United Nations A/CONF.203/13

# Eleventh United Nations Congress on Crime Prevention and Criminal Justice

Distr.: General
16 March 2005

Original: English

Bangkok, 18-25 April 2005

Item 6 of the provisional agenda*
**Economic and financial crimes: challenges to sustainable development**

## Workshop 5: Measures to Combat Economic Crime, including Money-Laundering**

### Background paper***

Contents



* A/CONF.203/1.

** The submission of the present background paper was delayed by the need for additional research and consultations.

*** The Secretary-General wishes to express his appreciation to the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders and the Government of Sweden for assisting in the organization of Workshop 5.

V.05-82371 (E) 300305 310305

# I. Introduction

1. In addition to the transformation of socio-economic structures, the recent rapid developments in communications technology and transportation have promoted globalization, with the growth of transactions and diversification of economic activities, which are becoming increasingly transnational in nature. Together with these changes, which have created new opportunities for growth and development, economic crime has also become a global concern, while the modus operandi of criminal groups has become more sophisticated and the scale of their activities has increased considerably. That trend has been accelerated by the rapid proliferation of computers, the considerable increase in the number of users of Internet services and the expansion of credit-card-based economies. By their very nature, crimes committed by using the Internet as a tool easily transcend national borders and spread all over the world. Criminals fully exploit the Internet and electronic commerce to commit economic crimes transnationally. The transnational nature of those crimes hampers their detection and makes investigation and prosecution more difficult. The tracing and return of proceeds of crime have also become much more complicated. Thus, economic crimes in a globalizing society present a serious problem to the international community and hinder the development of the world economy.

2. The Eleventh United Nations Congress on Crime Prevention and Criminal Justice will offer an opportunity for extensive discussion of the broad issue of economic and financial crime. For the purpose of that discussion, the Secretariat has prepared a working paper (A/CONF.203/7), which raises a number of issues for discussion and describes in considerable detail the problems posed by this form of crime, including the conceptualization of economic and financial crime, and the reasons for which such problems require particular attention by the international community.

3. Workshop 5 offers an additional opportunity for interactive dialogue among government representatives, experts and practitioners with a view to focusing on the extent and impact of economic crime in its multiple manifestations. Such focus will also be necessary in formulating viable and practical policy recommendations and exploring the requirements for national action and international cooperation, including technical assistance.

4. More specifically, Workshop 5 could serve as a point of departure for the consideration of measures to combat economic crime and money-laundering, including discussion of the following issues:

(a) Current trends in economic crime, including money-laundering, with special attention to the typology of such crime;

(b) The extent to which existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (General Assembly resolution 55/25, annex I) and the Protocols thereto and the United Nations Convention against Corruption (resolution 58/4, annex), could be used to counter them;

(c) The formulation of effective prevention strategies;

(d) New investigative techniques;

(e) The establishment of effective financial intelligence units, including better cooperation among them;

(f) International cooperation and technical assistance.

In order to maximize the practical orientation of the Workshop and to encourage interactive dialogue, the present background paper includes a hypothetical case for analysis and discussion (see annex).

# II. Identity theft

5. One of the principles guiding the work of the United Nations Crime Prevention and Criminal Justice Programme is the need to ensure that any increases in the capacity of perpetrators of crime are matched by similar increases in the capacity of law enforcement and criminal justice authorities. Another goal of the programme is to control crime both nationally and internationally. Consideration of domestic and international measures to address identity theft is consistent with both objectives.

6. "Identity theft" can be said to involve two alternative, distinct activities. The first is the preparatory stage of acquiring, collecting and transferring personal information, whether the information is intangible (e.g. virtual information on a computer screen) or tangible (personal information copied down on paper from a computer screen or from an actual document). At this stage, there has been no actual use of the information to try to commit, or actually to commit, a criminal offence, such as fraud, theft or impersonating another individual. The personal information is acquired as an instrument of crime for future use. The second, alternative component of identity theft involves the actual use of the personal information to attempt to commit, or actually to commit, a criminal offence. In this context, the personal information is used either to assume an entirely new identity in all aspects (A poses as B) or to convince a victim that an aspect of a transaction is something it is not (e.g. that the account balance in a bank account is $X rather than $Y because the account belongs to B rather than to culprit A).

7. Identity theft thus involves one or more actions along a continuum of behaviour that eventually leads to the commission of a crime, usually of an economic nature. In most States, if the perpetrator does not commit a criminal offence in order to obtain the personal information, as for example by committing theft, the acquisition and possession of the personal information itself do not constitute an offence. There is increasing evidence, however, that identity theft facilitates the commission of economic crime, both nationally and internationally.

8. In many if not most States, criminal liability often attaches only after the perpetrator actually uses the personal information rather than at the time that the perpetrator acquires the personal information with the intent of using it for future criminal use. For example, the criminal can surreptitiously obtain personal information in order to assume the identity of the victim and thereby commit fraud, evade capture or detection or, in some instances, to commit offences associated with organized crime or terrorism. In many States, unless a conspiracy or organized criminal activity can be established, one or more of the following acts may not be criminalized: collecting, acquiring, storing, possessing, buying, selling, importing

and exporting personal information that is not tangible (e.g. personal information available on a computer or written lists of personal information copied from identification documents).

9. The means by which perpetrators obtain personal information vary in terms of their technical sophistication. Some of these activities are crimes in almost all countries (e.g. theft) and some of them are not. Examples of the more common ways in which personal information is obtained for later criminal use are as follows:

(a) Theft of purses and wallets; theft of documents from the mail; redirection of mail from the victim's home to the perpetrator's home;

(b) Recovering from trash documentation that identifies personal information relating to the victim, for example, a credit card or bank account number ("dumpster diving");

(c) Unauthorized copying of digitized data (e.g. "skimming" devices that record credit card and/or debit card numbers; a hidden camera to record personal identification numbers (PIN) accompanies the skimming of debit cards);

(d) Obtaining personal information in respect of a dead person in order to assume their identity ("tombstoning");

(e) Obtaining personal information from public sources (e.g. "shoulder surfing", which involves looking over someone's shoulder while they are entering their PIN when using a debit card);

(f) Obtaining personal profile information on an individual from the Internet with a view to using that information to impersonate them;

(g) Using the Internet to direct victims to a website that looks like that of a legitimate business. At the website the victim is asked to disclose his or her personal information. The personal information is collected by the criminal for later use to commit fraud or another form of economic crime (this activity is called "phishing");

(h) Compromise of large databases (e.g. hacking into public or private computer databases to obtain personal information in order to make false identification documents);

(i) Using personal information supplied by corrupt government or company employees to make forged documents (e.g. false driver's licences) or obtaining false identification documents from such employees.

10. One of the challenges many States face in addressing identity theft is that personal information generally does not fit the definition of "property". Traditionally, the offence of theft requires that the intangible and/or tangible "thing" taken must be capable of being characterized as "property". Also, for the elements of the offence to be present, the actions in respect of the "thing" must involve actual deprivation to the owner. In many States the mere violation of the confidentiality of personal information, in and of itself, may not be sufficient to satisfy the elements of either theft or fraud. Thus, in many States, if no criminal offence is involved in obtaining the personal information itself, then merely copying it or deceiving others into disclosing that information may also not be an offence. The distribution of personal information that does not meet the definition of "property" is also not a criminal offence in most States. In that context, the personal information becomes

an instrument to commit crime, but its acquisition, possession and transfer to others is not itself a crime.

11. In addition to the limitations in many States concerning legal definitions of "property" or the requirement of deprivation of the "thing" misused, developments in technology have also changed the way that economic crime is committed through the misuse of personal information. For example, prior to the invention of the computer and the Internet, a typical fraud case could have involved an individual stealing the identification of another person and then using that identification to pretend that he or she was someone else in order to secure a loan or borrow money from a bank. The accused was involved in all the aspects, both physical and mental, of the crime. Usually there was also physical contact between the criminal and the victim.

12. The advent of computers and the Internet has facilitated the commission of crimes that involve different actors along a continuum of criminal activity. Their detection has been hampered by the anonymity that computer technology typically provides. This encourages the use of multiple actors who act either in concert with each other or else independently from each other but with the knowledge that the personal information is being gathered and transferred for criminal purposes. The challenge for law enforcement is that no one actor has committed all of the acts along the continuum of behaviour that ultimately results in the commission of a traditional economic crime. Each person is responsible for a particular aspect of the activity that cumulatively produces the crime, such as fraud. This method of committing economic crime has been used by organized criminal groups to insulate individuals from criminal prosecution.

13. An example of the use of multiple actors to commit crime is as follows: A may copy personal information relating to various individuals from a computer. A then sells the personal information to B. This may be done using sophisticated technology such as the Internet or it may be done in a more traditional way, such as actually handing over money in exchange for information. B may act as an intermediary and may sell the information to C, who uses the information to produce false identification. C sells the false identification to customers in different countries. Some of the customers use the false identification to commit frauds against victims in other countries. Other customers sell the false identification to organized criminal groups or to terrorists to facilitate the commission of other crimes, such as drug trafficking, money-laundering or trafficking in contraband. Subject to any laws relating to conspiracies or modes of participation in the commission of an offence, in many States no offence has been committed by A or B, even though their activities are integral to providing the necessary information to C to make the false identification.

14. Most States do not have a crime of "identity theft". It is difficult to determine from a statistical point of view, therefore, whether fraud involving identity theft is subsumed in fraud statistics generally. This complicates efforts to track international trends in the growth of crime involving the misuse of personal information. It is hoped that a better understanding of domestic and transnational trends in fraud and the criminal misuse and falsification of identity may be generated by a study requested by the Economic and Social Council in its resolution 2004/26 of 21 July 2004.

15. Recent statistics from Canada and the United States of America relate to fraud committed by the misuse of personal information and confirm an explosive growth in the nature of such crime. The Phonebusters National Call Centre in Canada reported 8,187 identity theft complaints in 2002, a number that had increased substantially, to 13,359 complaints, by 2003. Losses from complaints of identity theft were reported by Phonebusters to have been 11.8 million Canadian dollars in 2002 and up to Can$ 21.6 million in 2003 (see http://www.phonebusters.com). For the past four years the Federal Trade Commission of the United States has reported that identity theft has topped the list of consumer complaints filed with the Commission. In September 2003, the Commission released a survey indicating that 27.3 million Americans had been the victims of identity theft in the previous five years. The cost to consumers and businesses in 2002 was reported to have been 53 billion United States dollars.[1] Another survey conducted for the Commission in 2003 estimated that the 10 million victims of identity theft that year spent 300 million hours trying to restore their financial losses, credit ratings and reputations.[2] The Canadian Council of Better Businesses estimated that total consumer and commercial losses from identity theft in 2002 was Can$ 2.5 billion.[3]

16. The free flow of information, which is the lifeblood of the Internet and, therefore, also of the trade conducted over the Internet, offers innumerable opportunities for criminals to misappropriate personal information and use it to commit crime. Surreptitious collection and transfer of personal information for subsequent criminal use have the potential to undermine the economic and national security of member countries.

# III. Money-laundering

17. “Money-laundering” is generally understood to mean the processing of criminal proceeds to conceal or disguise their illegal origin. Criminals try to secure and further enjoy or use financial profits from their crimes through money-laundering. Money-laundering is therefore a very important process for most criminals, especially in relation to financial crimes committed mainly with a view to obtaining financial profit. Money-laundering is also exploited by criminals, as it allows them to engage in further criminal activity or finance their criminal organizations.

18. As money-laundering is in most cases committed by misusing or abusing existing financial systems, it presents a serious threat to the integrity of financial systems and financial institutions. Financial institutions corrupted by money-laundering have higher risks of being a target of further financial crimes and are thus caught in a vicious circle. In developing countries, money-laundering hampers or slows down economic development. A large amount of laundered money that has escaped the national financial authorities’ supervision and regulation impedes the formulation of precise national monetary policies and taxation systems.

19. The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988[4] was the first milestone in the continuous United Nations efforts against money-laundering. The fight against money-laundering began by targeting the laundering of proceeds of drug-related crimes, but it gradually became clear that money-laundering in relation to other serious crimes

caused similar threats to society and should therefore be addressed similarly. As a result, more recent international instruments call on States parties to punish money-laundering arising from all or most serious offences.

20. The terrorist attacks of 11 September 2001 in the United States brought to the forefront global concerns about terrorism and the international community soon agreed to make intensive efforts to prevent and stop terrorist financing. Given the commonality of detecting and analysing potential money-laundering activities and potential terrorist financing activities, it is more effective for major organizations that have been leading efforts to combat money-laundering also to address the issue of terrorist financing. The Security Council responded quickly to that need by establishing, in its resolution 1373 (2001) of 28 September 2001, the Counter-Terrorism Committee, with the Terrorism Prevention Branch of the United Nations Office on Drugs and Crime (UNODC) playing an integral part in the United Nations collective action against terrorism. It should be noted, however, that a sense of urgency prior to 11 September 2001 had already led to the successful conclusion in 1999 of the International Convention for the Suppression of the Financing of Terrorism (General Assembly resolution 54/109, annex), which came into force in 2002. The Financial Action Task Force on Money Laundering has also expanded its mandate to include terrorist financing.

21. Typologies or techniques of money-laundering develop constantly. It is widely recognized that criminals tend to be one step (or more) ahead of their adversaries, that is, investigative authorities, in finding loopholes in a State's legislation against money-laundering. Being familiar with the latest typologies is therefore a prerequisite for investigative and other relevant authorities to crack down effectively on money-laundering.

22. As cash-based economies allow criminals to transfer money or transform the form of assets without leaving financial transaction records, there are serious difficulties for investigators in tracing and securing evidence about money flow. Even in countries with the most sophisticated financial systems, there is a certain level of cash-based economy to meet certain needs. In many developing countries where formal financial sectors are not fully developed, the cash-based economy is the most common and credible financial system and to regulate it by any means is not an easy task. The common use of jewellery or precious stones as a means of holding assets poses the same problem when they are used as an alternative to cash.

23. Alternative remittance systems that transfer money or other assets using conduits other than formal financial institutions can similarly be an obstacle to combating money-laundering. Many alternative remittance systems have their source of credibility in cultural, ethnic or religious communities and usually require neither customer identification nor the keeping of financial transaction records, as provided for by international standards regulating financial institutions. In some States where money or value transfer services are allowed only to institutions licensed or registered as banks, alternative remittance systems are automatically an illegal and underground form of banking. In many other States, such systems are legitimate financial systems that have existed since long before the development of modern banking services.

24. The involvement and potential misuse of non-financial businesses and professions for money-laundering have attracted international concern recently, as more cases of such involvement have emerged. Those involved have included lawyers, notaries, other independent legal professionals, accountants (known collectively as "gatekeepers" because of their professional role to safeguard the integrity of financial transactions), dealers in precious metals or stones and trust and company service providers. Considering the important role that these businesses and professions play in financial transactions, agreement is emerging that regulations to police money-laundering should encompass them in certain circumstances, without prejudice to privileges related to professional secrecy.

25. Offshore financial centres have long been the centre of attention in addressing money-laundering problems, in view of their potential use as safe havens for money-launderers. However, thanks to concerted international efforts, many offshore financial centres have already improved their practices by revoking the licences of shell banks or strengthening customer identification requirements for corporations. Public campaigns at the national, regional and international levels have had considerable success in raising public awareness about the risks of using offshore financial centres that are not transparent in their structure and operations. The issue of such centres, however, needs continuous review and supervision, in particular because of the increasing ease of doing business with them from any part of the world via the Internet and other advanced technologies.

26. A number of international standards to combat money-laundering are already in place. As mentioned earlier, the United Nations has long been a champion in this area, in the development of a number of important legal instruments. In 1988, the General Assembly adopted a Political Declaration (resolution S-20/2, annex) and action plan against money-laundering (resolution S-20/4 D). The Organized Crime Convention and the United Nations Convention against Corruption call on States parties to strengthen their regimes to combat money-laundering and their implementation. The United Nations has also provided considerable technical assistance in this area through the UNODC Global Programme against Money-Laundering.

27. Another main source of international standards in this area is the Financial Action Task Force on Money Laundering. Its Forty Recommendations, originally issued in 1990 and revised in 2003, provide detailed technical standards. The Task Force also issues a typologies report annually. Though its membership is limited, related regional bodies around the world assist other States in complying with the Recommendations.

28. Other sources of international standards include the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, the International Association of Insurance Supervisors and the Wolfsberg Group, which consists of 12 major international private banks in cooperation with Transparency International.

29. In recent years, the International Monetary Fund and the World Bank have also strengthened their involvement in combating money-laundering and the financing of terrorism and have developed a comprehensive compliance assessment methodology in cooperation with the Financial Action Task Force on Money Laundering.

30. Financial institutions have at their disposal a wealth of useful information emanating from regular business transactions being conducted at any given moment. In that respect, a regular and functioning cooperation mechanism between private financial institutions on the one hand and relevant national authorities on the other is critical to dealing effectively with information that may lead to the investigation and prosecution of money-laundering cases.

31. If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity, it should be required to report its suspicions promptly to a body specially set up to collect and process such information, such as a financial intelligence unit. A financial intelligence unit is a national centre for receiving (and, as permitted, requesting), analysing and disseminating suspicious transaction reports and other information regarding potential money-laundering. The establishment of a financial intelligence unit is one of the important initial steps in establishing an effective national regime against money-laundering. Financial intelligence units are typically located in the central bank, the ministry of finance or the police, but what is important is not their location, but whether they are fully operational. Suspicious transaction reports are important as a means of ensuring customer due diligence in identifying potential money-laundering activities. The relevant national authorities are expected to provide practical guidance as to what constitutes suspicious transactions for the use of financial institutions.

## A. Criminalization of money-laundering: legal framework

32. An effective legal framework is essential in order to fight money-laundering. Material elements for the offence of money-laundering are included in relevant international legal instruments, especially in the 1988 Convention, the Organized Crime Convention and the United Nations Convention against Corruption. States parties to those conventions are under an obligation to have in their domestic legislation sufficient provisions to criminalize the conduct defined in those instruments. Moreover, parties are also called upon to take into account the provisions of the conventions that stipulate that knowledge, intent or purpose required as an element of the offence may be inferred from objective factual circumstances.

33. Nevertheless, many variations can be observed in how States define and punish money-laundering activities. For example, in defining predicate offences of money-laundering, some States enumerate them in a list attached to a piece of legislation, whereas some States take a so-called threshold approach, defining the predicate offences as crimes punishable in a certain way. In any event, the Organized Crime Convention and United Nations Convention against Corruption call upon States parties to include a broad range of serious crimes as predicate offences.

## B. Investigation of money-laundering offences

34. As noted above, money-laundering techniques develop constantly and investigative techniques tend to lag behind. It is therefore critical for investigators

to obtain the fundamental knowledge and necessary skills about money-laundering investigations, including those of forensic investigation and accounting, and to continuously follow the latest typologies. More importantly, investigators should be provided with adequate technological facilities and support for use in their daily operations, as well as training opportunities to strengthen their professional investigative capacity. In that respect, provision of technical assistance by countries with advanced knowledge and skills in money-laundering investigation to countries suffering from weak institutional capacity is to be further encouraged in order to avoid providing money-laundering havens for criminals.

### C. International cooperation

35. As financial crimes are committed increasingly across national borders, so does money-laundering acquire a transnational character more often than not. It is always a challenge for investigative authorities to trace and prove complex transnational money flows and, for that purpose, international cooperation is extremely important, as in the investigation of any other transnational financial crime. An example of such cooperation is the Egmont Group of Financial Intelligence Units, an international organization set up to facilitate international cooperation among financial intelligence units around the world.

### D. Control of the proceeds of crime

36. Since economic crimes, including money-laundering, are committed for the purpose of obtaining profit, tracing, freezing, seizing and confiscating the proceeds of crime are the most effective measures against those criminal activities. The latest sets of measures that the international community agreed to take can be found in the Organized Crime Convention and, more recently, in the United Nations Convention against Corruption, especially its chapter on asset recovery. There is an urgent need to enhance domestic and international efforts to further develop and utilize those measures to the full.

## IV. Technical assistance

37. The primary aim of the United Nations Crime Prevention and Criminal Justice Programme is to assist the international community in meeting its pressing needs in the field of crime prevention and criminal justice and to provide States with timely and practical assistance in dealing with problems of both national and transnational crime.

38. One of the priorities of the programme is to give consideration to the need for developing countries and countries with economies in transition to have recourse to expertise and other resources necessary for establishing and developing technical cooperation initiatives that are appropriate at the national and local levels.

39. The workshops to be held within the framework of the Eleventh Congress will provide an opportunity to deliver practical assistance in the form of the direct contribution of experts, as well as through the sharing of information and experience. The workshops will also enable consideration of technical cooperation

ideas and projects related to addressing priority needs and enhancing bilateral and multilateral efforts in technical assistance and training.

40. Developing effective technical cooperation programmes requires mechanisms and projects that are flexible and appropriate to the identified needs of the requesting country and that do not duplicate the activities of other entities. In addition, an efficient approach to combating economic crime and money-laundering requires delivery of sequential technical assistance across several sectors, including awareness-raising and policy development; establishment and implementation of the appropriate legal infrastructure; development of measures relevant to the regulatory and financial sectors; and assistance to support law enforcement processes.

41. The assistance provided may include research and information exchange; needs analysis; consultancies and advisory services; study tours; awareness-raising seminars; development of model laws and regulations; drafting assistance for legislation and regulations; local, national or regional training courses; computer-based training modules; mentoring, secondments and attachments; guidance notes and best practice tools; and communication and information technology support and training. The training and assistance may be delivered through country or regional projects and may involve local, bilateral and multilateral cooperation.

42. One of the fundamental challenges in developing timely and practical programmes appropriate to each country is the ability to identify with accuracy the relevant technical assistance and training needs. This information is usually compiled from a wide variety of sources and frameworks—bilateral and multilateral needs assessment studies and missions; compliance assessments and mutual evaluations in relation to relevant global standards; self-assessments; and country statements in the context of regional and international forums.

43. Efficiently designed needs assessments can provide a solid foundation for effectively sequencing and coordinating the delivery of assistance. While a number of countries may complain of “assessment fatigue”, both in general and in relation to specific technical assistance and training, others are still calling for such assessments to assist in defining and refining their needs. In the absence of a standard framework, there is an opportunity for enhanced international cooperation in developing and implementing needs assessments to enhance consistency and reduce duplication.

44. Associated with the preparation of needs information is the identification of priorities for assistance. Technical cooperation can only be effective if national and local needs are the primary concern in determining priorities and appropriate modes of delivery, rather than the policy or operational imperatives of bilateral or multilateral donor organizations.

45. In considering the requirements for technical cooperation that respond to the needs of each country without duplicating the activities of other existing mechanisms, the call for effective coordination is inevitable. Determining how such coordination might be organized and implemented has been the subject of significant international debate, in particular in the context of international efforts to combat money-laundering and the financing of terrorism. While the need for coordination is frequently emphasized, it is equally stressed that coordination mechanisms must not act to control or constrain the mandates and activities of the donors and providers, nor act as a “buffer zone” between the State requesting

assistance and the provider. It is clear, therefore, that for the coordination of technical cooperation to be successful, the process needs to be voluntary and flexible and it must add value but not costs, and the individual mandates of donor and provider organizations must be respected.

46. Beyond coordination, the requirement to build sustainable capacity is one of the most significant issues challenging technical cooperation activities. This is especially so given the diversities in location, size, economic and social development, institutional capacity and legal and administrative systems of Member States. The consistent call from recipient countries is for donors and providers to move away from short-term, short-impact assistance towards longer-term in-country training, secondments, study tours, training of trainers and mentor attachments. The assistance provided needs to be supported over a number of years and, where shorter-term in-country or regional training is delivered, this needs to be followed up to consolidate and institutionalize both knowledge and skills. In the field of economic crime and money-laundering there are, however, few suitably qualified and experienced experts available. Accordingly, careful planning and coordination are required by the international community. There is clearly an opportunity for bilateral and multilateral donors to support the development of sustainable capacity by increasing the availability of longer-term training courses, mentors, secondments and technical attachments.

47. In addressing measures to combat economic crime, including money-laundering, it is important to recognize the contribution of the private sector. While private sector organizations are frequently the unwitting vehicles for perpetration of such crimes, those same organizations can also be active partners in compliance and prevention. Given those roles, there is a significant technical cooperation contribution to be made by the private sector at the national, regional and international levels. This raises the challenge of identifying opportunities to engage the private sector in collaborative technical assistance and training activities, involving both public and private-sector organizations.

# V. Conclusion and recommendations

48. Workshop 5 will provide an opportunity for the international community to consider practical ways of addressing more effectively the issues mentioned above, taking into account the proposals made by the regional preparatory meetings for the Eleventh Congress. Questions raised in the discussion guide for the Eleventh Congress (A/CONF.203/PM.1) will also serve to focus the discussion, such as (a) success stories and obstacles encountered in the fight against economic crime and in the prosecution of money-laundering cases, including the confiscation of proceeds of crime completed pursuant to legislation to combat money-laundering; (b) how financial intelligence units can work with their counterparts and other institutions to ensure best practice in national and international cooperation; and (c) how best to implement standards in countering money-laundering in the informal and cash-based economy. Further, Workshop 5 will attempt to promote the ratification and implementation of the Organized Crime Convention and the United Nations Convention against Corruption, in particular as regards their provisions relating to money-laundering.

49. With a view to achieving those objectives, a hypothetical case has been devised to facilitate interactive discussion among participants (see annex).

*Notes*

[1] Adam B. Schiff, in the 23 March 2004 proceedings of the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, United States House of Representatives, 108th Congress, 2nd session, Serial No. 74, p. 15.

[2] Synovate, *Identity Theft Survey Report*, prepared for the Federal Trade Commission (September 2003) (http://www.ftc.gov/os/2003/09/synovatereport.pdf.), pp. 4 and 6.

[3] Canadian Bankers Association, "Identity theft: an old problem needing a new approach" (unpublished), May 2003, p. 5.

[4] United Nations, *Treaty Series*, vol. 1582, No. 27627.

# Annex

## Hypothetical case for use at Workshop 5: Measures to Combat Economic Crime, including Money-Laundering

### A. Introduction

1. The following hypothetical case is designed to facilitate discussion among practitioners attending Workshop 5 and to stimulate practically oriented discussion with a view to focusing on truly effective measures to combat economic crime and money-laundering. In the hypothetical case, various issues pertaining to prevention, information-gathering, investigation and prosecution of economic crime and money-laundering are raised, such as:

(a) Preventive measures for economic crime and money-laundering;

(b) Informants (whistle-blowers);

(c) Use of information technology both by criminals and investigators;

(d) Liability of legal persons;

(e) Identity theft;

(f) Shell companies;

(g) Customer due diligence;

(h) Conspiracy or participation;

(i) Investigative techniques for economic crime and money-laundering;

(j) Use of information technology, both by offenders and investigators;

(k) Inter-agency cooperation;

(l) International cooperation, including mutual legal assistance and extradition;

(m) Criminalization of money-laundering;

(n) The role of financial intelligence units, including cooperation among units;

(o) Suspicious transaction reporting;

(p) Typology or modus operandi of money-laundering;

(q) Issues related to the informal and cash-based economy, including alternative remittance systems;

(r) Use of insurance and negotiable instruments;

(s) The role of professionals in activities to combat money-laundering;

(t) Control of the proceeds of crime, including freezing, confiscation, civil forfeiture or asset sharing;

(u) Victim restitution.

Those who wish to participate in Workshop 5 are invited to study the hypothetical case presented below in advance.

2. The case is divided into two parts, the first depicting breach of trust and international fraud, which include various issues commonly found in economic crime and could be regarded as predicate offences of money-laundering. The second part describes unlawful activities relating to concealing and disguising, and further utilization, of the proceeds of crime depicted in the first part.

## B. Hypothetical case

3. In the following description, suggested issues for discussion are presented in italics:

### 1. Breach of trust by a bank manager

1. Mr. Alan was a national of country Xanadu and a manager of Finebills Bank, established in that country.

2. Mr. Banner was also a national of Xanadu and ran a real estate agency, Kondo Inc., also established in that country.

3. The financial situation of Kondo Inc. deteriorated and Mr. Banner asked Mr. Alan to grant the company a loan of $1 million.

4. Since Mr. Alan was an old friend of Mr. Banner, he agreed to grant the loan without any collateral, although he knew that there was a possibility that the loan would not be paid back (Mr. Alan's decision was against the internal regulations of Finebills Bank) (*improving integrity in the public and private sector, corporate governance and other preventive measures*).

5. After three months, it became evident that Kondo Inc. could not repay the debt (*informants or whistle-blowers, assuming that the bad loan contract was reported by a bank employee*).

### 2. Consumer fraud

1. Mr. Alan feared that he would be held responsible for the bad loan and asked Mr. Banner to find a way to pay it back.

2. Mr. Banner consulted his mistress, Ms. Chung, a national and resident of country Youngland, about the matter, and Ms. Chung proposed the following:

   (a) Ms. Chung would set up a shell company, Lownet Inc., in Youngland to conduct a consumer fraud;

   (b) Ms. Chung would place an advertisement via the Internet (*use of information technology*) stating that Lownet Inc. could teach consumers how to purchase foreclosed and distressed real estate properties and promising that it would provide the capital for such purchases;

(c) Lownet Inc. would further promise to pay each customer $2,500 every time they partnered with it in a real estate deal and claimed the company could split the profits after the property was sold. Lownet Inc. would lure each consumer into purchasing an introductory videotape for $60 and advertise a 30-day full money-back guarantee. A portion of the $1 million would be used to produce videotapes;

(d) Lownet Inc. would also sell additional videotapes, which would be much more expensive than the first videotapes sold;

(e) The purpose of the advertisement would be to lure consumers into buying the videotapes and Ms. Chung had no intention of actually helping customers to obtain real estate;

(f) Customers would be requested to transfer the price of the videotapes to the bank account of Lownet Inc.;

(g) When approached by possible customers, Ms. Chung, introducing herself as Ms. Petal, an executive of Lownet Inc., would say that her company had many transactions with Finebills Bank and give them the name of Mr. Alan as a reference;

(h) When contacted by customers enquiring about Lownet Inc., Mr. Alan would assure them that Lownet Inc. was a company in good standing (*liability of legal persons*);[a]

(i) Ms. Chung would pay $2 million to Mr. Alan and Mr. Banner if the scheme succeeded.

3. Mr. Alan and Mr. Banner agreed to Ms. Chung's proposal.

4. Ms. Chung asked a friend of hers who was a bank employee about the disposal of bank records and this employee indicated that all bank trash was simply left outside of the bank in a large bin (*integrity of the system*).[b] Ms. Chung accessed the bank trash and collected personal information from discarded bank records for the purpose of opening bank accounts in another country (*identity theft*).[c]

5. Ms. Chung set up a shell company Lownet Inc. (*shell companies, role of professionals*)[d] in country Youngland, which was considered an offshore centre by the international community, and opened an account at Goldfingers Bank in that country (*conspiracy or participation, customer due diligence*).[e], [f]

---

[a] That is, the possibility of whether Finebills Bank can be held legally responsible for the action of Mr. Alan.

[b] This fact raises the issue of confidentiality of the institution's data and the protection of that data from interference by third parties.

[c] "Identity theft" involves the collection of personal information data for future criminal use. In this instance the specific form of identity theft is called "dumpster diving".

[d] Identity theft could also be discussed. If Ms. Chung set up a shell company with the help of a lawyer, participants may wish to discuss, at the beginning of its discussion in the money-laundering part, the issue of the role of professionals in preventing such activities.

[e] By asking the question "What can be done if law enforcement officials know about the scheme

6. Lured by an Internet advertisement and sometimes with the assurances of Mr. Alan, many customers worldwide purchased the videotapes and the proceeds of this fraudulent scheme amounted to $5 million which was remitted to Lownet Inc.'s account at Goldfingers Bank (*investigative techniques, immunity, inter-agency cooperation*).[g]

### 3. Money-laundering and control of the proceeds of crime

1. Ms. Chung transferred the $5 million proceeds in Goldfingers Bank to 15 bank accounts in country Zeitstaat (*suspicious transaction reporting*).[h]

2. Ms. Chung provided the personal information from the bank trash to Ms. Dee and asked Ms. Dee to use the information to forge false identification documents (*identity theft*).[i] Ms. Dee used the false identification to open 15 bank accounts in Zeitstaat. Ms. Dee was a national of Zeitstaat and worked as an accountant there (*role of professionals as gate-keepers*).[j]

3. Ms. Dee withdrew the funds ($5 million) from the 15 individuals' accounts from numerous automatic teller machines in small denominations in Zeitstaat over a period of time (*suspicious transaction reporting, including the use of information technology for the purpose of its analysis*).

4. At the request of Ms. Chung, Ms. Dee brought $2 million in cash into Xanadu and handed it to Mr. Banner. Ms. Dee did not declare that she was carrying $2 million to the authorities of Xanadu or Zeitstaat (*cash courier and possibly controlled delivery of cash*) and handed it to

---

before any consumers actually become victims?", participants can discuss the application of conspiracy or participation, stipulated in the United Nations Convention against Transnational Organized Crime.

[f] At the beginning of the discussion on money-laundering, participants may wish to discuss what should have been done by Goldfingers Bank to prevent the opening of accounts by a shell company.

[g] The investigative technique could be introduced whereby a law enforcement officer pretends to be a potential customer and approaches Ms. Chung to get information. Also, the issue of granting immunity can be discussed here by asking "What could prosecutors do to obtain enough evidence to prosecute Ms. Chung?" Issues related to mutual legal assistance could also be dealt with. In addition, issues related to inter-agency cooperation could be discussed here by introducing the scenario that claims to the consumer protection agency lead to the law enforcement agencies getting involved.

[h] It could be noted here that the criteria for suspicious transaction reporting vary from one State to another; some set out a certain amount of money as the threshold for reporting, whereas others take a more generic approach, where banks are required to report transactions they think are "suspicious", regardless of the amount. If the transfer was made by electronic methods such as SWIFT, issues related to the use of information technology by money-launderers could also be discussed.

[i] These facts illustrate another form of "identity theft", which involves the actual use of personal information data to make false documents and to use those documents to commit additional crimes (in this case the offence is money-laundering).

[j] Criminalization of money-laundering, including the issue of laundering of self-proceeds as far as Ms. Chung is concerned, could also be discussed here.

Mr. Banner. Mr. Banner deposited $1.2 million into an account of Kondo Inc. at Finebills Bank, using numerous automatic teller machines in small denominations (*suspicious transaction reporting, information sharing among financial intelligence units, role of financial institutions*), which was used to pay back the loan of $1 million and its interest.[k] Mr. Banner kept $400,000 for himself and gave $400,000 to Mr. Alan. Both of them kept the money for their personal use.

5. At the request of Ms. Chung, Ms. Dee purchased a villa in Zeitstaat on her behalf for $2 million. Ms. Dee sent the rest of the money ($1 million) to Ms. Chung in Youngland, through an underground banker, Mr. Ezura, in Zeitstaat, who had his counterpart, Ms. Jabbar, in Youngland (*alternative remittance system*).[l] Ms. Chung paid $10,000 to Ms. Dee as a fee for her services and spent $90,000 for her personal pleasure (gambling, wining and dining, etc.), purchased bearer securities amounting to $500,000 from the security company Midmint Securities and kept $400,000 in cash in her residence. The bearer securities were kept in a safe deposit box at Handyfunds Bank in Youngland.

6. *Issues to be discussed relate to the recovery of the proceeds of the fraud from both countries (i.e. Xanadu and Zeitstaat) and Youngland (domestic measures and international cooperation in the control of the proceeds of crime, including freezing, confiscation, civil forfeiture or asset sharing) for the purpose of restitution to the victims, in addition to the criminal liabilities of all the persons involved.*

---

[k] It could be mentioned here that, in some States, Mr. Alan would not be criminally responsible for the breach of trust since the loan had been repaid.

[l] Other forms of alternative remittance system, such as *hundi* or *hawala*, could be discussed here. In addition, other modi operandi (typologies) of money-laundering could be discussed.