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"

Second meeting of the Core Group of Experts on Identity-Related Crime (Vienna, Austria, 2-3 June 2008)

I. Opening of the meeting and adoption of the agenda

1. The second session of the Group was convened by the Chairman, ***Ambassador Eugenio Curia***, representative of the Government of Argentina in Vienna. In his absence, parts of the meeting were chaired by ***Mr. Ariel W. Gonzalez***, Counsellor of the Permanent Mission of Argentina. In attendance were the following experts: ***Christopher Ram***, Counsel, Department of Justice, Criminal Policy Section, Canada, Rapporteur of the core group; ***Jonathan Rusch***, Special Counsel for Fraud Prevention, Department of Justice, Criminal Division, Fraud Section, United States of America; ***Fons Knopjes***, ID Management Centre, Netherlands; ***Anko Blokzijl***, CEO, Sdu Identification, The Netherlands; ***Zan Jovanovski***, Risk Manager South-East Europe I, Visa CEMEA; ***Prof. Marco Gercke***, Germany; ***Brigitte Acoca***, Policy Analyst, Consumer Policy, Privacy and Information Security, OECD; ***Kate Lannan***, Legal Officer, International Trade Law Division, UNCITRAL Secretariat; and ***Pier Rossi-Longhi***, Head, IOM Technical Cooperation Centre in Vienna.

2. The provisional agenda provided by the secretariat was adopted without amendment. The substance of the provisional agenda was introduced by Ms. Kuniko Ozaki, Director, Division for Treaty Affairs, UNODC. She welcomed the experts to Vienna and summarized the discussions held at the first session of the Group, on 29-30 November 2007, in Courmayeur, Italy. The first session was seen as a general "brainstorming" discussion which had produced five or six key items for further discussion, and these were reflected on the agenda for the second session. Regarding the need for gathering and analysis of data, Ms. Ozaki reminded the

* E/CN.15/2009/1 and Corr.1.

group that the accumulation of entirely new data was not seen as feasible owing to the scope of the task and the lack of resources. Instead, she suggested that the task at hand was to gather the data which already existed, assess them and use them to advise the process. A second key element of future work arising out of the previous meeting was the question of legislative measures. It was noted that identity-related crime was a new issue and many legislative approaches were possible. In the area of criminalization, most countries had long-established offences relating to specific forms of identification or elements of their domestic identity infrastructure, but some countries were now going beyond this and developing new offences focusing on abuses of identity per se. The range of legislative options was broader than just criminalization and also included a balanced approach to both criminal and non-criminal law and an equilibrium between criminal justice and administrative measures. Aside from criminal offences, the broader range of legislative options included possible elements such as the protection of identities of legal persons and measures against the creation of totally-fictitious identities. Ms. Ozaki suggested that one task for the group would be to develop a set of core issues or elements of possible legislation which would be sufficiently general to be useful to legislators and policymakers in all legal systems.

3. Another key issue was international cooperation. This included finding ways to use existing international legal instruments, especially the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cybercrime. With regard to preventive measures, Ms. Ozaki noted that they covered a range of specific areas of prevention, including awareness-raising and education in general, and the use of legal and technical means to protect identity infrastructures and make them more resistant to crime. Prevention was seen both as a domestic issue for developing and developed countries alike and an international issue shared among them due to the transnational nature of much of the crime. The establishment and strengthening of identity infrastructure, using means such as stronger documents and information systems was not seen as an exclusively crime prevention issue, but it was one in which crime prevention and criminal justice elements would be a factor, and in which UNODC could usefully play a role in concert with other entities. A group of issues related to victims was also highlighted in the previous meeting. This included different groups of victims, a range of harms suffered by each group, and questions of how to provide compensation and assistance in repairing or restoring identity. In addition, the questions of what role the private sector could play, and how it could participate effectively in an intergovernmental process were also raised. To some extent, this issue was seen as cross-cutting, since cooperation with the private sector was a factor in many other areas, especially the development and use of prevention materials and the investigation and prosecution of crimes.

4. In closing, Ms. Ozaki also noted that, since the first meeting of the core group, the Commission on Crime Prevention and Criminal Justice had chosen economic fraud and identity-related crime as a thematic topic for its eighteenth session, to be held in Vienna in April 2009, and that identity-related crime was a major issue for the upcoming ministerial meeting of the G8, set for Tokyo, on 12-13 June 2008. Mr. Costa, the Executive Director of UNODC, had been asked to make a statement, and it was hoped that the G8 would provide some guidance and support for future work in this area.

5. One speaker made a technical presentation to the group. He noted that, while it raised many commercial and private sector issues, identity itself was at its most fundamental level a public function, an individual right and a State obligation, which was not always met in every State. Identity infrastructures could fall short in many areas. It was necessary to ensure as much accuracy and reliability at stages such as registration and the input and updating of information, as well as the security of documents and identification systems. Machine-readable documents and technological systems were only as valid as the information they contained, and technical security was moot, if the basic data were not collected and authenticated by the State concerned to ensure their integrity. He identified several stages that required attention, including basic registration and data-entry, as well as means of verifying that the data were accurate and linked to the appropriate individuals. A broader range of challenges emerged with respect to various ways of managing the data, regularly verifying it and using it in practice. The speaker underscored that each of these challenges could be different depending on the specific purpose for which the identities or identity information was to be used. An example mentioned was that of the differences between the use of passports and payment cards.

II. Agenda item 4: The accumulation and analysis of data

6. The Rapporteur of the core group reviewed the Courmayeur discussions, noting that, while it was not feasible to carry out new research and data-gathering exercises, this was also not necessary in order to accomplish the mandates of the core group, UNODC or the Commission on Crime Prevention and Criminal Justice. A great deal of information was in existence, much of it in the hands of private companies which had gathered it for specific purposes using specific and individual methodologies. The challenges were, first, to build confidence and reassure companies that their commercial or other essential interests would not be prejudiced by sharing the information in general terms, and, second, to compile and analyse the data in ways that would draw together diverse information, reconcile methodological differences and generate an accurate and useful picture for both Member States and private companies. There was also a challenge to reassure the Commission and other stakeholders about the validity of the data and analysis process.

7. There was substantial discussion about the standard to which analysis could be carried out. Generally it was noted that the differences in methodology, lack of forensic or criminological definitions and general lack of comprehensive data would make it impossible to provide the same accuracy and reliability as existed in the Member States' domestic systems, although this was not essential for success. It was also argued that the function of an expert group was to review what information was available, or could reasonably be obtained, and to draw conclusions from it, as well as provide the best advice possible to the Member States. As noted in the 2007 United Nations study on "fraud and the criminal misuse and falsification of identity",[1] time and definitions were also a major factor. It was not possible to count identity-crime cases without first defining what was being counted, while at the

[1] The report containing the results and findings of the study on "fraud and the criminal misuse and falsification of identity" was submitted to the Commission on Crime Prevention and Criminal Justice at its sixteenth session (E/CN.15/2007/8 and Add. 1-3).

same time, governments were often reluctant to enact definitions and offence provisions without statistical evidence of the scope and seriousness of the problem. Further, even when systems were set up to gather information, it could take some time to establish basic levels and identify factors needed to assess the data and rates and trends in offending.

8. One speaker noted that it would be difficult to develop a global analysis result that would be valid in concrete statistical terms. He stressed, in this connection, the problem of lack of data and numbers of reported crime encountered in developing countries. Another speaker underlined that, although more data existed in the United States, the methodology to gather and analyse statistics was not always the same. Those statistics tended to be subject-specific. He also noted, however, that some results were essential, because it was necessary to document the extent and seriousness of the problem so that governments were motivated to respond with legislation and advised on how to respond. Cross-border offending and the links between identity crimes and other offences led to a distribution of results between different jurisdictions, which was also seen as a significant obstacle to getting a complete picture. Thus, there could be substantial differences in what sorts of offence were counted, which could lead to missed offences or double counting. Another speaker noted that comparison of numbers was a major problem which was also highlighted by OECD. Existing numbers were coming mostly from developed countries, which raised issues as to whether information was representative enough to reflect a fully accurate global picture. In the case of private sector sources, commercial interests were also sometimes an obstacle to the disclosure of data. The Rapporteur of the core group noted, however, that in many cases the information needed by UNODC and the Commission on Crime Prevention and Criminal Justice was of sufficient generality and not likely to raise major privacy or commercial concerns, provided that confidence could be built between companies and governments. He also noted that, while there were many concerns about the quality of data and analysis, the sort of qualitative assessment needed to advise Member States relied more on expert assessment and opinion than on strict statistical methodology. One viable approach might be to work at a general level to guide and assist Member States in conducting more specific and rigorous work within the frameworks of their national criminal justice statistical systems.

9. There was some discussion of the range of options for definitional and classification work and the relationship between definitions, criminalization and data-gathering. One speaker noted that a possible basis for classification could be the offender's motivation or the nature of secondary or related crimes linked to identity offences. He also pointed out that, while there was much attention to economic offences and motives, passport, travel and migration-related offences, as well as abuses of asylum systems, also accounted for a major portion of identity crime. Another speaker mentioned that definitional work was proceeding, but should not be rushed. One speaker noted that classification work in the G8 Lyon/Roma Group included the development of a typology which avoided forensic definitions and, instead, focused on a phenomenological approach. Under this approach, the aim was to look at the specific conduct actually engaged in by offenders and attempt to develop an inventory which would highlight the conduct to be suppressed by criminalisation. This endeavour was without prejudice to the decisions of States with respect to whether existing criminal offences were sufficient or how to formulate new offences if they felt these to be necessary. The same speaker noted

that the Lyon/Roma Group had also re-circulated the UNODC questionnaire used for the purposes of the 2007 United Nations study. Referring to efforts by the United States to gather data, he also noted that some of the web sites established to allow voluntary reporting by self-identified victims of identity-related crime had been expanded to allow foreign victims to report as well.

10. The Rapporteur of the core group stressed that a related issue to the definitional problem was the question of harmonization of offences, which had arisen in the intergovernmental expert group entrusted with the task to elaborate the 2007 United Nations study, and subsequently, in the G8 context. He underlined that, on the one hand, international cooperation was best supported by the establishment of national offences which were as similar and consistent as possible. On the other hand, however, most States were not willing to re-open or modify existing offences, and had concerns about the fact that national offences had to fit within the context of other domestic offences and national identity infrastructures, all of which varied from State to State. Further, private sector entities had voiced substantial support for harmonization, citing difficulties faced by multinational companies and operations in complying with a range of different, and sometimes inconsistent, domestic legal requirements in the States where they were active.

11. In conclusion, Ms. Ozaki compared some of these issues to a "chicken and egg" problem. Without legislation, there was no definitional basis for data gathering and an analysis and without data there was often no basis or perceived need for policy development and legislation. She noted that this was not necessarily an insurmountable obstacle. An example mentioned to justify this was that of terrorism for which no global definition existed, but a reliable typology of some of the more problematic types had been developed and on that basis international legal instruments, statistical analysis and technical assistance work had all been successfully carried out. If the core group and UNODC could come up with a viable typology, there was probably enough data available to move forward. There would be the need to discuss issues of cooperation and confidence-building between public sector and private sector interests, but these were practical matters, and fundamental interests of both sectors favoured developing an agreeable and viable typology and moving forward.

III. Agenda item 5: Legislative measures against identity-related crime: policy issues and the formulation of offences

12. The Rapporteur of the core group reviewed some of the discussions from the previous meeting, noting that there had been a range of views with respect to whether and how States should establish new identity offences. He suggested that a key output of the core group could be a review of the arguments for criminalization and the concerns of some States about overlapping with existing crimes, criminalizing conduct they saw as merely preparatory, or establishing offences that could be over-broad and criminalizing relatively innocuous conduct. He also noted that the basic arguments in favour of criminalization of identity offences per se included the following, which could prove equally valid for both common law and civil law countries, as well as for developed and developing countries.

- First, the mere acquisition or possession of identity information of others in preparation for crime was a separate social harm that should be addressed by the criminal law. While other crimes might or might not later be committed, harm was caused to victims whose identities were compromised either way;
- Second, specific offences responded more effectively to changes in criminality related to the involvement of technologies and organized criminal groups. These had led to the fragmentation of offences, with specific stages of identity-crime schemes being carried out by offenders in different jurisdictions. With specific offences, each offender could be prosecuted for each element in the place where it was committed, whereas criminalization based on proof that the activity was in preparation for another crime required proof of the other crime, which might not exist or might be in another State. In this way, specific offences increased the likelihood of successful investigations and prosecutions, and might alleviate some of the demands placed on over-stretched international cooperation frameworks;
- Third, in many systems, criminalizing specific abuses of identity information could increase the effectiveness of investigations, by triggering the application of investigative powers as soon as it was clear that identity information might have been compromised, rather than having to wait until secondary offences such as fraud or acts of terrorism were committed; and
- Fourth, specific crimes could, if well formulated, form a more concrete basis for international cooperation, both by clarifying the scope of crimes and by ensuring that the United Nations Convention against Transnational Organized Crime would apply, if the offence is transnational in nature and involves an "organized criminal group".

13. One speaker raised the question of whether criminalization was effective and whether this could be established. The United States, for example, had established the new offences, but it was not necessarily clear that the conduct criminalized had actually been reduced as a result. Another speaker highlighted the question of consistency, noting that it would be very difficult for States to develop offences so similar as to eliminate problems with international cooperation. He noted that it was the offences, and not just the labels, that would have to be consistent. This would also be important for applying the double criminality requirement in international cooperation cases. Another speaker expressed the view that the offences established in the U.S. jurisdiction had an effect. Whether or not they reduced offending rates, they enabled law enforcement and other State entities to intervene on behalf of victims, interrupt and halt ongoing schemes and formed the basis for better information gathering. Ms Ozaki noted that, if there was agreement on conceptual issues, definitions could be put in place, but if not, the Member States would, instead, need UNODC's assessment of why definitions could not be agreed, as well as an assessment of the elements which would be common to most or all States and the elements where needs or views diverged. There was also some discussion of whether there was a relationship between discrepancies in domestic law and displacement or "forum shopping" by offenders. It was noted that in view of the easier access to information technologies, it was possible for offenders to route communications or target victims to take maximum advantage of any gaps in offence provisions or investigative powers or capacity.

14. One speaker made a technical presentation on the elements of identity theft, similar to some degree with the typology being developed in the G8 context. He highlighted several stages of conduct, including obtaining, transferring and using identity documents or information. He also noted that law makers were starting to criminalize preparation in order to intervene at an earlier stage, but there were problems with this, as some preparatory conduct, such as obtaining personal information from open public sources, could be done for innocuous purposes unrelated to identity crime. This was also complicated by differences in national identity infrastructures and the fact that different additional identifiers were used by different systems. In addition, identity information was sometimes offered voluntarily and not stolen, and as in cybercrime offences, theft and property offences did not always extent to taking or copying intangible data. National approaches to criminalization included attempts to develop single comprehensive offences and clusters of offences covering specific aspects of the problem. Consideration of pre-existing offences was also a factor. In some areas, such as cybercrime, conduct was already criminalized whether related to identity crime or not.

15. There was some discussion of the legal and criminal concepts of preparatory acts. While it was useful in criminological terms to describe the complex identity and identity-related crime schemes that had been encountered, the legal concept of preparation raised questions of how each legislature chose to define crime and what specific crime a preparatory step was associated with. The members of the core group highlighted the need to devote particular attention to that issue.

16. Another speaker reviewed the progress made in the G8 context with regard to the development of a typology of identity offences. The G8 concept was to break down the conduct under scrutiny into four process stages: acquisition, transfer, manipulation and use. The focus was not on legal constructs but on what offenders actually did in each of these stages, in the hope that this would be equally useful as the basis of legislative advice in both common and civil law systems, and as a basic justification for each State to take legislative action, as appropriate. Under this concept, consideration was given, among others, to the difference between theft of tangible documents and "theft" of intangible data. Another parameter for further consideration included the kinds of techniques used by offenders, such as physical theft from locations or postal mail and theft from digital locations. The nature of the locations was also significant, as theft concepts tended to take place in locations which were not openly available. The problem of fragmented schemes involving various elements of crime in different jurisdictions was also significant, especially where early elements could be seen as preparatory for later ones or not. Efforts to protect the information could further be defeated by deception schemes that were not restricted within national boundaries such as "phishing". A range of secondary motivations was also considered, including fraud and concealment of criminal identity for various reasons. Overall, it was hoped that this approach would transcend differences between common law and civil law approaches, because of its focus on what criminals were doing, which was consistent globally.

17. In conclusion, it was agreed that some specific criminalization was beneficial and that it would not be practicable for the core group to try to engage in a definitional exercise itself. This, if it could be done at all, would be a matter for Member States. One option might be a procedural approach, in which issues and a

process could be suggested to competent national authorities. There was also agreement that the use of criminological descriptions was a way forward, in the sense that while national concepts and approached varied, they were all faced with essentially the same criminal behaviours. The need was to identify and describe those behaviours and further develop a typology so that Member States could decide how to respond, both individually and collectively. The role of UNODC as a "clearing house" to that effect was encouraged.

IV. Agenda item 6: International cooperation: the use of existing international legal instruments against transnational organized crime, corruption and cybercrime

18. Under this agenda item, the Rapporteur of the core group noted that the intergovernmental expert group in charge of the United Nations study had concluded that, while evidence was limited, it was likely that the majority of serious transnational identity crime would involve "organized criminal groups" within the meaning of Article 2, subparagraph (a) of the United Nations Convention against Transnational Organized Crime (Palermo Convention).[2] It had therefore recommended that further deliberations focus on the development of materials to support the most effective use of the existing international legal instruments, as opposed to the creation of any new ones. He also noted that, unlike international cooperation with respect to some other forms of crime, the role of private sector entities complicated international cooperation with respect to identity-related crime. With the involvement of multinational companies and transnational criminal investigations, two cooperative frameworks existed in effect, each operating in accordance with different principles. Where the public sector was constrained by factors such as sovereignty and human rights considerations, the private sector had concerns about customer privacy and confidence, commercial and other interests. There were also constraints on the sharing of information between these two systems.

19. The Rapporteur also noted that one specific option raised at the first meeting of the core group in Courmayeur had been the possibility of developing materials to support the use of the Palermo Convention and its Protocols against identity-related crime. It was pointed out, in this connection, that identity-related crime per se was not expressly mentioned in the text of the Convention, but two closely-related offences, participation in an organized criminal group and money-laundering, were specifically established by that instrument. Furthermore, other offences such as identity theft, identity fraud, trafficking in identity information or documents and conventional economic fraud would fall within its scope of application for purposes of investigation and prosecution if they were criminalized as "serious crimes" within the meaning of Article 2, and met the transnationality and organized crime requirements of Articles 2 and 3. With respect to the strengthening of identity and document or information infrastructures, Articles 12 and 13 of the Protocols against trafficking in persons and the smuggling of migrants both dealt with the creation and verification of travel or identity documents. The third Protocol on the illicit manufacture of and trafficking in firearms focused on the unique identification of

[2] General Assembly resolution 55/25, annex I.

firearms and not persons. However, it contained provisions governing record-keeping, tracing, and the licensing of import, export and brokering activities that would generally require the ability to identify the legal or natural persons permitted to operate legally under the Protocol and the implementing legislation in various States Parties.

20. There was general agreement that the core group should recommend that the United Nations Office on Drugs and Crime pursue the development of materials on the use of the Convention, in line with the mandate of ECOSOC resolution 2004/26 (paragraph 5). It was further agreed that this would also be a matter for the Conference of the Parties to the Convention. It was also felt that the formulation of the materials and the extent that they would be a separate document or integrated into more general materials on the use of the Convention could be left to the secretariat.

21. There was also discussion of the fact that a significant part of the identity-crime problem involved information and communications technologies and that conventional approaches to mutual legal assistance were not seen as adequate to deal with many cybercrime cases. Where the Internet and similar technologies were used for purposes such as obtaining or trafficking in identity information, much faster forms of cooperative investigative measures were needed to deal with the offences in real time, as opposed to the more formal and time-consuming channels for mutual legal assistance. Otherwise significant evidence could be removed or destroyed by offenders or lost through automatic erasure. It was noted that legal aspects of these faster forms of investigation were addressed by the Council of Europe Convention on Cybercrime,[3] while practical aspects were addressed by the "24/7" network for cooperation in such cases. There was also discussion of the relationship between the Convention on Cybercrime and its secretariat and UNODC, in its capacity as guardian for the implementation of the Palermo Convention and secretariat of its Conference of the Parties. Bearing in mind that the Convention on Cybercrime was open to non-European countries and was in fact being recommended to other States as a global legal instrument, there was agreement that more enhanced cooperation be pursued between the two secretariats and that UNODC might also take advantage of materials relating to the implementation of the Convention on Cybercrime.

22. The possibility of cooperation with UNCITRAL and other intergovernmental bodies, as well as the use of international instruments relating to non-crime matters was also discussed. The representative of the UNCITRAL secretariat noted that there had been a long and useful collaboration between those engaged in work on commercial fraud issues mandated by UNCITRAL.[4] However, the focus was on issues of commercial issues, leaving work on the criminal aspects of fraud and identity-related crime to the Commission on Crime Prevention and Criminal Justice. She also noted, however, that UNCITRAL could continue to play some role, particularly with respect to generally bringing the commercial perspective to the present deliberations.

---

[3] Council of Europe, *European Treaty Series*, No. 185.

[4] Secretariat Note to the 36th session of UNCITRAL: "Possible future work on commercial fraud", E/CN.9/540, 2003, Report of UNCITRAL to the UNGA, A/58/17, paragraphs 231-241, and report on the April 2004 Colloquium on commercial fraud, A/CN.9/555.

23. The possibility of using other European instruments and other intergovernmental organizations was also raised and it was noted that a list of possible organizations was compiled following the Courmayeur meeting with the assistance of the representative from the OECD. Members of the core group agreed to consider whether other organizations and instruments should be added, and if so, to provide details to the secretariat or Rapporteur in order to expand the list.

V. Agenda item 7: Public/private partnerships to prevent and control identity-related crime

24. The Rapporteur of the core group reviewed issues raised in the Courmayeur meeting, noting that while there were some differences in the motivations and concerns of companies and governments, at a more fundamental level, both shared the goals of suppressing identity-related crime, protecting customers from victimization and fostering conditions in which commercial and other activities could be carried on with confidence in an environment of relative safety and security. The Chairman called for concrete suggestions as to how public and private cooperation should be structured. Questions raised, in this regard, revolved around the needs of each sector, who should define them, and on what basis. One speaker commented that a recurring issue, and common to concerns on both sides, was the need for accuracy and reliability with respect to the initial input of information or registration of individuals. Without verifiable accuracy at that stage of the process, even the most sophisticated biometric technologies could not be relied upon, and could actually cause harm if the most basic information for critical functions was incorrect. Examples of this had also been encountered with attempts at the establishment of basic digital identities, in which offenders had simply created false ones. Another speaker mentioned cases where offenders had represented themselves as victims of identity-theft to obtain official assistance in obtaining new, and false, identities. Another speaker pointed out that, even if the basic identity information could be verified, failures were experienced in applications such as passport controls, where high volumes were a disincentive to verify significant numbers of persons, documents and identities. He also noted that many of these issues differed significantly within the private sector, depending on the nature of the business, availability of technologies, applicable laws and assessment of criminal threats.

25. These issues were seen as a challenge for the private sector in several ways:

- First, there were many commercial applications where companies faced the same challenge of establishing large numbers of basic identities, and verifying them in systems with high transaction volumes;
- Second, the demands posed by these fundamental challenges could be different depending on specific applications or fact situations, which was a challenge for companies tasked with developing and marketing appropriate technologies; and
- Third, the legal and technical operating environments in which systems needed to function efficiently and accurately varied widely, a particular challenge for multinational companies or those with wide-ranging or diversified activities.

26. There was discussion of issues raised by the need for information-sharing for preventive, investigative or other purposes. Companies often had commercial concerns that disclosure would deter customers or generate civil liability, while government entities (and in some jurisdictions, companies) were generally bound by privacy rights and restrictions. The need for high-speed sharing in some investigative scenarios and for situational crime prevention was also raised. Another concern was the need to bring together expertise. One speaker noted that some of those issues differed with respect to different forms of crime. To a certain extent, commercial activities tended to cluster themselves around common activities or interests, and one speaker suggested that it might be useful to consider a typology of different crimes, developing clusters on the basis of developing common solutions to some of the problems. Another speaker noted that, while cooperation was desirable, it might not have much impact in the absence of practical advice on what sort of crime was being committed and what should be done in response. He also noted that general statements about the importance of cooperation were useful, but more focused attention was needed to deal with differences in the need for, and nature of, cooperation in different circumstances. Another speaker noted that the UNCITRAL secretariat had used a colloquium to assemble diverse interest and draw common lessons, which had eventually led to the development of commercial fraud indicators used in awareness-raising and prevention. The idea had been to develop and disseminate general materials in a form that would then allow each industry to make individual adjustments to suit particular needs. Several speakers observed that it was usually easier to obtain cooperation in sharing information for prevention than for criminal investigations, both because of the reason for sharing and the nature of the information likely to be involved. The Chairman summarized the general discussion, and suggested that the core group focus on specific partnerships between companies and governments, as well as on how UNODC could be advised to facilitate them, taking into account objectives and obstacles. The Rapporteur of the core group also noted that the participation of the in the work of the intergovernmental process was desirable, and that cooperation with the private sector was a probable issue for thematic discussions at the eighteenth session of the Commission on Crime Prevention and Criminal Justice, to be held in April 2009. However, the exact nature of participation would have to be considered in accordance with more fundamental and general United Nations practice.

27. One speaker noted that there were many forums where public and private organizations and experts already collaborated. Examples included the Anti-Phishing Working Group and the Digital Phishnet (DPN), which was established in 2004 as a collaborative enforcement operation to unite industry leaders in technology, banking, financial services and online retail services with law enforcement authorities to combat phishing. An additional example was that of the London Action Plan, an international spam enforcement network aimed at promoting cooperation to address spam-related problems.

28. It was further noted that some of the Courmayeur deliberations on this agenda item had a practical focus, while others were more directed towards policy or legislative issues, and given the nature of the subject matter, many were international in nature. Policy issues went beyond information-sharing and there were some differences in the interests of each side. One example was policy proposals suggesting that companies be required (in some jurisdictions they are already required) to disclose the risks of victimization and/or actual breaches of data

security or compromises of customer data. It was argued, in this regard, that crime prevention and mitigation generally favoured such requirements, but companies had concerns about loss of customer confidence. The dynamics of cooperation were also considered. One speaker noted that, given the incentives, cooperation could be driven from either the public or private side, and by the specifics of particular commercial interests and State interests, as well as forms of crime or crime prevention and other factors. In that sense, there would be no general pattern.

29. Some other concerns commonly raised by companies were also discussed. One that seemed common to many companies was the concern about prescriptive requirements from governments without the necessary assistance to meet them. One example of this was requirements that companies such as financial institutions or communications providers know or identify their customers in jurisdictions where the infrastructure or capacity needed for them to check identities against public records were lacking or legal restrictions on access existed. One speaker noted that there was a difference in such cases between obligations to obtain and record identity information in commercial dealings and obligations to actually identify the parties involved. The Rapporteur of the core group questioned whether this also raised more fundamental issues with respect to the boundary between public and private functions. While companies often had commercial reasons for identifying customers, identification to prevent or prosecute crime was a State function. The Chairman noted that some aspects of those issues went beyond the scope of measures against identity-related crime and could be matters of some sensitivity to governments. Several speakers noted that, while crime-control and national security applications tended to attract prescriptive responses from governments, there were more consultative and less prescriptive models which could help assess the problem of identity-related crime and develop appropriate responses. There was general agreement that further consultations between UNODC and private sector entities should be carried out with this model in mind.

VI. Agenda item 8: Prevention of identity-related crime

30. Previous discussions and research on this issue had considered prevention to be divided into situational, strategic and technical prevention. The Rapporteur of the core group explained that this typology had been developed in view of the range of specific measures likely to be developed and the proponents and audiences for each. Generally, strategic and situational prevention both involved the development and dissemination of information to alert target audiences of the risks and means of prevention or reduction of those risks. Strategic prevention was of a very general nature and would be directed at relatively large audiences, such as the entire customer base of a company or industry or the population of a Member State, based on the general characteristics of identity crimes. Situational prevention was more focused and had a reactive nature, particularly focusing on gathering information about specific criminal schemes and disseminating it to individuals or groups seen as likely to be targeted or other specific groups such as commercial employees in a position to identify and disrupt or report the offences as they occurred. A key difference was that situational prevention would often require the rapid sharing and dissemination of information. Technical prevention focused on the use of technologies, as opposed to information-sharing, to secure information and systems

against intrusion and the theft and trafficking of data or to identify suspicious activities in time to allow for them to be interrupted if necessary. It was noted that those categories were not necessarily intended to be definitive or mutually exclusive, but were seen as useful in view of the range of prevention materials and activities that might be developed.

31. The role of technologies in prevention was also discussed. It was noted that many new technologies had been effectively deployed to protect documents, systems and identity information. For example, the International Civil Aviation Organization (ICAO) technical standards had led to improvements in machine-readable and forgery-resistant passports, and public key infrastructure (PKI) encryption technologies were protecting most government and private identity and commercial systems. The advent of technologies to generate, store and read biometric identifiers was seen as a major step forward, but as with other identity infrastructure elements, it was noted that the technologies could only ever be as reliable as the information initially recorded in them. It was still essential, in the case of biometric systems for example, to ensure that the initial identification of each biological individual linked to the data be accurate and verifiable.

32. The core group also considered the role of UNODC and the private sector in the field of prevention. It was noted that, in general terms, the area of prevention was the one likely to engage the most private sector interests and the greatest need for cooperation, because the private sector generally had the best access to both up-to-date information from customers and the customers and employees themselves. Companies were also the source of security and prevention technologies, as well as the operators of many of the identity systems in which such technologies were applied. Regarding UNODC, given the availability of the necessary resources, it had some in-house capacity, but often functioned as a linkage or broker, identifying problems or needs, and bringing these together with the donor resources and technical expertise needed to respond. This was more practicable in some scenarios than others. It was a viable model, for example, for drawing together the experts needed for general policy development and training matters, and for assembling and disseminating strategic prevention materials. However, it did not meet the legal standards needed for functions such as mutual legal assistance, and it was not fast enough for UNODC to play a role in the transmission of information for situational prevention. In relation to technologies, the members of the core group agreed that UNODC could play a general role in assessing and disseminating information about technological options and focus on awareness raising activities, but that it was neither feasible nor desirable for it to take a more active role in dealing with specific products.

33. The question of whether the core group could propose or recommend the development of minimum standards for basic identity registration, or the initial linking of each individual to his or her biometric and other identity information, was raised. It was noted that, as a matter of general identity infrastructure, the implementation of such a recommendation would go beyond the prevention of crime, but UNODC could be asked to identify this as a fundamental problem and one in which crime prevention experts should be involved in addressing. It was also noted that this applied equally to public and private sector infrastructures.

VII. Agenda item 9: Protection of victims

34. There was discussion of the different types of victims created by identity offences, including both natural and legal persons whose identities were misused, as well as natural and legal persons victimized by secondary or related offences such as fraud or terrorism. There was general agreement that the core group should recommend that future work focus on natural persons whose identities were compromised for several reasons. Those victimized by secondary offences were generally already the subject of policy and legal measures and processes outside of the scope of identity-related crime, while the compromise of the identities of legal persons was considered by most States as a criminal or civil problem relating to trade-marks and other forms of intellectual property. Generally, the group felt that the new issues to be addressed related to natural persons, including matters such as compensation, mitigation and the repair or restoration of identity information in public and private sources and at the domestic and international levels.

35. The core group also devoted attention to best practices with respect to victims and the possible compilation of a compendium containing such practices. It was noted that, while there had been extensive work done on victims issues, identity-related crime was still an emerging concept requiring further attention especially regarding its impact on victims. It was also pointed out that, as with other aspects of identity-related crime, much of the information and practices with respect to victims would have been developed within various elements of the private sector. Bearing this in mind, the core group decided to recommend that the UNODC, in consultation with appropriate private sector sources, develop a compendium of best practices for dealing with victims.

36. The members of the core group also exchanged views on the legal basis for identity and the relationship between basic human rights at the domestic and international level and identity. Recalling the discussions of the Courmayeur meeting, the group noted that identity was a basic human right in international law. One issue emerging, in this regard, was the extent of the obligation that this might create upon States to take criminal or other measures to protect identity, and whether it triggered any further rights, such as a right to the restoration of identity, for victims whose identities had been compromised. The group stressed the need to take into account in this context the fact that victimization and further harm tended to continue to accrue to victims as offences continued, and in many cases even after offenders had been caught and convicted. One speaker referred to the use of judicial orders or public declarations to limit the damage, noting that while victims had privacy rights, their interests and right to mitigation, if any, favoured public disclosure of the offence and notification that they, as individuals, were not legally responsible for the actions of offenders taken in their names. In such scenarios the right to identity might have priority over the right to privacy. This, however, did not address the problem beyond the jurisdiction of the court which convicted the offender or made an identity declaration. Another expert noted that offenders sometimes were trying to use victim mechanisms themselves, to create new false identities. The core group agreed that this area needed further consideration, possibly involving experts on international legal standards relating to human rights and identity, and decided to recommend that UNODC undertake an assessment of the international legal basis of identity and rights to identity.

VIII. Agenda item 10: The protection of corporate identity and other intellectual property rights

37. The core group agreed that crimes involving the identities of legal persons were part of the overall subject of identity-related crime. However, they also raised a number of civil and other non-criminal legal issues which were the subject of deliberations in other forums. It was acknowledged that the taking and misuse of the identities of legal persons, including commercial companies and intergovernmental and non-governmental entities was often encountered both as an element of identity crimes against natural persons and an element of identity-related crimes such as economic fraud schemes. The group felt that many issues relating to corporate identity crime could probably not be addressed by Member States until they had first done more to assess the nature and scope of identity-related crime in general, as well as the more immediate challenges of dealing effectively with crimes against the identities of natural persons. There was general agreement that, in view of the other work recommended to UNODC, identity crime committed against legal persons was not a priority and should not be the subject of further attention at that stage of the process, except to the extent that matters of intellectual property and corporate identity might influence the development of policy options with respect to issues of more immediate priority. The Rapporteur of the core group and several speakers noted, however, that this might not necessarily extend to work on prevention or investigation.

IX. Agenda item 11: Technical assistance

38. There was general agreement that the development and delivery of technical assistance would emerge as a major part of the overall work on identity-related crime, bearing in mind that UNODC had already been mandated to do this, subject to the availability of the necessary resources on an extrabudgetary basis.[5] Several speakers noted that UNODC would not be in a position to deliver most forms of assistance until much more information had been gathered and assessed and the necessary resources contributed. They also noted that even at that stage, its role would in some cases be more in the nature of a broker, identifying needs and assembling appropriate experts from public and private sources to respond. Most speakers agreed that the preliminary requirements would also include some form of framework for assessing and classifying needs and that these might vary depending on the extent of the assistance required. Project requests might range from relatively straightforward advice on legislative drafting or international cooperation matters to the establishment of complete public identity infrastructures in the context of major development or reconstruction projects and might be deliverable by UNODC alone or in coordination with other entities.

39. The Chairman stressed the importance of awareness-raising in terms of alerting Member States about the nature and extent of possible problems and the sources and availability of technical assistance for assessing and addressing them. It

[5] See E/RES/2007/20, paragraph 14, referring to "…, legal expertise or other forms of technical assistance …".

was also noted that identity-related crime and the need for reliable identity infrastructures was a global problem and that awareness-raising targeting aid donors was an important element of the technical assistance agenda. In practical terms, as with other areas, the experts felt that UNODC had an important role, but that there were some limits on what it could realistically accomplish. Several speakers focused on the issue of the necessary resources and noted that UNODC would not generally have all of the in-house expertise or personnel needed, including the ability to advise with respect to specific technical products or keep such advice up-to-date.

40. The core group concluded that much of the early work needed to support the delivery of assistance was already underway, or would be undertaken if other recommendations were to follow. One key purpose of recommendations for gathering information and the development of materials on matters such as prevention and legislative measures was to form the basis of future technical assistance. The group therefore decided to recommend that the focus of immediate work in this area be on issues relating to assessment. Over the longer term, bearing in mind the group's recommendations in other areas, UNODC should:

- Develop capacity to deliver assistance in crime areas, such as criminalization, investigation and international cooperation, bearing in mind concerns about harmonization and common approaches;
- Develop the capacity to participate effectively in broader projects, conferences, and other identity-related events or processes, to ensure crime prevention and criminal justice aspects are recognised;
- Compile an inventory of materials and sources of assistance, as well as a roster of experts that could be made available to Member States or other processes where appropriate; and
- Generally seek to leverage its resources by functioning as a broker, helping to bring together Member States with sources of assistance.

X. Agenda item 12: Future composition of the core group

41. Regarding the size of the core group, it was the general view that meetings should involve 15-20 experts, although it was noted that the group itself might be larger, if not every member attended every meeting, depending on availability and the subject-matter on the agenda. There was general agreement that more representation was needed from the private sector and that such representation should reflect a greater diversity of commercial and other private sector interests. One speaker suggested that more than one companies from each sector could be represented and another raised the possibility of inviting experts from industry associations, where possible, to represent an entire range of companies. There was also general agreement that regional representation and representation from developing countries was a concern, which, in turn, raised the question of whether resources could be made available for the travel of experts from developing or least-developed countries. To manage overall size, one speaker raised the possibility of a small core group to ensure continuity and core expertise with a larger group or roster of experts to be invited when the subject matter on the agenda warranted this. Others suggested that the core group be maintained and that additional experts

simply be invited as necessary. The latter concept received general support. Several members of the core group offered to try to identify other experts in relevant areas, such as human rights, privacy, security, technological issues and development and reconstruction. The group decided to recommend that UNODC should develop an inventory of public and private sector expertise, bearing in mind the future work of the group.

XI. Resource issues

42. The core group noted that the relevant mandates of UNODC to carry out work in this field were all made contingent on the availability of the necessary extrabudgetary resources and that none of the recommendations could be implemented unless the financial resources, and in some cases the expertise, was first provided by Member States. It therefore decided to recommend that UNODC seek the necessary resources as expeditiously as possible, and expressed the hope that Member States would respond generously to ensure that work on this pressing problem would commence as quickly as possible.

XII. Conclusions and recommendations

43. At its first meeting, the core group made a number of observations about possible areas of work for UNODC and the report of that meeting also set out a number of possible recommendations. It was agreed that, subject to recommendations about possible priorities, a complete set of recommendations for future work should probably encompass the results of both meetings.

(a) *Further information gathering*. Both meetings noted the need to review existing sources of information and compile as much as possible for analysis, bearing in mind that most of the information available would be either qualitative assessments of the problems and solutions from other expert sources or quantitative information gathered by specific sources, usually commercial ones, for purposes different than those of UNODC. **Accordingly, the core group recommends that UNODC undertake further information gathering and analysis with respect to the extent of identity-related crime, specific cases or scenarios and specific responses proposed or implemented by governments and various private sector entities.**

(b) *Further consultations with the private sector*. Both meetings noted that, while private sector entities had begun to be involved in related issues, there was still a general lack of information as to what some key private sector interests were and whether they were specific to individual commercial sectors or were shared more broadly. **The core group therefore recommends that UNODC conduct further consultations, in cooperation with the UNCITRAL secretariat, to encourage participation, generally build confidence and identify specific private sector concerns, including in areas such as information-sharing, bearing in mind also the ongoing work of the OECD in this area. Such consultations could be of a general nature, but the inclusion of specific issues or elements was deemed appropriate. In particular:**

(i) A range of prescriptive and consultative models for assessing problems and developing and implementing policy options is available. While prescriptive models have often been followed by governments in national security and crime-control matters, bearing in mind the need for effective cooperation against a mutual problem, consultative options should be identified, considered and recommended to companies and Member States to the greatest extent possible;[6]

(ii) Private sector entities gather information and often have more extensive and detailed information than governments, but such information is gathered for commercial purposes and often considered as sensitive in commercial and privacy terms. Consultations should consider ways and means of reassuring and persuading private sector entities to share appropriate information, as well as ways of analysing and reporting on information which takes into account the reasons for which it was collected and the private and public sector need to develop effective strategies against crime;

(iii) Strategies for preventing and responding to identity-related crime should take into account underlying identity infrastructures. State infrastructures vary, but the private sector also has its own approaches to establishing and verifying identity, taking into consideration its commercial nature and needs. Consultations should explore the similarities and differences between public and private identity infrastructures at the domestic and international levels, with a view to developing comprehensive and coordinated strategies;

(iv) The intergovernmental expert group noted that the development of criteria that could be used to identify suspicious activities or transactions could be used to screen mass telecommunications or commercial transactions for possible cases of economic fraud and identity-related crime. Consultations should explore, inter alia, the following:

- **What criteria may serve such a purpose;**
- **How those criteria can be developed and kept up to date;**
- **How they can be used effectively to identify suspicious activities, bearing in mind commercial considerations and the need for privacy, human rights or other safeguards; and**
- **How public and private sector entities can effectively follow-up in cases where suspicious activities are identified.**

(v) Strategies for the prevention of economic fraud and identity-related crime encompass both situational elements and strategic elements, as well as a combination of technical security elements and awareness-raising, education or training elements. The private sector is both the primary source of technical prevention measures and the market for them, and is often in the best position to develop, update and implement education and training initiatives. The core group therefore recommends consultations in the following prevention areas:

---

[6] Paragraph 22.

- **The commercial and regulatory framework surrounding the development, marketing and use of technical security measures, and how the benefits of each can be maximized in terms of preventing, detecting and investigating crime, in reducing and recovering economic losses, and in reducing or mitigating non-economic harm associated with identity-related crime;**
- **The gathering and analysis of information from public and private sector sources needed to develop, implement and regularly update education and training programmes; and**
- **The nature and extent of programmes to educate customers and train employees to recognize, prevent or interrupt economic fraud and identity crime schemes, and how these can be coordinated or shared across both the public and private sectors and at the domestic and international levels.**

(vi) Joint consultations between law enforcement and the private sector can consider the incentives and impediments to effective cooperation in investigating and prosecuting offences and preventing and recovering losses, at the domestic and international levels, with a view to building confidence and maximizing investigative cooperation; and

(vii) The intergovernmental expert group in charge of the 2007 United Nations study identified particular concerns with respect to individual victims of identity-related crime whose identities have been misused. The restoration, repair or remediation of damage to identity and reputation poses a serious challenge, which involves domestic and international elements in both private and public sector identity infrastructures. The core group therefore recommends that consultations between public and private sector entities consider the range of remedial measures needed, and how these can be coordinated among the various interests and entities involved. Such consultations should also involve individual victims or representative interest groups, if possible.

(c) *Legislative measures against identity-related crime*. The report of the first meeting of the core group in Courmayeur set out a list of factors to be taken into account and interests to be protected should a State decide to develop identity-related offences. At its second meeting, the core group considered arguments for and against criminalization and the development of a typology based on criminal conduct rather than forensic definitions or criminal offence provisions. **The core group therefore recommends that UNODC be asked to develop or ensure the availability of the following materials, in coordination with ongoing work in the G8 Lyon/Roma Group, where appropriate:**

(i) A discussion paper setting out a typology of identity crimes. This can be based on one or more perspectives, including breaking down offender conduct into stages, as in the G8 work, but will be based on offender conduct, commercial practices and other factors which do not vary from one legal system to another. Work in this area should be done in coordination with the ongoing efforts of the G8 Lyon/Roma Group;

(ii) A discussion paper setting out the arguments in favour of establishing specific identity crimes, the concerns expressed by some States, and assessing the extent to which the same justifications applied in different legal systems, taking into consideration the arguments and issues set out in the present report, the report of the first meeting of the core group and the report of the intergovernmental expert group;[7]

(iii) A discussion paper assessing the various possible elements of criminal offences and issues that will at least need to be considered by drafters and legislators, with a view to developing a compendium of issues and options likely to be common to all types of legal system, and lists of issues likely to arise in or apply to only specific legal systems;

(iv) A discussion paper considering other relevant non-criminal legislative responses, including procedural, commercial, privacy and other matters;[8] **and**

(v) A compendium of examples of relevant legislation so that these can be made available to Member States. These may include both identity-specific offences and offences of more general application that States feel are useful in combating identity-related crime.

(d) *International cooperation in criminal matters*. There was general agreement that one priority task for UNODC in this field should be to develop materials relating to the use of the United Nations Convention against Transnational Organized Crime, in consultation with the Conference of the Parties to the Convention, for the assistance of legislators, investigators and prosecutors to ensure that this instrument will be available in appropriate cases.[9] There was also agreement that in fulfilling this task, the UNODC may also take advantage of other materials, including the Council of Europe Convention on Cybercrime and materials relating to its implementation and use. The UNODC can consult with the secretariat for that Convention with a view to exploring ways to share relevant materials and cooperate effectively.

(e) *Victims*. It is recommended that:

(i) UNODC should analyse the range of persons who are victims and focus future work on individual victims of primary identity-related crime;[10]

(ii) UNODC should assess the legal basis for establishment and restoration of identity and personal integrity; and

(iii) UNODC should compile an inventory of best practices for domestic and international remediation.

(f) *Technical assistance*. Bearing in mind that the capacity and materials to deliver technical assistance will be in place automatically if many of the other recommendations in the present report are implemented, the primary need at present

---

[7] See E/CN.15/2007/8, paragraph 22, and E/CN.15/2007/8/Add.3, paragraphs 2 and 12.

[8] See *OECD Policy Guidance On ID Theft*, http://www.oecd.org/dataoecd/49/39/40879136.pdf (English) and http://www.oecd.org/dataoecd/51/59/40883671.pdf (French).

[9] Paragraph 16.

[10] Paragraph 27.

is to build the necessary capacity to assess technical assistance needs. **The immediate focus should be on assessing the needs of the requesting State, taking into consideration the context in which the assistance will be delivered, including factors such as the requesting State's approach to other relevant criminal offences, migration and passport issues, human rights issues, commercial issues and the state of its general identity infrastructure. It is further recommended that:**

(i) UNODC should develop capacity to deliver assistance in crime areas, such as criminalization, investigation and international cooperation, bearing in mind concerns about harmonization and common approaches;

(ii) UNODC should be able to participate effectively in broader projects and conferences to ensure crime prevention and criminal justice aspects are recognized;

(iii) UNODC should compile an inventory of materials and sources of assistance and leverage its resources by functioning as a broker, helping to bring together Member States with sources of assistance; and

(iv) UNODC should develop a roster of experts for assessing the needs or the delivery of technical assistance.

(g) *Composition of the core group and future proceedings*. The core group is of the view that future work on identity-related crime and economic fraud will have to be dealt with separately, but bearing in mind the need for close coordination to exploit synergies and avoid duplication of work in both areas. It is recommended that:

(i) UNODC should follow a separate but coordinated approach to work on economic fraud and identity-related crime;

(ii) UNODC should develop an inventory of public and private sector actors needed for the future work of the core group; and

(iii) UNODC should consider the invitation of additional experts to meetings of the core group, where appropriate, to expand the scope of its expertise on an ad hoc basis.

(h) *Resources*

Bearing in mind that the implementation of all of its recommendations is contingent on the contribution of the necessary extrabudgetary resources by Member States, the core group recommends that UNODC seek the necessary resources as expeditiously as possible and expresses the hope that Member States will respond accordingly.