United Nations E/CN.15/2014/17

Economic and Social Council

Distr.: General
3 March 2014

Original: English

Commission on Crime Prevention and Criminal Justice
Twenty-third session
Vienna, 12-16 May 2014
Item 7 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 2013/39 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 the work of the United Nations Office on Drugs and Crime to raise awareness about identity-related crime and the appropriate responses to it. The report further contains information on planned activities of the Secretariat geared towards enhancing the capacity of Member States to prevent and combat identity-related crime.

* E/CN.15/2014/1.

V.14-01364 (E) 250314 260314

I. Introduction

1. In its resolution 2013/39, entitled “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime”, the Economic and Social Council took note of the report of the sixth meeting of the core group of experts on identity-related crime.[1] The Council also took note of the outline for model legislation on identity-related crime, as well as the checklist of strategic elements in developing national strategies for the prevention, investigation, prosecution and punishment of identity-related crime, both of which are contained as appendices in the above-mentioned report. The Council further took note of the document on the development of a framework containing the basic components of a national strategy on the prevention, investigation, prosecution and punishment of identity-related crime, as well as the document on successful cases of public-private partnerships to address identity-related crime.

2. In the same resolution, the Council encouraged Member States to consider the adoption and implementation of national strategies on the prevention, investigation, prosecution and punishment of identity-related crime, including the use of public-private partnerships to address identity-related crime. The Council also invited Member States to provide information to the United Nations Office on Drugs and Crime (UNODC) on national efforts, if any, to develop strategies for the prevention, investigation, prosecution and punishment of identity-related crime.

3. Also in its resolution 2013/39, the Council requested UNODC to continue its efforts, in consultation with the United Nations Commission on International Trade Law, to promote mutual understanding and the exchange of views and expertise between various stakeholders, in particular between public and private sector entities, on issues pertaining to identity-related crime through the future work of the core group of experts on identity-related crime, including draft model legislation on identity-related crime. The Council also invited UNODC to continue to cooperate with other international and intergovernmental organizations and academic institutions active in this field by enabling their participation and active involvement in the future work of the core group of experts on identity-related crime.

4. In the same resolution, the Council invited Member States and other donors to provide extrabudgetary resources for the purposes indicated in the resolution, in accordance with the rules and procedures of the United Nations, and requested the Secretary-General to report to the Commission on Crime Prevention and Criminal Justice at its twenty-third session on the implementation of resolution 2013/39.

5. The present report provides information on the efforts of Member States to implement Economic and Social Council resolution 2013/39 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 the work of UNODC to raise awareness about identity-related crime and the need for appropriate responses to it. The present report further contains information on

[1] E/CN.15/2013/25, annex.

planned activities of the Secretariat geared towards enhancing the capacity of Member States to prevent and combat identity-related crime.

II. Overview and analysis of information provided by Governments

6. At the time of submission of the present report, the following Member States had provided information and relevant material on the implementation of Economic and Social Council resolution 2013/39: Algeria, Armenia, Australia, Bosnia and Herzegovina, Chile, China, Dominican Republic, El Salvador, Germany, Guatemala, Iceland, Latvia, Mexico, Poland, Qatar, Russian Federation, Spain and Turkmenistan.

Algeria

7. Algeria reported that it did not have a definition of the concept of identity. However, the ratification of the United Nations Convention against Transnational Organized Crime and its three protocols, as well as the United Nations Convention against Corruption, had an impact on existing domestic legislation. The Criminal Code had been modified to take into account offences related to new information technologies, the use of false identification and false certification and unlawful trading in influence. The Act against money-laundering and financing of terrorism introduced the verification of the identity of natural and legal persons by banks at the time of opening of an account.

8. Moreover, the Criminal Procedure Code had been amended to include new investigation techniques. A 2009 law on data retention obliged service providers to retain the data of their customers, thus allowing the identification of service users. Earlier, in 2004, the Criminal Procedure Code had established special pools of magistrates with ad hoc responsibilities regarding drug trafficking, transnational organized crime, offences involving the automatic processing of data, money-laundering and terrorism. Algeria also reported that the statute of limitations for crimes related to transnational organized crime had been abolished. A bill was being drafted to introduce a protection regime for personal data and the rules for the protection of rights and freedoms, particularly the right to privacy.

Armenia

9. Armenia listed provisions of the national Criminal Code establishing identity-related crimes, fraud and offences involving the use of computer technology. Armenia further referred to its legislation against money-laundering and the financing of terrorism. Currently, a package of 15 draft laws was being discussed by the National Assembly in order to improve the existing legislation in that field.

10. In 2010, the first National Strategy for Combating Money-Laundering and Terrorism Financing had been adopted, followed by the second one in 2012. The National Strategy was aimed at putting in place the legislative and institutional

framework and developing the capacities of stakeholders in the fight against money-laundering and the financing of terrorism.

Australia

11. Australia reported that it had a robust legal framework to combat economic fraud and identity-related crime, which included specific identity-crime offences, as well as privacy legislation that placed safeguards on the use of personal information. Australia's legislative framework was supported by national policies for preventing and addressing identity-related crime. The National Identity Security Strategy outlined how all state governments responded to current and emerging identity security challenges and opportunities. The Strategy had been revised in 2012 to ensure that Australia's approach was appropriate for responding to the rapidly evolving nature of identity-related crime. The Strategy included the establishment of the Document Verification Service and the development of several national standards related to identity management. Australia explained that the Document Verification Service was an online system that allowed agencies to verify in real time the information on key identity documents (e.g. passports and driving licences). Australia stated that its Government was currently working to expand access to the Document Verification Service to certain private sector organizations.

12. Australia reported on other work currently under way to achieve the objectives of the Strategy, including the enhancement of identity proofing by government agencies, the development of measurement indicators to improve the monitoring of identity-related crime, the enhancement of the interoperability of biometric systems and the improvement of support for victims of identity crime.

13. With regard to domestic legislation, Australia reported that it had comprehensive offences to address economic fraud and identity-related crime. The national Criminal Code contained provisions criminalizing, if committed with a certain intention, the acts of dealing in identification information, possessing identification information and possessing equipment to create identification documentation. Australia's privacy legislation ensured that appropriate protections were afforded to identification information and regulated the ways in which such information could be used. Recent changes to the legislation ensured greater consistency by applying the same privacy principles to the public and private sectors. Victims of identity crime could apply for a certificate to assist them in resolving problems caused by identity-related crime.

Bosnia and Herzegovina

14. Bosnia and Herzegovina noted that it had recognized economic crime as a part of organized crime. Currently, the adoption of a national strategy on combating organized crime was pending. That strategy would define the goals, roles and responsibilities of all stakeholders.

15. Bosnia and Herzegovina reported that its State Investigation and Protection Agency carried out prevention activities and investigated economic crime. That Agency would welcome training on the content of Economic and Social Council resolution 2013/39 and the obligations under it. The Agency did not possess any

data on identity-related crime, since such offences related to the competences of the entities of the State. Likewise, the Federal Police Administration did not have information on criminal offences in the field of identity-related crime. However, the Border Police investigated cases of falsified documentation. The national Indirect Taxation Authority and other taxation authorities investigated cases relating to economic fraud, including identity-related offences.

Chile

16. Chile reported that the Public Prosecution Service had, in general, a constitutional mandate to investigate deeds that might constitute crimes and to protect victims and witnesses. There were general criteria with regard to the criminal prosecution and investigation of identity-related crimes.

17. In the field of training, the Money-Laundering and Economic, Environmental and Organized Crime Unit of the National Prosecuting Authority was responsible, within its areas of competence, for the design and implementation of national plans aimed at internal training. Since 2009, issues pertaining to identity-related crime had been included in the training courses. In addition, professionals and Money-Laundering and Economic, Environmental and Organized Crime Unit prosecutors had participated in various training courses organized by international bodies. Furthermore, that Unit had organized jointly with universities academic activities to raise awareness about weaknesses and strengths of the national legal system with regard to related issues. As a result of those actions, the ability to develop effective research had been steadily increasing, while good practices and successes at both the national and international levels had been disseminated to prosecutors and other competent officers.

18. Reference was made to two practical manuals on computer crime and computer fraud. Those manuals presented the most important elements and patterns of computer crime and computer fraud, as well as the most effective measures to investigate and adjudicate relevant cases in court. Both manuals were developed by professionals from the Money-Laundering and Economic, Environmental and Organized Crime Unit and were available to all members of the prosecution.

19. Chile further reported that the Public Prosecution Service participated actively in inter-agency coordination with public sector agencies that had jurisdiction over related issues. For example, the Public Prosecution Service was part of an advisory board that evaluated the state of national legislation and its compliance with international standards, such as those enshrined in the Council of Europe Convention on Cybercrime. Moreover, channels of communication between prosecutors and private sector entities, such as financial institutions and Internet service providers, had been established in the context of specific investigations.

20. The Public Prosecution Service, with the collaboration of specialized police on certain identity-related crimes committed through technological means, had successfully led prosecutions directed against criminal organizations at both the national and international levels. International cooperation could be pursued using the Council of Europe Convention on Cybercrime as a legal basis.

21. In separate information provided by the Ministry of Interior and Public Security, Chile reported on national strategies for the prevention, investigation, prosecution and sanctioning of identity crimes. On 4 August 2010, the Government had launched a plan for public safety, entitled “Safe Chile 2010-2014”, designed by the Ministry of Interior and Public Security, which included a series of actions to combat crime in the areas of prevention, protection, punishment, victim support and rehabilitation of offenders. Part of the plan focused on developing initiatives to reduce the vulnerability of potential victims through personal prevention measures.

22. Chile also referred to a number of guides and manuals on crime prevention, including a guide entitled “Prevention of trade crimes: a collection of international experiences”, which had been published in 2011 and reissued in October 2012. That guide had a chapter on economic crime, cybercrime and manipulation of information, in which the offences were described and relevant recommendations were made.

23. Further reference was made to the development of a programme called “Barrio en paz comercial”, which involved commercial entities affected by high levels of crime. The aforementioned guide on the prevention of trade crimes was distributed to provincial authorities, chambers of commerce and business entities.

24. Chile also reported on a campaign entitled “Secure card”. The campaign had been launched jointly by the National Consumer Service (SERNAC) and the Chilean Investigative Police in June 2013 to provide advice to consumers on how to avoid becoming victims of scams or cloning, especially involving the use of credit cards. The campaign was hosted on the website of SERNAC and contained a number of safety tips and other information. Another campaign, called “Digital consumer: it is good to be informed”, was a joint initiative of the Modernization and Digital Government Unit of the secretariat of the presidency and SERNAC. Its objective was to inform citizens about their rights when shopping or conducting transactions over the Internet so that they could protect themselves from scams and unfair practices involving the use of their personal data. A third campaign, called “Trade prevention and protection”, was run by the National Chamber of Commerce and Tourism Service of Chile. It was reported that the Chamber of Commerce was developing a plan aimed at producing a series of national seminars on the topic “Prevention and protection: keys to trade”, with the collaboration of law enforcement agencies and private companies. The objective of the seminars was to provide traders with tools and knowledge to prevent crime and strengthen the protection of their business.

25. In addition to its investigative duties in the field of identity-related crime, the Chilean Investigative Police offered lectures to students and teachers in primary and secondary education centres about the prevention of cybercrime, including crimes involving identity theft. On 6 May 2013, the Investigative Police had signed an agreement with the National Service for the Elderly to make joint efforts to contribute to the prevention of economic crime committed against the elderly. Through the National Office of Public Affairs of the Investigative Police, efforts were being made to raise awareness through the media about new criminal patterns and modi operandi of fraud. The police had special officers for the investigation of economic crime and cybercrime.

26. Reference was also made to the Carabineros, a police institution with a special unit responsible for the investigation of economic crime and cybercrime. The Office of Financial Research and Money-Laundering also undertook investigative and preventive actions against economic fraud and identity crimes. Furthermore, the Carabineros were involved in preventive activities with other institutions such as the Public Ministry, the customs service and banks.

China

27. China reported on provisions of its domestic legislation that were applicable in cases of identity abuse. The Chinese Criminal Code established a number of offences relevant to identity data, e.g., Impairment of Credit Card Usage (art. 177), Bill (Banknote) Fraud (art. 194), Letter of Credit Fraud (art. 195), Credit Card Fraud (art. 196), Contract Fraud (art. 224) and Forgery and Alteration of Resident Identity Cards (art. 280, para. 3). The rationale behind those provisions was that the above-mentioned offences infringed citizens' identity data and right of privacy, destroyed the normal functioning of the market and seriously harmed society.

28. In recent years, certain legislative measures had been undertaken to counter the increase in crimes related to citizens' identity data. In February 2005, the Standing Committee of the National People's Congress had adopted the Fifth Amendment to the Criminal Code and by article 1 of the Amendment had added to article 177 of the Criminal Code the offences of Impairment of Credit Card Use and Theft, Purchase and Illegal Supply of Credit Card Data, thereby establishing the collection of financial information and the falsification (forging) of personal data, as well as credit card fraud and committing other offences by using credit cards, as distinct criminal offences in order to counter those complicated modern economic crimes.

29. In 2009, the Supreme People's Court and Supreme People's Procuratorate Clarifications on Certain Questions of Detailed Application of Law in Cases of Impairment of Credit Card Use had been published, wherein detailed rules had been established with regard to the offences of Impairment of Credit Card Use and Theft, Purchase and Illegal Supply of Credit Card Data. Based on law and judicial clarifications, the competent units of procuratorate bodies had continued to strengthen their efforts in fighting relevant offences.

30. In February 2009, the National People's Congress had adopted the Seventh Amendment to the Criminal Code. In article 7 of the Amendment, the offences of illegal supply of citizens' personal information and illegal obtainment of citizens' personal information had been added to article 253 of the Criminal Code. Those provisions had incorporated the legal framework of protection of citizens' personal data and criminalized the illicit conduct of committing fraud by using stolen identities.

31. In order to more efficiently counter and punish criminal offences infringing citizens' personal information and to fully guarantee the safety and legality of the individual private data of citizens, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security had jointly issued on 23 March 2013 the Notification on Punishment of Illicit Conduct Infringing Personal Information of Citizens. At the same time, they had required security

bodies at every level, procuratorate bodies and People's Courts to increase their knowledge, apply laws justly, strengthen coordination, decisively fight illicit conduct infringing people's personal information and set up long-term mechanisms for protecting against and fighting crime.

32. Attention was also being devoted to elements of economic fraud crime. China was actively promoting the build-up of a credit network and constructing a mechanism for countering the criminal environment associated with offences relevant to personal information through, for example, the establishment of databases of filed and investigated cases of bribery and the provision of information to the public on relevant inquiries.

33. From January 2010 until December 2012, the People's Courts had adjudicated 192 cases of selling, illegally providing and illegally obtaining personal information of citizens. Convictions were issued in 276 cases.

34. In the field of international cooperation, China had been actively conducting exchanges of information to combat transnational crimes involving bank cards with Canada, Denmark, the United Kingdom of Great Britain and Northern Ireland and the United States of America. Plans for broadening law enforcement cooperation with more countries and regions in certain areas included the following:

(a) Strengthening intelligence exchange, especially by strengthening cooperation in the investigation of transnational crimes involving bank cards; informing foreign counterparts in timely fashion of the mutually relevant transnational bank cases and relevant investigation details; and annual reporting on the general national aspects of transnational bank cases;

(b) Establishing a system of mutually exchangeable blacklists of suspects in crimes involving bank cards. The investigation bureaus of the Ministry of Security had already created the blacklist of suspects in banking fraud crimes. It was suggested that each year mutually relevant blacklists of suspects in financial crimes would be exchanged with foreign police forces in order to facilitate the provision of information to law enforcement authorities;

(c) Strengthening mutual visits and exchanges and actively promoting multifaceted training activities. Such training activities could include the exchange of information on legal systems, recent methods of committing banking card crimes and exchanges of experience in fighting identity-related crime.

35. China stressed that the Government attached great importance to the prevention of and fight against identity crimes and that the judicial and law enforcement authorities undertook considerable efforts in that area. Currently, China viewed the following areas of the prevention of and fight against identity crimes as priority issues:

(a) Addressing the falsification (forgery) of identity with a focus on the element of defrauding the victim;

(b) Responding to the crime of using media to falsify (forge) personal identity;

(c) Combating the crime of transmitting falsified (forged) identity and other data via radio and television;

(d) Addressing the crime of committing fraud by disseminating multiple text (SMS) messages involving falsified (forged) identities via mobile phones;

(e) Preventing and combating Internet fraud committed by using forged identity.

Dominican Republic

36. The Dominican Republic reported on its national strategy against identity fraud (2012-2013), aimed at ensuring the issuance and renewal of passports according to international standards of quality and safety. The national strategy was intended to enhance security controls and raise the technological level of security standards for passports, including through preventive and reactive security measures, in accordance with Law No. 208-71; the modernization of technological platforms and communications; the enhancement of security measures in the administration of passports (transport, design, production and storage); the enhancement of inter-agency collaboration and exchange of information; collaboration with the General Directorate of Migration; institutional collaboration with the Office of the Attorney General; strategic partnership with the Central Electoral Board; institutional collaboration with the National Investigations Department, the National Police and International Criminal Police Organization (INTERPOL); and training, workshops, presentations and courses.

37. The national strategy also included policies and measures for strengthening the investigation, prosecution and punishment of identity crime. Such policies were implemented by the Fraud Department, which collaborated with the Central Electoral Board, the General Directorate of Migration, the National Police, the Central Directorate of Criminal Investigation, the Public Prosecutor and INTERPOL. Resolution No. 3/2013 established penalties for stealing passports, the gravity of which was subject to the number of passports stolen. Resolution No. 6/2010 established the investigative procedure to be followed by the Fraud Department in cases of suspected fraud and detection of false documents. Those resolutions facilitated the investigation and prosecution of a significant number of offenders, who were sentenced to terms of imprisonment ranging from six months to one year, plus a fine.

38. The Dominican Republic also referred to a project to amend the aforementioned Law No. 208-71. The most important amendments included more streamlined regulations on the establishment of the legal personality of entities, which would allow the General Directorate of Passports of the Ministry of External Relations to initiate legal proceedings; the adoption of protocols of action and cooperation for the pursuit of identity-crime offenders; the application of special sanctions in case of unusual recurrence of losses; and the centralization of the passport system.

El Salvador

39. El Salvador provided information on national initiatives focusing on the prevention, investigation and punishment of identity-related crime. A group of prosecutors had been established to investigate relevant cases. There was an

anti-organized crime unit and an anti-financial crime unit within the General Prosecution, entrusted with the investigation of such cases. There were also teams within the national Civil Police that acted jointly with prosecutors in investigations.

40. With a view to enhancing the effectiveness of investigations, there was constant communication and coordination with banks and financial institutions, which reported the detection of fraudulent economic activities or any kind of identity fraud. Moreover, there was an agreement on cooperation between the National Registry of Persons and the General Prosecution for the exchange of information to facilitate investigative action. That enabled the prompt determination as to whether information about the identity of persons had been fraudulently used. When repetitive patterns of fraud were detected in a certain group of people, the information was disseminated through the media to alert the citizens and prevent them from becoming victims.

Germany

41. Germany stated that existing criminal provisions were used to deal with identity-related crime. Such offences included acts of data espionage, “phishing”, theft, fraud, computer fraud, forgery, tampering with official identity documents, acquisition of false official identity documents and misuse of identity documents.

42. Germany reported that the Federal Criminal Police Office was dealing with identity crime cases. To the extent possible and necessary, it also exchanged information with non-governmental organizations. In particular, the national Information and Communications Technology Strategy, which was developed on the basis of the Council of Europe Convention on Cybercrime, provided for close cooperation with industry associations and security authorities.

43. Germany highlighted that its Police Crime Prevention Programme addressed identity fraud and identity theft. A so-called security compass, which was introduced by the Federal Office for Information Security, provided the public with simple rules on how to use the Internet safely, thus providing effective protection from identity-related dangers posed by the Internet. A collection of leaflets informed users about the risks of using computers, smartphones and similar devices, and social networks.

Guatemala

44. Guatemala reported the lack of specific guidelines on identity-related crime despite the existence of statistical data reflecting the occurrence of such crimes. For the period from 2005 to 2013, the following categories of identity crime had been reported: negligent and intentional fraud, use of forged documents, illegitimate use of identification, misuse of uniform and insignia, public use of a false name, usurpation of position and usurpation of functions.

45. The largest number of complaints about identity crime had been reported in 2012 (9,383 cases, almost the same number as in 2007). In 2013, only 6,712 cases had been reported. Every year, the most documented type of identity crime was intentional fraud: from 2005 to 2013 there were 26,890 cases of intentional fraud.

Iceland

46. Iceland reported that it did not have a national strategy for the prevention, investigation, prosecution and punishment of identity-related crime. Furthermore, no national efforts were ongoing to develop such strategies. However, it was underlined that the national authorities were currently preparing a national cybersecurity strategy that would take into consideration measures against cybercrime, possibly including online identity-related crimes.

Latvia

47. Latvia provided information on the policy documents, legal acts and reporting mechanisms established to fight identity-related crimes. Reference was made to the National Security Concept of 2011, the development of a passport system and a unified migration information system, the National Strategy for the Prevention of Child Criminality and Protection of Children from Criminal Offences of 2013 and the Action Plan on Preventing and Combating Organized Crime for the period 2014-2016. Latvia also highlighted its existing mechanisms (hotlines, websites of the police and the Safer Internet Centre) for reporting economic fraud and identity-related crime.

48. The Safer Internet Centre had the task of informing and educating children, teachers and parents about potential threats on the Internet, including identity theft and misuse of personal data. In addition, the Information Technology Security Incident Response Institution had been established in 2006 to provide support, inter alia, to State institutions in safeguarding national information technology security. The Latvian law enforcement authorities had submitted a project application to the European Commission regarding the development of uniform standards for identity documents in the European Union.

49. Latvian criminal law provided for liability for economic crimes, including fraud and fraud in automated data-processing systems, acquisition of personal identification documents, concealing personal identity and various types of information technology-related criminal activities.

Mexico

50. Mexico confirmed that, although at the state level there were laws establishing identity abuses as offences, there was no federal legislation punishing identity-related crime. The following legislative initiatives were currently pending before the Congress for approval:

(a) Draft decree incorporating article 287 bis in the Federal Criminal Code. That provision would criminalize the impersonation of identity and would establish punishment by deprivation of liberty for a term of two to six years and a fine of 500 to 700 days of minimum wage for any person who used any means to misappropriate personal data or unlawfully impersonate another person, with or without his or her consent, for the purpose of causing damage or taking undue advantage for himself or herself or for another. Penalties would increase by one half

for those who used homonyms or physical or vocal resemblance, deceptive methods based on similarity or likeness;

(b) Draft decree incorporating in the Federal Penal Code the description of behaviours related to human trafficking and the offences of unlawful disclosure of information, crimes against peace and security, and economic crimes such as fraud and extortion that were committed through the use of computer systems;

(c) Draft initiative decree amending article 211 bis of the Federal Criminal Code. The amendment would penalize identity theft and would establish punishment by deprivation of liberty for a term of six months to one year and a fine of 100 to 1,000 days of minimum wage for any person who sought profit by creating replicas of systems to get access to information that he or she was not entitled to possess;

(d) The initiative to amend and supplement certain provisions of the Federal Penal Code to criminalize various behaviours related to the use of computer systems. The aim was to establish or increase penalties in relation to crimes conducted through information technology. Another aim was to increase penalties for those involved in child pornography, as well as those involved in stealing or destroying personal information and those who covered up operations involving illegal proceeds.

Poland

51. Poland reported that in February 2013, the Government adopted the Efficient State Strategy 2012, one of nine country-development strategies. That Strategy underlined the necessity of activities to reduce economic crime. To that end, it was highlighted that an economic crime prevention programme was currently being prepared by the Ministry of the Interior. The aim of the economic crime prevention programme was to increase the effectiveness of the instruments to prevent and combat economic crime in specific areas. Those areas included fraud and financial crime in the banking sector, insurance fraud and money-laundering. The programme called for attention to the risks associated with “phishing” and skimming (the illegal copying of payment cards).

52. Poland noted that the implementation of the economic crime prevention programme was planned for 2014. It would be accompanied by appropriate legal or organizational changes, as well as by specialized training modules or preventive actions. The national law enforcement authorities also planned to strengthen the division responsible for the protection against economic crime by organizing training courses and increasing the number of employees.

Qatar

53. Qatar reported that its Ministry of Interior had developed strategies to prevent economic fraud and identity-related crime. In the field of international cooperation, Qatar was one of the founders of the Information Technology Expert Group for the Middle East and North Africa region and participated in the development of strategies and plans to counter computer crime, including computer fraud.

54. The Ministry of Interior established partnerships with telecom companies, service providers and websites to identify suspects in order to prosecute them. Furthermore, there was cooperation with credit card companies to identify fraudulent operations. Efforts were being made to keep pace with technological developments through the use of modern technological devices and software, as well as staff training.

55. Qatar confirmed its coordination with other countries in the Gulf region, including through the exchange of information on economic fraud (criminal methods, personal photos, copies of passports etc.) in order to prevent the occurrence of such offences.

Russian Federation

56. The Russian Federation referred to the national legislation on the management of personal data, as contained in Federal Law No. 152-FZ of 27 July 2006, on personal data. Liability for the violation of the provisions of the law entailed disciplinary, administrative and criminal sanctions. In order to counter the use of personal data during the process of setting up legal persons, new types of criminal offences had been established through articles 173.1 (illegal organization of legal persons) and 173.2 (illegal use of documents for the organization of legal persons) of the Criminal Code.

57. In the area of protection of the constitutional rights of Russian citizens, the Criminal Code established liability in articles 137 (violation of privacy and private life), 140 (refusal to provide information to a citizen), 159.6 (fraud in the area of computer information) and 272 (illegal access to computer information).

58. Pursuant to article 151 of the Code of Criminal Procedure, the offences stipulated in articles 137 and 140 of the Criminal Code fell within the jurisdiction of the Investigative Committee, whereas the crimes stipulated in article 159.6 of the Criminal Code were under administrative jurisdiction. The investigation of criminal cases of an economic nature had demonstrated the frequent use of personal data in fraudulent schemes in banking transactions, as well as the usage of sham legal persons.

59. It was further reported that the Bank of Russia adopted measures on a regular basis for the identification of clients and beneficiaries, including in the area of countering illegal financial transactions.

Spain

60. Spain reported on legal measures implemented in the field of identity-related crime, including measures geared towards enhancing protection in the administrative and commercial spheres. In that regard, reference was made to the European Union regulatory and “soft law” framework (recommendation 88/590/EEC of the European Commission on payment systems and the relationship between card users and the card issuers; recommendation 97/498/EEC of the European Commission, on the payment transactions by electronic instruments; and directive 2009/136/EC of the European

Parliament and the Council of the European Union amending directive 2002/22/EC, on users' rights relating to electronic communications networks and services; directive 2002/58/EC, concerning the processing of personal data and protection of privacy in the electronic communications sector; and regulation (EC) No. 2006/2004, on cooperation between national authorities responsible for the enforcement of consumer protection laws. At the national level, Law No. 15/1999, on the protection of personal data, Law No. 7/1996, on fraudulent purchases, and Royal Decree 1720/2007 provided the relevant protective framework. Any company that dealt with personal information should apply a series of measures to ensure the confidentiality and security of documentation.

61. With regard to measures providing administrative and commercial protection in transactions involving information, and communications technologies, and supplementing civil sanctions and criminal investigations, Spain made reference to Law No. 32/2003, on general telecommunications; Law No. 34/2002, on services of the information society and electronic commerce; Law No. 59/2003, on electronic signatures; Law No. 25/2007, on preservation of data and electronic communications and public communications networks; and Royal Decree 424/2005.

62. With regard to substantive and procedural criminal aspects, the Penal Code established a series of criminal offences of relevance, such as those on fraud (article 248) and fraud related to documents (articles 390-403). Furthermore, the Criminal Procedure Code established measures in articles 301, 302 and 579 to ensure the confidentiality of proceedings and the possibility of intercepting communications for the investigation of crimes. Law No. 10/2010, on money-laundering and the financing of terrorism, provided for control measures, as well as for the prevention of fraud and the use of proxies to hide the identity of persons involved in fraudulent practices.

63. In general, Spain indicated that there was no legal vacuum regarding protection from the criminal misuse and falsification of identity. However, it was stated that some aspects of the domestic legal framework could be improved to ensure the imposition of stricter measures for perpetrators of relevant criminal activities. Spain also stressed the lacunae in international cooperation to combat related offences owing to divergent national legal approaches.

64. Spain referred to the creation of a national centre for the protection of critical infrastructure with the aim of providing protection in cases of cyber attacks within the scope of organized crime and terrorism. Moreover, it was reported that a national security scheme had been put in place through Law No. 11/2007 to strengthen the security of information systems and communications networks and support critical infrastructure. Security was further increased regarding access to personal, commercial and administrative data in all digital files.

65. It was also noted that various initiatives had been developed by the Interbank Cooperation Centre and the National Association of Financial Institutions to establish an early warning system to reduce the incidence of fraud. The Bank of Spain had developed a code of conduct regarding card payment systems.

Turkmenistan

66. Turkmenistan reported that the Ministry of Internal Affairs carried out preventive and investigative searches, as well as operational activities focusing on prevention, tracing and the interlinkages of economic crimes. Specialized units of the Ministry carried out fact-finding searches and investigations for those involved in economic crimes. The evidence gathered was sent to the investigative units of the Ministry for further investigation and subsequent transmittal to the judicial authorities.

67. Turkmenistan also referred to the domestic legal framework on money-laundering and financing of terrorism, as well as the provisions of the Criminal Code establishing offences of an economic nature.

68. In the preparation of analyses of economic crimes, special attention was given to violations constituting illegal business-related activities. On a case-by-case basis, an assessment was made regarding the legal relationships affected by and the duration and nature of the violation, together with the measurement of the proceeds derived from the offence, in order to classify the illegal activity as being business-related or not.

69. Turkmenistan highlighted that educational capacity-building seminars, with the participation of international organizations, were held for staff of the Ministry of Interior and students of the Police Institute to improve their professional skills in the detection of economic crimes and the identification of relevant criminal patterns. It was stressed that the emergence of new types of crime in this area required further capacity-building for identifying organizations and individuals involved in committing economic crimes and tracing funds illegally transferred through the use of banking systems.

III. Raising awareness about identity-related crime

70. With a view to raising awareness about the impact and the consequences of, as well as appropriate responses to, identity-related crime, UNODC was invited to attend the Technology against Crime International Forum on the topic “Technologies for a safer world”, held in Lyon, France, on 8 and 9 July 2013. Organized with the sponsorship of the French Ministry of Interior and INTERPOL, the Forum’s objective was to allow forward-thinking discussions and raise awareness on how technology could contribute to enhancing crime reduction policies and addressing new challenges posed by crime.

71. UNODC participated in the panel of the second round table of the Forum, on the topic “Protecting identity”. The discussion revolved around the “basis of identity” as a means of identification, the different concepts of identity, the challenges posed by the criminal misuse and falsification of identity and the legal responses to identity-related crime. The protection of victims of identity-related crime, issues of international cooperation and the role of the private sector were also analysed. In the ensuing discussion, focusing on prevention, UNODC contributed to the exchange of views on the twofold interrelationship between technology and identity: how technology could facilitate the exercise of the basic right to an identity, and how technology was likely to reinforce trust in the use of identity.

UNODC presented the options offered at both the legislative and policy levels for more effective criminal justice and law enforcement responses to identity-related crime.

IV. Planned activities of the United Nations Office on Drugs and Crime

72. Owing to a lack of extrabudgetary resources, the Secretariat was not in a position to organize an additional meeting of the core group of experts on identity-related crime. The availability of the necessary resources for the organization of such a meeting would enable UNODC to comply with the mandate contained in Economic and Social Council resolution 2013/39 "to promote mutual understanding and the exchange of views and expertise between various stakeholders, in particular between public and private sector entities, on issues pertaining to identity-related crime through the future work of the core group of experts on identity-related crime". It would further provide the opportunity to use the core group of experts on identity-related crime as a "platform of expertise" for the development of model legislation on identity-related crime, addressing the needs of both common-law and civil-law systems and taking into account the views and remarks of different stakeholders from Member States, international organizations, the private sector and academia.

73. Looking ahead, UNODC is also planning to develop, subject to the availability of extrabudgetary funds, a web-based repository of information on identity-related crime. It is envisaged that such a repository will include:

(a) Relevant national legislation from Member States;

(b) Statistics on the nature and extent of identity-related crime from different jurisdictions, where available (including, where feasible, from the victim's perspective), on the relationship of identity-related crime with other criminal activities and on the impact of identity-related crime on private entities;

(c) Information and good practices for the development and implementation of national strategies or programmes against identity-related crime;

(d) Information on initiatives and measures that have been taken by the private sector against identity-related crime;

(e) Information and good practices of public-private partnerships for use against identity-related crime;

(f) Useful practices and efficient mechanisms for supporting and protecting victims of identity-related crime, for restoring victim identity and for victim remediation, including measures that have been taken by the private sector to protect customers from being victimized;

(g) Links to other relevant existing reports, studies, policy papers, assessments, handbooks and other tools for practitioners.

74. UNODC is further planning, depending on the availability of extrabudgetary funds, to develop a comprehensive package of training tools as follows:

(a) A comprehensive training manual for law enforcement and other relevant officials specialized in identity-related crime;

(b) Modular material, to be annexed to the above-mentioned training manual or for inclusion in existing training materials for law enforcement and other relevant officials, on the links between identity-related crime and other forms of crime, including economic fraud, money-laundering, corruption, terrorism and cybercrime.

75. That package of training tools will supplement the study on fraud and the criminal misuse and falsification of identity commissioned by UNODC and submitted to the Commission on Crime Prevention and Criminal Justice at its sixteenth session,[2] as well as the practical guide to international cooperation to combat identity-related crime, contained in the UNODC *Handbook on Identity-related Crime* (2011).[3] It will further address the needs of both common-law and civil-law systems, as well as differences between Member States with centralized infrastructures for identity matters and those with ad hoc approaches to identification information. The development of the training materials will facilitate, in the long run, the organization of regional training courses by UNODC, with a view to improving international cooperation.

V. Conclusions and recommendations

76. 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. The Commission may also wish to encourage the core group of experts on identity-related crime to take that information into consideration when discussing elements of a multidisciplinary approach to preventing and combating identity-related crime.

77. The Commission may also wish to consider the future directions of the work of the Secretariat in the field of identity-related crime and, in so doing, focus on planned UNODC activities and provide further guidance on ways and means to provide more effective and efficient technical assistance to requesting Member States.

78. The Commission may further wish to recommend that particular attention be devoted, as appropriate, to the challenges posed by identity-related crime in the preparatory phase for the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, particularly when preparing the draft declaration of the Congress, as well as in the deliberations of the Congress, when discussing item 5 of its provisional agenda, entitled “Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime”.

---

[2] See E/CN.15/2007/8 and Add.1-3.

[3] www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.