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"

Third meeting of the Core Group of Experts on Identity-Related Crime (Vienna, Austria, 20-22 January 2009)

I. Opening of the meeting and adoption of the Agenda

1. The third meeting of the core group on identity-related crime was convened by the Chairman, Ambassador Eugenio Curia, representative of the Government of Argentina in Vienna, on 20-22 January 2009. The meeting was based on a multi-stakeholder concept and, in addition to the Chairman, the following experts representing different stakeholders attended it:

a. Public sector: *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; *Betsy Broder*, Assistant Director, Privacy and Identity Protection, Office of International Affairs, Federal Trade Commission, United States of America; *Luc Vanneste*, Director General Institutions and Population Home Office, Belgium.

b. Private sector: *Caspar Bowden*, Chief Privacy Advisor for Europe, Middle East and Africa, Microsoft; *Darren Bird*, Regional Head Data Security & Fraud Control, PSR, Visa CEMEA United Kingdom; *Zan Jovanovski*, Data Security and Fraud Control Manager South Eastern Europe, Visa CEMEA; *Fons Knopjes*, ID Management Centre, Netherlands; *Lynn Griffin*, Barrister, Anti-Counterfeiting Group (ACG); *Peter Cassidy*, Anti-Phishing Working Group (APWG); *Anko Blokzijl*, CEO, Sdu Identification, Netherlands; *Ferdinard Piatti*, Price Waterhouse Coopers, Austria.

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

c. International organizations: *Brigitte Acoca*, Policy Analyst, Consumer Policy, Privacy and Information Security, OECD; *Jitu Thaker*, Facilitation Officer, Aviation Security and Facilitation Policy (SFP) Section, ICAO; *Kate Lannan*, Legal Officer, International Trade Law Division, UNCITRAL Secretariat; *Luca Castellani*, Legal Officer, International Trade Law Division, UNCITRAL Secretariat; *Demostenes Chryssikos*, Crime Prevention and Criminal Justice Officer, UNODC Secretariat.

d. Individual experts: *Marco Gercke*, Germany; *Philippa Lawson*, Canada.

2. The meeting was addressed by the Director of the Division for Treaty Affairs, UNODC, who welcomed the group to Vienna. She reviewed the proceedings of the first two meetings and the findings and recommendations made at the second meeting. She recommended that the core group go into more detailed review of key substantive issues, particularly with respect to victims of identity-related crime and legislative and legal issues. She also noted that the timing of the meeting was important, for several reasons. The subject matter was a thematic discussion topic at the forthcoming eighteenth session of the Commission on Crime Prevention and Criminal Justice, to be held in Vienna, Austria, on 16-24 April 2009. In addition to the items set out in the provisional agenda of the core group, she noted that the present meeting afforded the group an important opportunity to provide feedback on the structure and content of the thematic debate at the Commission. She further pointed out that the thematic discussion would likely result in a Commission resolution for adoption by the Economic and Social Council (ECOSOC), and invited experts to consider the subject matters that might be included in such a resolution. She also referred to the ongoing work of the G-8 Lyon/Roma Group, which was also considering policy and legal issues pertaining to the criminalization of identity abuses, and invited the members of the core group to consider this work with a view to identifying possible synergies.

3. The Chairman reviewed the ongoing work of the core group, as well as issues set out in the provisional agenda and matters arising from its previous meetings. He noted that the core group still lacked equitable geographical representation and that this was perhaps inevitable given the nature of the subject matter. He commended efforts of the secretariat to broaden the base of the core group and hoped that it would gradually become more representative in its future meetings. The Chairman reviewed the conclusions and recommendations of the 2007 intergovernmental expert group report[1] and the second meeting of the group, as well as the mandates arising from the two resolutions of the Economic and Social Council.[2] He further reviewed the provisional agenda and plan of work for the three days of the meeting. He noted that, in discussing identity-related crime, it was important to include the broader context of identity infrastructures from one State to another, and that some issues, such as the relationship between public and private sectors, were cross-cutting, touching on many different aspects of the subject matter. He also referred to the forthcoming thematic discussion at the eighteenth session of the Crime Commission, noting that he had taken up in the Commission Extended Bureau 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).

[2] ECOSOC resolutions 2004/26 and 2007/20.

discussion outline proposed by Canada. He suggested that the core group consider this draft and, if appropriate, propose revisions for the next Commission Bureau meeting. Over the longer term, the Chairman also noted that substantive preparations for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, to be held in Salvador, Brazil on 12-19 April 2010, were already underway and that identity-related crime was expected to arise both in its own right and as a possible sub-theme of other crime topics.

4. The members of the core group reviewed their experiences and work on identity-related crime, referred to practical aspects and pertinent problems and expressed the hope that the UNODC process would develop concrete practical responses.

II. Agenda item 5: Consideration of the discussion paper on "Legal approaches to criminalize identity theft"

5. The expert assigned by the secretariat to elaborate the paper (Prof. Marco Gercke) presented a brief overview of it. He outlined the gradual shift in means of establishing and using identity from face-to-face recognition and paper documents into more remote and automated electronic technologies. He further noted that this shift had been mirrored in patterns and methods of identity-related crime, as offenders had adapted sophisticated modus operandi to take advantage of new opportunities and weaknesses. One example was the rise in mass-scale crimes, which was made possible when offenders effectively automated criminal techniques and targeted large numbers of potential victims all at once. This was a dominant pattern in cybercrime and economic fraud and was now expanded to identity-related crime. The discussion paper included a range of terminology and definitions issues and set out problems encountered in developing precise criminological and legal definitions or descriptions. That was deemed appropriate in view of the different views of States and experts about what constituted identity theft/identity fraud, the typology of related conduct and whether criminalization per se could be a possible step. A major challenge which was underscored was to conceptualize the harmful conduct in a criminological sense and construct applicable legal definitions. This would have to be addressed both in general deliberations such as those in the present meeting or meetings in other forums, and in more practical processes in individual Member States focusing on the need to develop new or expanded criminal offences.

6. Another major challenge highlighted in the presentation of the discussion paper was the fact that many possible constituent elements of offences or other legislative measures, such as the concept of "identity information", were difficult to clarify or were subject to variations and divergent approaches among Member States. The expert/drafter of the paper reviewed four phases of identity-related crime, including:

- Preparation;
- Obtaining of identity information;
- Transfer of the identity information; and
- Eventual use of the identity information to commit further offences.

He raised doubts as to whether a single unified offence would be viable in most legal systems, but noted that it should be possible to address the problem through a combination of adjustments to existing crimes and the development of a series of new offences to address the novel forms of crime. He also noted that this was more than a legal challenge, and that it was necessary to take into account the technical aspects of identification, infrastructures and the methods of offenders.

7. The Rapporteur of the core group raised the question of terminology and definitions which had also emerged in the responses of Member States on which the 2007 study on “fraud and the criminal misuse and falsification of identity” had been based. With respect to conduct such as “phishing”, for example, three different approaches were reported: some Member States saw it as the taking of identity information and therefore as identity theft; others saw it as obtaining identity by deception, and therefore as a form of identity fraud; others, finally, argued that identity fraud was limited to scenarios involving deception using the false identity information as opposed to deception used to obtain it. This was the reason, along with the need to include trafficking in identity information, that the intergovernmental group had decided to discuss the issues in relation to “identity crime” or “identity-related crime”, as the context required.

8. Several members of the core group raised issues relating to the question of how preparatory conduct should be treated and defined. It was stressed that, as a substantial part of the exercise confronting the core group and Member States was to decide what forms of conduct were sufficiently harmful to warrant criminalization, the designation of preparatory conduct was similarly elastic and required serious consideration to ensure clarity. A number of experts noted that a key scenario in considering preparation issues was that of identity information being entirely fabricated and not taken from a real person. They underlined that, while the mere taking of genuine identity information caused harm to the person it identified and could therefore form the basis of a new or expanded criminal offence, the mere fabrication of false identities lacked that element and could in many cases only be dealt with as preparatory to other crimes that might be committed at a later stage, such as fraud.

9. At a more general level, the members of the group agreed that, in developing materials with respect to criminalization and other legislative responses to identity-related crime, it was important to adopt a flexible approach. It was not necessary to produce fully-developed materials such as model laws, as these were problematic for some Member States and would often not be viable without substantial modifications that would take into account the domestic context and requirements. A better approach was to develop more basic constituent elements which could be used by national authorities to meet their own individual needs, as well as by the secretariat in developing technical assistance materials for use at the national, regional or subregional levels.

10. One speaker noted that criminalization needed to be considered in the more general context of identity infrastructures. He stressed that the means of establishing identity and linking identifying information to actual persons needed to be sufficiently reliable to support criminal and other measures. He also pointed out that it was necessary to consider offences in terms of seriousness, as there were minor abuses of identity documents, such as false proof of age used to purchase alcohol,

which would technically qualify as identity crime offences, but were not sufficiently serious to warrant international attention.

11. Another speaker referred to the ongoing work of the G-8 Lyon/Roma Group on related issues. In this connection, he identified a number of similarities and differences between the G-8 approach to the typology of identity-related crime and that reflected in the discussion paper under consideration. He also made reference to the February 2009 meeting of the G-8 Group and its aim to finalize a report on typology and criminalization of identity-related crime. From a substantive point of view, the expert stressed that the G-8 had decided to follow a practical approach focusing on the actual act of identity abuse and resorted to a five-phases typology breakdown to describe the criminal offence in question, as follows:

- Acquisition of identity, involving both cyber and non-cyber acts, as well as from public and private (theft) sources;
- Transfer (trafficking) of basic identity information or data (also divided into cyber/non-cyber acts and from public/private sources);
- Manipulation of basic identity information, consisting of changing or using the identity information to produce documents or other instrumentalities capable of use for other crimes;
- Transfer at a second level, where further transfer of manipulated information or documents was made to other offenders for actual use in crime; and,
- Actual use of the manipulated information or documents for other crimes such as fraud.

12. The same speaker also noted that the G-8 was focusing on a more empirical typology of identity-related crime based mostly on law enforcement and intended to be broad enough to meet different national needs. He further mentioned that, although the G-8 approach was intended to be technologically neutral, much of the work would involve changes needed to address the evolution of old crimes towards exploiting new technological opportunities. The Rapporteur of the core group pointed out that all complexities of identity crimes were driven by the evolution of technologies and the conduct of offenders exploiting them. Another speaker agreed that the basis of the G-8 work was to develop concepts of identity crimes on a factual and empirical basis, but noted that the challenge was to develop legal structures that would include all essential elements without being overbroad. In general, the agreement emerging on basic elements and typological phases was seen as a very positive development. Other speakers noted that there was a range of approaches possible to limit the scope of offences in different legal systems to ensure that innocent conduct was not criminalized, including limiting crimes to conducts such as possession or transfer without authorization or lawful authority, or to conducts undertaken for the purpose of committing other offences.

13. There was also discussion of the approach taken by the G-8 in cases where identity information about real persons and fictitious identity information were involved. It was stressed, in this regard, that complete fabrication raised many similar issues at the later stages of the typology of identity-related crime, but was more problematic at the early stages, because it was less harmful than the taking of the information of a real person. One speaker highlighted the implications of cyber

versus non-cyber aspects of the various phases. This could have significant implications for national legislative responses.

14. There was also discussion on the links between the output of the G-8 process and the UNODC work to develop materials that would be useful for non G-8 States. Possible complementarities were discussed, while the Rapporteur of the core group recalled that an important function of UNODC, arising from its mandates, was to develop useful practices, guidelines or other materials in the prevention, investigation and prosecution of identity-related crime and deliver legal expertise or other forms of technical assistance in this field, subject to the availability of resources.

III. Agenda item 6: Compilation of examples of legislation on identity-related crime – Inventory of materials and sources of assistance

15. The Chairman noted that, as identity-related crime was a relatively novel concept, the range of materials was limited. The Rapporteur of the core group underlined that the group and UNODC had proposed a compilation of national legislation, but this had raised a number of questions as to what sorts of legislation should be compiled. While there were a few examples of specific identity crime offences, there was also a broader and richer array of other laws addressing the subject in part or dealing with related conduct and problems. In addition, there were also questions regarding the compilation of other sources and materials and the gathering of information in other languages. The number of academic articles was not excessive at present, but the number of mass media articles was far too large and the only viable approach was to collect representative samples.

16. Another issue raised was the basic purpose of assembling the information. Among the objectives mentioned were the conducting of basic research, the assistance to Member States in this field, the support of technical assistance and the provision of materials to raise awareness and motivate action against the problem. Each of these objectives, however, might have different informational requirements. The Chairman noted that other UNODC compilations of material, especially those of legislative nature, had taken a broad approach to permit ready access and handle high volumes of material. It was further recalled that in the study on “fraud and the criminal misuse and falsification of identity”, the broad scope and various parameters of the problems posed by identity-related crime had been highlighted with the note, at the same time, that the only available government statistics thus far had come from the United States, supplemented by some limited statistics from specific elements of the private sector. One speaker suggested that there was a need for compiling information on both identity crime and related offences or problems, such as hacking and other forms of cybercrime, to ensure a complete picture. It was the general understanding of the group that its members could submit items they felt were relevant for compilation by the secretariat and that some thematic labelling and sorting might be helpful.

17. There was also discussion about how articles and data compiled should be analyzed and used. Several speakers raised concerns about methodological challenges for classifying and counting identity-related offences. One speaker noted

that occurrences could be divided into computer offences and non-computer offences, although there would be some that fell into both groups. Another speaker noted that there would be some similarity to counting predicate offences in money-laundering schemes, in the sense that identity crime offences could often be associated with secondary crimes committed through the use of stolen or fabricated identities. The core group saw a need to develop a metric framework for types of crime and for analysis of specific aspects of the problem. One speaker raised the issue of international counting: given the transnational nature of the crime, and similarly to fraud, a single offence could be counted in one or more countries, and the frequency of mass-victim offences would make a substantial difference between statistics based on counting offenders, offences, or victims. It was also noted that, while measurement was important, there was also a need for qualitative analysis both to advise on how to gather data and to provide appropriate explanations and substantive feedback. In discussing the possibility of further research, concerns about potential "questionnaire fatigue", raised in the context of the Commission on Crime Prevention and Criminal Justice and the Conference of the Parties to the United Nations Convention against Transnational Organized Crime, were outlined.

18. Possible data sources and methodologies for counting cases to demonstrate the true levels and seriousness of offending were discussed. It was stressed that there were several possibilities, each with strengths and weaknesses, and multiple sources were seen as necessary for a complete picture. One good source identified was that of the victims. Moreover, private sector entities could further provide assistance, although data available to them were often not disclosed due to client privacy issues.

IV. Agenda item 7: Investigative and law enforcement approaches to identity-related crime

19. Under this agenda item, one speaker outlined case experience gained by the U.S. Federal Trade Commission (FTC). She stressed that one of the issues encountered was that of information-sharing and the subsequent conflicts related to the commercial value of information and the various obligations between providers and customers to keep such information confidential unless required to disclose it. Other issues included the obligation of commercial providers to protect data, as well as the misrepresentations to customers about the degree of protection accorded to sensitive data containing personal or identity information. Regulators also faced a challenge in setting standards and norms based on experience with criminal offences and practices, while, at the same time, reflecting practical approaches and commercial realities. It was further mentioned that many cases arose where even the most basic reasonable steps to protect data were not taken, such as major databases accessible by a single password available to large numbers of employees, or software not modified to be secure against well-known threats. The failure to act quickly to limit harm when an intrusion occurred was also a problem, and this triggered debates around the question of whether companies should be required to disclose intrusions or not. The approach of the Federal Trade Commission was mostly injunctive, using court orders to require businesses to fix problems, followed-up by regular audits to check compliance. Types of harm encountered included financial, reputational and systemic or State damages. As a regulatory

agency, the FTC considered law enforcement as an important, but not the only element of counter-action. Non-coercive tools were often faster, easier and could in some cases be more effective.

20. One speaker suggested that UNODC could gather as much information as possible about how investigators were dealing with identity crime cases, synthesize models based on typical cases, and then use these as the basis for developing technical assistance materials to train investigators. A number of speakers stressed the need to include that type of information in a format that would be useful for technical assistance, but no longer sensitive to its sources, although it was acknowledged that this might raise commercial and law enforcement concerns.

21. The Chairman noted that the development of materials and delivery of training was also affected by the rapid evolution of technologies and criminal methods, as well as by resource issues, but that many of the same methods used for economic crime in other areas would probably also work in the field of identity-related crime. However, as other speakers pointed out, the lack of a single typology for identity-related crime might make it difficult to develop universally applicable materials.

22. The Rapporteur of the core group noted that technical assistance materials should address both economic fraud and identity crime in a modular fashion to permit use in different scenarios. He further underlined that these materials should incorporate:

- Information about the content and possible use of the United Nations Convention against Transnational Organized Crime; and
- Elements and, if possible, case studies relating to the involvement of the private sector, including investigative cooperation and the design of technical and information systems in ways which, subject to privacy and other concerns, were supportive of crime detection and investigation.

23. Moreover, the members of the group agreed that technical assistance materials should also include elements to support the domestic aspects of multinational investigations. It was argued that such materials should suggest ways to leverage investigative resources and demonstrate to sceptics that multinational investigations could be successfully completed. One of these ways could be the establishment at the regional and subregional levels of dedicated law enforcement units with appropriate training and expertise. In the same vein, the following were suggested as possible good practices:

- The compilation of case studies illustrating the possibility of cooperation with counterparts in foreign countries; and
- The development of guides designed to enable law enforcement officers to identify elements of identity-related crime when the latter was encountered in other investigations;[3]

[3] One speaker noted that the Council of Europe had adopted in April 2008 “Guidelines for the cooperation between law enforcement and internet service providers against cybercrime”, which did not cover other crimes, but contained a number of suggested measures that could be of relevance in the field of identity-related crime.

24. One speaker expressed his concern that there might be a large number of cases never attracting the attention of investigators. He further noted that investigative steps could be quite complex and referred to the example of research in Dutch police databases which had found cases where one set of fingerprints were linked to up to 50 identities. The same speaker noted that law enforcement was only one element of a successful strategy against identity abuses for criminal purposes. Therefore there was a need to work out a broad package of different measures for training, including basic awareness-raising, as well as focus on preventing specific identity crime elements within bigger criminal schemes. Moreover, the overhaul of entire identity infrastructures might be required in some cases although it was a major and very expensive effort.

25. To further elaborate on his arguments mentioned above, the same speaker delivered a technical presentation on materials developed for use in teaching “master classes” on identity management aspects. The materials summarized the major issues encountered in establishing and managing identity infrastructures, focusing on the overall process and result. In discussion, consideration was given to elements to build and maintain public understanding and support and to address concerns such as the need for privacy protections and safeguards against use for repressive purposes. Several speakers raised the fact that there was, on the one hand, a technical element in relation to assuring that identity infrastructures were effective, efficient, reliable and resistant to deception or subversion, and a policy, political and human rights element, on the other, in that human rights were affected by the gathering, retention and use of data. This was also a factor in assessing the overall viability and structure of technical assistance for individual States. In some cases, broader protections and safeguards were already in place, while in others such elements might need to be included. Some of these questions would be beyond the scope of identity issues and expertise and would generate a need to coordinate with other groups and experts.

26. A second technical presentation on “European Governmental Identity Systems” was also made by the same speaker focusing on crime and trends of identity-related crime in Europe. A key element arising from that presentation was the fact that not much actual data had been gathered or compiled and that there was a need to accomplish this through the identification of certain criteria. There was also a need for greater coordination and cooperation across Europe with respect to identity infrastructures and management. In discussion, the members of the group exchanged views on the scope of the working definitions used in the presentation. It was mentioned that the definitional concepts used were narrow to enable more manageable approaches (e.g., limited to specific uses and public documents). One more fundamental underlying issue with respect to further work and technical assistance would be to identify similarities and differences between public and private sector identity infrastructures and the implications for criminalization, crime prevention and other such areas. It was also noted that there were concerns on the part of privacy groups about biometric technologies which could be very reliable, but, when successfully subverted by offenders, may result in much more serious offences.

V. Agenda item 8: International cooperation: challenges and difficulties pertaining, in particular, to mutual legal assistance and law enforcement cooperation

27. Under this agenda item, the Chairman noted that, despite the transnational nature of many forms of identity-related crime, not much was known about mutual legal assistance or law enforcement cooperation to combat it, especially from a practical standpoint. Unlike the subject of money-laundering, for which the Egmont Group has accumulated much experience, there was little available for this new form of crime. One speaker highlighted that some useful indications might be drawn in this field from the extensive experience of the investigative authorities in Canada and the United States dealing with cross-border fraud cases, many of which involved identity elements.

28. In general, the core group was of the opinion that particular attention should be devoted in future to strengthening law enforcement cooperation to combat identity-related crime, because, similarly to cybercrime, cooperation in real time was often essential to obtaining critical evidence and halting ongoing schemes before large numbers of victims could be targeted. It was further underscored, in this regard, that the traditional mutual legal assistance mechanisms might be adequate to support prosecutions, but were not fast enough to support modern high-tech investigations. An additional issue raised by one speaker was that in formal mutual legal assistance requests the application of the double criminality requirement might be more problematic, as few States had established identity offences per se.[4] Therefore the use of informal schemes of cooperation, in accordance with the domestic laws of the cooperating States, was recommended. In addition, administrative cooperation was also seen as an important tool deserving significant attention.

29. At the normative level, the members of the core group stressed that the United Nations Convention against Transnational Organized Crime[5] and the Convention on Cybercrime,[6] as well as existing bilateral or regional treaties, agreements or arrangements, provided a solid basis for international cooperation and therefore needed to be promoted. But there was also the need to bear in mind that, subject to applicable legal and constitutional human rights constraints, States did not require an instrument to cooperate if they wished to do so, especially in the field of information-sharing. However, it was similarly essential to ensure that shared information was not used improperly or for purposes other than intended.

30. The Chairman stressed the need for enhanced cooperation and coordination in cases where multiple States or chains of communication were involved. Reference was made to the "24/7" network and the way it operated in practice. One speaker was of the view that the network was in general functional, but the degree of its effectiveness depended on the ability of call recipients to receive and pass on requests quickly and the availability of competent personnel to carry them out.

[4] Some speakers noted, in this connection, that, if specific identity crimes were not in place, other more generally applicable offences, such as cybercrime offences, might form a suitable basis for international cooperation.

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

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

Another speaker added that the network was more effective for the fast freezing of data or preservation of records than for more intrusive interception or search requests which usually required judicial authorization in the requested State before competent officers could act.

VI. Agenda item 9: Protection of victims

31. The expert assigned by the secretariat to elaborate a paper on “Identity-related crime victim issues” gave a presentation summarizing its content. The paper covered the following distinct issues:

- The range and types of victims of identity-related crime;
- The legal bases for restoration of victim identity;
- Human rights issues; and
- An inventory of practices for victim remediation.

32. In discussion, it was noted that, to a certain extent, the materials dealing with victims would be directed at a different audience than criminalization or legislative materials. For victim elements, the audience would include experts and officials dealing with victims at a personal level, who needed to understand the psychological and social impact of the offences. Reference was further made to the difference between the taking of actual identity information which victimized the person identified by such information and the fabrication of information, which created only victims of secondary offences such as fraud. There was also general discussion on the various ways in which victims could be classified and some reasons why it might be appropriate to choose one or another. Such approaches would by and large depend on why victims were being considered (e.g., as a target of remedial support or as a source of research information) and could only be formulated when it was clear how and why victims or victim information would be involved in specific materials or projects.

33. Furthermore, it was highlighted that most aspects of work on victim issues could reflect an objective (system-based) or subjective (victim-based or victim-defined) approach. This included all areas, but would be particularly critical in areas such as the use of victims as a data-source, and in assessing the extent of harm suffered, which could be different for victims depending on their individual characteristics. The potential mandates and uses for victim-based information were also discussed. There was general agreement that victim issues needed to be raised at the forthcoming session of the Commission on Crime Prevention and Criminal Justice to provide a substantive basis for the approval of an ad hoc resolution. It was further recognized that additional work would be needed on victimization aspects, given the novel concept of identity-related crime, its substantial impact on victims and the complex challenges raised by the restoration of victims’ identities. Such additional work included, inter alia, efforts to bring together experts on victim issues, as well as high-tech and identity-related crime.

34. In discussing other issues covered by the paper on victims issues, the members of the core group acknowledged that, despite extensive provisions on the protection of victims in general, identity crimes posed a unique challenge and options for

restoration of identity were limited. Mutual legal assistance schemes might also not apply to attempts to obtain victim remediation from other countries. Civil remedies might be available in theory but could be difficult to apply in practice, especially in international cases. Possible options for civil remedies included tort actions based on data protection, privacy, appropriation of personality, defamation and intellectual property actions, but the costs and difficulties could be considerable and damages might not be obtainable.

35. Attention was devoted to the recent decision of the European Court of Human Rights in the case of *K.U. v. Finland*,[7] which established the relationship between the privacy rights of victims and criminal suspects in European law. In that case, the European Court held that a provision of the Finnish law denying access to a suspected offender's IP address based on his privacy rights could not be enforced in the face of a greater infringement of the child victim's privacy rights, which had been violated by the offence. There was also discussion of rights related to the creation of identity, including rights to registration and identity, especially in the case of children and in the light of the Convention on the Rights of the Child.[8] As far as victim remediation is concerned, elements of the paper on best practices were reviewed. With respect to institutional capacity, there was discussion of factors such as costs, coordination among State agencies and coordination with the private sector. It was also noted that a threshold question for victim support and remediation measures of any kind was the ability to accurately determine who was a victim and distinguish between victims and offenders, which could be difficult in many cases.

36. One speaker made a presentation on the work of the anti-phishing education programme. He indicated that researchers had identified "teachable moments" at which there was added ability to communicate information to potential victims. The programme consisted of identifying and taking down fraudulent or phishing websites and replacing them with a link that, when the site was accessed, would take the browser to an education site containing information on the nature of fraud and/or phishing and how to avoid being victimized. Another focus of the educational materials was to encourage practices that limited the scope of harm if some information was compromised, such as warning users to ensure that different accounts used different passwords or other identifiers.

VII. Agenda item 10: Preventive measures

37. Under this agenda item and its particular focus on awareness-raising activities, one speaker stressed the importance of measures geared towards educating the consumers about the problems posed by, and the impact of, identity-related crime. In this context, she referred to the work of the Federal Trade Commission (FTC) in the United States on prevention and regulatory and civil enforcement. The ultimate goal was to raise awareness of the public and try to disseminate materials to targeted groups of potential victims whenever they could be identified. To this end, the FTC employed a range of dissemination strategies, including producing and disseminating materials under its own "brand", as well as making materials or

[7] *K.U. v. Finland*, Appl. No. 2872/2002, Decision of 2 December 2008.

[8] Adopted by General Assembly resolution 44/25 of 20 November 1989.

information available to other entities to disseminate with their own materials in the course of their own business or other practices.

38. In the context of the discussion on ways and means to promote technical means of prevention of identity-related crime, one speaker delivered a technical presentation on improving the security of authentication processes. He reviewed the adoption of strong cryptographic technologies as new elements of MS Windows, and some innovations that Microsoft, in particular, hoped would increase use of new security technologies, while reducing the amount of identity information which was transferred, used and stored in the course of computer transactions. In particular, a new application, known as “U-Prove” would provide technological security options for users, and leave the exact use of applications to them, with varying degrees of security as appropriate for each specific use. Regarding the actual design of the new application, its function was to allow for the establishment of on-line identity, while, at the same time, reducing to a minimum the identity information shared among parties, and allowing for the transfer of only as much information as was needed for each individual use or transaction.

39. The policy issues relating to the new product and the reasons for its development were also discussed and focused on the balance between identity and privacy. Systems increasingly collected and retained transaction data, and one issue was whether mass retention of data opened a field for unlimited surveillance, as opposed to judicially authorized and targeted surveillance. It was mentioned, in this connection, that the new product of Microsoft allowed for much closer tailoring in a range of specific situations, with (hopefully) a net increase in both privacy and security. Microsoft’s approach was to provide customers with a system that could be adapted accordingly to address security and/or privacy concerns. Another issue discussed was that of the basic data retention itself. The new Microsoft product aimed at reducing information transferred, but there remained the question of the basic requirements and criteria on the information to be retained and how it would be used. An example mentioned to highlight potential risks and difficulties was that of the loss of identity data in the United Kingdom as a result of a request for their transfer made by another agency for verification purposes.

40. Another speaker briefed the core group on the ICAO measures against identity-related crime, including the adoption of instruments establishing legal and normative (recommended practices) standards, as well as technical prevention standards. ICAO had developed 18 technical annexes to the 1944 Chicago Convention on International Civil Aviation covering the full range of technical issues. Annex 9 dealt with immigration matters and, among others, obliged States Parties to update document security measures and establish standards for travel documents. The use of digital biometric data in machine-readable travel documents (MRTDs) was also recommended. ICAO Document 9303 called for all passports to be machine readable by April 2010, and the speaker expressed the hope that 170 of 190 Member States would be in conformity by then. The ICAO standards also provided for interoperability in formats, so that the various documents could be read in all States Parties. The speaker further noted that the security of documents had to include issuance processes as well and that ICAO also assisted States Parties in making such processes resistant to subversion and other problems. ICAO was also trying to engage on problems with “breeder documents”, such as birth certificates used to obtain passports.

VIII. Agenda item 11: The role of the private sector in the fight against identity-related crime

41. Under agenda item 11, the Chairman inquired about the need for, and the scope of, private sector involvement in policies and strategies against identity-related crime. He further drew attention to the references in the 2005 Bangkok Declaration regarding the engagement of the private sector in the field of high-technology and computer-related crime.[9] The Rapporteur of the core group indicated that the prevention of that form of crime was a major focus for such involvement, together with the investigative cooperation which was identified as a field of collaboration by many Member States that provided information for the purposes of the United Nations study on “fraud and the criminal misuse and falsification of identity”.

42. An issue raised by several speakers was how to inject private sector perspectives into what was otherwise an intergovernmental exercise and process. One speaker mentioned, in this regard, the extensive experience of UNCITRAL in working with private commercial interests, especially on commercial fraud issues. She also referred to the forthcoming product of that work, an UNCITRAL document containing 23 indicators of commercial fraud, which were developed by a panel composed of governmental and non-governmental/commercial experts and intended for use by commercial interests in training employees and detecting fraud incidents. Some of these indicators dealt with identity aspects of fraud.

43. One speaker suggested that the core group should not try to define the role of the private sector in related matters *ab initio*, but, instead, try to cross-reference best practices. The Rapporteur of the group reviewed the discussion on the private sector involvement and cooperation, as reflected in the United Nations study and the previous reports of the core group. He argued that it would be helpful if commercial issues were raised and addressed at the forthcoming session of the Commission on Crime Prevention and Criminal Justice. In further discussing the matter, the members of the core group were of the view that the private sector itself had a wide range of divergent interests that needed to be taken into consideration. One speaker noted that some standards had been developed by payment card industry purely for its own needs. In some cases the private sector could move faster because it did not encounter legislative or other government and public administration issues. One speaker stressed, however, the need for strategic thinking and the establishment of concrete private sector standards to address related problems.

44. One speaker referred to privacy-enhancing technologies, noting that those could be driven by both consumer demand or legislation and the private sector. Another speaker argued that thus far consumers had not necessarily been willing to pay extra for privacy technologies. An approach suggested was that such technologies should be incorporated into basic service packages. One speaker noted that in some cases non-competitive options had worked well, citing, as an example, a private sector identity theft centre in the United States based on pooled resources from companies.

[9] See para. 16 of the Bangkok Declaration on “Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice”, endorsed by General Assembly resolution 60/177 of 16 December 2005.

IX. Agenda item 12: Technical assistance activities for capacity-building

45. The secretariat drew the attention of the core group to the links between specific technical assistance in the area of identity-related crime and other technical assistance activities covering various forms of crime. It further made reference to ECOSOC resolution 2007/20, which already contained mandates on technical assistance initiatives. One speaker suggested that the area of training materials and programmes for law enforcement in multiple countries should be seen as a priority. It was further argued that, although thus far the core group had not established a sub-group consisting of law enforcement experts, this might be a suitable body to develop such materials. The Rapporteur of the core group noted that all the subject areas discussed within the group provided potential for technical assistance interventions of some kind, and that an important task for both the core group and the Commission on Crime Prevention and Criminal Justice would be that of sequencing and setting priorities. In general, the concept of brokering, under which UNODC would develop pools of experts in each region and support them with updated materials and basic training, was discussed as an option for future action.

46. The Chairman noted that one of the immediate tasks of the core group would be to focus its work on the specific aspects of fraud and identity-related crime, but also link them to the broader context of other crimes, such as cybercrime and transnational organized crime. The Rapporteur of the core group underlined that, while technical assistance questions needed to be raised for all the areas considered by the group, some of those areas might be accorded higher priority as they were more developed or because they called for more urgent work. Priority, for example, could be accorded to criminalization issues through the drafting of elements of actual offences and the establishment of a pool of experts. Building upon concrete results in this area, a second step could be the building of investigative capacity of competent national authorities. Other views supported the prioritization of victims assistance and protection.

47. In an effort to “blend specificity and flexibility”, the core group was of the view that there was a need for core materials on different aspects, and not only law enforcement issues, which should be developed in basic modules to permit flexible application. Some modules could be based on specific legal instruments, while others would be stand-alone materials. It was further argued that identity crime might be the primary focus of some projects and/or a substantial component of other broader activities. Therefore the materials would need to be broad enough to support both scenarios.

48. It was acknowledged that some of the technical assistance activities could be costly and therefore suggested as a possible solution that private sector resources be engaged, either through financial support or in-kind contributions. One speaker noted that the private sector was not just a source of resources, but could also be useful in helping identify issues and needs for materials and assistance. He further referred, as an example, to the cooperation of Microsoft with the Economic and Financial Crimes Commission in Nigeria with a view to reducing incidents of fraud, including cases of transnational nature. Another speaker highlighted the problem of the rapid evolution of cybercrime and identity-related crime and the consequent need for constant vigilance and updating of technical assistance, which should better

reflect privacy concerns. Another speaker drew attention to the need for capacity-building in both private and public sectors.

49. The members of the core group agreed upon the following recommendations on technical assistance issues, which could be considered by the Crime Commission at its 18th session:

- Materials should be prepared to assist Member States in developing and drafting new identity offences and in reviewing and modernizing related existing offences, and a pool of experts should be developed for the purpose of providing assistance in the preparation of such legislation, taking into consideration identity crime issues in the context of more general legislative projects;
- Materials should be prepared to assist investigators and prosecutors in building capacity for dealing with identity-related crime in domestic and transnational cases, bearing in mind the available international legal instruments, including the United Nations Convention against Transnational Organized Crime, the Convention on Cybercrime and any other relevant instruments;
- Materials should be compiled to assist competent authorities of Member States in building effective preventive strategies and policies, bearing in mind the need for involvement of the private sector at the domestic and international levels, and the need to take into account the protection of privacy interests and human rights; and
- Further work should be carried out with respect to victims issues in the field of identity-related crime, including commencement of the accumulation and development of best practices for the support and assistance of victims at the domestic and international levels.

X. Agenda item 13: Thematic debate at the 18th session of the Commission on Crime Prevention and Criminal Justice

50. Under this agenda item, the Chairman provided clarifications on the way that the thematic debate on identity-related crime at the 18th session of the Commission on Crime Prevention and Criminal Justice would be conducted and noted that the regional groups were called to identify panellists for the purposes of the debate. He also underscored that the report of the forthcoming session of the Commission would reflect the discussion, while an ad hoc resolution might be proposed for further discussion and approval. The Rapporteur of the core group outlined the procedure of the thematic debate, in which the members of the group concurred. It was specified, inter alia, that the discussion papers on criminalization and victims issues, together with the reports of the three meetings of the core group, would be submitted to the Commission as Conference Room Papers. Thus, they would be disseminated for the reference of delegations, without being edited and only in their language of origin (in all cases, English). As such, they would not be official documents of the United Nations, but Member States would be invited to review them and provide comments to the secretariat for consideration at the next meeting of the core group.

XI. Agenda item 14: Mapping out a course of future action for the core group

51. The members of the core group agreed that its future work would depend to some degree on the outcome of the Commission thematic debate and resolution, and, to a certain extent, the outcome of the G-8 Lyon/Roma Group process.