"Criminal Misuse and Falsification of Identity – Identity Theft as a Precursor to Other Crime"

Mr. Donald Piragoff
Senior General Counsel, Criminal Law Policy Section, Department of Justice, Canada

One of the principles guiding the work of the United Nations crime prevention and criminal justice programme is to ensure that any increases in the capacity and capabilities of perpetrators of crime are matched by similar increases in the capacity and capabilities of law enforcement and criminal justice authorities. One new crime that is challenging these capabilities is that of "identity theft".

I will address a more detailed definition of identity theft in a moment but if identity theft can be described as the criminal misuse and falsification of a person's identity, it is clear that this crime is growing rapidly. While global statistics are not currently available, there is evidence of rapid growth of this crime in a number of countries. In Canada, for example, identity theft has grown rapidly over the past three years and is estimated to cost consumers and businesses as much as 2.5 billion dollars a year. The 2001/2002 Annual Report of the New South Wales Crime Commission reported that identity theft cost the Australian community more than $3.5 billion dollars annually.

In a survey conducted in 2003, the Federal Trade Commission in the United States found that in the twelve months preceding the survey, 10 million people had been victims of identity theft. The survey found that businesses suffered nearly 48 billion dollars in losses; individuals suffered nearly 5 billion dollars in losses, and that victims spent about 300 million hours trying to reverse the impact of the identity theft. There is also growing evidence that identity theft is being used by organized crime and by terrorist groups to facilitate their activities and to commit crimes that fund their activities.

There are very few countries in the world that have a specific crime relating to "identity theft". I thought it would be helpful to provide a working definition of "identity theft" for the purposes of our discussions today.

In its most basic form, identity theft can be described as the collection, possession, transferring or use of personal identification information for the purpose of committing crime. Some of the ways in which this can be done are very familiar to us and are characterized as crimes in many countries. For example, Mr. Abel pretends that he is Mr. Bond by using a stolen cheque belonging to Mr. Bond and using it to buy goods from Ms. Cantor. In this case, Mr. Abel has committed all of the physical and mental elements of the offence of fraud and has assumed the identity of Mr. Bond only for the purpose of obtaining goods illegally from Ms. Cantor.

There are, however, new ways in which crime is being committed by misuse of the identity of other persons. Identity theft invariably involves the use of personal identification information. Personal identification information can be defined in a number of ways, but it can generally be understood to be information that either alone, or in conjunction with other information, identifies a specific person or provides access to assets held by that person or to benefits or services to which the person is entitled. For example, personal identification information could include a person's gender, age, name, race, address, telephone number, bank account number, bank account balances, investments, lines of credit, credit rating, credit card number, a PIN number (personal identification number), etc. The personal identification information can be tangible, such as information recorded on a piece of paper or contained in an identification document, or it can be virtual information, such as personal data on a computer screen.

Personal identification information can be obtained in a variety of ways, some of which involve the use of new technologies, such as the Internet and computers, and some of which do not. Examples of identity theft that do not involve advanced technologies are as follows:

- Personal identification information, including financial information, can be copied by hand from the files of clients by a dishonest employee or government official and sold to people who want to use the information to make false identification documents in order to commit crime.

- Sometimes personal identification information is taken from trash bins. This has been called "dumpster diving".

- Another way to commit identity theft is to fraudulently redirect mail from the victim's home to the perpetrator's home or to a post office box. The perpetrator then collects the victim's mail and uses the personal identification information set out in various bills and letters addressed to the victim to impersonate the victim and defraud banks, retailers, etc.

- Another method of committing identity theft is called "tomb stoning". It involves the perpetrator collecting information about a person who has died. The perpetrator uses the personal identification information to pretend that he or she is the dead person.

- Other people commit identity theft by positioning themselves in such a way that they can see a victim enter his or her personal identification number (PIN) into an automated debit card system. This PIN number is used in conjunction with a device (called a "skimming device") which surreptitiously records the numbers of the victim's debit card. The perpetrator is then able to match up the PIN number with the debit card number in order to withdraw funds from the victim's bank account.

Examples of identity theft that involve more advanced technologies are as follows:

- The perpetrator hacks into a computer database to obtain the personal identification information of victims for the purpose of making fraudulent identification documents.

- A second example of "high-tech" identity theft is the surreptitious installation of software in a computer system that enables the perpetrator to record the key strokes of victims as they use their computer. This software is called "spyware".

- A third example of identity theft that involves the Internet is called "phishing". This involves directing victims to a false website and inducing them to disclose their personal identification information by advertising products and services that are false.

The advent of computers and the Internet has changed the way that economic crime is committed. It has facilitated the commission of crimes that involve different actors along a continuum of criminal activity. No one actor has committed all of the elements of the crime. Each is responsible for a particular aspect of the activity that cumulatively produces the crime. This represents a significant change in the way that crimes are committed and highlights a need to enhance our domestic and international capacity to address these crimes.

I think I can best illustrate my point by setting out a case scenario. For example:

1. Mr. Abel in Canada works for a bank and copies personal identification information relating to a number of different customers from one of the bank's computers.

2. Mr. Abel then sells the personal identification information to Mr. Bond over the Internet. Mr. Bond lives in Germany.

3. He, in turn, sells the information to Ms. Cantor who lives in Australia.

4. Ms. Cantor uses the information to produce fraudulent identification documents. The "identity" of the various bank customers in this context is now on fraudulent identification documents and in the hands of people who will use it to commit crime.

5. Ms. Cantor sells the fraudulent identification documents to Mr. Douglas.

6. Mr. Douglas distributes the fraudulent identification documents to a couple of his friends.

7. His friends use the fraudulent identification documents to pose as Canadian tourists and commit large scale frauds on local businesses.

8. They sell the goods on a black market.

9. They then share the proceeds of crime with Mr. Douglas.

10. Mr. Douglas channels these moneys back into a money-laundering scheme involving organized crime.

The original bank customers in respect of whom Mr. Abel copied the personal identification information will only become aware that they are victims of identity theft after they start receiving calls from credit card companies demanding that they pay for the purchases made in Australia. They are the first group of victims and will face the long and arduous process of reclaiming their credit ratings. The second set of victims is the businesses and/or credit companies that suffered losses due to fraud. The fact that the monies from the sale of goods obtained by fraud are being used, in part, to finance organized crime highlights the fact that society at large is also victimized.

In the absence of proof of a conspiracy, most countries do not have an offence to cover the activities of Mr. Abel or Mr. Bond (i.e. stages 1, 2 and 3) even though their collection, sale and transfer of personal information of the various bank customers were the initial activities that made it possible for other actors to commit crimes. One of the legal limitations in addressing this form of identity theft is that personal identification information generally is not regarded as property, unless it has a commercial value in and of itself. Also, personal identification information that is copied, either by hand or from a computer screen, does not result in the owner of the personal identification information being deprived of it. It is the confidentiality of the personal identification information that may be breached, rather than any possessory or proprietary rights in that information.

In view of the fact that personal identification information is not characterized as property in most countries, traditional property offences are not an effective means for addressing identity theft involving the copying, collection, transferring and selling of personal identification information as a precursor to committing crimes. This fact highlights a need for countries to address this activity in their domestic legislation.

The example I have given also highlights the need for countries to work collaboratively to respond to persons who traffic personal identification information across borders for criminal purposes that need not be restricted to the commission of economic crime. Identity theft can also be used to help criminals evade capture or detection, to produce fraudulent identification for the purposes of facilitating the movement of terrorists in and out of countries, or to commit transnational crime such as human trafficking.

One of the challenges in formulating possible responses to identity theft, both at the domestic and international level, is to ensure that the scope of domestic offences or international measures are not cast in overly broad terms so as to capture activity that is either legitimate or that does not justify the use of the criminal law. Persons may be in possession of personal identification information in respect of other persons for a variety of legitimate commercial or other reasons. It can be argued that if personal identification information is obtained without the consent and knowledge of the person to whom it relates, an appropriate remedy may lie in civil mechanisms to protect and/or retrieve this information. From a criminal law perspective, the position can be taken that it is not the possession of the information *per se* that generates the social harm that should be addressed but, rather, the intended or actual use of the personal identification information to commit criminal offences. Following this argument, once a person has obtained personal identification information without the consent and knowledge of the person to whom it relates, and has done so with the intent of using that personal identification information to commit criminal offences, he or she has committed behaviour that is more appropriately addressed by criminal, rather than civil, mechanisms.

A strategy to stem the growth of identity theft at both the national and international level will invariably involve both civil and criminal mechanisms. It will also involve co-operation and co-ordination amongst countries. In this regard it is interesting to note that in May 2004, the United Nations Commission on Crime Prevention and Criminal Justice adopted and referred to the Economic and Social Council a resolution proposed by Canada calling for international cooperation in the prevention, investigation, prosecution and punishment of fraud, criminal misuse and falsification of identity and related crimes. The resolution mandates the convening of a group of experts to conduct a study of fraud and criminal misuse and falsification of identity in order to support the development of further measures such as useful practices, guidelines or technical materials for legislators, law-enforcement or prosecutorial officials or other officials. The Commission decided to mandate the study on the understanding, in part, that it would survey Member States and develop a broadly-acceptable model or definition/description of the problem as the basis for further action.

Canada was pleased to sponsor the initial meeting of the group of experts, which was held in Vienna last month. The meeting was held as an open-ended meeting and was attended by representatives of 33 Member

States. As required by the convening resolution, it has submitted a Progress Report on its work to the 14th session of the Crime Commission, and that Report has now been issued in languages as document E/CN.15/2005/11. It contains the preliminary observations of the experts on the nature and scope of the problems of fraud and identity theft, and sets out agreement on the methodology and some of the priorities for the study itself, which include the use of a questionnaire and specific research by the expert group and its members which will extend to both governmental and private-sector sources of information. We expect that the study will provide concrete information about patterns in transnational fraud, and will assist Member States in developing a common concept of identity-theft which can support further work in this area, both within and among Member States.

To ensure adequate regional representation, the process will be run as an open-ended intergovernmental process, but the interim work of the group – the actual gathering and analysis of the data – will require a smaller group of experts in the subject-matter, and the Report calls upon interested Member States to consider designating appropriate experts to participate in this work.

Canada was pleased to be able to provide the extra budgetary resources needed to hold last month's preliminary meeting, and we hope that other delegations will also recognize the importance of this work and provide further resources as the work of the study proceeds. Many delegations here have had experience with the growing tide of transnational fraud, and we have seen the role of telephones, fax machines, e-mail, the Internet and other factors which have contributed to the problem. But all we have is anecdotal information from a few countries. We believe that it is essential that we obtain more information from a representative sample of Member States, in order to obtain an accurate and comprehensive picture and permit evidence-based policy-making at both the national and international level.

In summary, I would encourage us to work together to better understand these emerging forms of crime and to enhance our capacity to address them. I believe there are steps that can be taken in both the domestic and international context to stem identity theft as a precursor to other crime.