

MODULE 5: RESPONDING TO INSTITUTIONAL VICTIMS OF IDENTITY CRIME

A given instance of identity crime typically involves two different kinds of victims: the *individual* whose personal or account information has been stolen and/or fraudulently used, and the *institutions* that have been burgled and/or defrauded. Sometimes you will be contacted first by a business or government agency reporting the theft of personal data in its possession, or the fraudulent use of its trade-mark in a phishing or other scheme designed to steal identity information from unsuspecting individuals. The following are guidelines for responding to and working with institutional victims of identity crime.

5.1 FRAUDULENT USE OF CORPORATE OR GOVERNMENT TRADEMARK

If the case involves fraudulent use of a corporate or government trademark (e.g., logo, website), it constitutes *intellectual property crime* and may be a candidate for prosecution as such. It may also constitute an offence under the *Competition Act* (false or misleading representations). Victims of such offences have a statutory right to sue for damages even if the matter is not prosecuted. Law enforcement officials should

1. Direct the corporation or government to:

a) the RCMP's online guide entitled "Reporting Intellectual Property Crime: A Guide for Victims of Copyright and Trademark Infringement", available at <http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/guide-eng.htm>

b) the Competition Bureau to report the matter and for more information on offences and remedies under the *Competition Act*: <http://www.competitionbureau.gc.ca>

50 Victoria Street
Gatineau, Quebec
K1A 0C9

Telephone: 819-997-4282

Toll-free: 1-800-348-5358 (Canada)

Fax: 819-997-0324

2. Gather the information listed in the above RCMP Guide (under "Checklist for Reporting Copyright and Trademark Offences") from your corporate/government victim contact, and contact the RCMP's intellectual property crime coordinator in your region to determine whether/how to proceed with an investigation. For a list of contacts by region, see: <http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/cont-eng.htm>

3. Contact the Competition Bureau to determine whether it plans to investigate the matter, and to ensure that investigations of the same matter are coordinated.

5.2 THEFT OF PERSONAL INFORMATION FROM CORPORATE/ GOVERNMENT HOLDINGS

If the case involves suspected theft of customer or citizen records, it may be the first step of a potentially larger case of identity crime. It is essential that mitigating measures be taken immediately by the affected body in order to prevent identity fraud based on the stolen information. Law enforcement and prosecutors should:

1. Inform the affected (or reporting) entity that it has a responsibility to take immediate measures to prevent both further theft of data and identity crime based on the information that was or may have been stolen. This common sense responsibility is set out in various privacy-related statutes, sometimes explicitly and sometimes implicitly. Refer them to the Privacy Commissioner for their jurisdiction for further direction on their responsibilities under privacy legislation to notify affected individuals and other authorities of the breach.
2. Take down a full incident report, and file it in such a way that it can be linked to incidents of identity crime in the future. This could be relevant investigatory information if the stolen information is indeed used to commit further identity crimes.
3. Ask the reporting entity to inform you immediately if it receives information of any sort suggesting that identity crimes may occur, be occurring or have occurred based on the stolen information.
4. Keep in touch with the reporting entity and update the report accordingly.

Best Practice: Develop a system for linking reports of identity crime over time and across jurisdictions. As part of this effort, establish a national database of lost, stolen and fraudulent identity documents.

5.3 WORKING WITH INSTITUTIONAL VICTIMS IN THE INVESTIGATION AND PROSECUTION OF IDENTITY CRIME

Many identity crimes involve theft of personal information from public or private sector institutions, and/or fraudulent use of corporate identities (e.g., trade-marks) to lure individuals into providing their personal information. In such cases, police officers and investigators will need to work closely with the organization in question to identify individual victims and ensure that they are properly notified and advised, as well as to investigate and prosecute the case generally.

Most identity crimes involve fraudulent use of the victim's financial accounts or fraudulent creation of financial accounts in the victim's name. In such cases, the creditors/banks/merchants in question must be contacted to determine how the accounts were opened and to gather relevant evidence including:

- if the account was opened or accessed via the internet, relevant IP addresses;
- if the account was accessed via the telephone, any telephone number captured;

- if the account was accessed or opened in person, the employee/witness who opened the account or conducted the transaction;
- all other information about the suspicious accounts and transactions: customer records, signatures, transaction history, application forms, videos or photographs, etc.
- statements from witnesses regarding the transactions and the suspect.

Organizations may be reluctant to disclose facts about the incident, such as obvious security failures, that put them in a bad light. They may insist that certain information be treated as confidential and not disclosed to individual victims. However, the organization should be advised that they may be required by law to notify authorities and/or affected individuals of the breach,³⁷ and that in any case individuals are entitled to information about their accounts under privacy/access to information legislation.³⁸

³⁷ See s.37.1 of the Alberta *Personal Information Protection Act*; and Bill C-29, proposed amendments to the federal *Personal Information Protection and Electronic Documents Act* as of March 2011.

³⁸ See *Personal Information Protection and Electronic Documents Act*, Schedule 1, Principle 4.9 and similar rights under provincial and territorial data protection legislation requiring that organizations provide individuals with access to their personal information held by the organization, upon request.

