United Nations E/CN.15/2009/2

Economic and Social Council

Distr.: General
3 February 2009

Original: English

Commission on Crime Prevention and Criminal Justice
Eighteenth session
Vienna, 16-24 April 2009
Items 3 (a) and 4 of the provisional agenda*

Thematic discussion: "Economic fraud and identity-related crime"

World crime trends and responses: integration and coordination efforts of the United Nations Office on Drugs and Crime and by Member States 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

Contents

* E/CN.15/2009/1.

V.09-80493 (E)

I. Introduction

1. In its resolution 2007/20, entitled "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime", the Economic and Social Council recalled its resolution 2004/26, in which it had requested the Secretary-General to convene an intergovernmental expert group to prepare a study on fraud and the criminal misuse and falsification of identity and to submit a report containing the results of that study to the Commission on Crime Prevention and Criminal Justice at its fifteenth or, if necessary, sixteenth session, for its consideration, welcomed the report of the Secretary-General on the results of the second meeting 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), which had been submitted to the Commission at its sixteenth session, and encouraged Member States to consider the report and, as appropriate and consistent with their domestic law, national legal framework, including jurisdiction, and relevant international instruments, to avail themselves of its recommendations when developing effective strategies for responding to the problems addressed in the report, bearing in mind that further study might be appropriate.

2. Also in its resolution 2007/20, the Economic and Social Council encouraged Member States to consider updating their laws in order to tackle the recent evolution of economic fraud and the use of modern technologies to commit transnational fraud and mass fraud; and also encouraged Member States to consider establishing or updating, as appropriate, criminal offences for the illicit taking, copying, fabrication and misuse of identification documents and identification information.

3. Also in its resolution 2007/20, the Economic and Social Council encouraged Member States to take appropriate measures so that their judicial and law enforcement authorities might cooperate more effectively in fighting fraud and identity-related crime, if necessary by enhancing mutual legal assistance and extradition mechanisms, taking into account the transnational nature of such crime and making full use of the relevant international legal instruments, including the United Nations Convention against Transnational Organized Crime[1] and the United Nations Convention against Corruption;[2] and also encouraged Member States to consult and collaborate with appropriate commercial and other private sector entities to the extent feasible, with a view to understanding more fully the problems of economic fraud and identity-related crime and cooperating more effectively in the prevention, investigation and prosecution of such crime.

4. Also in its resolution 2007/20, the Economic and Social Council requested the Secretary-General to report to the Commission, at its eighteenth session, on the implementation of Council resolution 2007/20.

5. The present report provides an overview and an analysis of the replies received from Member States on their efforts to implement Economic and Social Council resolution 2007/20 and their domestic policies and measures in the areas of prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

---

[1] United Nations, *Treaty Series*, vol. 2349, No. 42146.

[2] Ibid., vol. 2225, No. 39574.

II. Overview and analysis of replies received from Member States

6. The following Member States provided input and relevant material: Austria, Azerbaijan, Bahrain, Belarus, Bulgaria, Canada, Egypt, Estonia, Germany, Greece, Japan, Jordan, Kuwait, Latvia, Mexico, Morocco, Saudi Arabia, Serbia, Spain, Tunisia, Ukraine and Uruguay.

Austria

7. Austria noted that economic fraud and identity-related crime were associated with corruption and that the implementation of the corresponding provisions in chapters III and IV of the Convention against Corruption should, therefore, be supported by appropriate national legislative measures. Austria stressed the need for enhanced international coordination and cooperation to effectively combat those forms of crime. In that regard, reference was made to an initiative of Austria to establish, in 2004, the European anti-corruption contact point network (European Partners against Corruption), which Austria had chaired since its establishment. Furthermore, it was reported that, with a view to improving cooperation with the business and private sectors, the national authorities had organized annual events, such as "Austrian Anti-Corruption Day" and international anti-corruption summer schools, which had provided a platform for national and international experts to exchange experiences and discuss various aspects of countering corruption.

Azerbaijan

8. Azerbaijan referred to domestic legislation containing provisions on the criminalization of numerous offences, including the following: fraud; the illegal acquisition and disclosure of data constituting commercial or bank secrets; illegal access to computer information; counterfeiting; the sale of official documents, State awards, seals, stamps and blank forms; the use of forged documents and larceny; and the destruction of official documents, stamps and seals. Those provisions were to be considered, as appropriate, jointly with other provisions of the national legislation on the criminalization of corruption, money-laundering, illegal migration and trafficking in persons.

9. In the field of international cooperation, Azerbaijan stated that it had concluded a number of bilateral and multilateral agreements to combat economic crime and had participated in regional schemes and organizations, such as the Black Sea Economic Cooperation Organization, the Commonwealth of Independent States, GUAM and the Economic Cooperation Organization. Azerbaijan was also a party to a number of relevant international instruments, including the United Nations Convention against Transnational Organized Crime and the Protocols thereto[3] and the Convention against Corruption.

10. Azerbaijan further reported on national action to gather data on crime trends, specifically with regard to identity-related crime committed with the aim to

[3] Ibid., vols. 2225, 2237, 2241 and 2326, No. 39574.

facilitate the procurement of the illegal entry of migrants and trafficked persons in the national territory. Further reference was made to measures taken to ensure the integrity of identification information systems, including the establishment of consolidated databases and ongoing efforts to put in place a system of biometric identification, taking into account international practice.

Bahrain

11. Bahrain provided information on its legislation to combat economic crime, fraud and money-laundering. To that effect, the establishment of a special unit within the Ministry of the Interior responsible for the prevention of economic crime was emphasized.

Belarus

12. Belarus reported that its Criminal Code was being updated to keep up with developments in the field of economic crime. Besides criminalizing fraud, the Criminal Code would also criminalize: the commission of theft using computer technology; the unauthorized access to computerized information; the modification of computerized information; computer sabotage; the wrongful appropriation of computerized information; the manufacture or sale of special tools for illegally obtaining access to computer systems or networks; the development, use or dissemination of harmful programs; and the violation of the rules for operating computer systems or networks. Furthermore, under the Criminal Code the following were also considered as offences: acts related to the theft of passports and other personal documents and the illegal acquisition, counterfeiting, manufacture, use or sale of official or forged documents.

13. Belarus stressed that it was a party to the Organized Crime Convention and the Convention against Corruption and that cooperation with other countries in the fields of extradition and mutual legal assistance was provided on the basis of those legal instruments. Law enforcement cooperation with other States members of the Commonwealth of Independent States was based on the Intergovernmental Programme of Joint Measures to Fight Crime, approved in 2007. Other bilateral instruments on law enforcement cooperation had been concluded with Lithuania, Moldova, the Russian Federation and Ukraine. With regard to economic and identity-related crimes, the national law enforcement authorities were cooperating closely with their counterparts in other countries through the International Criminal Police Organization (INTERPOL) and on the basis of bilateral agreements. Belarus also reported on efforts to intensify cooperation with tax (financial) investigation agencies in other countries. Statistical data on recorded fraud cases, including cases of a transnational nature, were also provided.

Bulgaria

14. Bulgaria provided an overview of national criminal law provisions pertaining to computer-related fraud and the forgery of documents. It was reported, in this connection, that in 2002 a new provision on the criminalization of computer-related

fraud was introduced in the domestic legal system and further amended in 2007. The unauthorized access to computer data of any kind, including identification information, was also criminalized. In addition, criminal offences for drawing up untrue official documents or forging the contents of an official document were in place and included provisions for aggravating circumstances where identification documents or personal or registration data were the subject of the criminal behaviour.

15. Bulgaria was a party to the Organized Crime Convention and the Protocols thereto, the Convention against Corruption and the Convention on Cybercrime.[4] The requirements contained in articles 2 and 3 of the Organized Crime Convention had been fully implemented. To the extent that offences related to the criminal misuse and falsification of identity were serious crimes under domestic legislation and were aligned with the requirements of the Organized Crime Convention, the provisions of that Convention were also applicable to those offences. Furthermore, Bulgaria reported that it was a party to the European Convention on Mutual Assistance in Criminal Matters,[5] as well as the European Convention on Extradition[6] and the Additional Protocol[7] and the Second Protocol to that Convention.[8] Bulgaria also incorporated into its domestic legal framework the Council of the European Union framework decision 2002/584/JHA on the European arrest warrant and the surrender procedures between member States,[9] and the Council of the European Union Act 2000/C 197/01 establishing, in accordance with article 34 of the Treaty on the European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[10] Accordingly, Bulgaria had in its legislation a comprehensive framework allowing for efficient legal cooperation in criminal matters, including controlled deliveries, videoconferencing and establishment of joint investigation teams.

Canada

16. Canada referred to the relevant work of the Commission on Crime Prevention and Criminal Justice and the United Nations Office on Drugs and Crime (UNODC), recalled the active participation of Canada in that work and reported that, in view of the broad scope of the subject matter of economic fraud and identity-related crime, it was necessary to focus on agreed priority areas. In that connection, it noted that some assistance might be needed by Member States seeking to update existing legislation on fraud to deal with large-scale fraud and other, new forms of fraud based on cybercrime, including updates on offences, and to ensure consistency with domestic and international standards and practices. That might involve the development of additional materials; however, to maximize synergies and avoid unnecessary duplication, existing material on cybercrime and fraud, including materials based on the Convention on Cybercrime, should be used wherever

---

[4] Council of Europe, *European Treaty Series*, No. 185.
[5] Ibid., No. 30.
[6] Ibid., No. 24.
[7] Ibid., No. 86.
[8] Ibid., No. 98.
[9] *Official Journal of the European Communities*, L. 190, 18 July 2002.
[10] Ibid., C. 197, 12 July 2000.

possible. Furthermore, Canada expressed the view that future work should focus on dealing with the emerging problem of identity-related crime. In view of the ongoing work of intergovernmental and non-governmental organizations in that area, there should be as much coordination as possible to avoid duplication and inconsistencies. Moreover, the role of the Commission on Crime Prevention and Criminal Justice and UNODC should be crime-based, focusing on the development and delivery of assistance to Member States for defining identity crimes and related concepts, establishing appropriate criminal offences and developing appropriate measures aimed at crime prevention and victim support. The United Nations bodies should also, to the extent feasible, provide assistance to other entities working on specific forms of identification documents, such as passports and commercial identification, to ensure that crime prevention and criminal justice concepts are taken into consideration. Other priority areas in that regard would include the enhancement of international cooperation for the investigation and prosecution of offences and the promotion of cooperation among relevant entities, including commercial entities and Member States, to assist victims in repairing or restoring damaged identities.

17. While Canada agreed that the major focus of future work should be on the emerging issue of identity-related crime, it also highlighted the close links between that form of crime and fraud and the fact that the intergovernmental expert group entrusted with the task of conducting a study on fraud and the criminal misuse and falsification of identity recommended ongoing coordination in work done in the two areas. In that connection, future work should take into account that it might be difficult, in the foreseeable future, to distinguish between identity crime and identity-related crime such as fraud, migration-related crime, offences relating to passports and other specific travel or identification documents, and offences relating to credit cards and other forms of commercial identification. While global research into the full nature and scope of identity-related crime was needed, Canada stressed that information on some aspects of the problem would only accumulate as Member States developed specific definitions and criminalized related acts in their domestic laws.

18. Canada also pointed out that investment in training and technical development and cooperation between the public and private sectors could generate substantial benefits with regard to the prevention and control of forms of fraud and identity-related crime committed with the use of sophisticated technologies. Moreover, the availability of technologies could contribute significantly to the effective prevention, investigation and prosecution of such crimes. Nonetheless, two issues had to be kept in mind. The first was that fighting computer-related crime, including many types of modern transnational fraud and identity-related crime, might require some States to assist other States in building the technical expertise and law enforcement capacity necessary for them to effectively prosecute suspected criminals and cooperate at the international level. The second was that appropriate procedural safeguards and human rights protections had to be taken into consideration and incorporated into international cooperation activities. In this connection, Canada reported on the continuous support offered by its authorities in the fields of training, technological development and upgrading of legislation on cybercrime issues, both at the bilateral level and through intergovernmental organizations such as the United Nations, the Council of Europe, the Group of Eight, Asia-Pacific Economic Cooperation, the Organization of American States and the Commonwealth. Canada recalled that it had been an active participant in the

negotiation of the Convention on Cybercrime and a founding member of and active participant in the "24/7" network, which linked the law enforcement agencies of participating States in real time. Canada emphasized the importance of supporting such initiatives and of making them more effective.

19. Canada underscored that, given the nature of identity infrastructure, a holistic approach to prevention and security was needed. That entailed, inter alia, auditing or examining the entire infrastructure, including the initial identification of users, issuance of documents and use of documents. Passport Canada was cited as an example of such a holistic approach. In addition to enhancing the security of passports, Passport Canada had promoted enhanced measures to combat fraud during the passport issuance process by placing applicants against watch lists, which would be expanded in 2009 through the use of facial recognition technology to detect individuals submitting multiple applications under different identities. Training and raising the awareness of staff involved in processing passport applications were also seen as key to the early detection and prevention of identity theft.

20. Canada further referred to the prevention of identity-related crime through technological means and to concrete measures aimed at incorporating new technical precautions against forgery, tampering or other criminal misuse (development of an electronic passport, or "e-passport"). The importance of the engagement of the private sector, both as a producer and user of security and prevention technologies, was also highlighted. In this regard, examples of private sector measures were reported, including the collaboration of financial institutions and the makers of automated teller machines with law enforcement authorities to fight the emergence of new criminal methods used by those committing fraud. Preventive measures further included the use of Internet sites by the Government of Canada, provincial governments and relevant commercial and non-governmental entities to educate consumers about the risks of fraud and identity-related crime.

21. Given that the globalization of commerce, transportation and communications and information technologies had created an increasing need for international cooperation in matters related to identification, prevention, investigation and prosecution of identity-related crime, Canada expressed the view that all Member States had a collective interest in assisting one another in the development of secure documents and the establishment of institutions in charge of protecting the integrity of such documents and the associated records in the course of their issuance and use. Such assistance should aim at speedy and reliable verification of the identity of nationals and long-term residents. In this connection, Canada further reported on its participation and active involvement in a number of international organizations dealing with travel document security and identity management, including the Technical Advisory Group on Machine-Readable Travel Documents of the International Civil Aviation Organization, its New Technologies Working Group and its Implementation and Capacity-Building Working Group; the 5 Nations Anti-Fraud Working Group; and the G8 Roma/Lyon Migration Experts Subgroup.

22. Canada was a party to the Organized Crime Convention. All major fraud offences under Canadian law and most existing offences in the area of identity-related crime met the threshold requirements for "serious crimes" in line with article 2 (b) of the Organized Crime Convention. In that context, Canada underscored that the vast majority of major transnational fraud cases involved

organized criminal groups and that the focus of further work should be on finding ways to use the Organized Crime Convention more effectively instead of developing any further instruments. With respect to identity-related crime, more information and assessments might be needed before a similar conclusion could ultimately be drawn, but, in general, Canada was of the view that additional international legal instruments should only be developed if, for example, a clear need had been determined for specific criminal offences that did not already exist, specific investigative or international cooperation measures or specific measures to assist victims, at the international level, in repairing or restoring their identities, to the extent that such issues were not adequately addressed in existing applicable international legal instruments. In general, Canada emphasized the need to assist Member States in updating provisions relating to fraud, identifying elements to be considered in the formulation of new identity-related crimes and using existing international legal instruments.

23. Although it was not yet a party to the Convention on Cybercrime, Canada had implemented a number of its criminalization requirements, including those dealing with forms of computer-related crime such as computer-related fraud. Canada expressed the view that the general provisions of the Convention on Cybercrime were useful models for legislation and international cooperation on cybercrime and that non-European States should consider either acceding to the Convention or using it as a model for the formulation of domestic legislation. Canada further stated that, while the role or mandate of UNODC was not to promote the Convention on Cybercrime, it should work as closely as possible with the Council of Europe body in charge of its ratification and implementation to exploit synergies and avoid inconsistencies.

24. Canada also reported on the provisions in domestic legislation covering offences such as consumer and commercial fraud and cybercrime, credit-card and other related offences. It was noted, in that regard, that fraud-related offences had been updated in 2004 and that all criminal legislation was monitored to ensure that new trends and developments were identified quickly and, where necessary, appropriate legislative amendments could be promoted. Resources were provided for research, in order to gain more detailed information about rates, trends and types of fraud, and other information to assess the utility of existing legislation and whether further improvements could be made. In the area of identity-related crime, in particular, it was stated that no specific behaviour had been criminalized but that, depending on the case, a range of existing provisions could be used to prosecute for such crime, including general provisions against offences such as forgery and the use of forged documents and specific provisions against offences such as the forgery or falsification of specific identity documents, including credit cards and Canadian passports. The national legislation of Canada also included provisions against cybercrime, including against the unauthorized use of computers, networks, data and passwords, and made it an offence to impersonate another person with the intent of committing fraud or a similar offence. Canada further reported on ongoing national efforts to revise the domestic legal framework with regard to identity-related crime. More specifically, in November 2007 the Government of Canada had introduced in Parliament amendments to the Criminal Code creating new offences (identity theft and trafficking in identity information) and modifying existing provisions to address identity-related crime.

25. In the field of research and analysis, Canada pointed out that its national authorities gathered and maintained data on occurrence and conviction rates for all criminal offences, including various forms of fraud. This would be expanded to include data on identity-related crimes upon enactment of the modified legislation. However, it was likely that considerable time would be needed for the accumulation of sufficient data to permit an assessment of overall rates and trends. In addition to regular assessments of fraud, a survey on fraud against businesses had been conducted focusing on the retail, banking and insurance industries. The survey sought to improve understanding of the nature and extent of various types of business fraud in Canada, as well as the impact of economic fraud on Canadian businesses. The results of the study were expected to be released shortly. Furthermore, academic research had also been carried out; one of the resulting studies, released in 2008 and based on Internet responses, estimated that about 6.5 per cent of Canada's adult population had been victimized by some form of identity fraud, the most common form being credit card fraud, which accounted for 60 per cent of cases.

26. Canada also emphasized the need for effective cooperation between the private sector and criminal justice and law enforcement authorities, both at the national and international levels. It was argued, in that regard, that, while the priorities of commerce and criminal justice did not always coincide, there were many synergies that could be exploited, especially in the area of the prevention of fraud and identity-related crime, and cooperation with law enforcement agencies. Private companies in key sectors such as banking, finance, credit card, information and communications and travel also had an important role to play. The same also applied to academic institutions, as the interest of academic experts in both commercial and criminal law issues had added a valuable perspective and led to the organization of a number of events, at which governmental, commercial, academic and other perspectives (e.g., privacy interests) had been represented.

Egypt

27. Egypt provided information on the applicable legal framework for the investigation and prosecution of economic crimes, including money-laundering, corruption and identity-related crime. It was reported that the provisions of the Criminal Procedure Code gave the prosecution agencies extended competence and powers to deal effectively with such crimes, including powers to examine bank accounts during an investigation and request States to confiscate assets derived from those crimes. Egypt also referred to domestic legislation establishing ad hoc courts for the adjudication of cases related to economic crime. It was further reported that an independent body affiliated to the Central Bank had been established to combat money-laundering and facilitate mutual legal assistance in related cases. With regard to international cooperation in criminal matters, a specific section within the prosecution office acted as a central authority for dealing with requests for cooperation. The commitment and readiness to enhance such cooperation was demonstrated by the fact that Egypt was a party to a series of international legal instruments, including the Organized Crime Convention and the Convention against Corruption. Egypt also emphasized the importance of providing training activities, both through the organization of internal training courses for competent officers and

the participation of prosecutors in international and regional training programmes organized by UNODC and the United Nations Development Programme, through its Programme on Governance in the Arab Region.

Estonia

28. Estonia reported that its domestic criminal legislation contained provisions criminalizing fraud, forgery and the unlawful use of identification information to facilitate the commission of other crimes. Estonia provided information on ongoing national efforts to amend the Criminal Code to provide for the criminalization of identity theft and reported being a party to the Organized Crime Convention and the Convention on Cybercrime.

Germany

29. Germany stressed that it attached great importance to combating crime relating to personal data espionage for abusive or fraudulent purposes and that strategies had been developed to address new threats associated with the criminal abuse of data processing systems in business and administration. In the field of criminal legislation, elements of existing offences could be applied to criminalize the use and forgery of and tampering with identity-related or identification data. In that context, in most cases the focus was not on the act of obtaining personal data but on the act of misleadingly or fraudulently using such data. “Phishing”, for example, which was seen as an attempt to gain access to bank accounts using a false identity, might involve elements of the criminal offences of data espionage, fraud, forgery and illicit data collection and processing.

30. Germany further reported that although it was not yet a party to the Convention on Cybercrime, recent amendments in criminal legislation aimed at addressing loopholes and gaps took into consideration the provisions of that Convention. National action on the ratification of the Convention on Cybercrime was ongoing. Moreover, while Germany had not yet ratified the Convention against Corruption, national authorities were not prevented from assisting other countries in investigating and fighting corruption-related offences. Relevant requests for extradition and mutual legal assistance were dealt with on the basis of bilateral and multilateral treaties and agreements or in accordance with the provisions on international assistance in criminal matters.

31. Germany was also a party to the Organized Crime Convention and the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime,[11] and the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime.[12] Agreements or arrangements concluded for giving practical effect to the provisions contained in articles 16 and 18 of the Organized Crime Convention could constitute an additional legal basis for the provision of

[11] United Nations, *Treaty Series*, vol. 2237, No. 39574.
[12] Ibid., vol. 2241, No. 39574.

cooperation. At the operational level, the effectiveness of such cooperation had been further enhanced through the establishment of contacts with counterparts in other countries, including within the context of the European Judicial Network, as well as through the provision of specimen mutual legal assistance requests and the use of the Mutual Legal Assistance Request Writer Tool developed by UNODC.

Greece

32. Greece reported that its national legislation included a considerable number of provisions on combating economic fraud and identity-related crime. A significant part of such provisions concerned the incorporation and adaptation of European Union law, including on the protection of the financial interests of the European Communities. Further, the crimes of fraud and falsification of documents or false statements were among those listed in provisions regarding the involvement of a criminal organization in the commission of crimes, thus entailing more severe sanctions.

33. Greece also reported that it was a party to the Criminal Law Convention on Corruption,[13] the Additional Protocol to the Criminal Law Convention on Corruption[14] and the Convention against Corruption. With regard to the latter, Greece participated in the pilot programme for reviewing its implementation and, in that context, experts and UNODC officers carried out in May 2008 an evaluation of anti-corruption issues with the assistance of national authorities. Greece further reported that national efforts were being made to enact legislation through which the provisions of the Organized Crime Convention and the Convention on Cybercrime would be adapted to the domestic context.

Japan

34. Japan reported that its authorities had encountered serious problems with the so-called “furikome” frauds, which had been committed in an organized manner and using the bank accounts and mobile telephones of third persons.[15] To address the problem, an action plan had been released in July 2008 with the aim of raising awareness and promoting cooperation among financial institutions.

35. Japan also referred to domestic legislation criminalizing fraud or computer-related fraud, including its aggravated form, as the activity of a group. Legislative provisions also established extraterritorial jurisdiction for that criminal act. In the field of identity-related crime, national laws not only established traditional crimes such as counterfeiting and the circulation of counterfeit documents, but also criminalized a range of other behaviours associated with the misuse of credit card information, including the unauthorized creation, possession or illicit acquisition of electromagnetic records encoded in a credit or a bank card and the obtaining of credit card information through fraudulent acts such as cheating, selling, buying or

---

[13] Council of Europe, *European Treaty Series*, No. 173.

[14] Ibid., No. 191.

[15] In “furikome” frauds, offenders contact victims, typically by using a mobile telephone instead of seeing them in person. In many cases, offenders deceive victims and then instruct them to transfer money to a bank account held by the offenders.

keeping such information for the purpose of sale. Moreover, new legislation was to be enacted to improve the procedure for collecting evidence related to electromagnetic record mediums, as well as allow for the submission of requests for keeping communication records.

36. With regard to prevention, Japan made reference to domestic legislation that imposed strict customer identification requirements on mobile telephone carriers and mobile telephone rental shops. In addition, law enforcement authorities had strengthened collaboration with mobile telephone carriers and financial institutions and had encouraged them to take appropriate measures to prevent the use of mobile telephones and bank accounts by customers who were not identifiable.

37. In the area of international cooperation, Japan reported that national legislation on extradition and international assistance in investigations and other related matters could be used as a legal basis for dealing with requests for extradition and mutual legal assistance. Moreover, Japan had concluded a number of bilateral treaties or agreements on mutual legal assistance with China, the Republic of Korea and the United States of America, while negotiations for the conclusion of additional treaties with other countries were under way. Japan had not yet ratified the Organized Crime Convention or the Convention against Corruption, but the text of legislation for implementing both instruments was before Parliament, pending approval. Japan further reported that its competent law enforcement authorities cooperated actively with counterparts in other countries, including by exchanging information through the mechanism of INTERPOL and diplomatic channels.

Jordan

38. Jordan reported on the establishment of specific bodies and agencies in charge of reporting and investigating economic crime and cybercrime, as well as preventing economic fraud through the provision of a safe environment for foreign investment. Jordan also provided information about the cooperation of its national authorities with INTERPOL in the field of exchange of information to combat economic crime. Jordan further reported on training programmes to enhance the required skills and capacity of competent authorities.

Kuwait

39. Kuwait underscored that its national Penal Code addressed the criminalization of identity-related offences and that existing legislation aimed at fighting money-laundering was under review to keep up with new developments. Kuwait further expressed its commitment to developing new laws and filling existing gaps in the domestic legal framework, as well as enhancing international cooperation in criminal matters at both the bilateral and regional levels. In this context, it reported that bilateral treaties or agreements had been concluded with certain States, including Bahrain, India, Iran (Islamic Republic of), Pakistan, Turkey and Uzbekistan, and that its national authorities were working with counterparts in other countries to negotiate and conclude additional treaties. Moreover, Kuwait was a party to the Organized Crime Convention and the Convention against Corruption.

Latvia

40. Latvia presented an overview of national criminal legislation on economic fraud and identity-related crime. Latvian legislation did not identify certain behaviour as economic fraud, but contained several provisions covering related issues. Such provisions established as criminal offences a broad range of conduct, including: fraud and its aggravating circumstances (recidivism and the involvement of an organized criminal group); computer-related fraud; intentional destruction, damage or concealment of property for the purpose of receiving insurance money; repeated commission of small-scale theft, fraud and misappropriation; smuggling; counterfeiting; insider trading; money-laundering; non-declaration of cash; defrauding consumers; and violation of provisions regarding accounting documentation or the conduct of procedures regarding compilation of annual accounts or statistical reports.

41. With regard to identity-related crime, Latvian legislation contained provisions criminalizing the concealment of personal identity and the use of the document of another person or a forged personal identification document. Aggravating circumstances were also established where forms of such conduct were carried out for the purpose of avoiding criminal liability or of committing another criminal offence. Other provisions established as criminal offences several forms of conduct, such as impersonation for the purpose of acquiring citizenship, the forgery of documents and the intentional issuance or use of forged documents by a State official. Aggravating circumstances were also established where the conduct was committed repeatedly or for the purpose of acquiring property.

42. Latvia was a party to the Organized Crime Convention and reported that the implementing legislation incorporating its provisions in the domestic legal system was in line with requirements set forth in articles 2 and 3 of the Convention on issues associated with both identity-related crime and other offences. Latvia was also a party to the Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.[16]

43. In the field of international cooperation in criminal matters, the legal system of Latvia allowed for extradition, mutual legal assistance, transfer of criminal proceedings and transfer of sentenced persons. The extradition process, in particular, was governed by Council of the European Union framework decision 2002/584/JHA on the European arrest warrant and the surrender procedures between member States.

44. Latvia further reported on the ongoing national efforts to adapt to the domestic context directive 95/46/EC of the European Parliament and of the Council of the European Union on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[17] Amendments to the legislation had been made to ensure the full implementation of the provisions of the directive and set out the sanctions to be imposed in case of infringement of those provisions.

---

[16] Council of Europe, *European Treaty Series*, No. 189.

[17] *Official Journal of the European Communities*, L. 281, 23 November 1995.

Mexico

45. Mexico referred to existing domestic legislation on the prevention and combating of money-laundering and financing of terrorism that imposed obligations regarding the validation and authentication of identities. Financial institutions in particular were required, according to national law, to verify the identity of customers and identify suspicious transactions for the purpose of reporting to the competent authorities. Mexico further reported that it was a party to the Organized Crime Convention and the Protocols thereto and that it had made progress in aligning domestic legislation with the provisions of the Convention on Cybercrime.

Morocco

46. Morocco provided information on its legislation against cybercrime and offences related to the use of automated systems to process data. It also stressed that protective provisions regulating trade had been reinforced by the introduction, in 2007, of legislation on the electronic exchange of judicial data. In addition, domestic legislation aimed at countering money-laundering introduced a series of provisions to foster international cooperation in that field and a financial intelligence unit was to be established shortly under the authority of the Prime Minister.

47. At the institutional level, Morocco reported that its General Directorate of National Security was engaged in fighting organized crime in all its forms, including those associated with identity-related crime and economic fraud. National law enforcement authorities were also actively engaged in cooperating with counterparts in other countries, including through the exchange of information and use of INTERPOL mechanisms, rogatory letters for assistance, controlled deliveries and, more specifically, requests for the identification of digital fingerprints. In an effort to enhance institutional capacity to combat fraud associated with the criminal misuse of identities, national training courses and seminars were organized by the national Judicial Police.

48. In the field of prevention of identity-related crime, Morocco reported on the introduction of national electronic identity cards containing biometric data that were difficult to forge and that were aimed at securing identity documents and avoiding fraud resulting from their misuse. Biometric passports were expected to enter into force shortly.

Saudi Arabia

49. Saudi Arabia reported on national action to investigate, prosecute and effectively combat economic crime. In this context, information was provided on the country's bank law and on legislative action to criminalize money-laundering, bribery, forgery and cybercrime. Strategies and broader plans involving, inter alia, civil society and the private sector had also been developed to tackle corruption. Such strategies also included the adoption of preventive measures focusing mainly on raising awareness and supporting research centres. In order to achieve better coordination, multisectoral policies involving different governmental entities were

being promoted. Saudi Arabia reported that it had concluded a series of bilateral and regional agreements to combat related crime and was a party to the Organized Crime Convention. The country also reported that it had adapted its policies aimed at countering money-laundering to conform with the Forty Recommendations on Money-Laundering of the Financial Action Task Force on Money Laundering and that national authorities had cooperated with INTERPOL and the Egmont Group of Financial Intelligence Units to exchange information.

Serbia

50. Serbia provided an overview of the provisions of its Criminal Code on related offences, including fraud, counterfeiting, forgery of securities, forgery and misuse of credit cards, forgery of value tokens, unauthorized use of another company's name and offences against the security of computer data.

Spain

51. Spain underscored that, under its domestic legal system, the falsification of identity documents and the use of such documents for criminal purposes were considered as related to criminal offences, such as forgery, committed to facilitate the basic offence of "usurpation of civil status". With regard to fraud committed through the Internet, Spain reported on domestic legislation regarding the conservation of data related to electronic communication and public communication networks, in line with the provisions of directive 2006/24/EC of the European Parliament and of the Council of the European Union on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/EC.[18] Under that legislation, telecommunication operators were obliged to retain certain data so that the police could utilize them in the course of an investigation.

52. Spain referred to the collaboration between its competent authorities and private entities in the financial sector, especially credit card companies. It reported, in that connection, that the Ministry of the Interior had signed cooperation agreements with associations grouping a large number of financial credit and insurance companies, with the aim of facilitating the prevention and detection of fraud. Those agreements had contributed to the establishment of cooperation mechanisms used for obtaining specific information on illicit activities and avoiding the victimization of consumers. Spain also reported that consultations were under way with financial institutions to implement measures such as the installation of early warning and control systems necessary for the detection of forged identity documents.

53. Spain further stated that new technologies for combating identity-related crime were being used chiefly to make the process of issuing identity and travel documents more secure. To put in place biometric identification systems and promote the use of physiological and/or behavioural indicators for the effective

[18] *Official Journal of the European Communities*, L. 105, 13 April 2006.

verification of identity, work was being carried out, in accordance with the standards set by the International Civil Aviation Organization and Council of the European Union regulation No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member States. Spain began issuing electronic identity cards and electronic passports in 2006.

54. In the field of international cooperation aimed at combating economic fraud and identity-related crime, Spain was party to the Organized Crime Convention and the Convention against Corruption. Spain had also entered into treaties and agreements on international judicial and law enforcement cooperation. Its authorities were cooperating with INTERPOL and the European Police Office (Europol), in addition to exchanging information with counterparts in other countries, including through the Supplementary Information Request at the National Entry (SIRENE) mechanism, which is part of the Schengen Information System.

Tunisia

55. Through its Ministry of Justice, Tunisia highlighted that domestic legislation was in place to combat money-laundering and the financing of terrorism. That legislation required financial institutions, including banks, to report all suspicious transactions and operations. Moreover, rigorous due diligence standards had been established through requirements for customer identification and the preservation of evidence regarding the identity of persons involved in transactions and the traceability of transactions. In addition, an ad hoc committee had been established to carry out financial analyses of suspicious transactions and promote coordination between different departments and agencies, both at the national and international levels, and the involvement of financial and non-financial professionals in efforts to combat money-laundering.

56. Further, the legislation of Tunisia contained provisions on a broad range of economic crimes and offences related to the improper use of modern technology for the purpose of committing illicit activities, including: corruption; alteration and counterfeiting of seals and coins; bankruptcy; fraud and other deceptive behaviour; illicit enrichment; misappropriation, copying, manufacturing and misuse of documents or identification information; manufacture and use of fake passports and other items; access, alteration or destruction of existing data from the content of a computerized document; manufacture and use of fake national identity cards; and falsification of passports and travel documents to facilitate the illegal entry of a person in, or the departure from, the national territory. Additional pieces of legislation had been enacted to preserve the security of information systems.

57. The authorities of Tunisia had also adopted partnership and collaboration strategies with the private sector to ensure the effective prevention of identity-related crime. To that end, mechanisms had been established to oversee credit settlements and preserve the stability, integrity and security of the financial and economic system, as well as to promote cooperation with the regulation authorities of financial sectors and foster information exchange. In addition, programmes had been launched to provide a better understanding of the mechanisms and techniques used to facilitate the recycling of assets of criminal origin, especially assets gained through the commission of economic fraud and identity-related crime.

58. In the field of international cooperation in criminal matters, Tunisia was a party to numerous treaties and agreements on extradition and mutual legal assistance. Tunisia was a party to the Organized Crime Convention, the Convention against Corruption and the International Convention for the Suppression of the Financing of Terrorism.[19] Tunisia regarded the principle of mutual recognition of judicial decisions as a cornerstone of international cooperation to combat economic crime.

59. Through its Ministry of Commerce, Tunisia underscored that it had constantly endeavoured to create a climate favourable to business. To that end, communication infrastructures had been set up and the use of modern means of communication in economic activities was encouraged, taking into account the need to ensure the security of users of communication and information technologies and the need to combat the illegal or fraudulent use of information networks.

60. The legislative framework of Tunisia on economic fraud and identity-related crime in commercial transactions, in particular, included provisions on the protection of industrial and commercial property rights, electronic exchanges and commerce, and international trade activities. With regard to the protection of industrial, commercial and services trademarks, national legislation was being developed to implement the World Trade Organization conventions, especially the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights.[20] That agreement provided for the criminalization of counterfeiting of industrial, commercial and services trademarks and all related operations. Furthermore, it established, as a general principle, that the perpetrator of any violation of the rights of the proprietor of the trademark by way of counterfeiting incurred civil and criminal liability. It also criminalized the supply of goods carrying a counterfeit trademark. In October 2008, Tunisia signed the Cannes Declaration against Counterfeiting, which deals with combating the counterfeiting of industrial trademarks.

61. In the area of electronic exchanges and commerce, Tunisian legislation contained provisions aimed at ensuring that such exchanges were carried out in a manner that promoted security and confidentiality while also preventing all forms of illicit exploitation. The legislation also imposed on electronic exchanges a set of guarantees for different users and criminalized a number of illicit practices.

62. With regard to external trade, Tunisian legislation provided for the freedom to undertake import and export activities and included regulations aimed primarily at protecting the interests of those involved in economic activities and combating all forms of economic fraud and crimes related to identity falsification, including by identifying persons wishing to carry out import and export operations as wanting to be “involved in external trade”.

63. With regard to the institutional framework related to commercial transactions, Tunisia provided information on its competent authorities and an overview of measures taken and services provided by such authorities, including: the provision,

---

[19] United Nations, *Treaty Series*, vol. 2178, No. 38349.

[20] See *Legal Instruments Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, done at Marrakesh on 15 April 1994* (GATT secretariat publication, Sales No. GATT/1994-7).

annulment, publishing and maintenance of electronic certifications; the granting of authorizations to perform the activities of an "electronic certifications server" and monitor the extent to which the law was being complied with; the preparation of technical specifications for electronic signature; the requirement that every user of an electronic signature system inform the electronic certifications server of every illicit use of his or her signature; the requirement that electronic signatures be registered; the imposition of a number of obligations on the electronic certifications server, including the obligations to protect the confidentiality of the information entrusted to it, maintain an electronic register for the conformity certificates and suspend the validity of a certificate used for fraudulent purposes or whose content has been changed; the provision of a Web distributor certificate confirming the identity and preserving the security of electronic commercial sites with a view to creating a relationship of trust with customers making electronic purchases through a website; the provision of an electronic signature certificate identifying the author of the signature.

64. Moreover, Tunisian authorities pursued cooperation with foreign electronic certification authorities through the conclusion of mutual recognition treaties and agreements.

Ukraine

65. Ukraine emphasized that its authorities had devoted special attention to the prevention and investigation of economic fraud and identity-related crime. In 2001, a specific section to fight cybercrime and intellectual property offences was established within the Ministry of Internal Affairs and as part of the overall fight against economic crime. Ukraine also provided information on its legislation covering related issues. It further reported that, in Ukraine, there was an increasing trend of economic fraud being committed by "phishing" or by interfering in the websites of banks and financial institutions with a view to stealing confidential information. Other trends reported were: the involvement of bank personnel in the commission of economic crime; the use of money transfer schemes for money-laundering; and the use of sophisticated methods to get information on credit card owners, as well as other confidential information located on credit cards.

66. Further, Ukraine further underscored that the rate of crimes related to the use of fake payment cards had increased fivefold over previous years. Enhanced efforts by the national authorities to detect and prosecute such or similar crimes had been successful in several cases.

Uruguay

67. Uruguay referred to provisions in its national legislation on forgery and the criminal misuse of documents, including identity cards and passports. Uruguay was a party to the Organized Crime Convention and the Convention against Corruption.

III. Conclusion

68. The information received by the Secretariat pursuant to Economic and Social Council resolution 2007/20 confirms that Member States attach great importance to the fight against economic fraud and identity-related crime. That information supplements the material and feedback provided by 46 Member States contained in the report of the Secretary-General on the results of the second meeting 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). While the information provided by Member States in that report illustrates the problems caused by such crimes and the consequent challenges encountered by criminal justice and law enforcement authorities in tackling them, the information contained in the present report highlights the necessity of carefully developing comprehensive, multifaceted and coherent strategies that encompass targeted and well-planned interventions aimed at:

(a) Improving legislative responses, taking into account new needs and developments;

(b) Enhancing the law enforcement and investigative capacity of competent institutions to deal effectively with economic fraud and identity-related crime;

(c) Strengthening international cooperation to combat those forms of crime;

(d) Developing and implementing effective preventive policies, including through the appropriate use of new technical means for prevention;

(e) Developing partnerships and synergies between the public and private sectors in the field of prevention, investigation and prosecution of those crimes, bearing in mind the need for appropriate safeguards to ensure the independence of investigative, prosecutorial and judicial functions;

(f) Further promoting training and technical assistance activities to increase the institutional capacity of competent authorities to deal with related challenges.

69. The Commission on Crime Prevention and Criminal Justice may wish to explore and recommend ways to further enhance and enrich the debate at the international level on the issues under consideration. The thematic discussion on "Economic fraud and identity-related crime", to be held at the eighteenth session of the Commission, provides an opportunity for such a debate and could substantially contribute to the delineation of a guidance framework on the most appropriate initiatives to be prioritized and pursued in future.