14 April 2009
English only

Commission on Crime Prevention and Criminal Justice
Eighteenth session
Vienna, 16-24 April 2009
Item 3 (a) of the provisional agenda*
Thematic discussion: "Economic fraud and identity-related crime"

First meeting of the Core Group of Experts on Identity-Related Crime (Courmayeur Mont Blanc, Italy, 29-30 November 2007)

I. Opening of the meeting

1. The first session of the Group was convened by Ms. Kuniko Ozaki, Director, Division for Treaty Affairs, UNODC, on 29 November 2007. She welcomed the experts and indicated that Ambassador Eugenio Curia, representative of Argentina in Vienna, had agreed to serve as Chairman of the Group, and that Christopher Ram had agreed to serve as Rapporteur. As Ambassador Curia was unavailable, Ms. Ozaki chaired the first session. She noted that further experts would need to be identified, both as possible members of the group and to serve in consultative roles. She also emphasized that, to ensure the broadest possible coverage of the issues, experts were invited to participate primarily as individual experts and not as representatives of individual Member States or specific commercial entities.

2. Ms. Ozaki indicated that misuses of identity were not new, but that concerns were now being raised by the effects of globalization, the spread of information and communications technologies, and other factors. She noted that the establishment of the group was the first step in the process of creating a consultative platform on identity-related crime aiming at bringing together various stakeholders to develop strategies, facilitate further research and agree on practical counter-action. She also noted that there was a pressing need for more information, and for a global strategy for responding based on such information. There was little concrete data on the nature and scope of the problem and on rates and trends of offending. She also noted

* E/CN.15/2009/1.

V.09-82587 (E)

that the establishment and verification of identity in general went beyond the scope of the work of UNODC and the Core Group. The key issue was to consider what should be the role of UNODC as an element within a broader global strategy, taking into consideration the crime prevention and criminal justice role of UNODC, and the emerging roles of other intergovernmental organizations, the Member States, and relevant private sector interests.

3. She suggested that some objectives for UNODC might include general awareness-raising of the problem, identification of gaps and the development of a comprehensive approach with respect to crime prevention and criminal justice elements of the strategy. Assessing the interests of developing countries was also seen as a key issue, including both domestic and transnational identity-related crime. Ms. Ozaki also noted that it was not necessarily expected that UNODC would be called upon or have the capacity to address all of the issues that might be raised. Another key issue for the core group of experts would be to advise UNODC and the Commission on Crime Prevention and Criminal Justice with respect to the setting of priorities. The Rapporteur briefly reviewed the history of the 2007 study on "fraud and the criminal misuse and falsification of identity", and the major recommendations contained therein,[1] as well as the scope of the mandates established for UNODC with respect to the subject-matter of identity-related crime.[2]

II. Assessing the challenges of identity-related crime and the gathering, analysis and dissemination of information

4. Several experts highlighted the lack of data, and the need to establish legal and research definitions, classifications, as well as identify and fill gaps. It was noted that several sources of data might be available, and that data received from the public and private sector might vary significantly. There were very few offences specific to identity-related crime, but many countries had offences covering part of the problem, such as the forgery of identity or other documents, impersonation, and some forms of cybercrime offences. In addition, many companies assembled data on crimes in areas within their specific areas of interest. A major challenge would be to identify, gather and integrate the data to form a comprehensive picture, bearing in mind that some information was not disclosed for commercial, security or other reasons and that it was difficult to compare data gathered for different reasons using different methods. It was noted that, at the international level, it was seldom if ever possible to obtain statistical data sufficient to support the kinds of analysis and conclusion usually applied in domestic crime statistics and that more general reviews of data and the collective opinions of the experts would be more important. Based on existing work, the available data, and those who had assessed it, did not

[1] See E/CN.15/2007/8, paragraphs 16-37.

[2] See E/RES/2004/26, paragraph 5, calling for the development of "… useful practices, guidelines or other materials in the prevention, investigation and prosecution of fraud and the criminal misuse and falsification of identity …", and E/RES/2007/20, paragraph 14, calling for the provision, inter alia, of "… legal expertise or other forms of assistance to Member States reviewing or updating their laws dealing with transnational fraud and identity-related crime …", paragraph 17, encouraging promotion of "… mutual understanding and cooperation between public and private sector entities …", and paragraph 18, recalling paragraph 5 of E/RES/2004/26. All these mandates are subject to the availability of extrabudgetary resources.

always agree on the seriousness of the problem and what should be done in response. It was therefore stressed that attention should be paid to ways that would allow the better organization of data gathering and the shaping of more precise frameworks and terms of reference with a view to raising awareness about the impact of the problem even in countries where identity-related crime was not yet encountered on a large scale.

5. Beyond the scope of crime issues, the question was raised on how to use the more general non-crime assessments of the OECD, UNCITRAL and commercial entities to establish the appropriate context. Within the scope of crime issue, there was the challenge of developing specific typologies and sub-categories to support research, criminalization and other responses. A further need was to develop a picture of the relationships between identity-related crime and other offences, both overlapping, such as impersonation, and related or secondary offences such as fraud, organized crime and money-laundering. Several existing sources of data or information were identified, including the OECD, which focused only on the economic aspects, and the private sector. Among Member States, only the United States of America gathered specific crime statistics, and those had limits, although work was underway to broaden the base of the data to include victim and offender-surveys and to obtain a more global picture. Data biases, especially the emphasis of victims and companies on economic aspects, were also discussed.

6. There was general agreement that identity-related crime would have to be considered in the context of more general identity infrastructures, which at the State level could be centralized or not, and in the private sector varied depending on commercial considerations. There was also agreement that, while infrastructures would vary, the underlying concept of identity information, was in general terms likely to be fairly consistent from one State or application to another, and that most forms of identity offences could focus specifically on the protection of identity information. It was noted, however, that there were significant differences in what constituted “identity information” as between natural and legal persons, the former focusing on individual and biological characteristics and the latter tending towards trade marks and other intellectual property used to identify a company and link it to products or services. The degree of protection could also vary, depending on a cost-benefit assessment of the offences and security measures weighed against the extent of the security. Over time, additional variations would be encountered due to the advent of new technologies, and the constant reciprocal evolution of offender techniques and security countermeasures, such as biometrics and encryption.

7. Questions related to what sorts of data would be needed and why were also considered. Generally, there was a need for quantitative data about how offences were committed (methods and techniques involved) and the influences of technology and other environmental factors on offending patterns. There was also a need for data about the prevalence of various types of offences to support analysis of offending rates and trends, as well as for information about the range of costs (economic/non-economic/direct/indirect) and how losses and other costs were allocated. Such data were needed for many purposes, including to establish the seriousness of the problem, suggest proactive and reactive responses and assist the core group, UNODC and the Commission on Crime Prevention and Criminal Justice in the setting of priorities for work in this area.

8. In summing up this subject, the Chairman noted that the core group could not conduct a global survey and, instead, would have to focus on the assessment of available data and on raising awareness to promote responses and the gathering of more accurate information. She also noted that there was a need to develop a basic typology or other frame of reference, bearing in mind that this was a global issue and the interests of developing countries and the private sector would have to be considered. There would also be differences in national and commercial identification systems or infrastructure, triggering differences in the ways existing data were gathered and assessed. The need to ensure confidentiality of data was also noted.

III. Interests and work of various stakeholders to address identity-related crime

9. There was general agreement that there was a range of stakeholders, and that a full assessment of their interests and how these were inter-connected was needed both to obtain a full picture of the problem and to support a comprehensive and integrated response. It was noted that, in addition to the division of issues between the public and private sectors, there was also a range of stakeholders in each of these groups. Identifiable public sector interests included national security, criminal justice, social security or other public benefits, customs and immigration and the licensing of publicly-regulated activities such as driving. There were also differences between the political, legislative, enforcement and other functions. In the private sector, several specific sectors were identified, including the payment-card industry, developers of hardware, software and other security or commercial technologies, providers of internet, telecommunications and similar services, and more generally, companies involved in electronic commerce or similar non-commercial activities. An area of shared concern was the regulation of commercial activities, which was done by the public sector, but with a significant interest on the part of private commerce.

10. In discussion, it was noted that there were significant differences in the thinking of experts on crime and commerce, both nationally and internationally. Lack of harmonization of relevant laws was a recurring concern for most companies, who operated in a global environment, because this made compliance difficult. Another major concern was the existence of obstacles to information-sharing, which were different in various sectors, but appear to be a problem for all, in one form or another. A third concern for the private sector was the multiplicity of public agencies involved in this field, which resulted in lack of coherence and concerted action. For States, the problems included privacy rights, as well as security issues. For companies, customer privacy was the main concern, due to the potential for criminal victimization or other losses to the customer, and attendant risks of civil liability, reputational damage and economic losses to the company. A balance between customer privacy and anonymity, on the one hand, and accountability and investigative capacity, on the other, had for some time also been a major underlying issue. Another concern, especially in the private sector, was the allocation of responsibilities, protection costs and losses among the various industries and their customers. In the private sector, for example, the emphasis could be on security measures to protect personal identity and other information

from disclosure, or on measures to prevent its misuse if disclosed. The public sector, on the other hand, was more likely to seek protection at every level and stage of the process as crime-prevention, but be less sensitive to the cost-benefit analyses used by commercial entities.

11. There was general agreement that the subject matter was novel and cross-cutting, which made it difficult to ascertain which interests and stakeholders ought to be engaged, and that this was common to both public and private interests. In developing the original U.S. legislation and establishing administrative mechanisms to support it,[3] consultations with groups of companies representing a series of commercial sectors were held, and this continued with further discussions on how to expand the measures to protect the identities of legal and natural persons.

12. There was also discussion about the relationship between public and private sector interests. Generally, governments might establish standards or practices prescriptively through legislation, or through the use of more positive incentives, when such could be found. For commerce, cost-effectiveness and maintaining competitive position were the dominant considerations. While these could conflict, it was also noted that harmony was possible at least for some of the areas of interest. One function of regulations establishing security standards, for example, was to ensure adequate security for all while maintaining a fair competitive environment by preventing competitors from adopting less costly and secure options. Generally, the objective should be a coordinated and comprehensive strategy, providing the optimum security, privacy and commercial conditions for all stakeholders, including ways and means to render data less useful for criminal purposes and financial transactions after the identity takeover. In addition to government and commercial interests, other stakeholders included victims, who had interests unique to this form of crime, such as the restoration or repair of identity. It was noted, in this regard, that banks and financial institutions were also included among the victims of this crime. The role of the media, which could range from useful education and awareness-raising, functioning as a conduit to convey messages and information to the public, to more sensationalist and negative influences, was also considered.

IV. Developing domestic criminal justice responses and fostering international cooperation

13. While the United States, Canada and some Australian states had proposed or established new crimes, some countries were not convinced that the problems were not addressed by fraud, forgery, impersonation and similar existing offences, and most countries did not appear to have considered the options at all. While it was clear that in many cases existing crimes overlapped, some experts noted that there would always be cases in which only identity abuses were committed or could be proved. The additional offences were also seen as having significant advantages in terms of evidentiary and dual criminality requirements for purposes of mutual legal assistance and extradition. At a more fundamental policy level, one question was whether the prejudice or harm to the holders of identity which was abused was sufficiently serious to warrant application of criminal justice powers, offences and

[3] Discussions included the President's Task Force on Identity Theft, established in March 2006, and some of the issues before it. See: http://www.usdoj.gov/ittf/.

punishments even if the abuses did not amount to other criminal offences, or if the mere risk of such harm was sufficient. Identity abuses were also associated with some forms of harmful conduct which did not constitute a separate crime, such as harassment and cyber-bullying. Another added value of additional offences, as a matter of policy, was denunciation, i.e. the idea that the abuse of another's identity should be a separate crime. A further trend noted was that, as some of these activities became the focus of organized crime, overall criminal schemes tended to be fragmented among offenders or groups with specific skills, as in cases where one or more offenders might engage only in the fabrication or falsification of identity, while others then used it to commit the more established and conventional offences. There was general agreement that a key challenge for all stakeholders, including Member States, the international community, and relevant private sector interests, was the need to raise awareness of the nature and scope of the problem, the ways it arose in individual States, bearing in mind factors such as degree of technological development and access to information and commercial technologies, and of the possible options for prevention, criminalization and other countermeasures.

14. Several experts noted that the establishment of new offences extended the ambit of criminal liability to conduct which was seen only as preparatory to existing crimes. Therefore the utility of intervening before crimes such as fraud and money-laundering could be committed was raised. Some civil law countries also criminalized preparatory acts per se. It was also noted that, when extending the ambit of criminal liability, as with similar developments in money-laundering, careful consideration of the necessary limits and exclusions was needed to avoid criminalizing innocuous conduct. One means discussed was to incorporate an additional element of intent or knowledge with due consideration to the burden of proof needed for establishing the mens rea, where applicable. Illicit possession could be limited to possession for criminal purposes, for example, and trafficking or transferring identity information could be limited to cases where there was intent or recklessness to use such information for crime or some activity prejudicial to the owner of the identity. A further question of ambit, for both fraud and identity-related crime, was whether any new criminal offences would be limited to specific conduct such as taking or falsifying identity, or whether they should extend to the operation of an ongoing fraud or identity crime scheme such as a mass-fraud or "phishing" scheme. Aside from questions of criminal liability and proof, this had also implications for the ability of service providers, law enforcement or others to intervene and halt a scheme in progress. Another concern raised was that the enactment of new offences raised public expectations that they would be enforced and effective, and that such expectations could not always be met. Other issues related to criminalization were also considered, including jurisdictional aspects. It was noted that offenders tended to exploit loopholes in national laws and their implementation and shift their operations to countries where appropriate and enforceable laws were lacking, in order to launch attacks on victims in other countries. This "forum shopping" could only be addressed if appropriate jurisdictional rules, which would also foster international cooperation, were in place.

15. Other types of legislative or other measures, beyond criminalization, were also mentioned, including administrative and other measures to establish focal points and

repositories at the national level. Only a few States had established focal points,[4] but they were likely to be useful for a range of applications. These included gathering victim complaints both for investigative and statistical purposes, information-sharing among law enforcement agencies, the general development and dissemination of expertise and advice, and victim-support measures as a basis for the remediation or restoration of identity information.

16. There was discussion of the state of consideration or action in various countries. The United States of America had established some offences and was considering expansion to cover abuses of the identity of legal persons. Some U.S. and Australian States had also established offences, while in Canada legislation containing identity offences per se were presently (November 2007) before the legislature for approval. China and Japan remained to be convinced of the need for new offences. European countries appeared to have a range of views: the Netherlands was studying or considering the options, while France had rejected them. The United Kingdom was considering offences, but the situation was complicated by the ongoing establishment of a centralized national identification system and the recent (November 2007) loss of a large volume of identification data by a government department. The recent (May 2007) communication of the European Commission "towards a general policy on the fight against cybercrime", according to which "EU law enforcement cooperation would be better served were identity theft criminalized in all Member States", paved the ground for conducting consultations to assess whether specific legislation was necessary and appropriate in EU Member States. One issue, particularly for Europe, seemed to be the search for a balance between criminal offences and preventive measures to protect identity.

17. For the private sector, views on legislative or other measures depended, to a certain extent, on what specific measures consisted of and how they fit into the relevant commercial and regulatory environments. There were generally concerns about measures which might be costly or affect competitive interests or corporate and customer privacy. There was, however, some support for measures which set common and effective standards for all competitors and for criminalization and other measures intended to deter crime and reduce commercial costs and losses. Most of the major private sector interests functioned in a multinational environment and one of the major concerns for them was not the content of legislative measures, but the lack of standardization or harmonization among individual national regimes. Measures were sometimes inconsistent and the need to ascertain and meet a wide range of differing standards in each State where a company did business was a major cost and compliance issue for them.

[4] See, for example, the identity theft unit established within the U.S. Federal Trade Commission (FTC), http://www.ftc.gov/bcp/edu/microsites/idtheft/.

18. Ms. Ozaki raised a series of possible elements that could be considered by States when deciding whether the problem of identity abuses was sufficiently serious to warrant the application of offences and other criminal justice measures, and if so, how to frame appropriate criminal offences. These included the consideration of what specific legal rights or interests should be protected by the criminal law, including:

(a) The interests of individuals whose identity information is taken, copied, altered or misused;

(b) The extent to which relevant rights existed and were affected by the abuses, including privacy rights, intellectual property rights (corporate identity), and if applicable, the right to have an identity;

(c) The need to protect the integrity of various models of identity infrastructure, including national identity systems, subject-specific identity systems (such as passport systems) and relevant private sector commercial identity systems;

(d) Within the scope of each identity infrastructure, what specific types of document and information should be protected;

(e) Whether the criminalization of specific identity abuses per se was necessary or justified to prevent or suppress secondary crimes such as fraud, money-laundering, terrorism, or the smuggling of migrants or trafficking in persons;

(f) Whether criminalization was needed or justified on national security grounds;

(g) Which specific forms of conduct should be criminalized and how offence provisions should be framed, for example in respect of conduct such as acquiring, taking or copying, falsifying, possessing, transferring or trafficking in identity information or documents, or the subsequent illicit use of identity documents or information in other offences;

(h) At a general level, how the scope of identity offences would fit within each State's existing criminal law, bearing in mind the need to avoid gaps; and,

(i) At the international level, the appropriate balance between international cooperation and common approaches to criminalization, on the one hand, and the individual aspects of each State's criminal law and identity infrastructure, on the other.[5]

[5] Following the core group meeting, discussions at the International Conference on "The Evolving Challenge of Identity-Related Crime: Addressing Fraud and the Criminal Misuse and Falsification of Identity", organized jointly by the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC) and UNODC, identified the underlying concept of "identity information" as a possible basis for common ground in formulating criminal law and other provisions in each State. While the details of law and identity infrastructure varied from State to State, the ISPAC meeting concluded that the underlying elements of information used to establish identity were likely to be the same in all systems and might therefore form the basis of common approaches to criminalization.

V. Enhancing cooperation between the public and private sectors

19. There was general agreement that cooperation between the public and private sectors was critical at all stages of the process, from gathering and assessing data, to investigation and prosecution of offences and matters of prevention. Numerous issues arose with respect to specific forms of cooperation, however, and each form was likely to vary with the respective strengths and weaknesses of each sector in each area. In prevention, governments might set overall priorities and mandate security, service or other standards, but companies usually had the best access to customers and employees in positions to prevent crime. In assessment, companies usually had data which were accurate and reliable, but limited in scope to commercial purposes. In terms of investigative cooperation, companies and State agencies were subject to different rules and requirements. While the mandates and powers of the State were to investigate and prosecute crime, companies had concerns about customer privacy, the allocation of investigative costs and exposure to civil liability if they disclosed private information without lawful authority. Prevention was likely to involve a range of measures, with a public lead for some and a private lead for others. Data assessment and prosecution were more in the nature of parallel activities and structures, which made the relationships between each more complex. Governments and companies had different reasons and methodologies for gathering data, and different concerns relating to the ways in which it was used or shared with other entities. Investigative and prosecution functions also differed, with State entities focusing on criminal deterrence and punishment, and companies on the prevention and recovery of losses. In many scenarios, cases first came to the attention of private companies through monitoring or customer complaints, and only later found their way to the attention of criminal law enforcement agencies. Further layers of complexity were added for international cooperation. Generally, companies and commercial sectors were multinational and could cooperate fairly easily and efficiently. International cooperation in criminal matters was the subject of many more safeguards and was more formal and time-consuming. Mutual legal assistance requests for information in the possession of multinational companies represented further challenges, including difficulties to determine which jurisdiction should be asked to obtain the information, provide sufficient or appropriate assurances to the company from which it was obtained and find ways to request, obtain and transmit some data in the short time-frames often needed for success in some investigations. Cooperation between public and private interests could also be proactive, in areas such as developing prevention measures, or reactive, such as alerting one another to ongoing offences in a timely manner.

20. Information-sharing appeared to present a challenge for both sectors, for different reasons. The public sector faced security, privacy and similar constraints, whereas the private sector was more concerned about commercially sensitive information which might affect competitive positions if disclosed. The concerns of each sector applied equally to information shared within each sector and between the two. However, a lot of the information-sharing needed might not necessarily involve information that was sensitive, either criminally or commercially. Investigative cooperation raised a number of specific issues. The costs and other effects of executing judicial search orders could be significant, especially if volumes were high, where companies required such orders for disclosure to protect

themselves against civil liability. A recurring concern was that companies routinely erased temporary data when no longer needed to reduce storage space and costs, whereas law enforcement would prefer longer retention periods to ensure records and traffic information would be available if there was an investigation. Another issue was how to ensure that fast reaction capabilities of companies could be used effectively in ongoing offences on computer or telecommunications networks, while still respecting domestic and transnational legal safeguards.

VI. Prevention of identity-related crime

21. The role of the private sector in prevention was seen as critical, because companies were usually in the best possible position to implement most preventive measures. Generally, prevention included both strategic prevention and situational prevention. The first included measures such as programmes to educate customers and employees about fraud, identity-related crimes and similar risks and technical security measures to protect identity and commercial data from theft or illicit interference. The second involved the rapid identification of ongoing fraud and identity crime schemes to stop them quickly and prevent further offences and victimization. Generally, companies had the best access to systems for technical measures and to employees and customers for education, although it was noted that the commercial sector was divided into different functions and not all companies had such direct access or influence. Vertical coordination among segments of the payment system was needed, for example. Another issue for both types of prevention was the need for capacity and mechanisms to continually update measures as technologies, offender methods and other factors were constantly evolving.

VII. The way forward: possible activities for UNODC

22. A number of general areas were identified where work within the capabilities of UNODC could usefully be carried out. A key issue relating to the general scope of work and the scope of individual projects was that any proposals to prevent identity-related crime, or to establish and apply appropriate offence and investigative powers, was likely to be linked to the more general mechanisms by which Member States and commercial entities established and verified identity in general. In considering most of the possible crime prevention and criminal justice work raised in discussions of the Core Group, it would be important to ensure that non-crime aspects were taken into consideration and that specific projects were consistent with more general identity infrastructure and its development.

A. Possible partners for UNODC and other stakeholders

23. From an institutional standpoint, at the international level, the novelty of identity-related crime issues and the links to broader domestic and international policy issues made it important for UNODC to determine which other entities were working in related areas to establish communications and ensure consistency. It was noted that the OECD had reached a similar conclusion and had already started

developing an inventory of relevant international organizations with interests in this field, including UNODC's mandates and involvement. In addition to UNODC and the OECD itself,[6] experts identified the following intergovernmental organizations which were already engaged or were likely to have an interest in this area:*

- International Organization for Migration (IOM, primarily travel and migration identity issues);
- Council of Europe (cybercrime issues, including the implementation of the provisions of the Council of Europe Cybercrime Convention)
- European Commission : Justice, Liberty and Security Directorate (privacy and identity issues)- ENISA (European Network and Information Security Agency)
- Asia Pacific Economic Cooperation (APEC), in cooperation with OECD (cybercrime and "malware" issues)
- Interpol and Europol (general law enforcement and register of stolen passports)
- G8 "Roma" (terrorism issues) and "Lyon" (crime issues) groups
- ITU, taking into account the parallel process of the High-level Expert Group on Cybersecurity in the context of the ITU Global Cybersecurity Agenda
- International Chamber of Commerce
- UN Development Programme*
- "24/7" cybercrime group
- International Civil Aviation Organization (ICAO, passports and travel documents)
- Organization for Security and Cooperation in Europe (OSCE)
- Southeast European Cooperative Initiative (SECI) (within the general framework of combating transborder crime in the region)
- World Society of Victimology (victim issues)
- World Intellectual Property Organization (WIPO, trade marks and other indicia of corporate identity)
- UN Commission on International Trade Law (UNCITRAL, commercial/corporate identity issues, general private sector interests)
- UN Department of Peacekeeping Operations*
- UN Human Rights Committee and other international human rights bodies*

---

[6] The primary agency within the OECD is its Working Party on Information Security and Privacy (WPISP).

* Not raised in the meeting but also likely to be of relevance were the United Nations Department of Peacekeeping Operations (DPKO) and the United Nations Development Programme, which might have general interests with respect to the establishment of identity in development and reconstruction projects and specific applications such as identity in military forces, police forces and for the conduct of democratic elections. There was also some discussion, in the core group and subsequent ISPAC panels, of the concept of identity as a human right, raising the possible inclusion of United Nations and other bodies concerned with human rights.

B. Possible subject matter and areas of work

24. Discussions addressed the need for work in several areas, including: further accumulation and analysis of data; prevention; criminalization; domestic investigation and prosecution; international criminal and commercial cooperation; domestic and international mechanisms for victim support and the restoration of identity information; the assessment of technical assistance needs; and the addition of further experts to the core group itself. Aside from the accumulation of data and expansion of the core group, most of the possible work would appear to involve the development of a range of materials to support education and training, criminalization and various forms of cooperation between States and other key entities. Preparation of such materials generally consisted of the identification of issues or subject matter to be covered, accumulation of appropriate content, review and refinement of the content by experts representing the key perspectives or interests affected, as well as production, dissemination and use of the finished materials. Generally, materials for the private sector would be developed by the companies themselves, but it would be important to ensure that crime prevention, criminalization, investigative matters and other criminal justice issues were taken into consideration and that information was shared internationally for purposes of global consistency.

(a) Prevention

25. There was general agreement that there would be some role for UNODC in the development and dissemination of prevention-related materials. However, it was noted that the subject of prevention was complex, with many different roles for commercial entities and for criminal and other governmental entities. In the private sector, the role of each company might vary depending on its commercial function, the information it had and the extent to which it was in direct contact with victims, offenders or customers. In the public sector, there was a need for the involvement of both commercial and crime-prevention experts to ensure that mechanisms were both effective in preventing crime and viable from a commercial cost-benefit standpoint. The context of prevention and related matters were also discussed. For example, it was noted that information-sharing was critical both for situational and strategic prevention, and that the incorporation of technical prevention elements into identity systems depended, to a large degree, on the overall design of the systems themselves and the ways in which they established and verified identity and inter-operated with other systems. It was also noted that a clearer understanding was needed of what conduct should be criminalized to bring into focus what should be prevented.

26. Within the overall topic of prevention, the need to support both strategic and situational approaches was raised. Regarding strategic or systemic prevention, materials or advice would be needed for the general education of consumers and general groups of potential victims, the training of appropriate public and private sector workers, as well as the establishment of commercial and identity systems that could be resistant to criminal attacks. Much of the necessary material would come from commercial and other sources outside of the criminal justice system, with UNODC and national criminal justice sources playing a contributory role. Another

possible role for UNODC might be the dissemination of such materials and other awareness-raising activities.

27. Situational prevention required fast assessment and intervention to halt ongoing identity crime schemes, which was a matter for appropriate companies and law enforcement agencies, but a role for UNODC in developing general materials and raising awareness of the need for situational prevention might be appropriate. Another point raised, in this connection, was to examine the ways and means to abuse electronic identities and how to prevent such abuses.

28. Target groups for awareness-raising discussed within the core group included governments, companies, customers and general populations, as well as specific groups such as law enforcement personnel and private employees in positions where exposure to crime was likely. Possible mechanisms included events, such as conferences, symposia and regional meetings and a range of printed and other materials.

(b) The development of criminal offences

29. It was noted that, while several States were in the process of considering or establishing new criminal offences, others remained to be convinced that a new perspective on criminalization would be a sufficient improvement over existing offences such as fraud, forgery and impersonation, or that it was justified, given the security of identity information and other means used to protect it. Thus, an early role for UNODC, as well as other intergovernmental organizations, could well be to generally raise awareness of the issues and options, and to better inform the discussion by disseminating the 2007 United Nations study and other information relating to the advantages offered by criminalization. Governmental experts raised arguments to the effect that criminalization would make prosecution easier and better protect victims of identity-theft in particular. Private sector experts noted that encouraging governments to criminalize abuses of trademarks and other indicia of the identity of legal persons would be a welcome development for companies. They also noted that consistency with work on corporate identity in other public- and private sector forums would be important.

30. Another important role for UNODC would also be the preparation of a range of materials to assist countries wishing to establish new criminal offences. There would be a need to tailor each country’s legislation to ensure consistency with its existing related offences, taking into consideration its general national scheme or approach to identification. This suggested that standard materials such as model laws would not be appropriate. There was general agreement that a better approach would be to develop materials such as outlines of policy issues and options and general elements to consider when formulating offences, as well as outlines or descriptions of the sorts of conduct that could be criminalized. Materials should cover the range of means of establishing identity, including paper documents, digital and other means. As more States adopted relevant offences, outlines or copies of the relevant legislation could also be collected and disseminated, as had been done with other emerging transnational crime issues.

(c) Investigation and prosecution

31. UNODC could well be involved in the preparation of useful practices, guidelines or other materials in the investigation and prosecution of identity-related crime, as mandated by paragraph 5 of ECOSOC resolution 2004/26. A cautious and step-by-step approach was needed to ensure that material focusing on strengthening criminal justice and law enforcement responses was to be considered in conjunction with legislative material, mentioned above under (b).

(d) International cooperation (criminal and commercial)

32. While it seemed clear that there would eventually be a need for some form of support to build domestic capacity in investigation and prosecution of domestic identity-related crime and to provide appropriate cooperation in transnational cases, this was premature given that so few States had specific criminal offences. Based on the evidence of serious transnational fraud cases, it seemed likely that the necessary conditions for applying the United Nations Convention against Transnational Organized Crime (elements of transnationality and the involvement of an organized criminal group) would also be present in many identity-crime cases, but it was likely to take some time to accumulate sufficient data on this issue. To the extent that most identity-related crime was found to be related to transnational organized crime, some materials could be developed and incorporated into existing projects supporting implementation and use of the existing Convention.

33. Training materials for investigators were often based on the nature of criminal activity and techniques used by offenders rather than on legal definitions or offence provisions, and some materials to build capacity to identify, investigate and prosecute identity-related crime under whatever existing criminal offences each Member State had available could be considered.

(e) Technical assistance needs assessment

34. There was not much discussion of this issue, but it seemed clear that in future there would be a need for capacity building within the UNODC and other organizations to assess the needs of Member States requesting technical assistance. In addition to formulating and prioritizing actual projects, some assessment of needs might also be needed at an earlier stage, to inform decisions about the content of technical assistance materials and priority-setting with respect to the development and use of such materials. As with other aspects of identity-related crime, some non-crime areas, including public identity infrastructure and private sector interests and capacity, were likely to be significant factors in assessing needs and coordinating crime-related and other forms of assistance.

(f) Victim support and the restoration of identity information

35. Several experts pointed out that providing assistance to victims in minimizing economic losses and other harm and in restoring or repairing their identity information was a critical element of any overall strategy. They also noted that this need extended to public and private sector identity and related information, and that in many cases to both domestic and foreign information sources. Most of the discussion focused on the immediate task of raising the awareness of governments and companies of the problem. Over the longer term, materials to support public and

private sector training and remediation mechanisms would probably be needed. Such materials would require input from a range of public and private sector perspectives and the role of UNODC in contributing to, assembling, and disseminating such materials would have to be considered.

(g) Corporate identity (identity of legal persons)

36. There was also discussion among the members of the core group on issues relating to the identity of legal persons and abuses thereof. It was noted, in this connection, that there were significant differences in the ways corporate identity was established and protected by law. It was further pointed out that the United States was considering how to expand or modify its existing identity crimes so as to extend them to corporate identity. This was an area in which close cooperation with UNCITRAL and private sector entities was essential, as existing legal protections tended to focus on civil litigation based, inter alia, on intellectual property (protection of trademark) interests. This could have a significant effect on national decisions as to whether to extend the protection of the criminal law, and if so, how to accomplish this in the additional context of commercial law interests. In addition to fundamental relationships between commercial and criminal law, it was also noted that there were a number of practical links. Experts underscored that abuses of the identity of natural and legal persons were often intermingled, and that both were also linked to secondary crimes such as fraud. For example, “phishing” attacks often exploited the trust relationship of financial institutions with customers to fuel identity-related crime and fraud. Bearing in mind the need for close coordination, it appeared that there was a significant role for the criminal law and criminal justice measures in this area, and hence a role for UNODC in bringing a criminal law perspective to the discussions.

C. Future composition and operation of the core group

37. There was discussion on how the work of the core group should proceed. Generally, the experts agreed that as much as possible should be done by e-mail or Internet communications, and then followed up with one or more future meetings, as needed, to further develop and finalize advice and recommendations. The secretariat would further consider modalities for intersessional communication. There was also general agreement that the core group represented a good start, but that some expansion was required to cover the full range of issues and expertise needed to advise UNODC. It was further noted, however, that excessive expansion could make the deliberations less flexible, manageable and productive.

38. Regarding public sector issues, there was general agreement that more representation from developing countries was needed. Few, if any, developing countries had experts specialized in identity-related crime, but the need would be to have experts who could assess the viability of proposed materials or projects in the context of local approaches to identity, technologies, commerce and other functions.

39. Regarding the private sector, it was apparent that a number of key commercial sectors would have potentially different interests or perspectives. These includes companies which developed commercial and security technologies, including equipment and software; providers of internet, telecommunications and similar

services; companies involved in electronic commerce or similar non-commercial activities; the finance, banking and payment industries; and other interests. The members of the core group agreed to consider what other interests might need to be included or represented.

40. A further perspective identified as one which might require representation was that of victims. In this regard, the participation of a representative of a victims' organization with appropriate expertise could be considered. Unlike some other areas of crime, victim interests with respect to economic fraud and identity-related crime could involve the interests of both persons who had actually been victimized, and members of identifiable groups who had an established but hypothetical risk of being victimized, such as credit-card owners, senior citizens, or consumers in general. In this connection, the interests of consumers and the possible role of the Transatlantic Consumer Dialogue[7] was also considered.

41. It was also noted that the overall size of the core group should not become too large for it to be efficient. One way to maximize representation while limiting size would be to have representation from industry associations or umbrella-groups so that one member could effectively represent an entire sector. Another would be to identify additional consultant experts who would not be members of the group, but could be called upon to provide advice on specific issues where needed.

42. As far as intersessional work and immediate next steps are concerned, it was agreed that channels of communication among experts of the core group would be established and maintained, in an effort to continue the exchange of views on what should be done in future. The development of a secure website forum or bulletin board might be an option and its feasibility could be considered. For the time being, communication through e-mail was to be pursued. UNODC and members of the core group would continue to consult with a view to identifying additional interests to be incorporated and appropriate experts who could represent those interests. To assist in planning a strategy for future work, UNODC would develop a chart setting out possible areas of action, specific options within each area and suggestions or advice with respect to prioritization and the sequencing of elements of the work.

---

[7] The Transatlantic Dialogue is a forum of US and EU consumer organizations which develops and agrees joint consumer policy recommendations to the US government and European Union to promote the consumer interest in EU and US policy making. See: http://www.tacd.org/index2.htm.