



Economic and Social Council

Distr.: General
31 January 2011

Original: English

Commission on Crime Prevention and Criminal Justice

Twentieth session

Vienna, 11-15 April 2011

Item 6 of the provisional agenda*

**World crime trends and emerging issues and responses in
the field of crime prevention and criminal justice**

International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime

Report of the Secretary-General

Summary

The present report provides information on the efforts of Member States to implement Economic and Social Council resolution 2009/22 and domestic policies and measures in the areas of prevention, investigation, prosecution and punishment of economic fraud and identity-related crime. It also provides information on action taken by the United Nations Office on Drugs and Crime to promote mutual understanding and the exchange of views between public and private sector entities on issues related to economic fraud and identity-related crime by supporting and servicing the meetings of the group of experts on identity-related crime held in 2010. The present report contains information on the technical assistance provided on identity-related crime.

* E/CN.15/2011/1.



Contents

	<i>Page</i>
I. Introduction	3
II. Overview and analysis of information provided by Governments	5
III. Work of the core group of experts on identity-related crime	19
IV. Technical assistance materials on identity-related crime	20
V. Conclusion	20

I. Introduction

1. In its resolution 2009/22, the Economic and Social Council took note of the report of the Secretary-General on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime (E/CN.15/2009/2 and Corr.1), which contained information on the efforts of reporting Member States to implement Council resolution 2007/20 and on their strategies for responding to the problems posed by such forms of crime. The Council also took note of the thematic discussion of the Commission on Crime Prevention and Criminal Justice at its eighteenth session on the theme “Economic fraud and identity-related crime”. The Council acknowledged the efforts of the United Nations Office on Drugs and Crime (UNODC) to establish, in consultation with the United Nations Commission on International Trade Law, a core group of experts on identity-related crime and bring together on a regular basis representatives from Governments, private sector entities, international and regional organizations and academia to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime. The Council took note of the work of the core group of experts on identity-related crime at its meetings held in Courmayeur, Italy, on 29 and 30 November 2007 and in Vienna on 2 and 3 June 2008 and from 20 to 22 January 2009.

2. In that same resolution, the Economic and Social Council encouraged Member States, taking into account the recommendations of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity (E/CN.15/2007/8 and Add.1-3), convened pursuant to Council resolution 2004/26:

(a) To combat economic fraud and identity-related crime by ensuring adequate investigative powers and, where appropriate, by reviewing and updating the relevant laws;

(b) To develop and maintain adequate law enforcement and investigative capacity to keep abreast of and deal with new developments in the exploitation of information, communications and commercial technologies in economic fraud and identity-related crime, including websites and other online forums used to facilitate trafficking in identity information or documents, such as passports, driving licences or national identity cards;

(c) To consider, where appropriate, the establishment of new offences and the updating of existing offences in response to the evolution of economic fraud and identity-related crime, bearing in mind the advantages of common approaches to criminalization, where feasible, in facilitating efficient and effective international cooperation;

(d) To strengthen international cooperation to prevent and combat economic fraud and identity-related crime, in particular by making full use of the relevant international legal instruments;

(e) To develop an approach for the collection of comparable data on the nature and extent of identity-related crime, including, where feasible, from the victim’s perspective, that would allow the sharing of data among appropriate law

enforcement entities and provide a central source of data at the national level on the nature and extent of identity-related crime, taking due account of national law;

(f) To study, at the national level, the specific short- and long-term impact of economic fraud and identity-related crime on society and on victims of such forms of crime and develop strategies or programmes to combat those forms of crime;

(g) To adopt useful practices and efficient mechanisms for supporting and protecting victims of economic fraud and identity-related crime and, to that effect, enable effective cooperation between public and private sector entities through computer emergency response teams or other mechanisms providing an emergency response capability to public and private organizations requiring technical support and advice during periods of electronic attack or other network security incidents.

3. In addition, the Economic and Social Council requested UNODC, in consultation with Member States and taking into account relevant intergovernmental organizations and, in accordance with the rules and procedures of the Council, experts from academic institutions, relevant non-governmental organizations and the private sector, to collect, develop and disseminate:

(a) Material and guidelines on the typology of identity-related crime and on relevant criminalization issues to assist Member States, upon request, in the establishment of new identity-based criminal offences and the modernization of existing offences, taking into account the pertinent work of other intergovernmental organizations engaged in related matters;

(b) Technical assistance material for training, such as manuals, compilations of useful practices or guidelines or scientific, forensic or other reference material for law enforcement officials and prosecution authorities in order to enhance their expertise and capacity to prevent and combat economic fraud and identity-related crime;

(c) A set of useful practices and guidelines to assist Member States in establishing the impact of such crimes on victims;

(d) A set of material and best practices on public-private partnerships to prevent economic fraud and identity-related crime.

4. The Economic and Social Council also requested UNODC to provide technical assistance, including legal expertise, upon request to Member States in reviewing or updating their laws dealing with economic fraud and identity-related crime in order to ensure that appropriate legislative responses are in place, and to continue its efforts, in consultation with the United Nations Commission on International Trade Law, to promote mutual understanding and the exchange of views between public and private sector entities on issues related to economic fraud and identity-related crime, with the aim of facilitating cooperation between various stakeholders from both sectors through the continuation of the work of the core group of experts on identity-related crime, the composition of which should respect the principle of equitable geographical distribution, and to report on the outcome of its work to the Commission on Crime Prevention and Criminal Justice on a regular basis.

II. Overview and analysis of information provided by Governments

5. The following Member States provided information and relevant material on the implementation of Economic and Social Council resolution 2009/22: Algeria, Armenia, Australia, Belarus, Belgium, Bosnia and Herzegovina, Brunei Darussalam, Canada, China, Cyprus, Czech Republic, Egypt, El Salvador, Germany, Ghana, Guatemala, Japan, Jordan, Mauritius, Mexico, Morocco, Netherlands, Norway, Panama, Philippines, Poland, Republic of Moldova, Russian Federation, Serbia, Sudan, Sweden, Switzerland, Thailand, Togo, Trinidad and Tobago, Ukraine and United Kingdom of Great Britain and Northern Ireland.

Algeria

6. Algeria reported that its domestic legislation criminalized the use of false identification, false certification and the unlawful taking of interest. Moreover, in the context of recent reforms to the Penal Code, offences relating to new information technologies had been established, and investigative powers to enable law enforcement agencies to identify the offender and collect evidence required for criminal proceedings had been strengthened. In 2004, the Criminal Procedure Code had established special pools of magistrates with ad hoc responsibilities and competence regarding drug trafficking, transnational organized crime, offences involving the automatic processing of data, money-laundering and terrorism. Algeria also reported on national legislation containing provisions on mutual legal assistance and on bilateral agreements on mutual legal assistance and extradition concluded by its authorities.

Armenia

7. Armenia made reference to provisions of the national Criminal Code establishing as criminal offences a series of behaviours that constituted economic crimes and that were linked to economic fraud and identity-related crime, or that involved the use of computer technology.

8. Armenia reported that its law on personal data regulated issues of identity management. The law determined the fundamental principles of personal data processing, rules of database maintenance, access to the databases and procedures for lodging a complaint for actions taken by those working with such data.

9. Armenia also reported that the General Prosecutor's Office had conducted several pretrial investigations into fraud and money-laundering cases, in which the alleged offenders had employed false credit cards to steal money from banks or used false or stolen credit cards to pay for purchases. An increase in the use of falsified identity documents to cross borders was noted.

Australia

10. Australia noted that, under its federal system of government, fraud-related offences in which the victim was an individual or entity other than the Commonwealth were normally dealt with by each state and territory. Fraud-related offences dealt with under Commonwealth law were generally relevant to the administration of government. In general, the concepts of deception and dishonesty

underpinned fraud-related offences. Australia referred to provisions of its Criminal Code applicable to any conduct involving the use of a telecommunications network, a computer or the Internet for criminal purposes.

11. Australia reported that ensuring identity security was seen as central to national security, law enforcement, economic interests and personal safety, and that in several Australian states it was an offence to assume or steal another person's identity. Furthermore, the enactment of ad hoc draft legislation defining and criminalizing identity-related crime for use by both the Commonwealth and the states was pending. The draft legislation would insert three new identity-related offences into the Criminal Code: dealing in identification information, possessing identification information and possessing equipment used to make identification documentation. It also included provisions allowing victims of identity-related crime to apply for a certificate stating the manner in which the victim's identification information had been misused.

12. With regard to criminal justice responses, Australia had provided information on a range of operational initiatives aimed at combating identity-related crime and reported that identity-related crime had been identified as a key area requiring a strengthened national response. A report was being prepared to review and gather information about relevant work already taking place across the Commonwealth and to assess gaps and areas for improvement for the period 2010-2011.

13. With regard to prevention, Australia reported on the implementation of the National Identity Security Strategy, intended to protect the identity of all Australian citizens. The Strategy was designed to strengthen national identity management processes to prevent and combat identity-related crime. Moreover, educational materials had been published to inform the public of the threat of identity-related crime, while a website (www.scamwatch.gov.au) had been launched as a tool to assist people in identifying and reporting scams, including those related to identity theft. In addition, the private sector had developed materials to educate the public about the threat of identity-related crime. Close coordination between the Commonwealth, State governments and the private sector was being pursued, with a particular focus on including the banking and finance sectors.

14. Australia underlined the importance of carrying out research on identity-related crime and of improving the availability of accurate and comprehensive data on the issue. The Australian Bureau of Statistics had conducted a household survey in 2007 and plans were under way to carry out another such survey in future.

Belarus

15. Belarus reported on recent cases of fraud registered by the Ministry of the Interior. It was noted that national authorities were cooperating with other States to prevent and combat economic fraud and identity-related crime. In that connection, information was provided on recent requests for assistance made to the relevant law enforcement bodies of Latvia, the Russian Federation and Ukraine. Assistance had been provided in relation to most of those requests.

Belgium

16. Belgium provided information on its efforts to prevent and combat the abuse of identity for fraudulent purposes through the use of information technologies.

The Federal Computer Crime Unit had organized awareness-raising campaigns for all citizens who could be victims of such crime. The Unit cooperated with the competent authorities of other States and took part in the Anti-Phishing Working Group and the International Mass-Marketing Fraud Working Group, which share information to streamline efforts in the fight against such fraud. With a view to protecting victims, the European Union envisaged establishing a European strategy for identity management in the framework of the Stockholm Programme for the period 2010-2014,¹ in which the European Council reaffirmed the priority it attaches to developing an area of freedom, security and justice. Belgium underscored that identity fraud was also considered a priority in its National Security Plan for the period 2008-2011. With a view to improving Belgium's ability to fight identity fraud, stronger collaboration between experts on false documents and the Government was envisaged.

Bosnia and Herzegovina

17. Bosnia and Herzegovina noted that its criminal legislation provided for the punishment of all acts undermining confidence in the credibility of documents, and referred to national legislation aimed at protecting confidentiality in the processing of personal data. An agency for the protection of personal data had been established as an independent administrative authority in charge of supervising the implementation of laws on the processing of personal data and the monitoring of requirements for the protection of personal data.

18. Bosnia and Herzegovina reported that its competent judicial and law enforcement authorities were engaged in the fight against economic fraud and identity-related crime within the context of the fight against organized crime. Moreover, it referred to international instruments to which it was a party, including the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and the Council of Europe Convention on Cybercrime.

Brunei Darussalam

19. Brunei Darussalam made reference to relevant legislative measures aimed at criminalizing and punishing offences such as forgery, unauthorized access to computer materials and banking offences involving elements of fraud. It reported on domestic legislation focusing on the prevention of money-laundering and the financing of terrorism, as well as the confiscation of proceeds derived from offences other than drug trafficking. Reference was made to legislation providing for the legal recognition of electronic records and signatures and for requirements to carry out remittances.

Canada

20. Canada stressed its leading role in the elaboration of a 2007 United Nations study on fraud and the criminal misuse and falsification of identity and noted that it remained active in the ongoing work of UNODC through its participation in the core group of experts on identity-related crime and the development of materials for

¹ *Official Journal of the European Union*, 2010/C 115/01, 4 May 2010.

use in the provision of technical assistance for the direct and indirect criminalization of identity abuse, for increasing the effectiveness of the Organized Crime Convention and other existing international legal instruments, for developing useful practices and guidelines for preventing identity-related crime and for supporting and assisting the victims of such crime.

21. Regarding the establishment of new identity-related offences, Canada underscored that while each State should formulate offences to meet its own needs within the context of its existing criminal law, common approaches to criminalization were also important to ensure national laws could support the provision of mutual legal assistance and other forms of cooperation.

22. Canada recalled that in the 2007 study mentioned in paragraph 20 above many links had been identified between the availability and use of information and communications technologies and the prevalence of transnational economic fraud and identity-related crime. It noted the preparation of a comprehensive study of the problem of cybercrime, to be prepared pursuant to General Assembly resolution 65/230, and expressed the view that the study should include some examination of the role of economic fraud and identity-related crime both as a motive for and an element of cybercrime.

23. Canada highlighted that the development of appropriate measures for providing support and assistance to victims of identity-related crime remained a challenge and that, because of this, victim-based approaches were an essential element of a comprehensive response to the problem that included the development of holistic and multidisciplinary approaches to minimize persistent harm being caused to victims, prevent further crimes from being committed using stolen or copied identity-related information and assist victims in restoring and correcting falsified information.

24. Canada reported on amendments to its legislation criminalizing identity theft, trafficking in identity information and the unlawful possession of or trafficking in certain Government-issued identity documents and clarifying and expanding on existing offences to ensure that the problem of identity-related crime would be addressed. Information was provided on discussions on a national identity crime strategy, which had begun in 2010, among members of Canada's law enforcement community and other interested public sector entities.

25. Canada highlighted the work of the International Centre for Criminal Law Reform and Criminal Justice Policy on identity-related crime and, in particular, on victim issues. In that context, a manual providing guidelines to law enforcement agents and prosecutors on the protection of victims of identity-related crime was being prepared under its auspices and in cooperation with the core group of experts on identity-related crime.

China

26. China reported on national efforts to amend the Criminal Code to enhance international cooperation in combating economic fraud and identity-related crime. At the operational level, law enforcement authorities had taken action against organized criminal groups involved in fraud. At the judicial level, measures had been taken to support the development of an effective judicial system for the prosecution and punishment of individuals who committed economic crimes. At the

international level, efforts had been made to strengthen international cooperation in criminal matters, including extradition and asset recovery. In addition, campaigns had been launched to educate and raise awareness among public officials, civil society organizations, the private sector and the public about the impact of economic fraud and identity-related crime on the sustainable development of the economy.

Cyprus

27. Cyprus noted that although a formal definition of economic crime was not being used domestically any illegal activity generating proceeds for the offender was considered an economic crime. In recent years, there had been a few cases related to economic fraud and identity-related crime, such as e-banking scams (phishing) and e-commerce fraud, and a number of cases concerning credit cards, false representation, fraud, counterfeiting and crimes committed with the use of computers. There had also been incidents of cybercrime: identity theft, criminal breaches of the confidentiality, integrity and availability of computer data and systems, and offences related to child pornography.

28. Cyprus provided an overview of the preventive and reactive measures to economic crime it had implemented and reported that special law enforcement offices had been set up to combat cybercrime and economic crime. The investigation of fraud and financial crimes was the responsibility of the Economic Crime Unit, which cooperated closely with other governmental authorities and was also responsible for investigations and executing legal requests for assistance to other States.

29. With regard to international cooperation, Cyprus reported that its law enforcement authorities cooperated closely with international law enforcement organizations such as the International Criminal Police Organization (INTERPOL) and the European Police Office (Europol). In addition, Cyprus had ratified numerous international conventions and signed a number of bilateral agreements on cooperation between the police or other governmental authorities on matters related to the prevention and combating of international terrorism, drug trafficking, organized crime and other forms of serious crime. In its crime prevention strategy, drawn up in 2007, Cyprus accorded priority to closer cooperation with other European countries, the Federal Bureau of Investigation of the United States of America, INTERPOL and Europol with regard to exchanging information and training police officers.

30. Cyprus provided an overview of best practices in the fight against economic fraud and identity-related crime, including the organization of lectures to members of the various criminal investigation departments; the recruitment of specialists; the improvement of and increase in inter-agency coordination and cooperation with States and organizations in terms of information-sharing and training police officers; the enhancement of the administrative capacity of specialized law enforcement units; the establishment of a crime analysis office equipped with the appropriate software and technology; and the application of a central computerized system for producing data reports on serious and minor offences.

Czech Republic

31. The Czech Republic cited provisions of its domestic legislation criminalizing different forms of economic crime, including fraud, money-laundering, unauthorized access to a computer system and data carrier, unlawful procurement and possession of a device and password for accessing a computer system and data, negligent damage to a record in a computer system and data carrier, negligent interference in computer equipment, bribery, trading in influence, forgery and alteration of public documents. Statistics were provided regarding prosecutions and convictions for economic and identity-related crimes for the period 2007-2010. The Czech Republic also provided information on relevant multilateral treaties to which it was a party.

32. Reference was made to the competent authorities of the Czech Republic involved in the investigation of cases of fraud and identity-related crime, which included law enforcement entities at both the local and regional levels, as well as specialized police services. It was noted that the Financial Analytical Unit of the Ministry of Finance, in particular, was a member of the world network of financial intelligence units and that the tasks of the Unit were: to receive and analyse suspicious reports on transactions; to carry out supervisory activities; to coordinate the implementation of international sanctions at the national level; to promote international cooperation; to carry out legislative work and provide methodological guidance; and to carry out activities related to information technologies and the security of financial intelligence units. The Czech Republic provided an overview of activities of the Financial Analytical Unit for the period 2008-2009, including its participation in the work of international organizations such as the Council of Europe (through its Committee of Experts on the Evaluation of Anti-Money-Laundering Measures and the Financing of Terrorism (the Moneyval Committee)), the Egmont Group, the European Commission (through its Committee on the Prevention of Money-Laundering and Terrorist Financing and the European Union's platform of financial intelligence units) and the Organization for Economic Cooperation and Development. National law enforcement authorities were also cooperating with Europol in the fight against economic fraud and cybercrime.

33. The Czech Republic reported on the work of its Office for Personal Data Protection, aimed at supervising compliance with domestic legislation on the protection of personal data. The Office was cooperating with counterparts in other countries, European Union institutions and international organizations active in the field of data protection. As a result of its work, several legislative amendments had been enacted, including strict rules for the copying of identity cards and travel documents and rules restricting the use of birth certificate numbers. The Office was active in the fight against spam and was involved in revising legislation that permitted public access to certain data in the register of companies, as well as in developing new legislation to regulate the collection and use of DNA data.

Egypt

34. Egypt referred to national legislation on economic fraud and identity-related crime, and to institutional bodies dealing with such crimes. It reported that ad hoc courts dealing with economic crime had been established. Egypt provided information on national measures intended to ensure the security and integrity of identification data and documents. Reference was made to preventive measures,

including the elaboration of strategies, the organization of training activities, awareness-raising campaigns to increase knowledge about new developments in banking crimes and cooperation with banks and financial institutions.

35. Egypt further reported on its efforts to streamline mechanisms for international cooperation in criminal matters, including through the ratification and implementation of multilateral instruments to which it was a party, the conclusion of bilateral treaties, the promotion of information-sharing and cooperation with INTERPOL.

El Salvador

36. El Salvador reported on the establishment of several identity-related crimes under its national penal code. It also reported that various legal amendments had been enacted to enable the temporary interception of telecommunications as part of investigations into a crime, subject to judicial decision. In addition, specific legislation was in place to protect the rights of witnesses and victims. Information was provided on the new criminal procedure code, which granted further investigative powers to the attorney general and enabled the creation of investigation teams with foreign counterparts.

Germany

37. Germany pointed out that a number of elements of offences under general criminal law were related to behaviour such as obtaining the identification data of other people for fraudulent reasons, forgery, illicit data collection and processing and tampering with official identity documents. Germany referred to statistical data on relevant criminal cases and provided information on the competence of its Federal Criminal Police Office to fight cybercrime in Germany and the illegal trading in digital identities.

38. Germany highlighted that requests for extradition and mutual legal assistance could be granted on the basis of bilateral and multilateral agreements to which Germany was a party and the provisions of the German law on international assistance in criminal matters.

Ghana

39. Ghana provided an overview of the economic crimes established in its Criminal Code. It stressed that the national body charged with making laws was struggling to develop new laws dealing with emerging forms of economic crime and cybercrime. Special emphasis was placed on specific forms of fraud experienced and detected in Ghana and West Africa, such as advance fee fraud and credit card fraud.

40. Ghana drew attention to the challenges it encountered in the fight against economic crime, including the need to regularly train law enforcement personnel and employ more specialists, such as accountants, lawyers and information technology experts, to effectively deal with new trends in the area of economic crime. The framework of collaboration and information-sharing with INTERPOL was described, with the suggestion that such collaboration be strengthened in the future.

Guatemala

41. Guatemala provided information on its domestic criminal legislation to combat economic fraud and identity-related crime and reported on the establishment of different special public prosecutor's offices for dealing with economic crime and crimes involving intellectual property and stolen assets. Information was provided on efforts made to ensure integrity in the issuance of national passports and on training activities in the field of documents control and fraud prevention.

Japan

42. Japan reported on its continuing efforts to revise its legislation in order to keep up with the evolution of economic fraud and identity-related crime. In that context, specific legislation was enacted in 2006 and amended in 2008 to address the so called "furikome" frauds, in which criminals made improper use of mobile phones to avoid being identified by the authorities. Efforts were being made to improve procedures for collecting evidence in order to combat crimes involving sophisticated patterns of information processing.

43. Japan reported that its domestic legislation criminalized fraud, including computer-related fraud, as well as the counterfeiting of documents, the unauthorized creation of electromagnetic records of such documents, the possession of such documents with unauthorized electromagnetic records and the illegal obtention of information regarding electromagnetic records. Efforts were being made to criminalize new types of conduct, such as creating or utilizing computer viruses. Japan stressed that more streamlined legal provisions had been enacted to better protect the rights of the victims of crime.

44. Japan stressed that it could provide assistance to States or extradite persons in response to requests made by States even outside the framework of applicable treaties by resorting to applicable domestic legislation. Nevertheless, Japan had concluded agreements on extradition and mutual legal assistance with various States, and signed the Organized Crime Convention and the Convention against Corruption. While the signature of those conventions had been approved by the Diet, preparations for the elaboration of domestic legislation to implement them were still ongoing. In addition, the National Police Agency of Japan had been promoting mutual cooperation, including the exchange of information, with foreign investigative agencies through INTERPOL and diplomatic channels, and had created a database for collecting information, including on suspects' names and the means of committing crimes, for the investigation of "furikome" frauds.

Jordan

45. Jordan referred to national efforts aimed at establishing institutional bodies to combat economic crime and cybercrime. Particular attention was paid to enhancing international cooperation by promoting the exchange of information with foreign law enforcement authorities. Training programmes had been developed to enhance knowledge on that topic.

Mauritius

46. Mauritius provided an update of domestic legislation on economic fraud and identity-related crime. It reported that national authorities made use of the relevant

legal instruments available to review or update domestic laws, bearing in mind that the criminal misuse and falsification of identity were commonly associated with other illicit activities such as money-laundering, corruption and terrorism. Mauritius stressed that, in order to maintain adequate law enforcement and investigative capacity to keep abreast of, and deal with, new developments in the exploitation of information, communications and commercial technologies in economic fraud, the national police forces had invested substantially in training and equipment. Mauritius endeavoured to strengthen international cooperation, including through the implementation of the provisions of the Organized Crime Convention, as well as information-sharing with States members of the Southern African Development Community, the Southern African Regional Police Chiefs Cooperation Organization and INTERPOL.

47. Mauritius underlined that the National Police Force's Crime Records Office collected data on the nature and outcome of all types of crime, including identity-related crime. The data were published annually and were usually made available, upon request, to organizations for analysis and planning. Moreover, the Financial Intelligence Unit of Mauritius was the central national agency in charge of receiving, analysing and disseminating to investigative and supervisory authorities financial information regarding suspected proceeds of crime and alleged money-laundering offences, including any activities or transactions related to terrorism. The Unit was also responsible for exchanging information with the financial intelligence units of other States.

Mexico

48. Mexico reported that its Criminal Code established the crime of fraud, including specific forms of it. However, fraud committed through the Internet or by electronic means was not established. Furthermore, several fraud-related crimes were foreseen in different financial laws. With regard to the protection of personal data possessed by public and private entities, there had been a constitutional amendment to recognize personal data protection as an autonomous and fundamental right. In cases of crimes related to the financial system, special investigation and cooperation instruments were in place to detect and prosecute the perpetrators of such crimes. In addition, information-exchange mechanisms had been set up with financial institutions.

49. Mexico reported difficulties in promoting cooperation between the public and private sectors. The challenges were posed by massive financial frauds that showed the need for amendments to be made to the financial crime laws, and problems resulting from a lack of knowledge and awareness. Mexico stressed that awareness-raising efforts had been made through meetings with competent national and foreign bodies, such as the Department of Justice and the Securities and Exchange Commission of the United States. In addition, Mexico reported that a comparative catalogue of financial crimes in Canada, Mexico, Spain, the United Kingdom and the United States had been prepared.

50. Mexico reported that it was a party to the Organized Crime Convention and the Convention against Corruption, as well as to 14 international anti-terrorism instruments, and expressed interest in training sessions on criminalization and investigation in the framework of the strategic association with the European Union.

Morocco

51. Morocco highlighted the challenges posed by economic fraud and identity-related crime, particularly in relation to the development of legislation capable of addressing those crimes effectively. It stressed that most of those crimes were new and emerging forms of crime and that the national Penal Code, dating back to 1962, had not been revised to cope with them adequately. Moreover, there was no legislation in place to deal with digital documents, which meant that identity cards and passports could be falsified easily. An update of existing legislation was provided with the remark that the law on the fight against terrorism included provisions on identity fraud.

Netherlands

52. The Netherlands reported that in recent years a variety of measures against financial crime and fraud had been introduced and expanded and that relevant organizations had been strengthened. The instruments available for confiscation had been expanded and efforts against fraud had been increased significantly. Information was provided on a financial investigation project aimed at integrating financial investigations in the operations of all law enforcement authorities. In addition, a programme focused on implementing measures against fraud had run from 1998 to 2002. In its report, the Netherlands referred to a Cabinet plan to combat fraud and financial crime (2002-2006) and to a programme for reinforcing measures against financial and economic crime (2007-2011) that was part of a broader scheme to increase safety called "Safety begins with prevention". A description of that scheme was provided separately to the Secretariat.

53. The Netherlands reported that a proposal for a new law had been brought before the Parliament with the aim of expanding financial investigative measures in order to increase the chances of confiscating stolen assets and recovering such assets. Regarding the issue of proof of the legitimate origin of the proceeds of crime, the proposed law provided statutory presumptions of evidence that might concern assets acquired over a period of up to six years prior to the criminal offence.

54. With regard to identity fraud, the Netherlands had initiated a programme to avoid errors concerning identity. The programme included all agencies and institutions involved in issuing or processing identity-related information and documents and was based on the notion that a properly functioning public identity chain rested on ensuring the integrity and quality of all underlying processes, documents and registries.

55. It was reported that the Minister of Justice of the Netherlands had initiated legal research on the necessity and desirability of including identity fraud in national criminal law as an offence separate from other existing offences such as forgery. A summary of the study was submitted to the Secretariat. On the basis of the findings of the research, the option of criminalizing identity fraud separately was under consideration.

Norway

56. Norway made particular reference to a specific legal provision on identity theft that had been approved by the Parliament in 2009. Unlike the general provision on

fraud, the provision on identity theft included the unlawful taking of another person's identity. Moreover, the requirements set forth in the Council of Europe Convention on Cybercrime were considered fully implemented in domestic law.

57. Norway reported on special agencies that assisted the national and international police on the one hand and prosecutorial authorities on the other hand in effectively investigating and prosecuting economic fraud and identity-related crime. It noted that a national strategy on cybersecurity had been launched in 2009 to identify which measures were most appropriate for protecting critical computer systems against serious incidents. Since 2010, national passports contained biometric data and additional work was being done to create national identity cards containing similar biometric data.

58. Norway also reported on a national study on identity theft and identity abuses that had been launched in 2010. With regard to effective cooperation between the public and private sectors, reference was made to the Norwegian Centre for Information Security, which focused on information security and identity theft, among other issues, and was funded by the Government and private stakeholders such as banks and insurance companies.

Panama

59. Panama reported on the activities of specialized judicial offices that had been created since 2002 to deal with crimes against the economic order and provided information on the criminalization of some economic and identity-related crimes under its domestic law. Additionally, Panama described steps taken to increase the security of identity documents, such as the establishment of a biometric system capable of recognizing fingerprints.

60. Panama reported on progress made in connection with investigation techniques to deal with pertinent crimes and cooperation between public and private entities within the country. Panama referred to an identity verification system that had been created as a mechanism to combat identity fraud and to the activities of its Computer Forensics Section dealing with cybercrime, economic fraud and identity-related crime, among other issues. At the international level, Panama had participated in training sessions on money-laundering and other economic crimes.

Philippines

61. The Philippines provided a list of actions and measures adopted by its national Anti-Money-Laundering Council to address fraud and identity-related crime, including by bringing cases to court, confiscating the proceeds of crime, assisting the victims of such crimes and undertaking awareness-raising activities.

Poland

62. Poland emphasized the adoption and implementation of a multifaceted approach to countering economic fraud and identity-related crime. In that context, relevant legislation had been adopted to secure stored and transmitted information in electronic systems. Poland reported performing periodic reviews of existing legislation.

63. To make the fight against economic fraud and identity-related crime more effective, special units in prosecutors' offices had been established in Poland. That approach allowed for a more efficient investigation and prosecution of criminals, using the newest information and communications technologies. Moreover, an electronic database had been established allowing for the fast transmission of data and analyses of the typology of economic crime. Within the framework of international cooperation to combat economic fraud and identity-related crime, priority was accorded to collaboration with INTERPOL, Eurojust and the European Judicial Network.

64. Poland provided information on the activities of the National Police and the investigative powers of specialized police units to fight economic crime and cybercrime. The Bureau of International Police Cooperation of the National Police was responsible for international cooperation, training and information-sharing, while contributions concerning credit card fraud ("skimming") were made to Europol. The National Police cooperated with the Ministry of Finance, the Financial Supervision Authority and the financial intelligence unit, as well as the European Anti-Fraud Office, to protect the financial interests of the European Union. Close cooperation between national law enforcement authorities and private sector entities, such as banks and other financial institutions, was reported.

Republic of Moldova

65. The Republic of Moldova reported that the Ministry of the Interior had organized training sessions for staff on the prevention and efficient disclosure of economic crimes, including those involving the use of personal data, and on the content of a new chapter of the national Criminal Code on informational crimes and crimes in the field of telecommunications.

Russian Federation

66. The Russian Federation underlined that despite the fact that fraud appeared in the chapter of the national Penal Code on crimes against property committed in the sphere of business, fraud was not considered an economic crime. The Russian Federation noted that the means used to commit fraud could form a crucial part of other crimes, such as illegal entrepreneurship, illegal banking, money-laundering, the illegal obtention of credit, the counterfeiting of money, stocks and payment documents and fictitious bankruptcy.

67. The Russian Federation reported that identity was protected by the Constitution and the federal law on personal details and that the misuse of personal data was punishable under the Code of Administrative Offences. The problem of the vulnerability of people's identity, however, was also related to cybercrime, as the vast majority of cybercrime offences involved the illegal obtention of an identity. In an effort to develop effective countermeasures in that regard, the Russian Federation had ratified an agreement among the Commonwealth of Independent States on the fight against crimes in the sphere of computerized information.

68. The Russian Federation also reported on the coordination of national authorities to address economic crime effectively. The Ministry of the Interior had been implementing measures aimed at enhancing cooperation with the law enforcement authorities of other States to combat economic and identity-related

crime and at facilitating research into new information, communications and commercial technologies conducive to the commission of such crimes.

69. The Russian Federation referred to international, regional and bilateral treaties used as a legal basis for international cooperation to combat economic fraud and identity-related crime, among other crimes. It reported that the Office of the Prosecutor General was actively involved in increasing knowledge and expertise in the field of international cooperation in criminal matters.

Serbia

70. Serbia provided information on national legislation regulating the detection, prosecution and adjudication of criminal offences against the safety of computer data, as well as crimes related to intellectual property, sexual offences and crimes against the public peace and the constitutional order involving computer networks, systems and data. In addition, Serbia provided the text of criminal law provisions dealing with the crimes of identity theft, economic fraud and the misuse of credit cards. Serbia reported on the establishment of special departments for combating high-technology crime in the Higher Prosecutor's Office and the Higher Court.

Sudan

71. The Sudan indicated that no cases of crimes committed through the Internet had been reported. It pointed out that reports on economic fraud, tax evasion and the counterfeiting of foreign currency had been issued and that perpetrators of such crimes had been brought to justice. Reference was made to institutional mechanisms focusing on improving the detection and criminal investigation of money-laundering.

Sweden

72. Sweden underlined that its domestic legislation made it possible to investigate and prosecute economic fraud and identity-related crime. It reported on an ongoing review of the penal provisions on the forgery of original versions of documents in response to developments in information technology. In addition, the national prosecutorial authority had been conducting training on pertinent issues and produced various reports and guidelines. Action had been taken to improve the collection and quality of relevant data and crime statistics and to enhance support to the victims of economic fraud and identity-related crime. It was stressed that Sweden was a party to several international agreements on cooperation in criminal matters, which were being implemented through ad hoc domestic legislation on extradition, mutual legal assistance and international cooperation in criminal proceedings and through the enforcement of criminal judgements.

Switzerland

73. Switzerland reported on applicable domestic legislation containing provisions on corruption and money-laundering, among other crimes. Regarding the confiscation of the proceeds of crime, specific measures had been adopted to extend the competence of national authorities. The Penal Code had been reformed in the 1990s in order to tackle economic fraud and identity-related crime and, in that connection, the following had been established as offences: false certification, the

unauthorized obtention of data, the deterioration of data, the fraudulent use of computers and the abuse of credit cards and cheques.

74. Switzerland underscored that various institutions were in place for ensuring control of the identity management system and a web page was being used to gather information on identity-related crimes. An institute on the fight against economic crime had been established in 2000 in order to study the impact of economic crime on society and victims and to develop a strategy for fighting that type of crime. One element of such a strategy was cooperation between the public and private sectors, which was encouraged and supported.

75. Switzerland reported being a party to a series of multilateral instruments, including the Organized Crime Convention, the Convention against Corruption and 16 conventions and protocols against terrorism, as well as to all relevant instruments of the Council of Europe. Switzerland had, in addition, concluded bilateral treaties on mutual legal assistance with its neighbouring countries, several States members of the European Union and countries of South-Eastern Europe. The Federal Police Office had been collaborating with INTERPOL and Europol since 2006 and Switzerland had been a party to the Schengen Agreement and the Schengen Implementing Convention since 2008.

Thailand

76. Thailand reported that in 2009 it had amended the Anti-Money-Laundering Act in response to the evolution of economic fraud and identity-related crime. In addition, the Anti-Money-Laundering Office had a long-term plan to update and harmonize legislation with existing international standards.

Togo

77. Togo underscored that although it had not yet adopted specific legislation on economic fraud and identity-related crime, many of its measures currently in force were applicable, including legislative measures included in the provisions of the national Penal Code and other specific pieces of legislation. Togo reported that it had adopted legislation to facilitate international cooperation in criminal matters, including mutual legal assistance, at the regional and international levels.

78. Togo reported on the establishment of competent institutions for the detection and investigation of fraud. Moreover, digitalized systems for the issuance of driving licences and citizenship cards were in place. The Ministry of Security had established a system of issuing biometric passports, and border control mechanisms had been strengthened.

Trinidad and Tobago

79. Trinidad and Tobago reported that the Police Service's units against fraud and corruption were the main bodies tasked with investigating economic fraud and identity-related crime. To successfully pursue extra-territorial investigations, assistance had been sought from INTERPOL and the central authority of Trinidad and Tobago responsible for international cooperation requests. An additional unit, dedicated to cybercrime, was established in 2008 to support online investigations and the prosecution of the perpetrators of cybercrime.

80. Trinidad and Tobago highlighted that training activities for investigators and other officers had been organized in 2008 and 2009 to enhance expertise in cybercrime, forensic accounting, insurance fraud, the counterfeiting of currency, investigation techniques and computer forensics. Trinidad and Tobago referred to the applicable statutes and their amendments used to criminalize economic fraud and identity-related crime and to carry out relevant investigations and prosecutions.

Ukraine

81. Ukraine noted that its law enforcement authorities were involved in countering crimes committed in the sphere of business and identity-related crimes, and provided relevant statistics of action taken. Ukraine reported that a significant amount of fraudulent actions had been carried out using the Internet, primarily on commercial platforms such as online auctions and social networking sites. A stable increase in the unauthorized transfer of money via “Internet client banks” had been observed.

82. Ukraine provided information on legal provisions establishing criminal liability for identity-related crimes and reported on criminal cases instituted by its National Security Service in 2010. It noted that the Ministry of the Interior had developed a project for the period 2010-2015 to combat crime, including corruption, whose main objective was to enable the identification and prosecution of different forms of cybercrime.

United Kingdom of Great Britain and Northern Ireland

83. The United Kingdom referred to its national fraud strategy, which included a strategic review of national measures against identity-related crime. As a result of the review, there was a better understanding of the challenges posed by such crime and the key priorities for taking countermeasures in the future. The Identity Crime Task Force had been established to tackle identity-related crime by bringing together private and public sector organizations and law enforcement bodies with a view to delivering a more integrated response to such crime.

84. The United Kingdom stressed that, under a broader multi-agency programme of activities to combat identity-related crime, significant work had been done, including the following: the launching of a strategy for safeguarding identity; the assessment of the outcome of recent operations to disrupt identity fraudsters, leading to improved information-sharing and the identification of key criminals and organized criminal groups; and the expansion of the work of the Metropolitan Police to target the supply of specialist printing equipment that could be used to produce false identity documents.

III. Work of the core group of experts on identity-related crime

85. Building on practice followed consistently since 2007 and in line with Economic and Social Council resolution 2009/22, in 2010 UNODC held two meetings of the core group of experts on identity-related crime in Vienna, from 18 to 22 January and from 6 to 8 December 2010. The meetings of the core group were run on the basis of a multi-stakeholder approach whose objectives were to bring together representatives from Member States, the private sector, international

organizations and academia, and to pool experiences, develop strategies, facilitate further research and agree on practical action against identity-related crime. The reports on those meetings have been submitted to the Commission on Crime Prevention and Criminal Justice, for its information, as conference room papers (see www.unodc.org/unodc/en/organized-crime/index.html).

86. At the meetings mentioned above, the core group of experts on identity-related crime had the opportunity to review and provide feedback on materials developed by UNODC pursuant to the recommendations of the core group and the mandates contained in relevant resolutions of the Economic and Social Council. Those materials focused on the legal, criminal justice and policy aspects of identity-related crime, including the typology of such crime and approaches to criminalization, international cooperation, the protection of victims and the potential for synergies between the public and private sectors, mainly in terms of preventing identity-related crime. In addition, the core group of experts held in-depth and focused discussions on the use of forensics to combat and prevent identity-related crime and on the most effective means of protecting the rights of victims. The core group of experts served as a platform for conducting a comparative analysis of the problem of identity-related crime and for presenting an overview of the various approaches to tackling it adopted in different regions.

IV. Technical assistance materials on identity-related crime

87. In line with the conclusions and recommendations resulting from the meetings of the core group of experts on identity-related crime, UNODC has been working to promote further research and develop training materials on identity-related crime. In a handbook on the topic, to be published and disseminated in the near future to Member States, UNODC will lay out a range of options and considerations to be taken into account when addressing national criminal justice matters (such as the typology of crime, different approaches to criminalization and the protection of victims) and specific challenges to fostering international cooperation in criminal matters and the potential for synergies and partnerships to be forged between the public and private sectors, mainly with regard to the prevention of identity-related crime. The handbook includes research papers and practical material, including on international cooperation to combat identity-related crime.

88. The above-mentioned handbook on identity-related crime is intended for use by legislators, policymakers, prosecutors and law enforcement authorities and practitioners, as well as other stakeholders (such as representatives of relevant international and intergovernmental organizations, the private sector and academia). It is expected that the handbook could also be used as resource material in technical assistance programmes and capacity-building activities to increase expert knowledge on how to address legal, institutional and operational issues related to identity-related crime as an emerging form of crime.

V. Conclusion

89. The Commission on Crime Prevention and Criminal Justice may wish to take into account the information provided by Member States on national efforts to

implement measures and policies aimed at preventing, investigating, prosecuting and punishing economic fraud and identity-related crime. In doing so, it could provide further guidance to UNODC regarding the delivery of technical assistance to Member States, upon request, with a view to structuring adequate legislative responses to those crimes, developing and maintaining robust investigation and law enforcement mechanisms, adopting best practices and efficient schemes for the protection of victims and ensuring effective and timely international cooperation to curb related offences. The Commission may wish to consider the work of the core group of experts on identity-related crime when discussing elements of a multi-disciplinary approach to preventing and combating identity-related crime.
