United Nations E/CN.15/2007/8/Add.2

Economic and Social Council

Distr.: General
2 February 2007

Original: English

Commission on Crime Prevention and Criminal Justice
Sixteenth session
Vienna, 23-27 April 2007
Item 4 of the provisional agenda*
World crime trends and responses: integration and coordination of efforts by the United Nations Office on Drugs and Crime and by Member States in the field of crime prevention and criminal justice

Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity

Report of the Secretary-General

Addendum

Economic fraud

Contents

* E/CN.15/2007/1.

V.07-80545 (E) 120307 120307

IV. Relationship between economic fraud and other problems

A. Fraud and the involvement of organized criminal groups

21. Fraud can be committed by individuals, but expert opinion and the information provided by States suggest that most serious frauds involve "organized criminal groups" as the term is used in the United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, annex I, articles 2 and 3). States described both frauds committed by or on behalf of long-established organized criminal groups and the establishment or organization of new groups specifically for the purpose of committing fraud and related crimes. Established groups are attracted by the great potential proceeds, relatively low risks and possible complementarity with other criminal activities in which they are engaged. Smaller, more flexible groups are formed to commit some forms of fraud such as debit card or credit card fraud, sometimes moving from place to place in order to avoid law enforcement and target fresh victims. A third category is that of frauds committed by or on behalf of legal persons. In that connection, a company or group of employees may be considered an organized criminal group if they commit fraud or become involved in fraud. Some States reported that some types of fraud were more likely than others to involve organized groups, and many considered fraud committed by organized criminal groups to be more harmful, not only because it caused losses for victims, but also because the proceeds of such fraud were used for corruption or for strengthening in some other way the activities or influence of organized criminal groups. That was of particular concern in countries and areas with economies in transition, where institutions were weaker and well-financed organized criminal groups were thus a much greater threat.[1] A number of States had established more serious offences and harsher punishments for cases in which organized crime was involved. Several States mentioned their legislation against organized crime as a measure that was or could be useful in cases involving serious fraud, especially legislation covering areas such as investigative powers, sentencing and the tracing and confiscation of proceeds. The involvement of organized criminal groups meant that, in most cases, the Organized Crime Convention could be applied to facilitate mutual legal assistance, extradition and other forms of cooperation where the alleged fraud was transnational in nature. A number of States expressed the view that their existing legislation was sufficient to deal with the problem, and several emphasized the need for work in areas such as technical assistance and training to ensure that the Convention could be used as effectively as possible.

B. Fraud and the element of transnationality

22. States did not have statistical information concerning transnational fraud per se, although fraud of that type was common, and many national experts had had extensive experiences with it. Many States indicated that they had encountered such cases, and others expressed concern about the mere possibility of encountering such cases. The major concerns were that transnational fraud appeared to be increasing and that such offences were easy to commit but costly, difficult and complex to

[1] See the note by the Secretariat entitled "Possible future work relating to commercial fraud" (A/CN.9/540, paras. 3, 8 and 9).

investigate. Some States had seen evidence of offenders intentionally exploiting that difficulty by targeting only victims well away from the jurisdiction of their own local law enforcement officials.[2] Other States reported examples of frauds perpetrated by small groups of offenders that travelled within and among countries to target fresh victims and avoid prosecution.

23. A number of States noted the relationship between transnational fraud cases and the availability and use of information, communication and commercial technologies. They attributed both increases in fraud cases in general and increases in the portion of fraud cases involving some element of transnationality to the increasing availability of technologies to both offenders and potential victims. The most obvious relationship between technologies and transnationality was the fact that media such as fax machines, e-mail, telephones and the Internet could be used to establish contact between offenders and victims, but there were other links. One State noted that technologies made it possible for offenders from different jurisdictions to cooperate effectively with one another.[3] Others noted that information for use in fraud became an illicit commodity, with lists of potential victims and credit card data obtained by "skimming" or cybercrime bought and sold by offenders and often transferred by e-mail. Another link between technologies and transnationality was the practice by offenders of using call-forwarding, anonymous remailers and similar means in an effort to conceal their identity and location and avoid being traced by law enforcement.

24. Several States also described forms of fraud that were inherently transnational in nature. Examples included the smuggling of goods to avoid paying customs fees, a range of maritime transport frauds, immigration, passport and visa frauds and frauds involving vacation travel or accommodations such as timeshare arrangements. The use of third countries was found to be an element of money-laundering schemes and some forms of tax fraud, where records, other evidence or assets were concealed, out of the reach of investigators, as well as an element of forms of Internet fraud in which multiple jurisdictions were used to make the tracing of e-mail and other communications difficult.

C. The role of information, communications and commercial technologies in fraud

25. Most States did not have records or specific offences that linked the misuse of technologies to fraud, although many had found it necessary to ensure that existing fraud offences covered technological innovations as they were taken up by offenders. States parties to the Council of Europe Convention on Cybercrime[4] are required to criminalize computer fraud and forgery. There are clear links between information and communications technologies and commercial technologies such as payment cards and electronic commerce, as well as between commercial

---

[2] See the *Report of the Canada-United States Working Group on Telemarketing Fraud*, (http://www.justice.gc.ca/en/dept/pub/wgtf/headings.html); see also *Mass-Marketing Fraud: a Report to the Attorney General of the United States and the Solicitor General of Canada*, pp. 11-12 (http://www.usdoj.gov/opa/pr/2003/May/remmffinal.pdf).

[3] See *Libman v. the Queen* [1985] 2 S.C.R. 178 (Supreme Court of Canada) and *Secretary of State for Trade v. Markus* [1976] A.C. 35 (United Kingdom House of Lords).

[4] Council of Europe, *European Treaty Series*, No. 185, arts. 7 and 8.

technologies and many types of fraud, and there are many different ways in which technologies can be used to commit or support frauds. Such links were noted by the United Nations Commission on International Trade Law in its work on commercial fraud.[5] States that reported data generally described patterns suggesting a significant increase in information technologies, accompanied by a more gradual shift to the corresponding commercial technologies, and a corresponding shift by offenders to those forms of fraud which targeted or exploited commercial technologies and which took advantage of information technologies to reduce risks and increase potential proceeds and the number of victims. Other States, which did not have concrete data on that issue, either reported similar observations by national experts or indicated that they expected, or were concerned about, such a phenomenon. The limited statistical information available on the issue should be treated with caution. Transitions to new technologies and commercial practices, new forms of offender behaviour and law enforcement and legislative responses can all produce rapid and unpredictable changes in reported offending rates, and some such changes were described by States. Statistical variations are also due to the fact that the field of crime statistics is evolving and the fact that technologies are sometimes used to encourage reporting, which can generate apparent increases in offences that do not reflect actual changes.

26. Technologies affect fraud in a variety of ways. While they provide opportunities and reduced risks for offenders, they can also be very effective in preventing, controlling and deterring fraud. Several States noted that the impact of technology was by no means one-sided or completely to the advantage of offenders. The most common use of technology by offenders was for basic contact with victims, including initial identification, selection and contact of victims; the preparation of a deceptive solicitation; the victim's response; and the transfer of funds, first from the victim to the offender and then onward by the offender for purposes of money-laundering. In many fraud cases, different technologies were used at different stages. After initial contact by mass communication, persuasion might involve more personal contact through telephone calls, for example. Similarly, the transfer of funds from victims was carried out using fast, irrevocable means of payment to which victims have access, such as credit cards or wire transfers, while subsequent transfers between offenders might use other means less likely to be detected by measures to counter money-laundering. Technologies were also used to link offenders, to transfer information such as credit card data, to conceal offenders' true identities and locations and to make the tracing of communications as difficult as possible. Other roles of technology included the use of scanners and printers to produce high-quality forged documents, offenders using technology in research to make their fraud schemes plausible and credible and the dissemination of false information as part of larger fraud schemes, such as auction fraud or stock fraud.

27. A number of specific examples and suggestions for the use of technologies for the prevention, investigation and prosecution of fraud were put forward by both States and private commercial sources, and some States noted that those suggestions underlined a key area for effective cooperation between public and private entities.

---

[5] See the report of the United Nations Commission on International Trade Law on the work of its thirty-sixth session (*Official Records of the General Assembly, Fifty-eighth Session, Supplement No. 17* (A/58/17), para. 236).

Generally, technologically advanced investigative measures offer benefits for law enforcement and criminal justice officials, but they sometimes present commercial entities with conflicting pressure: supporting criminal justice while at the same time protecting customers and ensuring that operations remain competitive and commercially viable. The control of cybercrime is a major commercial activity in its own right, with companies producing security advice, training and technologies as a commodity for sale to other companies needing to protect customers and prevent monetary and other losses. Some States noted the need for close collaboration at all stages, including the development of new commercial and crime-control technologies, the need for a wide range of expertise and the need for resources and commitment to what most saw as a rapidly and constantly evolving problem. The technological applications that were mentioned included security and prevention elements such as firewalls and encryption and investigative methods such as the interception of communications and the use of "traffic data" to trace offender communications.[6] One State noted that authorities traced communications not only to locate offenders, proceeds and evidence, but also to identify additional victims of mass fraud cases that had not made a formal complaint about the fraud. One issue raised was the desire of law enforcement authorities to preserve such data for as long as possible, while commercial entities generally had concerns about storage costs and the implications for customer and subscriber privacy. The use of technologies to prevent fraud by quickly publicizing known schemes and new developments to alert law enforcement, private company officials and potential victims was also raised by a number of States. Commercial research had shown that most commercial fraud, including fraud using technologies, involved inside employees, highlighting the need for training in both the recognition and prevention of fraud and the importance of protecting the interests of companies and customers.

D. Fraud, the proceeds of fraud and money-laundering

28. Fraud and money-laundering are linked, but most States saw them as distinct issues. Fraud was considered an economic crime because its motive was to generate a financial or other material benefit for the offenders, whereas money-laundering, although it occurred in an economic environment, was not considered a form of economic crime because its purpose was to conceal and transfer proceeds only after they had already been generated by other crimes. Beyond providing information on relevant legislation, most responding States did not comment extensively on measures to combat money-laundering. From a procedural standpoint, some States noted that, while fraud and money-laundering were connected and there was a need for coordination in developing responses, money-laundering was already the subject of extensive work in other bodies and that future work on fraud should avoid any unnecessary duplication of effort. Most States considered fraud to be a predicate offence for the purposes of measures to counter money-laundering: 30 States identified one or more serious fraud offences as predicate offences, 12 States did not

---

[6] See, for example the Council of Europe Convention on Cybercrime, art. 1, subpara. (d): "'traffic data' means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

provide information and only 4 States did not consider fraud to be a predicate offence. A wide range of civil, criminal and evidentiary provisions governing the freezing, seizure, confiscation and return of the proceeds of fraud were included in the responses. Key issues with respect to fraud included the need for an assessment of overall national and global costs associated with it and the proceeds it generated; the relative importance of fraud, compared with other major predicate offences, as a source of proceeds used in money-laundering; and the ultimate destinations of fraud proceeds. In addition, commercial interests and some victim advocates had concerns about differences between the confiscation of criminal proceeds and the recovery of losses by businesses.

29. Only a few States provided information on total losses or proceeds, but it was clear that the losses and proceeds were substantial, with as much as several hundreds of millions of dollars generated by fraud and total losses of billions of dollars in some States.[7] Reported commercial sources were limited to specific sectors, such as the insurance and credit card industries, but their findings were consistent with those figures. The Financial Action Task Force on Money Laundering (FATF) does not report detailed statistics or estimates, but it generally considers fraud and related forms of financial crime to be among the top four crimes identified as single sources of illicit proceeds, the other three being trafficking in narcotic drugs, trafficking in weapons and the smuggling of migrants and trafficking in human beings.[8] Obtaining accurate information on the overall proceeds generated by fraud and other offences appeared to pose a formidable challenge. National financial intelligence units operated by investigating financial transactions that were reported as suspicious or which fell into other categories, such as large cash transfers, but information acquired was used for investigations not statistical purposes. At the investigative stage, it was not usually apparent whether funds were being laundered, and when it was, it was not apparent which predicate offences were linked to the funds. In addition, national crime statistics tended to be based on the number of occurrences, prosecutions, convictions and sentences. The proceeds, if known at all, were generally estimated, and such estimates might reflect only known transactions and victims, which represented only part of the actual total in most cases. The best information on the proceeds of fraud is in the hands of private companies, which track losses for business purposes. But that information is limited to the company's specific areas of business, and, in some cases, it is considered commercially sensitive. Further, actual losses due to fraud are much greater than the proceeds taken by offenders. Not all proceeds are reported, detected or counted, and loss calculations may include indirect costs, which one commercial source described as "collateral damage" from fraud.[9]

30. Fraud and money-laundering are conceptually different, but may resemble one another in practice.[10] The major difference is that fraud essentially converts legal

---

[7] See "Possible future work on commercial fraud: note by the Secretariat" (A/CN.9/540), paras. 5-11.

[8] See Financial Action Task Force on Money Laundering, *Report on Money Laundering Typologies 1995-1996* (Paris, Organization for Economic Cooperation and Development, June 1996), paras. 10-11; and Financial Action Task Force on Money Laundering, *Report on Money Laundering Typologies 2000-2001* (Paris, OECD, February 2001), paras. 52-53.

[9] Price Waterhouse Coopers Global Economic Crime Survey 2005, sect. 3.3.

[10] See Financial Action Task Force on Money Laundering, *Report on Money Laundering Typologies 2000-2001*, paras. 13 and 58.

funds into illicit proceeds, whereas money-laundering involves the subsequent transfer and concealment of those proceeds, although neither fraud nor money-laundering are usually that simple in practice. For example, apparently laundered money from one victim may be paid to others as "investment proceeds" in order to lure them into the scheme or may even be paid back to the same victim to encourage further participation or discourage complaints to authorities. The main similarity lies in the fact that both often involve means of deception and covert or unobtrusive transactions. The inherent deception of the two crimes and their resemblance sometimes create a challenge for law enforcement authorities, but may also represent an opportunity. Several States pointed out that mechanisms to counter money-laundering, such as requirements that suspicious transactions be reported, might also be used or adapted to identify instances of fraud, and some banks, telecommunications providers and other commercial or financial institutions already screened mass transaction data to look for unusual patterns suggestive of fraud for follow-up. As with other predicate offences, fraud cases may, from time to time, lead to money-laundering investigations and prosecutions and *vice versa*, underlining the usefulness of cooperation between the appropriate public and commercial entities.

31. Most States indicated that they had in place legislative provisions dealing with the confiscation of the proceeds of fraud and other crimes. Those included schemes based on the criminal conviction of offenders, *in rem* proceedings, hybrid processes in which types of civil forfeiture or recovery could be based on criminal proceedings and completely civil recovery schemes initiated by victims or, in at least one case, by the State. One State referred to a scheme under which some compensation could be claimed from the State itself when losses could not be recovered from offenders. The recovery and return of proceeds can pose major practical challenges, especially in major commercial frauds and mass frauds. In commercial frauds, the victims are often legal persons and, indirectly, investors, shareholders and customers, whose rights can be difficult to define. In mass frauds, very large numbers of small, competing claims in multiple jurisdictions may be so complex that the costs of assessment, adjudication and return exceed losses or available proceeds. Civil claims also face major obstacles, including the fact that criminal justice powers and remedies relating to tracing, freezing, seizure and forfeiture are usually not available.

E. Relationship between fraud and corruption

32. Information about the links between fraud and corruption was not directly requested in the survey questionnaire, but some connections were nevertheless disclosed by Member States in their responses. Those connections included situations where a case of criminal conduct was covered by both fraud and corruption legislation and situations where, although the offences were covered by different legislation, there were factual links between the two types of offences. For example, the diversion of funds might be considered fraud when committed by an outsider and embezzlement when committed by an insider. Most States that provided information concerning major transnational frauds noted that that type of fraud tended to involve organized criminal groups, which suggested that the proceeds of fraud were used to finance other activities of such groups, which, in

many cases, included bribery of officials and other forms of corruption used to shield criminal activities from detection. States also discussed the use of bribery to support forms of procurement fraud, such as the bribery of officials entrusted with detecting and preventing fraudulent transactions. One State noted that its legislation treated several common corruption offences as a form of fraud against the State or the Government. The types of fraud required to be criminalized under the United Nations Convention against Corruption (General Assembly resolution 58/4, annex),[11] may constitute forms of fraud in some circumstances or be linked to it, in the sense that the corruption offences may be committed as part of a fraud, or the proceeds of a fraud may be used to corrupt officials. Aside from embezzlement, for example, the offence of concealing property acquired through corruption (article 24), could be difficult to distinguish from concealment for the purposes of fraud. Trading in influence (article 18) could also be seen as a form of fraud, in the sense that a public official who sells influence is effectively selling something that he or she does not own and is not entitled to sell, and it is considered a form of fraud against the Government in the territory of at least one State that responded.

F. Relationship between fraud and terrorism

33. Unlike identity fraud, which can have non-economic motives such as concealment, economic fraud is committed for material gain, which makes it useful to terrorists primarily as a means of financing terrorist organizations and/or operations.[12] Reports of the Analytical Support and Sanctions Monitoring Team established pursuant to Security Council resolution 1526 (2004), responsible for monitoring sanctions against Al-Qaida and the Taliban, identify fraud, along with other offences such as kidnapping, extortion, robbery and narcotics trafficking, as potential sources of funds for terrorism.[13] A similar range of crimes has been reported by the Financial Action Task Force in its work on the financing of terrorism.[14] Several States indicated that they had encountered fraud cases, although rare, linked or believed to be linked to terrorist activities, and other States indicated that they had concerns about the problem. Small, local fraud and credit card fraud were used or were suspected of being used to sustain individuals or small groups

---

[11] General Assembly resolution 58/4, annex. The offences to be criminalized under the Convention against Corruption include bribery (articles 15, 16 and 21), embezzlement (articles 17 and 22), trading in influence (article 18), abuse of functions (article 19), money-laundering (article 23), concealment (article 24) and obstruction of justice (article 25).

[12] While there is no consensus on the definition of "terrorism" in general, for the purposes of financing offences, the term is clarified in article 2 of the International Convention for the Suppression of the Financing of Terrorism (United Nations, *Treaty Series*, vol. 2178, No. 38349). The question of the definition and scope of the term "terrorism" was left to Member States, and it is not clear whether responses were based on the Convention or on definitions and descriptions used by States themselves.

[13] See Security Council resolution 1267 (1999); the third report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities (S/2005/572), paras. 69-70; and the fourth report of the Analytical Support and Sanctions Monitoring Team (S/2006/154), paras. 63-66.

[14] See Financial Action Task Force on Money Laundering, *Report on Money Laundering Typologies 2001-2002* (Paris, Organization for Economic Cooperation and Development, February 2002) paras. 10-12.

and finance small operations, and more extensive, sophisticated credit card fraud schemes could be used to finance larger operations or generate more substantial, ongoing revenues for other purposes.[15] Sources suggest that there may be a trend towards smaller, more locally based fraud or other crime as a source of funds due to the low costs of many terrorist activities, the vulnerability of large, transnational activities to surveillance and the fragmentation of Al-Qaida.[16]

34. Major economic frauds encountered by States included insurance fraud, smuggling and excise tax fraud, fraud relating to currency exchange, fraud against public benefit schemes and business or commercial fraud. Benefit fraud and credit card fraud have been found to be used both as individual, direct sources for small, local terrorist operations and as the basis of large-scale, organized schemes. Several States also voiced concerns about the use of fraud targeting telecommunications providers in which the real motive was not to obtain free services but to gain access to anonymous, untraceable Internet, e-mail or mobile telephone services. That type of fraud has been associated with cybercrime offenders and organized crime for some time, but it has now been taken up by terrorist organizations for the same reasons.[17]

35. In their responses, several States voiced particular concern about the potential use of charity fraud to finance terrorism, and some States had encountered cases where such fraud had been detected or suspected. The abuse by terrorist organizations of charities and other non-profit organizations has also been identified as a matter of concern by the Financial Action Task Force,[18] as well as by academic and journalistic authorities.[19] In addition to fraud and the diversion of charitable donations as a source of funds, charities have been used as a means of money-laundering or covertly transferring funds from other sources.[20] The Counter-Terrorism Committee of the Security Council has noted the particular difficulties encountered by States in suppressing, pursuant to Council resolution 1373 (2001), the abuse of non-profit organizations as a source or conduit for funds for terrorism.[21] In 2004, the Consolidated List of individuals and entities identified as

---

[15] Ibid., para. 11, example 1.

[16] See third report of the Analytical Support and Sanctions Monitoring Team (S/2005/572), paras. 67-70; and Mark Rice-Oxley, "Why terror financing is so tough to track down", *Christian Science Monitor*, 8 March 2006.

[17] See, for example, the testimony of Richard A. Rohde before the Senate Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary of the United States of America, 24 February 1998 (http://www.fas.org/irp/congress/1998_hr/s980224r.htm); and Alan Sipress, "An Indonesian's prison memoir takes holy war into cyberspace: in sign of new threat, militant offers tips on credit card fraud", *Washington Post*, 14 December 2004.

[18] See Financial Action Task Force on Money Laundering, *Special Recommendations on Terrorist Financing* (22 October 2004), special recommendation VIII; and Financial Action Task Force on Money Laundering, *Annexes 2002-2003*, annex B, section entitled "Combating the abuse of non-profit organizations".

[19] See, for example, Martin Rudner, "Using financial intelligence against the funding of terrorism", *International Journal of Intelligence and Counter Intelligence*, vol. 19, No. 1 (2006), pp. 42-43; and Jeremy Scott-Joynt, "Warning signs for the funding of terrorism", *BBC News* (http://news.bbc.co.uk/2/hi/business/4692941.stm).

[20] Martin Rudner, "Using financial intelligence against the funding of terrorism", *International Journal of Intelligence and Counter Intelligence*, vol. 19, No. 1 (2006), pp. 43-44.

[21] See the report by the Chair of the Counter-Terrorism Committee on the problems encountered in

subject to measures targeting the financing of Al-Qaida and the Taliban included 17 charitable or non-profit organizations with 75 operations active in 37 States.[22]

36. The two major scenarios of concern are the creation of sham charities to finance terrorism directly, which defrauds donors, and the infiltration of legitimate charities in order to divert donations to terrorism, which can take the form of either fraud or theft against the charity itself. Legitimate charities also have concerns. Strict accounting requirements are difficult for them to meet and raise their administration costs, and even unfounded rumours of links to fraud or terrorism can have a major effect in deterring donors. A lack of State and charity capacity to combat infiltration and diversion has been identified as a serious concern, both for charities and for the States in which most of the work using charitable funds is carried out.[23]

37. A further concern relates to charitable organizations that address specific religious, ethnic or cultural communities and causes linked to areas where there are conflicts, because proceeds may be diverted to terrorist groups and because accounting and oversight safeguards are particularly difficult to apply. It can be difficult to distinguish between fraud and other crimes in such cases. Donations used for terrorism, are generally considered to be fraud if donors are deceived and considered to be extortion if donors are not deceived but intimidated. In cases where donors are aware of the true purpose of the organization and are not coerced, both donors and the recipient charity may be committing domestic offences relating to the financing of terrorism, including those established in implementation of the International Convention for the Suppression of the Financing of Terrorism.[24] Aside from playing a role as a source of funds, charities may be used as a conduit for funds generated by other crimes or from licit sources, and in such cases financing or money-laundering offences may apply.

G. Relationship between economic fraud and identity-related crime

38. To avoid duplication, the relationship between economic fraud and identity-related crime is discussed in the related addendum on identity-related crime (E/CN.15/2007/8/Add.3, paras. 13-14).

H. Impact of fraud in countries under reconstruction or with economies in transition

39. Economic fraud and related forms of corruption have posed additional challenges in places where the fundamental economic structures have been weakened or are in some form of transition, and States provided several examples of that. In situations of major economic transition, development, reconstruction or recovery from conflict or natural disasters, conditions may favour fraud more than

---

the implementation of Security Council resolution 1373 (2001) (S/2004/70, annex), sect. II.A.

[22] See the third report of the Analytical Support and Sanctions Monitoring Team (S-2005/572), para. 84.

[23] See the third report of the Analytical Support and Sanctions Monitoring Team (S/2005/572), paras. 85-88.

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

efforts to prevent, deter or control it. In such situations, safeguards against fraud and corruption may be weaker, additional opportunities for both may be generated, and the harm caused by cases involving corruption or successful fraud, especially major cases, may cause more damage than would a similar offence under other conditions. Economic losses due to major frauds may be large enough to damage economies already weakened or destabilized by other problems, and the financial gains from such fraud may considerably strengthen organized criminal groups that face already weakened criminal justice systems, a situation that only fuels corruption and other problems. The success of major frauds and the presence of pervasive corruption can erode confidence in new economic structures, impeding the effective implementation of reforms. Fraud is also a crime of deception, and the potential for deception increases in countries with economies in transition, where new social or economic rules and practices are not well understood. In some cases, conflicts and major natural disasters also create opportunities for offenders, because large amounts of money are solicited from charitable and other sources and must be spent quickly in places where otherwise applicable anti-fraud and anti-corruption safeguards are difficult to implement or may be less effective.

40. Fraud and corruption can be closely linked, and in some cases the two offences are identical or overlapping. For example, the diversion of funds from a development project would usually be considered to be fraud, but if the crime were committed by an insider, it might be covered by offences of embezzlement.[25] In other cases, such crimes may be separate but linked by the actions of offenders. As with procurement and other forms of common fraud, fraud offenders often provide a bribe or inducement to an insider to ensure that the fraud succeeds without detection.

41. Several examples of such cases were reported by States and experts. Frauds targeting reconstruction and transition projects were reported, including fraud targeting new taxation schemes, new procurement processes and privatization schemes. One State reported fraud targeting tax and privatization procedures, used as a major source of funds for organized criminal groups. Another State reported a fraud targeting its new value-added tax refund process that was sufficiently serious to negatively affect the national budget. International charitable and insurance-based efforts to rebuild after major natural disasters such as the 2004 Asian tsunami had also been exploited,[26] and, in at least two cases, major "Ponzi" pyramid-scheme frauds were cited as a factor in destabilizing countries with economies in transition.[27]

---

[25] See, for example, the *Convention against Corruption*, articles 17 and 21.

[26] Several national law enforcement efforts specifically targeted frauds exploiting disaster relief efforts; for example, the former National Criminal Intelligence Service of the United Kingdom of Great Britain and Northern Ireland issued a public warning ("Tsunami fraud threat: advice to the public"); see also the web page of the Federal Bureau of Investigation of the United States ("Tsunami disaster relief fraud alert: don't be scammed" (http://www.fbi.gov/page2/jan05/tsunamiscam010505.htm)). The United States Department of Justice established the Hurricane Katrina Fraud Task Force to deal with a range of frauds, including charitable fraud, public and private sector benefit fraud, identity theft, insurance fraud, procurement fraud and public corruption (http://www.usdoj.gov/katrina/Katrina_Fraud/index.html).

[27] Albania encountered serious problems, including violence and the looting of small arms from armouries, following the collapse of a pyramid investment scheme in the period 1996-1997 (see

V. International cooperation and jurisdiction

42. Major transnational fraud cases pose a significant challenge for international cooperation. They tend to be large, complex, costly and multi-jurisdictional and involve many offenders, large numbers of victims and investigative agencies and private sector institutions. In States where rules and practices for cooperation have evolved to deal with a small number of major cases, mass frauds can evolve to take on the appearance of a large number of relatively small frauds. Successful fraud generates substantial proceeds, which can be used to support organized criminal groups, protect ongoing fraud operations, conceal and launder proceeds and mount protracted legal challenges to mutual legal assistance and extradition. Many of the comments received highlighted the need for cooperation, but the prevalent view was that existing legal instruments, especially the Organized Crime Convention and, for those countries that are States parties to it, the Council of Europe Convention on Cybercrime provided a sufficient legal basis for such cooperation, and that the focus should be on measures to ensure that the available instruments could be and were used effectively, rather than on the development of new ones. It was also noted that no formal legal authority or basis of any kind was necessary in some important areas of cooperation against fraud, especially in areas such as prevention.

A. Mutual legal assistance and other investigative cooperation

43. A number of States highlighted the general need to deliver effective mutual legal assistance. Generally, investigators and prosecutors need information and evidence relating to communication between offenders and victims and the transfer of funds. That includes information to identify the sources and destinations of communications and offenders and victims and the content of communications to prove elements such as deception. Financial records proving the transfer of economic benefits are also needed. It is important to trace and identify proceeds, including initial transfers from victims to offenders, as well as subsequent money-laundering. Evidence of the harm caused by major cases involving transnational fraud is also important, and that may consist of direct evidence from individual victims or expert forensic evidence. Expert evidence may be needed to establish that offender conduct was not consistent with normal commercial practice. Several States raised the question of transferring testimonial evidence efficiently, and experts drew attention to the use of video-link evidence pursuant to the provisions of the Organized Crime Convention.[28] Effective cooperation in fraud cases does not always require formal mutual legal assistance, because some communications and evidence can be intercepted or accessed within the jurisdiction investigating the crime. The major challenges identified in that area included the complexity of cases and the length of time that cooperation required. Several States highlighted the

---

Carlos Elbirt, "Albania under the Shadow of the pyramids", *Transition Newsletter*, 2001 (http://www.worldbank.org/html/prddr/trans/so97/albania2.htm)). Similarly, some sources cite the collapse of a Government-sanctioned pyramid scheme as a factor in the fall of the Government of Haiti in 2004.

[28] See the *Report of the Canada-United States Working Group on Telemarketing Fraud* and article 18, paragraph 18, of the Organized Crime Convention which calls for the use of video conferences to provide evidence. Similar provisions are found in article 46, paragraph 18, of the Convention against Corruption.

importance of fast and informal cooperation among investigators. Most forms of cooperation involve the sharing of information, which entails balancing investigative interests and the appropriate safeguards. One State noted that while fast information-sharing was often important in transnational fraud cases, there was also a need for balance and transparency to ensure that shared information was accurate and used in accordance with the relevant legal rules.

B. Extradition

44. Most States indicated that they could extradite criminal suspects, and some indicated that they had the authority to prosecute offences committed outside of their territorial jurisdiction in cases where they could not extradite. Some reasons for the refusal of requests for extradition, such as bars on the extradition of nationals, amnesty laws and limitation periods, could become obstacles in fraud cases. Experts noted that article 11, paragraph 5, of the Organized Crime Convention called for long limitation periods in organized crime cases, especially in cases where the administration of justice had been evaded, and much the same rationale was applied with respect to more complex fraud cases.

45. The Organized Crime Convention obliges States parties to extradite offenders accused of most serious forms of fraud or to prosecute them, subject to the exclusions set out in article 16 of the Convention, but the obligation to prosecute applies only if the reason for refusal to extradite is the nationality of the offender. The basic requirements for extradition are that the type of fraud committed is considered a serious crime in the domestic law of both States parties and that the crime involves an organized criminal group and is transnational in nature.[29] The Convention also requires States parties to ensure that they have jurisdiction over extraterritorial offences committed by one of their nationals in the case that they cannot extradite by reason of nationality, and it allows for the transfer of convicted offenders to serve sentences in their home countries.[30] States parties are also encouraged to establish jurisdiction over offences in which the accused is present in their territory and they do not extradite him or her, but that is not mandatory.[31] Within the framework of the Convention, gaps that could be addressed include ensuring that all States parties fully implement the Convention, that they ensure that serious fraud meets the criteria for serious crime, and that States parties that do not extradite their nationals implement the requirements of the principle of *aut dedere aut judicare*. A further potential gap exists with respect to two other scenarios. States should ensure that they are willing and able to prosecute fraud offenders that are not extradited solely on the ground that they are nationals, in implementation of the optional article 15, paragraph 4. Finally, while most major fraud cases involve organized criminal groups, transnational offences committed by individuals are

---

[29] Organized Crime Convention, art. 2, subparas. (a) and (b), and art. 3, para 2.

[30] Organized Crime Convention, art. 15, paras 3-4, art 16, paras. 1 and 10, and art. 17; see *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations publication, Sales No. E.05.V.2) and the discussion of jurisdiction contained in the "explanatory report" to the Convention on Cybercrime, paras. 233 and 239 (http://conventions.coe.int/Treaty/en/Reports/html/185.htm).

[31] Organized Crime Convention, art. 15, para. 4.

possible and could be provided for by responses such as case-specific agreements or arrangements. The Council of Europe Convention on Cybercrime[32] also provides for extradition in cases where the States concerned are parties, and that is not limited to States that are members of the Council. However, under the Convention, extradition for the offences of fraud and forgery is possible only in certain circumstances, when the crime involves the use of computers, computer systems or data. The Convention on Cybercrime, however, is not limited to cases involving an organized criminal group and can be applied where computer fraud or forgery is committed by an individual.

C. Jurisdiction

1. Territorial jurisdiction

46. Transnational fraud is one of the most common forms of crime presenting challenges for conventional territorial jurisdiction.[33] Offences may be planned in one country and committed by offenders based in a second country, victimizing persons in a third country, with proceeds accumulated and laundered in a fourth country. Victims are often located in many countries, and additional countries may be used for other purposes, such as for example, as a location for "drop boxes" (to transfer funds) or as a base for fraudulent Internet sites. In sophisticated transnational fraud cases, offenders are aware of jurisdictional limits and are fully capable of structuring transactions to take maximum advantage of any gaps or weaknesses. In response, concepts of territorial jurisdiction have also evolved, extending territorial jurisdiction to include offences that take place in two or more countries at the same time, that continue from one country to another over time, or that take place in one country but have some tangible impact on another country. The assertion of jurisdiction over an offence commenced in the prosecuting State and completed elsewhere or an offence in which any essential element takes place in that State now seems common.[34] Some States base territorial jurisdiction on the place where the offence was planned or where the last element, or any essential element, of the offence took place, including in cases in which the place where the offence was committed is uncertain.[35] It is less clear whether jurisdiction can be based on the presence of non-essential elements in a State's territory. Only one State reported the possibility of going further.[36] In that State, a real and substantial link to its territory must be shown, including the presence of non-essential elements such as

---

[32] Convention on Cybercrime, articles 3 and 4 (criminalization) and 24 (extradition).

[33] See, for example, Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford Monographs on Criminal Law and Justice (Oxford, Oxford University Press, 2003) pp. 158-180.

[34] John Seguin, "The case for transferring territorial jurisdiction in the European Union", *Criminal Law Forum*, vol. 12, No. 2 (2001), p. 249.

[35] See, for example, the United Kingdom *Criminal Justice Act, 1993* (c. 36), part I (http://www.opsi.gov.uk/ACTS/acts1993/Ukpga_19930036_en_1.htm); and Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford Monographs on Criminal Law and Justice (Oxford, Oxford University Press, 2003), pp. 163 ff.

[36] In Canada, the test of whether there is a "real and substantial link" to its territory is based on case law. The case concerned a fraud planned in Canada but involving victims and proceeds in other countries. Jurisdiction was based on the fact that the fraud was planned in Canada and that proceeds were returned there via other countries, but some essential elements also took place in the country (see *Libman v. the Queen* [1985] 2 S.C.R. 178 (Supreme Court of Canada)).

planning, preparation or the presence of proceeds, but it is not clear whether jurisdiction could be based exclusively on those factors. National laws requiring the presence of an essential element as the basis for territorial jurisdiction also depend to a substantial degree on how offences are formulated and what elements are included as essential. Conspiracy-type offences are usually broader, for example, and the formulation of cybercrime and telecommunication offences may expressly include elements such as the sort of effect or impact that must take place within a State's territory in order to fall within its jurisdiction. Article 11 of the Council of Europe Convention on Cybercrime provides for the criminalization of attempting, aiding or abetting the substantive offences set out in the Convention, including computer-related fraud and forgery.

47. Often the strongest incentive to prosecute lies in those countries where the victims are found or the adverse effects are suffered. Many States assert jurisdiction based on the fact that a result or effect of the offence occurred in their territory. Most limit such effects to those that are deemed essential or factual elements of the offence, which in cases of fraud usually requires the presence of victims. Some may apply a broader version of the same principle, including indirect losses. Frauds against companies may affect shareholders or markets, for example. The strongest disincentives to prosecute, especially in major fraud cases, are the costs and complexity of the cases, the principle of *ne bis in idem* and the fact that essential requirements such as witnesses and evidence have to be imported and may not meet domestic evidentiary standards. Even when a State has legal jurisdiction, the above-mentioned obstacles may prevent the State from exercising jurisdiction or result in discussions with other States about which is the most convenient forum for a prosecution.

48. The nature of fraud itself and the fact that offenders take jurisdictional gaps and limits into consideration when planning and carrying out fraud schemes create significant challenges to existing concepts of territorial jurisdiction. On the one hand, the need to ensure that offences can be prosecuted at all and the need to avoid jurisdictional gaps that offenders can exploit suggest a relatively broad model of jurisdiction. On the other hand, the potential for jurisdictional conflicts and the problems of prosecuting costly and complex transnational crimes suggest a more cautious approach. The gradual trend toward the expansion of territorial jurisdiction is likely to continue, driven in part by the creativity of transnational fraud schemes and greater access to information technologies. A single, straightforward formula for determining jurisdiction is unlikely to be viable or valid for all cases, and no existing model covers every possible case. The best approach is probably to ensure that as many States as possible have relatively broad territorial jurisdiction, that the various interested States collaborate effectively, and that the one State that is in the best or most convenient position to prosecute actually does so.

49. To ensure that transnational frauds can be prosecuted effectively, a number of legal and practical possibilities exist, depending on what measures are already available in each State. Those measures include ensuring that sufficient jurisdiction exists, based on the various jurisdictional models discussed in the present report, and, where appropriate, considering non-essential elements such as the presence of planning, preparation and proceeds, which may be more important in fraud cases than in cases involving other types of crime. The formulation of legislation on fraud offences is also important, especially when territorial jurisdiction is based on

essential elements defined as part of the offence. In the case of fraud schemes based in, or committed using the territory of, countries that lack law enforcement or prosecutorial capacity, general technical assistance to build the necessary capacity could be offered, and assistance might be tendered with respect to specific offences as part of international cooperation programmes.

50. Given applicable jurisdictional claims, there are often several States that could claim jurisdiction, and consultations to decide which State should prosecute will be important. That may involve legal, diplomatic and practical issues, ranging from the relative strengths of jurisdictional and other legal claims of each State and the question of whether offenders can be extradited to the State that wants to conduct the prosecution, to pragmatic considerations such as the costs and obstacles to transferring evidence from one State to another, ensuring its admission into legal proceedings and effective presentation before the court. Where it is decided that one of several possible States should prosecute, the jurisdiction of other States can effectively be transferred. Provision for that is made in the Model Treaty on the Transfer of Proceedings in Criminal Matters (General Assembly resolution 45/118, annex), article 21 of the Organized Crime Convention and article 47 of the United Nations Convention against Corruption (General Assembly resolution 58/4, annex).[37] Where two or more States have jurisdiction and want to prosecute, the following criteria could be considered:

(a) *The State which has suffered the greatest direct and indirect harm*. Harm provides incentive and justification to prosecute, and usually means that evidence will be available;

(b) *The State in which most of the elements of the offence* were committed;

(c) *The State that has the greatest investment of investigative efforts in the case*. Aside from the commitment of resources, that usually means that the State has the evidence necessary for prosecution;

(d) *The location of witnesses and evidence*. Transferring large volumes of evidence, especially in complex or mass fraud cases, raises costs significantly and may have a bearing on legal admissibility and on whether the evidence can be used effectively;

(e) *The State that has the strongest case*. Taking into account the totality of evidence that can be assembled in or transferred to each State, the evidence laws of each State and similar criteria, it may become apparent that one State has a better chance of a successful prosecution;

(f) *The State with the best capacity*. The complexity of major fraud cases can place substantial demands on investigators and prosecutors in terms of both costs and expertise. States with extensive experience and resources may consider either taking jurisdiction, if that is legally feasible, or providing assistance to another State that has a stronger case or claim but less capacity;

(g) *The nationality of the offender and whether he or she can be extradited*. States with what are otherwise weaker claims may have to prosecute their own nationals if they cannot be extradited;

---

[37] See also John Seguin, "The case for transferring territorial jurisdiction in the European Union" *Criminal Law Forum*, vol. 12, No.2 (2001), Seguin, loc. cit., p. 249.

(h) *Other offences involved or which may be prosecuted*. While jurisdiction is usually linked to specific offences, major fraud schemes often incorporate other crimes, including identity-related crimes and money-laundering. In some cases, it may be advantageous to consider which State is in the best position to prosecute all the various crimes of the case together;

(i) *Other offenders that are involved or may be prosecuted*. Similarly, it may be advantageous in specific cases, to determine the most convenient forum to prosecute a number of members of a criminal group and then extradite the others in order to try all together;

(j) *The respective sentencing regimes*. Generally, States may be willing to cede jurisdiction to other States with similar punishments for the crimes committed and are less likely to cede jurisdiction to States whose prospective sentences they consider to be excessively harsh or lenient.

2. Extraterritorial jurisdiction

51. While concepts of territorial jurisdiction have expanded to keep pace with the evolution of fraud and other common transnational crimes, the application of extraterritorial jurisdiction in fraud cases is less common. Some States apply extraterritorial jurisdiction in cases where crimes are committed abroad by their nationals or persons with domicile or other connections in their territory, especially if such States have constitutional bars to the extradition of their nationals.[38] Jurisdiction based on the nationality of victims (passive personality) is also possible, although in economic fraud such a basis might be difficult to distinguish from territorial jurisdiction based on effects or results. Some States reported the adoption of extraterritorial offences to protect what they considered vital interests against specific types of fraud, based on the protective principle. Examples given included the counterfeiting of currency, passports or other essential documents and frauds that affected national immigration systems. Another area that was not mentioned but which could lead to the invocation of the protective principle is that of major frauds against Governments, which could also be considered corruption offences.

D. Limitation periods

52. Experts noted that limitation periods could be a problem in many fraud cases, due to the length of time needed to properly investigate and prosecute complex and transnational cases, and also noted provisions of the Organized Crime Convention and the Convention against Corruption[39] calling for the establishment of appropriate limitation periods taking into account offences covered by that Convention and cases where the offender had evaded the administration of justice. Several approaches to ensuring the application of appropriate limitation periods were considered, including the establishment of basic limits by statute that were

---

[38] States parties to the Organized Crime Convention and the Convention against Corruption that cannot extradite their nationals are obliged to provide for such jurisdiction (see the Organized Crime Convention, art. 16, para. 10, and art. 15, para. 3, and the Conventions against Corruption, art. 44, para. 11, and art. 42, para. 3).

[39] See the Organized Crime Convention, art. 12, para. 5, and the Convention against Corruption, art.29.

appropriate for the fraud offences to which they applied, provisions for the suspension of limits in some circumstances, such as when the offender delayed proceedings or evaded the administration of justice, and the development of legislative provisions allowing for the judicial extension of a limitation period under the appropriate circumstances prescribed by legislation. The option involving judicial extension was viewed as inconsistent with the fundamental principle of *nullum crimen sine lege* by some experts and by others as a potential infringement of rights established by fundamental laws, and thus was not considered a viable option.

E. Cooperation in prevention

53. Much of the focus in international cooperation against fraud is on reactive measures such as the investigation and prosecution of fraud when cases are ongoing or have already occurred. Most States did not discuss prevention in the information they provided on international cooperation. However, there are areas where international cooperation can play an important role in prevention, and the costs and complexities associated with investigating and prosecuting major transnational fraud cases suggest that the benefits of cooperative prevention efforts may be substantial. Transnational fraud consists of activities that are undertaken within individual States and that can usually be prevented by measures at the national level if the appropriate officials have the necessary information in time to act on it. International cooperation to prevent fraud includes general and specific elements. At a general level, assistance in developing and refining preventive techniques, sharing lessons learned and best practices and sharing the information needed to develop such techniques and make them effective are all important. In addition, information may be shared on specific cases, methods or fraud operations, and that does not necessarily include the types of personal or investigative information that requires a formal mutual legal assistance process.

VI. Cooperation between the public and private sectors

54. Economic fraud is a crime of commerce. Thus, there is a need and motivation for collaboration between commercial and criminal justice interests. In the report on its thirty-sixth session, the United Nations Commission on International Trade Law (UNICITRAL) noted the need for such collaboration and called for action by the Commission on Crime Prevention and Criminal Justice, which UNICITRAL would continue its own work; that call led, in part, to the present study.[40] However, criminal justice and commercial practices and objectives do not always coincide. Some forms of commercial fraud may not be recognized as offences by criminal law. Where as criminal justice interests tend to favour investigation, prosecution and punishment, commercial interests tend to favour dispute-settlement mechanisms and the recovery of losses. What is shared is an immediate interest in acting quickly against ongoing fraud and an overarching strategic interest in the prevention and

[40] *Official Records of the General Assembly*, *Fifty-eighth Session*, *Supplement No. 17* (A/58/17), paras. 238-241; see also Economic and Social Council resolution 2006/24, para. 6, and the *Official Records of the Economic and Social Council*, *2004*, *Supplement No. 10* (E/2004/30), para.82.

suppression of both fraud and organized criminal groups, which appear to be responsible for a large portion of cases.

55. In other areas, however, public and private interests diverge. Where as private interests are governed by commerce, the marketplace and fiduciary obligations to shareholders, public interests are more broadly accountable, with non-commercial considerations such as human rights, environmental concerns and the common good being more dominant. The rule of law and the maintenance of effective judicial and criminal justice institutions require that key functions, particularly prosecutorial and judicial functions, remain independent of external influences. While effective cooperation is important, it is essential that adequate safeguards ensure that commercial interests do not compromise judicial and prosecutorial independence. In a broad strategic sense, the public and private sectors have shared interest in effective criminal justice systems. And rule of law values and institutions are essential to the governance and regulation of commerce and the establishment and maintenance of the stable social and economic environments in which commercial enterprises can prosper.

56. The responses of States suggest that there is both a substantial need for the expansion of private-public cooperation and substantial potential for such expansion. Most States did not provide much information on cooperation, but many indicated that they saw a need for it. A number of responses described only coercive measures, such as legal requirements to report offences or disclose information on legal persons or employees involved in fraud. Some States mentioned regulatory and legislative standards. The United States of America described its 2002 legislation establishing a range of standards intended to address fraud and corporate governance issues.[41] Several other States mentioned commercial laws and regulations to encourage standards and practices for deterring and preventing fraud. Those regulations, among other things, promoted transparent reporting and auditing of companies, encouraged individuals aware of wrongdoing to report it or cooperate with authorities, and required senior officials to take responsibility for the accuracy of accounting and financial information. A few States reported national strategies for commercial and industrial development, including issues relating to fraud and other crime problems of mutual interest. Those strategies provided for consultations or meetings in which commercial and criminal justice experts could meet to identify new issues and develop common or coordinated approaches. Some States also indicated that joint consultative bodies had been established to deal with specific problems such as fraud and money-laundering.

57. The presence of coercive measures is not necessarily indicative of the overall public-private relationship. A number of States reported legal requirements that private companies protect privacy and personal information given to them in the course of business, and many companies could face civil liability if they disclosed confidential information (unless they had been compelled by law to do so). Nevertheless, in many countries there appears to be a significant opportunity for the development of regulatory standards and collaborative, rather than coercive, commercial and criminal justice practices against fraud, based on joint consultations between the appropriate public and private sector entities. The area of collaboration

[41] Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act of 2002) of the United States (Pub. L. 107-204, 116 Stat. 745) 15 U.S.C. 7201 ff.

most commonly noted was the sharing of information by commercial entities. Such entities are often the first to become aware of a developing fraud case, either because their customers report it or because unusual patterns of activity or commercial practice are observed, and the need to alert law enforcement authorities quickly in order to take effective investigative measures to halt ongoing frauds was considered important. The other major area of potential collaboration is that of prevention. Measures to prevent fraud, which are discussed in section VII below, can be broadly divided into two categories: measures addressing potential victims, to make it harder to deceive them; and measures directed at targeted commercial structures, to make them more difficult for offenders to attack or exploit.

VII. Prevention of economic fraud

58. A range of possible preventive measures were raised by the replies to the questionnaire. Fraud involves the deception of victims, and in their responses some States discussed information campaigns to warn and educate potential victims. Other measures raised focused on prevention measures that used technology to make fraud more difficult and to increase the likelihood of early detection and disruption before a major fraud was completed or before large numbers of people were victimized in a mass fraud. Several States noted the importance of fast and accurate information-sharing to permit timely and successful education and disruption efforts. Some States mentioned the education of persons other than victims, in particular employees of banks and financial institutions, who were likely to encounter frauds. Some cited the utility of methods to counter money-laundering and corruption in preventing and mitigating fraud. One noted that banning those convicted of offences from future participation in a business (for example, through the denial of a license) might be of use with repeat fraud offenders. Another noted that simple precautions such as safeguards on processes for changing postal addresses and redirecting mail, to be undertaken by businesses and customers, had a substantial potential for prevention.

59. A number of States suggested that technical security measures were important for prevention. The creation and use of modern cryptographic systems, for example, are widely credited with making modern payment card technologies feasible, and the international business community has led the way in the use of digital signatures and other adaptations to reduce fraud in larger commercial transactions.[42] Technical measures were seen as necessary for almost every element of a commercial system, including elements in the hands of individual users, communications between system elements, and system elements for processing and storing data. It was also noted that because of the global nature of commerce and identification, most technical measures had to be applied on a global scale. Otherwise, security measures applied in one country would be ineffective in others or could prevent the legitimate use of a card or other technology altogether. Another challenge faced in developing new security technologies is the constant evolution of technologies, commercial applications and offender techniques. Accordingly, it is essential that both public and private entities maintain constant vigilance and devote the necessary

[42] See the Model Law on Electronic Signatures of the United Nations Commission on International Trade Law (*Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 17* and corrigendum (A/56/17 and Corr.3), annex II).

commitment and resources to developing and disseminating new preventive measures as soon as existing ones become obsolete.

60. For commercial interests, issues of cost and competitiveness also arise when technical prevention measures are developed and implemented. There is sometimes controversy over whether crime control elements, especially those which support investigation and prosecution, should be paid for by Governments or by the companies and users of the technologies. Commercial interests tend to weigh their options in cost-benefit terms and have concerns that incorporating some security elements may make them less competitive in the global market, where competitors based in other jurisdictions do not have the same requirements. While the development and use of technical prevention measures may best be left to the marketplace, there are some roles that may involve Governments. Many States indicated that they set minimum standards to protect consumers from fraud and related practices such as deceptive or misleading advertising, and some set minimum standards to ensure the protection of customer information. States can play a useful role, both individually and collectively, in ensuring that the marketplace encourages effective prevention and security and that the competitive positions and interests of companies that implement effective anti-fraud measures are not prejudiced by having taken those measures.