contain provisions on travel

documents that are secure against falsification or tampering, enhanced security and systems for production, issuance, validation and verification and measures to implement machine-readable document forms to facilitate the rapid checking of passports. The experts further noted that the costs of research, development and implementation were a significant factor, however, especially for developing countries and for commercial entities concerned about cost-effectiveness and competitive advantages. The establishment of stronger identification systems in every State would bring collective benefits for the international community in controlling, for example, economic fraud and immigration or travel-related crime (such as trafficking in persons) and in general security. It is therefore recommended that:

(a) States should develop and implement measures to enhance the security of passports and other travel-related identification documents and the processes and systems used to produce, issue, validate and verify them, taking into consideration the measures called for in relation to passports and other travel-related identity documents in the United Nations Convention against Transnational Organized Crime and the Protocols thereto[8] and in ICAO document 9303,[9] on machine-readable travel documents;

(b) Technical information should be shared with developing countries, where feasible, and should be assisted in using such information to establish robust domestic identification infrastructures in support of both public and commercial functions;

(c) Government and commercial entities should cooperate to ensure that identification systems are robust and interoperable to the extent that that is feasible.

36. Criminological studies of the effectiveness of deterrence have shown mixed results for many offences. There are, however, some reasons why deterrence may be more effective in cases of fraud and similar types of crime, which are by their nature pre-planned and commonly involve some element of cost-benefit analysis on the part of the offenders. In addition to incarceration, the economic nature of fraud suggests that fines, confiscation and measures against money-laundering may be viable deterrents. Further study and consideration of deterrence measures are therefore recommended. In addition to introducing offences and punishments, there could be measures such as the introduction of specialized law enforcement units trained to deal with fraud cases, where such a measure is seen as increasing the probability of the offenders being detected, prosecuted and punished.

8. Training

37. One issue raised in some of the responses is the need to train investigators and prosecutors and to provide technical assistance for developing countries in that area. In the case of economic fraud, training must address the extremely diverse forms of fraud, the sophisticated nature of many of the offences, the involvement of elements of transnationality and organized crime and the criminal-commercial duality of fraud. In the case of identity-related crime, training must address the fact that such

---

[8] See the Trafficking in Persons Protocol, arts. 12-13, and the Migrants Protocol, arts. 12-13.

[9] The experts noted that the member States of ICAO had committed themselves to the implementation of the relevant portions of document 9303 by April 2010.

crime is a new and evolving concept that encompasses both new, high-technology forms of crime and long-established forms of crime such as document forgery. In both cases, training must also be regularly updated to keep pace with the rapid evolution of techniques used by offenders. The experts noted that such training often requires a multidisciplinary approach in the development and implementation of training programmes, including a range of disciplines from entities in both the public sector and the private sector. Modern fraud investigators, for example, require knowledge in areas such as accounting and the operation of commercial and financial systems and the investigation, preservation and presentation of evidence in cybercrime cases. Those investigating identity-related crime require not only knowledge of crimes such as impersonation and forgery, but also knowledge of the identification infrastructure and systems that support both government and commercial forms of identification. It is therefore recommended that:

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

(b) Member States should cooperate collectively in sharing information relevant to the development of training programmes and materials. That is important not only to ensure that useful practices are transferred from one State to another, but also to help ensure that officials responsible for fighting fraud at the national level are able to cooperate effectively to counter the growing number of transnational fraud cases;

(c) Materials and training programmes should incorporate a general overview of fraud, but should also be directed at specific forms or types of offending;

(d) There should be effective collaboration among those involved in providing training to counter fraud, money-laundering, corruption, terrorism and cybercrime and similar types of training, including in the private sector, with a view to exploiting synergies, ensuring consistency and avoiding duplication;

(e) Recommendations and materials for training on countering fraud should be disseminated to United Nations and other intergovernmental bodies so that they may be included in training and other material developed by those bodies;

(f) Member States should exchange information regarding the availability of existing training programmes on the investigation of computer crime and computer-related fraud and should increase and further systematize such training. A great deal of training is already available in those and related areas. Such training is given by and for many States, organizations and private companies and is available worldwide in many languages and for many levels of expertise. It has proved highly valuable in providing criminal investigators with the technical skills and knowledge necessary to investigate computer fraud and computer-related crime effectively;

(g) The *United Nations Manual on the Prevention and Control of Computer-related Crime*[10] should be updated by incorporating material dealing with computer-related forms of fraud and identity-related crime.

---

[10] *International Review of Criminal Policy*, Nos. 43-44 (United Nations publication, Sales No. E.94.IV.5).