IDENTITY THEFT

PROTECT YOUR BUSINESS

PROTECT YOUR CUSTOMERS

Canada

Ontario Québec

Nova Scotia New Nouveau Brunswick

British Columbia Manitoba

Prince Edward Island Canada Government of Saskatchewan

Alberta Government of Alberta Government of Newfoundland and Labrador

Yukon Government Northwest Territories Nunavut

Identity Theft Kit for Business

IDENTITY THEFT:

Recognize it.

Report it.

Stop it.

For more advice and tools on
ID theft visit cmcweb.ca/idtheft

PHONEBUSTERS™
The Canadian Anti-fraud Call Centre

Produced by the Federal-Provincial-Territorial
Consumer Measures Committee

Cat. No. Iu23-7/2005E-PDF
ISBN 0-662-39361-9
54238X

This Kit is provided for general information only, and is intended to emphasize the need for effective personal information policies and practices. Nothing in this Kit should be construed as legal advice. For your legal rights and obligations, you should consult the relevant legislation, regulations and your solicitor.

1. IDENTITY THEFT: A CONSUMER ISSUE FOR BUSINESS

Law enforcement agencies describe identity theft as the fastest growing crime that business, consumers, and governments face. "Inside jobs" are on the rise, as thieves increasingly steal clients' personal information from within organizations. Businesses can safeguard their reputation and avoid financial damages by planning and implementing polices to protect customers' personal information.

Most companies collect and retain personal information, but how many have implemented a plan for collecting and keeping it safe? Does your business? Consider that:

- A single computer can hold records for thousands of clients.
- An unlocked filing cabinet may contain the access codes, account or license numbers that a company shares with its partners, suppliers or vendors.
- Outside contractors hired to build and manage databases can view and copy information about a company's clients, including credit card and sometimes driver's licence numbers.

Privacy legislation requires that all businesses put systems in place to ensure that customer information is secure, accurate, gathered with consent and not used beyond a stated purpose. The federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* applies to businesses operating in provinces and territories that do not have substantially similar legislation. Quebec, British Columbia and Alberta have similar legislation. This guide will help you create a plan to avoid the theft of information, and it provides advice on what to do if your information is stolen.

Identity Theft:
Recognize it.
Report it.
Stop it.

What is Personal Information?

Any factual or subjective information, recorded or not, about an identifiable individual is personal information. This might include such things as the individual's name, address, age, gender, identification numbers, credit card numbers, income, employment, assets, liabilities, payment records, personal references and health records. Personal information does *not* generally include employees' contact information at their place of work but may include the employees' e-mail address. In general, data you collect from customers or employees must be used only for the purpose for which it was collected, or for an additional purpose to which the person has consented.

What is Identity Theft (Fraud)?

Obtaining another's personal information and using it without his/her knowledge or consent to commit fraud for financial gain or for another criminal purpose.

A thief does not need much information to steal and seriously disrupt someone's life: often a name, address, and date of birth are enough to get started.

Why Do Businesses Have To Protect Personal Information?

Increased Risks. Identity theft is growing rapidly. Each year thousands of victims have their personal information used by criminals to commit financial fraud such as creating false accounts in another's name. These crimes are growing because more personal information is collected and retained than ever before, and the risks of theft multiply every time that information is transmitted or retained or disposed of in an unsafe manner. A disturbing number of cases are inside jobs conducted by individuals who have access to an organization's sensitive data.

Customer Trust and Loyalty. Consumers are becoming wary of giving out information, and are learning more about their right to privacy every day. Increasingly, they are holding organizations responsible for protection of their personnel information – not just through the law – but also through the marketplace. If businesses lose consumer confidence and goodwill, it is their bottom lines that will suffer.

Managing Against Inside Jobs *

Hundreds of unsuspecting customers of a local gas station on Vancouver Island who used their debit cards to pay for gas were shocked to learn that their PIN and card number were recorded twice: once for the transaction, once for a thief.

When the police caught him, a former employee was charged with 178 charges of fraud using card data for over $200,000. He had been copying debit card information as he swiped customers' cards.

In accordance with the *Canadian Code of Practice for Consumer Debit Card Services*, victims were reimbursed by their financial institution. The gas bar was warned that if they did not apply appropriate security measures their access to the online payment service would be discontinued.

To guard against future thefts, the owner implemented new procedures: he tightened screening and background checks when hiring employees, and he began checking his equipment to ensure no one tampered with it.

** All the sidebar stories in this document are based on actual breaches, but all names, places and other details depicted are fictitious.*

2. TIPS FOR REDUCING THE RISK

Assess Your Business

Every organization should manage its own personal information "life cycle." Theft can occur when outsiders gain access to your information, but it can also occur through internal theft. A good security strategy has to address both possibilities.

Devote time to information privacy concerns. Appoint someone, or assume the responsibility yourself, to oversee the management and security of information you collect.

The individual in charge of privacy/security should assess:

- Your processes for gathering, handling, storing and disposing of electronic and paper data.
- The protection of your information technology systems, such as firewalls and audit trails.
- The role and level of security of individuals who have access to personnel and customer information.
- How to communicate with clients and the public about your policies and what to say in the case of a breach.

Gathering and using personal information usually involves five major aspects for a business: **Collection, Use, Disclosure, Data Security and Storage,** and **Disposal**.

Collection

Find out what you are collecting and why. Survey all of the personal information that your organization collects during the course of transactions and at other times. Do you gather data on clients? Identify the purpose(s) for which the information is collected, inform customers accordingly and obtain their consent. Ensure that staff can explain the purpose as they are collecting the information.

If you don't need it, don't collect it. Many businesses collect more information than they need, particularly when asking customers to fill out forms. Consider excluding the address, email and phone number if you only need a name. The Social Insurance Number (SIN) is a confidential number that is only required if a customer is earning income (either employment or investment) for tax reporting – it should not be collected otherwise.

Personal information is not for broadcast. Can people standing in line at your office or store overhear others give your staff telephone numbers or account passwords? Instruct employees who need to collect personal information to talk in a discreet and quiet manner. Turn computer screens so they cannot be viewed by anyone other than the operator.

Only Collect the Data You Need*

Every time the local Video Store in downtown Winnipeg set up a customer account, they collected credit card and driver's license numbers, home addresses, and phone numbers. They never thought twice about this data, so they never figured that retaining it would lead to 26 clients losing thousands of dollars each. But it did.

The data on their computer system was not password protected or encrypted, and one day a thief broke in and made off with the whole database. He then went on a spending spree. Luckily police apprehended him, and the clients were not on the hook for fraudulent credit charges.

Today the local video store avoids collecting driver's license numbers, they secure access to their systems with password protection, and firewalls guard their client database. They also provide customers with a simple one-page description of their privacy policy and information security practices.

** All the sidebar stories in this document are based on actual breaches, but all names, places and other details depicted are fictitious.*

Protect customer cards. When customers are making purchases, ensure that they have sufficient privacy to securely enter their PINs. Place shields on point-of-service terminals and check the terminals regularly to verify that equipment has not been tampered with. Locate security video cameras so that they cannot record the entry of customer PINs.

Be card smart. Staff should verify that customers are who they say they are by checking signatures on cards, and, as appropriate, photo ID. Consider using equipment that truncates debit/credit card numbers when printing receipts (i.e. does not print the whole card number) to better protect consumers. Don't copy down any card number you don't need.

Watch for credit changes. If you are issuing credit, watch for discrepancies or recent changes in applicants' addresses. Take extra measures to ensure the identity of the person, for example, by asking for additional identification. If there is a fraud alert on the customer's credit report, credit reporting agencies will provide you with the consumer's confirmed phone number to allow you to verify the validity of the application.

Secure online sales. There are risks associated with online transactions:

- Viruses can steal data transmitted.
- "Brand spoofing" can occur when the identities of legitimate organizations are used to create fake Web sites or "spoof" emails, to trick customers into providing their personal and financial information. Using "spoof" emails to commit this kind of fraud is sometimes called "phishing."

Best Practices for combating these risks include:

- Minimizing fraud when requesting credit card payments by using encryption software recommended by experts who know the best technologies and devices. Post your privacy policy, encryption levels, and other security features on your Web site.
- Informing customers as to exactly what information the company will, and will not ask for, on Web sites or via e-mail.
- Providing customers with information on inquiring about or reporting suspicious e-mails and Web sites.

- Ensuring that you are listed as the registrant and responsible entity for your corporate Web site, rather than the Web designer.
- Clearly advertising your valid Web site addresses on all communication.
- Registering variations of your corporate Web site domain URLs to keep others from using them.

The *Canadian Code of Practice for Consumer Protection in Electronic Commerce*, at cmcweb.ca/ecommerce, provides good business practices for merchants conducting commercial activities with consumers online.

Use

Limit Use. Data should be used only for the purposes stated publicly to consumers.

Limit access. Once you have taken an inventory of the data you collect, decide who should have the rights to access it. Limit access to a "need-to-know" basis and require passwords. Only let your system administrator handle back-up and other tasks that touch the company's network. Block access to idle computers with automatic locks or screensavers that require a password from an authorized user.

Encrypt your data. Stand-alone encryption packages can work with individual applications, and good software is available commercially. Should an intruder break through a firewall, network data has a better chance of staying safe if it is encrypted. Encrypt company laptops and devices used from remote locations, such as wireless devices (e.g. Blackberries). Remember to upgrade your encryption applications over time. Check the merchant agreements your company signs with payment card issuers for any encryption requirements. Where possible, avoid using communal computers and generic or group log-on identification numbers.

Passwords are essential. Require that employees use a combination of upper and lower case letters, numbers and symbols. Passwords should be changed regularly (e.g. every 90 days).

Check for suspicious activity online and offline. Almost all firewalls, encryption programs, and password schemes include audit functions that record activities on the network. Check logging data and audit trails for unusual or suspicious activity, e.g. employees accessing data that is not relevant to daily business transactions.

Disclosure

Know who you are talking to. Convicted thieves tell authorities how easily they can obtain valuable information just by asking for it. Posing as government officials or credit grantors, thieves concoct believable stories, call businesses and get staff to disclose information that they are otherwise careful to keep in locked file cabinets and password-protected computers.

Authority. If your organization discloses personal information to someone other than the owner, be sure that you have the legal authority to do so. Draft simple, strict policies telling employees how and when to disclose information.

Third parties. Ensure that organizations with whom you share client information (suppliers, contractors, clients, etc.) protect their data, and that you have the proper legal authority (i.e. client consent) to share data with them.

Be open about your policy and practices. Under privacy legislation, you are required to make your policies and practices readily available for anyone who requests them. Tell consumers about the steps your organization takes to protect their information. You can also refer them to the *Consumer Identity Theft Kit* on the federal, provincial and territorial Consumer Measures Committee (CMC) Web site **cmcweb.ca/idtheft**.

Data Security & Storage

If you keep it, physically secure it.

- Paper records with personal information should be locked, and computer terminals password-protected.
- Place your computer server(s) in a secure, controlled location, and keep other devices (e.g. back-up CDs or tape drives) locked away.
- Physically lock up all laptops to prevent thieves from walking away with one.
- Keep customers and other non-authorized personnel out of private and secure areas.

- Instruct employees to save data to network drives where these are available and not to "C:" hard drives, which are much less secure. Should someone steal the hard drive, information stored on network drives remains protected.
- Do not copy whole databases to devices when a partial list will do.
- Do not put modems/local area network (LAN) cards in computers that do not need them.
- Consider an alarm system, preferably one monitored by a security company. Your business insurer may be able to assist you with a security assessment of your operations.
- Prevent unauthorized photocopying.

When You Upgrade the System, Upgrade the Security Process*

Mid-sized Regional Insurance Company of Alberta almost gave away thousands of sensitive customer files – just because it upgraded some office computers.

Sensitive personal information was exposed including: names, addresses, phone numbers, account records, policy details, annual incomes, and home values. In the wrong hands, the data was sufficient for serious identity takeover of thousands of people.

It happened when old computers and their hard drives were sold to a small computer business that buys, fixes-up and sells computer equipment. The reseller discovered a hard drive with an operating system that granted him access to file folders belonging to the insurance company without a password. In the hands of a hacker, the databases could have revealed customer records.

Lucky for the insurer, the reseller was honest and immediately reported the oversight.

The company had software to properly "scrub" the hard drives and ensure no residual data would be left. What the company lacked was a procedure to see that this was done systematically. For future cases where hard drives would be disposed, the company decided to remove the hard drives altogether and have them destroyed.

** All the sidebar stories in this document are based on actual breaches, but all names, places and other details depicted are fictitious.*

Virus Protection. Install anti-virus protection software on all computers, and scan your systems for viruses regularly. Never disable anti-virus software, and update it frequently.

Firewalls. Firewalls should be installed at every point where the computer system touches other networks – including the Internet, a customer's system or a telephone company switch. They protect against unauthorized access to information. Ask your Internet Service Provider about other filters that can be used.

Install security "patches". Most software manufacturers release updates and patches to their software to fix bugs that can allow would-be attackers to gain access to your computer. Check with the manufacturer for new patches or to install automated patching features.

Disposal

Know which documents to shred. When obtaining information (paper or electronic) for a single transaction or temporary use, separate it from other files and safely destroy it. For example, resumes from applicants not hired contain many details that should be shredded. ID thieves know there's valuable information in paper bins and dumpsters. Ensure employees know which material is sensitive and needs to be shredded. Companies can be hired to shred disposed paper, or office shredders can be purchased inexpensively. "Cross-cut" shredders do the best job.

Destroying Data. Establish a timetable for retention of data based on legal, contractual or any redress requirements. Destroy data accordingly, erase files, remove copies from all databases and network directories, and be sure they are permanently deleted with "scrubbing" software (scrubbing minimizes the risk that residual data is left in the system). When disposing of equipment, it may be best to physically destroy the hard drive, CDs, tapes, diskettes, etc. or hire a company that specializes in destroying this type of equipment.

Employees and Information Security

Screen employees. To protect your business against internal fraud, consider background checks for employees who have access to sensitive information. There are companies who can complete these checks (including criminal background, references and education credentials) on your behalf. Consider conducting regular clearance checks for employees in high-risk areas (e.g. with employees' annual performance review) to ensure staff remain free of criminal records.

Train employees. Ensure staff understands privacy information policies and how to ask customers for personal information. Post the following requirements as a checklist recommending that everyone:

- Log-on to computers using alphanumeric passwords, and change them regularly.
- Don't ask for customers' personal data in front of others, and ensure they have privacy when entering PINs.
- Check signatures and verify that customers are who they say they are.
- If there has been tampering with terminals or databases, inform management.
- Keep customer information under lock and key.
- Shred all confidential waste, including payment card information and photocopies of ID documents.
- Clean desk tops every night.
- Only access databases when authorized.
- Lock systems when not in use.

Monitor threats. Have your information officer or a key employee track potential security threats and technology updates and report these to employees and managers as needed.

Fraudulant document training. Train employees how to detect fraudulent identity documents.

Network access. Only give access to networks to employees on a need-to-know basis. When an employee leaves, remove their network access immediately.

Evolve Your Practices

Over time, the information your business collects will change. So will your computer technology, databases and personnel. Ensure that you consider how any changes in your operations will affect your management of personal information.

3. WHAT TO DO WHEN A THIEF STRIKES

Steps to Take When Information is Compromised

If thieves strike, or if information goes missing, have an action plan to respond to the breach. Acting quickly can help reduce potential damage, and it may help your organization avoid liability in a civil action. To respond to a breach, you need to follow two tracks at the same time: investigate the problem internally, and devise a plan for notifying people outside the organization that a breach has occurred.

Investigating the Incident

You need to know what happened, so determine:

- What information was stolen?
- When it was stolen?
- How did the breach occur?
- Which files were affected?
- What action is needed to ensure no other data is taken or lost?
- Is advice required from your lawyer and/or accountant?

Informing Customers and Outside Organizations

If a breach does occur, you need to act quickly to inform affected customers. If the situations are not handled well, the damage to your company can be staggering and permanent. Timing is critical, as prompt notification might help prevent identity theft or mitigate the damage it causes. Tailor your letter to those who are affected. Ensure it is written on your company letterhead and signed by a key official, and place the company logo or name on the envelope. If a small number of individuals are affected, inform

them immediately. If a larger number are affected, i.e., more than 100, you may want to discuss the most efficient manner for advising potential victims by first consulting with:

Canada's credit reporting agencies:

Equifax (1-800-465-7166)
TransUnion Canada (1-877-525-3823); in Québec (1-877-713-3393)
Northern Credit Bureau (1-800-532-8784)

Law enforcement agencies
Affected individuals or businesses
Privacy Commissioners

Credit reporting agencies (CRA). Speak to fraud specialists at Equifax, TransUnion, and if appropriate Northern Credit Bureau to discuss the type of warning and assistance that is required to ensure that the breach is handled well. The CRAs will help determine whether or not a fraud alert is necessary.

A fraud alert tells creditors to contact the person affected before approving a new account or changing existing accounts and can be an effective tool in protecting your customers from theft. In discussion with the CRAs, you should request a *compromise number* and inform affected customers to use this *number* in all communication with the CRAs.

Law enforcement agencies. You should call your local police to inform them of the breach and, if recommended, to file a report of the theft. You should also report the breach to Phonebusters National Call Centre (phonebusters.com or 1-888-495-8501) or file an electronic report at the RCMP Web site for reporting economic crime, RECOL.ca.

Affected individuals and businesses. Decide what to say and how to report the breach to anyone affected. You need to convey the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from identity theft. Provide contact information for your organization, CRAs and, if applicable, the police. Include current information about identity theft. The CMC Web site at **cmcweb.ca/idtheft** has information to help individuals guard against and deal with identity theft.

Privacy Commissioners. The federal commissioner acts independently of government to help protect the privacy of personal information and ensure compliance with PIPEDA. Contact this office for advice on privacy issues related to the breach. Note that Quebec, British Columbia, and Alberta have separate privacy laws that are substantially similar to PIPEDA, so if you operate in one of these provinces, please contact the corresponding provincial commissioner. You can reach the federal Commissioner at 1-800-282-1376 or at privcom.gc.ca, where you will also find links to provincial commissioners.

Dealing with the Media

Depending on the nature of the breach and the number of people affected, you may have to answer calls from the media. As you prepare letters for notification, it would be wise to prepare a media response. Be candid and emphasize the steps you are taking to fix the situation. Disseminating information to the media can help to scare criminals away from using information they have stolen, because they will realize that CRAs and police are waiting for them to use the data.

You know who your customers are,
why let an ID thief steal them from you?

4. TOOLS: WHAT & HOW TO TELL CUSTOMERS ABOUT A BREACH

SAMPLE NOTIFICATION LETTER:

Date_____.

Dear _____,

We regret to inform you that an incident has occurred which may have compromised the security of a database containing some of your personal information. We apologize for any inconvenience this may cause you.

[*Describe the information compromise and how you are responding to it.*]

Canada's major credit reporting agencies, Equifax and TransUnion, have been notified of this breach and have provided the following compromise number: XXXXX. This number should be referred to in any communication with them. They recommend that you call their agents to discuss whether a fraud alert should be placed on your credit file and what other steps are required (Equifax: 1-800-465-7166 and TransUnion: 1-877-525-3823).

A fraud alert tells creditors to contact you before they extend credit, open a new account or change your existing accounts. You should be aware that while most creditors will call you, they are not obliged by law to do so, thus it is not fail-proof protection.

Report any unauthorized activity as soon as you are aware of it to your financial institution, the credit reporting and law enforcement agencies, and PhoneBusters National Call Centre (a national police anti-fraud unit, 1-888-495-8501).

A police report has been prepared on this incident; the number of the report is YYYYY. Your financial institution or other creditors may require the police report to clear you of any fraudulent charges that may occur.

With appropriate identification, you can also request that a copy of your credit report be mailed from the Credit Reporting Agencies to you free of charge. Visit their Web sites for details on what is considered to be acceptable identification. If you receive a copy of your report and do not find any unauthorized activity, it is recommended that you continue to check your credit reports periodically.

We are recommending that you take these precautions to reduce the risk of financial losses or your information being used for illegal purposes.

We recommend that you visit **cmcweb.ca/idtheft** to obtain information on identity theft including:

- Tips for Reducing the Risk of Identity Theft
- What to do if it happens to you
- Identity Theft Statement
- Frequently Asked Questions
- Consumer Identity Theft Checklist

Our organization's information officer is [*insert name of person responsible for administration related to breach*] and can be contacted at [*telephone number and address if applicable*] if you have any questions.

Once again, we regret any inconvenience this incident may cause you.

What to Say & How to Respond When A Thief Strikes

Sample Questions and Responses

If someone else's identifying information is breached, they are going to have questions. Prepare your staff to speak with whomever was affected – customers, suppliers, partners – or any other organization connected to your business. **Be specific and act quickly**.

Question: What personal information of mine was lost?

> Response: You will need to inform potential victims of what was lost to prevent or repair possible damage.

Question: Why did you have this personal information in the first place?

> Response: Under privacy laws, organizations must identify the purposes for collecting personal information at or before the time of collection. You should also be prepared to explain why it was necessary to store it.

Question: When was it lost?

> Response: Timing is important if a victim reports a possible theft, because credit issuers need to know when fraudulent charges might appear.

Question: How did it happen?

> Response: An explanation will be required. The more steps you have taken to prevent a breach, the safer your measures of prevention and management, the better your position for answering this question.

Question: What are you doing to fix the problem?

> Response: You should prepare a response carefully, including the corrective action you have taken.

Question: What can an ID thief do with my information?

Response: It will depend on what data was accessed. Common forms of fraud using personal information include: fraudulent charges to existing credit cards or bank accounts, opening new credit accounts in another's name, opening cell phone or other accounts in another's name.

Question: How can I protect myself now that this incident has occurred?

Response: Tell potential victims to contact credit reporting agencies and financial institutions to ask for a fraud alert, and to check their credit report at least annually.

Question: If I put a fraud alert on my file, does it guarantee that credit will not be issued without first contacting me?

Response: Let them know that, while most creditors will call, they are not obliged by law to do so, thus it is not a fail-proof protection.