

Identity Theft in Healthcare A White Paper

by

Dr Gordon Atherley

January 2006

Greyhead Associates
100 Lakeshore Road East, Ste 303
Oakville, ON L6J 6M9
Canada

905 842-9425
atherley@sympatico.ca

© Greyhead Associates

The moral rights of the author have been asserted

The author

Gordon Atherley holds the British equivalent of the Canadian MD and PhD degrees, and his British specialties are occupational medicine and community medicine. His honours include Officer (Brother) of the Most Venerable Order of The Hospital of St John of Jerusalem, Doctor of Laws, Honoris Causa, Simon Fraser University, and Fellow of the Royal Society of Arts, UK.

Contact Information

Dr Gordon Atherley
Greyhead Associates
100 Lakeshore Road East, Ste 303
Oakville, ON
L6J 6M9

905 842-9425

atherley@sympatico.ca

Preface

Identity theft, among the fastest growing crimes in North America, is now attacking the margins of healthcare in Canada. Various industries and sectors have accumulated much experience from which healthcare could benefit.

Teranet Inc, in particular, possesses specialized and relevant experience derived from its services for the land, legal and financial services industries, and its enabling of government electronic service delivery.

Greyhead Associates, a research and analysis practice, is working to raise healthcare's awareness by spearheading a direct dialogue for sharing with healthcare the hard-won experience of other sectors gained in struggling with identity theft and knowledge of the steps they have evolved to prevent it and to provide protection against it.

The objectives of the dialogue are to assist healthcare people with

1. assessing risk in individual healthcare facilities as well as throughout the healthcare system,
2. determining and implementing healthcare-appropriate steps for protecting patients and providers by strengthening vigilance through behavioural change and technology, and
3. evolving best practices.

This white paper is a contribution to the dialogue.

Acknowledgements

Greyhead Associates gratefully acknowledges the invaluable assistance of Teranet Inc in providing technical background information and support for the publication of this white paper.

Contents

PREFACE..... 3

ACKNOWLEDGEMENTS 3

EXECUTIVE SUMMARY 5

INTRODUCTION 6

BACKGROUND..... 6

ID THEFT 7

FOUNDATION DOCUMENTATION AND DATA 7

PROCESSES OF ID THEFT IN NON-HEALTHCARE SECTORS 8

ID THEFT IN HEALTHCARE 8

THE VALUE PROPOSITION FOR FRAUDSTERS 8

FRAUDSTERS’ HORIZONTAL METHODS 8

INSIDER ACTIVITY..... 8

POLICE REPORTS OF HEALTHCARE FRAUDS, 2005 9

ID THEFT RISK IN PARTICULAR HEALTHCARE CONTEXTS 10

THE ELECTRONIC HEALTH RECORD..... 10

PHARMACY 10

LONG-TERM CARE..... 11

FOUNDATION-DATA RISK, INFORMATION CUSTODIAN RESPONSIBILITIES IN HEALTHCARE..... 11

PREVENTION AND PROTECTION 12

PROTECTION OF FOUNDATION DATA IN RESEARCH AND HEALTHCARE SYSTEM MONITORING 14

SPECIALIZED TECHNOLOGY IN SUPPORT OF VIGILANCE..... 14

TABLE 1 FOUNDATION DATA..... 16

TABLE 2 SUMMARY OF ID THEFT RISKS TO PATIENTS AND HEALTHCARE PROVIDERS 16

TABLE 3 FOUNDATION-DATA RISK RELATIVE TO CRITICAL DATA REQUIREMENTS IN HEALTHCARE..... 17

APPENDIX 1 GREYHEAD ASSOCIATES 18

APPENDIX 2 PROTECTING ONESELF AGAINST ID THEFT: THE ONTARIO GOVERNMENT’S ADVICE TO CONSUMERS 19

Executive summary

1. Identity theft, among the fastest growing crimes in North America, is making consumers increasingly wary and is encroaching on Canadian healthcare.
2. Greyhead Associates, with assistance from Teranet Inc, produced this white paper to help healthcare protect its patients, providers, researchers and employees by safeguarding itself against threats of identity theft.
3. Governments can at this time reassure neither patients nor the physicians, pharmacists, nurses and the other healthcare professionals who provide patient care that their identities are fully protected throughout the healthcare system. Enhancement of healthcare's prevention and protection, already a requirement under Canada's health information and privacy laws, becomes urgent for healthcare as well as governments.
4. Successful thefts of the identities of patients and also of providers and employees undermine the quintessence of the healthcare relationship: the trust that they all are entitled to hold in the healthcare system. They increasingly and reasonably expect healthcare facilities to assure them their identities are properly safeguarded.
5. Identity theft involves an individual's presenting as someone he or she is not. Fraudulently presenting as someone entitled to healthcare, for example, is theft of an identity whether the identity belongs to an entitled individual or is simply false.
6. From a data-access perspective, sectors such as banking and healthcare operate as silos, and properly so because of privacy requirements. The fraudsters exploit the silos by extracting items of identity data, sometimes termed *foundation data*, from one (or more) silos and using it for fraudulent purposes in another.
7. Substantial experience in the financial sector, reinforced by police investigations, reveals the processes involved in identity theft. Some identity thefts are traceable to the victims' failing to protect their passwords or PIN numbers, losing their cards, giving identity-related information to unknown telephone callers, and responding by supplying account and other data to 'phishing' emails purporting to come from banks and other respected organizations.
8. Other identity thefts are traced by the police to the work of insiders, persons who themselves are authorized to access foundation data and who by error, want of vigilance, or intention misappropriate or misuse the data on their own account or who, inadvertently or for a fee, pass it on to others for fraudulent purposes. While disaffection and malice may play a part, the major motivation is the value proposition for the fraudsters.

Introduction

Greyhead Associates produced this white paper as part of a wider dialogue to help healthcare protect its patients, providers, researchers and employees by safeguarding itself against threats of identity theft (“ID theft”). Teranet Inc kindly shared its experiences and insights with the author.

Greyhead Associates is an independent practice which specializes in analysis, assessment and research relative to the risks of information technology used in healthcare, see also Appendix 1.

Background

ID theft, among the fastest growing crimes in North America, is making consumers increasingly wary.

The research group Forester reported in April 2005 that 74 percent of Canadian online consumers have concerns about email fraud and that the concerns affect their online financial behavior. Fear of email fraud, such as phishing, kept 22 percent of online consumers from applying online for a financial product, and stopped 19 percent from opening email from their financial providers.

The latter part of 2005 saw Canadian newspapers highlighting long-standing weaknesses in the way identity documentation is handled in the public and private sectors, further raising public awareness.

Governments can at this time reassure neither patients nor the physicians, pharmacists, nurses and the other healthcare professionals who provide patient care that their identities are fully protected throughout the healthcare system. Enhancement of healthcare’s protection of identities—already a requirement under Canada’s health information and privacy laws—becomes urgent for healthcare as well as governments.

Successful thefts of the identities of patients and also of providers and employees undermine the quintessence of the healthcare relationship: the trust that they all are entitled to hold in the healthcare system. They increasingly and reasonably expect healthcare facilities to assure them their identities are properly safeguarded.

ID theft puts at risk nothing less than the trust of patients, provider and employees.

Important insights emerge from Teranet’s experience with millions of transactions processed for the Ontario land registration system. Not one of those transactions is known to have been made by someone who gained fraudulent access to the system, whether by obtaining someone else’s access keys, or by tampering with data submitted by legitimate users. And yet instances of fraud, although proportionally infrequent, are still occurring.

ID theft

ID theft, broadly defined, occurs when

1. stolen or false identity is used to defraud banks, mortgage companies, government, and individual citizens, among others, and
2. stolen or false identity is created from information obtained by piecing together items of data harvested from multiple sources.

ID theft involves an individual's presenting as someone he or she is not. Fraudulently presenting as someone entitled to healthcare, for example, is theft of an identity whether the identity belongs to an entitled individual or is simply false.

Until recently, ID theft was viewed by the public almost wholly as a threat to large organizations such as banks, mortgage companies, and government. The increasing first-hand experience of individuals as victims of ID theft is shifting that perception, as is the advice given to the public by government, advice that strongly emphasizes self-protection, see for example Appendix 2. Greyhead Associates' preliminary findings from its ongoing studies suggest that about a third of Canadians have themselves or know someone who has been the subject of ID theft of some type, such as credit card fraud.

Foundation documentation and data

Founding documentation is police terminology for the types of identity documentation and data that fraudsters use to create false identities. They compile foundation data from items collected from electronic and hard-copy sources. For the common types of such sources, see Table 1.

Such sources extend across sectors as diverse as banking, land registries, driver's licencing, passports and residency permits. And healthcare, too, as the Toronto Police Fraud Squad confirms.

In October 2005, the Toronto Police Fraud Squad broke up a state-of-the-art ID theft ring. Armed with information stolen from credit and debit cards, the ring would pillage the accounts. The ring would then use the identity information to produce counterfeit health cards as well as driver's licences, credit cards, social insurance cards, permanent resident cards and passports.

The Fraud Squad believes that the ring was using the health cards as foundation documents for opening accounts for frauds against the banks.

From a data-access perspective, banking and healthcare operate as silos, and properly so because of privacy requirements. The fraudsters exploit the silos by extracting items of foundation data from one (or more) silos and using it for fraudulent purposes in another.

Processes of ID theft in non-healthcare sectors

Substantial experience in the financial sector, reinforced by police investigations, reveals the processes involved in ID theft.

Some ID thefts are traceable to the victims' failing to protect their passwords or PIN numbers, losing their cards, giving identity-related information to unknown telephone callers, and responding by supplying account and other data to 'phishing' emails purporting to come from banks and other respected organizations.

Other ID thefts are traced by the police to the work of insiders, persons who themselves are authorized to access foundation data and who by error, want of vigilance, or intention misappropriate or misuse the data on their own account or who, inadvertently or for payment, pass it on to others for fraudulent purposes.

Experts increasingly understand the motivations of fraudsters. While disaffection and malice may play a part, the major motivation is the value proposition for the fraudsters

ID theft in healthcare

The value proposition for fraudsters

According to the Toronto Fraud Squad, a fake health card would be worth around \$200 as foundation documentation. For fraudulently obtaining health care, it could fetch \$3,000 to \$5,000. Money of this magnitude represents an attractive value proposition for fraudsters especially in circumstances where repeated thefts of foundation data carry small risk of discovery.

Fraudsters' horizontal methods

The risk of ID theft in all sectors including healthcare is rooted in the fraudsters' operating horizontally across the silos while protection and prevention treat each silo as a self-contained system. Privacy procedures inhibit inter-silo coordination of prevention and protection.

Insider activity

The insider characteristic of ID theft presents a dilemma for healthcare's major information systems. The greater the number of persons with access privileges and the greater the number of accesses, the higher is the risk of ID theft. Yet the goal of healthcare information systems is wide and frequent access not only within healthcare facilities, but also among healthcare facilities, providers and ultimately patients at the local, regional, provincial, and even the national level.

Police reports of healthcare frauds, 2005

While all four of the alleged frauds in the following summaries involved cheating the healthcare system, the drugs or services falsely claimed for involved stealing or falsifying identities—and therefore the foundation data—some or even all of which pertained to legitimate patients.

In the latter part of 2005, the Ontario Provincial Police, Anti-Rackets, Health Fraud Investigation Team

charged a Toronto area pharmacist with fraud following an investigation into a complaint that false claims were submitted to the Ontario Drug Benefit Plan. The investigation revealed that the accused submitted false claims in 2001 totaling approximately \$144,000 for drugs that were not dispensed;

charged a Michigan, USA, man in connection with receiving insured medical services in the Windsor, Ontario area, which he was not entitled to, and for submitting fraudulent applications for an Ontario photo health card to the Ontario Ministry of Health and Long Term Care;

charged an Ottawa area medical doctor with fraud. The extensive investigation was conducted into allegations that a doctor was billing for services not rendered. The investigation found that between 1997 and 2005 he submitted approximately \$180,000 in false claims to the Ontario Health Insurance Plan for services that were not rendered;

charged a podiatrist and a chiroprapist, who operated a clinic located in Windsor, with fraud following an investigation into a complaint that fraudulent claims were being submitted to the Ontario Health Insurance Plan. The investigation revealed that the accused submitted approximately \$9,000 in fraudulent claims to the Ontario Health Insurance Plan, for foot care, examinations and x-rays from January of 2001 to December of 2004.

In all four of these scenarios, the possibility exists that, as a result of the abuse of foundation data, legitimate patients' records held in the healthcare system could contain erroneous health data. The addition of the erroneous data to a patient's medical record, which would occur without the knowledge of the patient concerned, could be misleading to healthcare providers perhaps even to the extent of endangering the patient.

Consider a pharmacy record that falsely states a patient is on a life-critical drug. Suppose a physician relies on the pharmacy record, a growing safety-related data interchange between pharmacists and physicians, for reliable information on a patient's medication history. Imagine the consequences if the physician is misled to the point of failing to prescribe the drug, with deadly consequences.

Patients may also face the risk of their being suspected of healthcare fraud. On top of that, they are at risk of the financial and social consequences of their being the victim of ID theft and all that goes with it.

Table 2 summarizes ID Theft risks to patients and healthcare providers.

ID Theft Risk in Particular Healthcare Contexts

Given what is now known about the processes of ID theft, risk assessment should focus closely on the foundation data associated with the health data of individual patients.

The electronic health record

Typically, an electronic health record contains the patient's foundation data and health data.

Generally, an electronic health record contains all or some of these items of foundation data: the patient's name, sex, date of birth, address and telephone numbers, along with the personal health number that would also appear on the health card. If the address is not given but the telephone number is, the address would be readily findable by a fraudster making use of on-line telephone directory services such as Canada411.

Such publicly available services enable a fraudster equipped only with the patient's name, home telephone number, and province of residence to obtain his or her address, complete with Postal Code and, under some circumstance, additional personal information.

The relative risk of the foundation data differs from that of the health data. The foundation data contains items usable for ID theft even though the health data is stripped off. It is thus always a source of risk.

But the health data stripped of the foundation data contains no information that leads directly to the patient's identity. Stripped of the foundation data and thus fully anonymized, health data is seldom if ever usable for ID theft.

Ongoing risk studies of healthcare by Greyhead Associates have already revealed weaknesses in the security afforded foundation data in certain fields of healthcare.

Pharmacy

In a pharmacy for which data services are provided by a pharmacy chain embracing some thousands of retail pharmacies, with the cooperation of the chief pharmacist, the investigator became a test subject. Relative to the test subject, the pharmacist entered various data into the computer according to the usual procedures.

The foundation data was principally the subject's name, address, Postal Code, telephone number, date of birth, and the Ontario health number and credit card data, which were entered from card swipes. The health-related information embraced matters such as allergies as well as prescription data. In combination, all the foundation data and health data were viewable on screen.

The pharmacist confirmed that all the onscreen information is accessible to and viewable by any person working behind the prescription counter. The pharmacist explained that the foundation and health data would be stored on the pharmacy chain's server, not the computer within the pharmacy.

While exposure of foundation data might be all too common in restaurants, gas bars, book stores, and retail stores, it is surprising to find it in pharmacies, especially given pharmacists' professional obligations to patients and pharmacies' legal responsibilities as information custodians under Canada's health information protection legislation.

The test subject observed that the slip issued to the patient or customer after a credit-card purchase carried the credit card number, date of expiry, and cardholder's name. The pharmacist explained that credit card validation was performed by the pharmacy chain and not the individual pharmacy.

At subsequent interview, senior managers of the pharmacy chain indicated concern about the security of the system as a whole because they felt they had insufficient control over ways in which data could be viewed by the pharmacy's prescription-counter personnel.

Long-term care

Greyhead Associates' studies of long-term care are in the early stages. So far, the findings indicate that the design of some data systems used in long-term care enables individual residents' foundation data as well as health and treatment data always to be viewable on any screen accessible by any staffperson in the facility. The next-of-kin of a resident of a facility confirmed that the resident's foundation data was fully in view after logon at screens throughout the facility.

Foundation-Data Risk, Information Custodian Responsibilities in Healthcare

Table 3 presents an analysis of the foundation-data risk relative to critical data requirements in healthcare. It emphasizes that, for the requirements with high foundation-data risk, prevention and protection are responsibilities not only for government, but also for healthcare facilities, providers and researchers.

Canadian information and privacy laws place upon the facilities and providers a particular set of rather onerous obligations collectively allocated to an *information custodian*. As information custodians, healthcare providers are required to protect the foundation data of their patients and of themselves.

Generally, healthcare facilities have obligations to protect the foundation data of all patients, all providers, and all the persons they employ.

In provider-to-provider communications, electronic or otherwise, the provider as sender and the provider as receiver are both information custodians with clear responsibilities for prevention and protection before the data is transmitted and after it is received. The same goes for electronic health records and the various form of order entry, such as e-prescribing.

Regardless of the efficacy of the security of the electronic system that mediates the transmission and receipt of foundation data, risks exist in the work spaces of the healthcare providers who originate data for transmission and those who receive and process it.

Prevention and protection

Prevention of and protection against ID theft calls for human vigilance and security technology. Both are necessary, but neither is of itself sufficient. Both together contend continuously with skilled, inventive and opportunistic fraudsters quick to perceive value propositions, and with lapses in human vigilance.

Vigilance begins with the recognition that foundation data should be the principal focus in preventive and protective efforts.

Because the theft of the identity-related information—especially name, address, date of birth, telephone number, health number, Social Insurance Number, and bank account number—can occur during an authorized access to a system, vigilance and awareness on the part of patients and healthcare staff provide crucial lines of defence.

The front lines in the defence are where the patient is admitted or accepted for care. It is here that the patient's identity is established, and necessarily so, for establishing (a) eligibility for healthcare and (b) identity for reliable aggregation of medical data to the correct medical record. Because the process by which eligibility is established exposes the individual's foundation data, vigilance begins here.

Thereafter, vigilance requires that the need-to-know principle should be followed throughout the processes of providing care.

In the clinical activities of providing care to a patient, no need-to-know exists for the health number, credit card number, street address, Postal Code, and the Social Insurance Number and other foundation data. Of all foundation data, only the name and age (in

preference to the date of birth) are strictly necessary in the clinical records. For the purposes of contacting next of kin and referral to other parts of the healthcare system, special arrangements may be needed to make the foundation data accessible to staff with relevant responsibilities.

Applying the need-to-know principle to the foundation data of patients and staff provides a sound starting point for a protective policy that, perhaps with some adjustments to the information system, can be readily monitored and effectively enforced throughout the facility, clinic, pharmacy, research team, or medical office.

Healthcare has to contend with simple methods by which authorized personnel steal foundation data from health records for use in a non-healthcare sector such as finance. Stealing the data may involve nothing more sophisticated than jotting the data down on paper. Such ID thefts are difficult or even impossible to detect.

To reduce risks of such ID thefts and other types of fraud in healthcare, interest is growing in use of background checks for healthcare facility staff, regardless of rank or profession, difficult though this topic is.

Like professionals in other fields, such as lawyers, bankers and chartered accountants, healthcare professionals stress their unique, trusted relationship with their clients/patients.

The professionalism of healthcare professionals is invoked by the requirement for vigilance because protecting the patient's foundation data is part of the professional responsibility to keep confidential things that the patient discloses in the course of receiving healthcare. Healthcare is compromised if loss of trust causes the patient to withhold medically significant information.

In the clinical delivery of healthcare, it is the healthcare professional not the patient who accesses the patient's record in the healthcare facility, clinic, pharmacy, research laboratory, or medical office.

For the data transaction involved in accessing the patient's record, the healthcare professional represents the patient. In matters like writing a prescription, the law requires the professional to do this for and on behalf of the patient.

In healthcare, as in information technology and many other fields, best practices guide professionals in understanding and complying with the obligations placed upon them. Interest grows apace in best practices for the protection of foundation data entrusted to healthcare.

The professional associations of healthcare need to frequently ascertain that the best practices followed by their members are kept abreast of ID theft risk as this evolves. For their members, failure of vigilance towards foundation data risks legal actions as well as loss of trust.

Protection of Foundation Data in Research and Healthcare System Monitoring

Medical and epidemiological research and monitoring of healthcare often involves access to patients' records.

An electronic health record fully anonymized by severance of all foundation data is unlikely to facilitate ID theft. In any case, organizations such as Statistics Canada have methods that can be used to conceal the identity of an individual with, say, a rare disease who happens to be the only patient with the disease in a particular Postal Code.

But severance of foundation data from health data is not always complete in government monitoring of healthcare and medical and social research of an epidemiological nature.

The Canadian Institute for Health Information, for example, is supported by provincial regulations requiring hospitals to submit patient data to the Institute. The foundation data that travels with the submissions consists principally of age, sex, health number, and Postal Code.

A decade ago, omission of a patient's name and address from the foundation data could reasonably be held to anonymize the data sufficiently for the protection of patients' identities. This degree of anonymization may no longer be sufficient given the growing knowledge of the ways of the fraudster in piecing together foundation data from a multiplicity of sources.

While such issues are matters for government decision makers, their recognition is helpful in highlighting the types of actions required from healthcare providers and patients.

Specialized Technology in Support of Vigilance

A near-universal truth is that transparency combats inappropriate behaviour. Banks are built with large windows not because glass is stronger than steel but because glass enables a person attempting to break into the vault to be observed. Vigilance thus involves transparency.

In the credit card industry, unusual activity on an account is detected by advanced computer technology such as pattern recognition, possibly utilizing neural nets. The victim, the card or account holder, is notified promptly and preventive action is urgently implemented. Credit card companies, necessarily keeping the nature of their detection tools confidential, have perforce become good at recognizing patterns of inappropriate behaviour. They are turning this ability into a competitive advantage to keep costs down.

With the land registration system, the challenges faced by the stakeholders and the solutions that they have adopted provide relevant guidance for healthcare, even if the

specific technologies and methodologies that offer good protection in the financial or real estate sectors may require adaptation.

Because of its role as operator for the land registration system in Ontario, Teranet is positioned at the focal point of the transactions within the system and of the individuals interacting with the system.

This focal-point positioning enabled Teranet to implement technologies, methodologies and services for targeting ID theft, fraud, misrepresentation and professional misconduct.

Teranet has created services and information products that professionals and in some cases consumers can use to reduce the risk of fraud or increase the probability of stopping a fraudulent transaction. Some of the Teranet technology solutions, for example, use the sophistication of pattern recognition to recognize transaction patterns associated with inappropriate behavior.

Even though unusual activity on a patient's electronic health record is hard to define let alone identify, technologically speaking it could be feasible—though costly—to routinely notify all Canadian patients of unusual or any activity in their electronic health records regardless of where these are stored. Early in 2006, interest is reviving in supplying individual patients with data on the costs of health services provided to them. In principle, such feedback could also serve to identify to patients the accesses to and use of their electronic health record data, and thereby assist them in identifying unusual activity.

To ensure prevention of and protection against ID theft risk, many systems and not just those of healthcare require continuously updated security and unrelenting vigilance, a challenging, ongoing task.

Table 1 Foundation Data

Name, sex, DOB
Home address, Postal Code, telephone number
e-mail address
Social Insurance Number
Numbers plus any confirmatory information from one or more of <ul style="list-style-type: none"> ▪ health cards ▪ driver’s licences ▪ credit cards ▪ bank cards ▪ debit cards ▪ hotel cards ▪ permanent resident cards ▪ passports ▪ named service providers ▪ any document or data source with ID information

Table 2 Summary of ID Theft Risks to Patients and Healthcare Providers

Patients

1. Financial loss and damage to their credit ratings
2. Themselves coming under suspicion of fraud
3. Inappropriate and possibly dangerous data aggregated to their health records without their knowledge

Healthcare professionals

1. Financial loss and damage to their credit ratings
2. Themselves coming under suspicion of fraud
3. Inappropriate and possibly dangerous data aggregated to their patients’ health records resulting in medical malpractice suits

Table 3 Foundation-Data Risk Relative to Critical Data Requirements in Healthcare

Context	Foundation Data	Risk
<i>Healthcare system administration and monitoring, research</i>		
Validation of eligibility for healthcare	Required	High
Government monitoring of the healthcare system	Required only in exceptional situations, such as public health emergencies	Low if government limits itself to ID-stripped data under non-exceptional circumstances
Research	Seldom necessary	Low with ID-stripped data
<i>Provision of healthcare within the circle of care</i>		
Provider-provider communications	Required	High
Electronic health records	Required	High
Prescribing and other forms of order entry, such as laboratory investigations	Required	High

Appendix 1 Greyhead Associates

Greyhead Associates provides analytical and advisory services to public-sector agencies, major hospitals, professional associations, and corporations on complex problems arising out of the use of information technology in healthcare. Greyhead's Principal, Dr Gordon Atherley, has authored several papers and lectured on the difficult subject of identity theft in healthcare, on which he has also completed a number of confidential assignments.

Appendix 2 Protecting Oneself Against ID Theft: The Ontario Government's Advice to Consumers

Protecting Yourself at Home

- Always store any cards and documents containing personal information in a secure place, and shred them after they expire.
- Review the balances on your statements from banks, credit cards and companies regularly and report any discrepancies right away.
- Once a year, get a copy of your credit report from the two national credit reporting agencies, [Equifax Canada](#) and [TransUnion Canada](#). The report tells you what information the bureau has about your credit history, financial information, any judgments, collection activity and who has asked for your information.
- If your bills don't arrive, or you applied for a new credit card that hasn't come on time, call the credit grantor immediately.
- If you are going to be away from home, ask a trusted neighbour to pick up your mail, or go to your local post office (with identification) and ask for Canada Post's "hold mail" service.

Protecting Yourself in the Marketplace

- Carry as few cards and documents as possible, and always check to see the credit card you get back is your own.
- Be wary of giving out any personal information over the telephone unless you've placed the call yourself or know the business.
- Never tell anyone the password you use at the Automated Banking Machine (ABM), and be sure no one is watching when you use an ABM. Financial institutions and police will never ask for your passwords.
- Don't put more than your name and address on your personal cheques.

Protecting Yourself Online

- Fake or "spoof" websites are designed to trick consumers and collect their personal information. Be cautious when clicking on a link or an unknown website or unfamiliar e-mail. The link may take you to a fraudulent site.
- Be wary of computer start-up software that asks for registration information.
- Never share your passwords.
- Don't use e-mail to send personal information.
- Discourage harvesting of your e-mail address—think about creating "disposable" e-mail addresses for online purchases, mask your address or use a unique e-mail address.
- Beware of Internet promotions that ask for personal information. Identity thieves may use phoney offers to get you to give them your information.
- After completing any sort of financial transaction online, make sure you sign out of the website and clear your internet file/cache. Most financial institutions provide instructions on how to clear the caches under their "security" section.
- Don't give a credit card number or other identification information to a company that doesn't provide their name, business address, telephone number and e-mail address.
- Before giving your credit card number or other financial information to a business, make sure that their website is protected and secured. Look for a lock symbol located somewhere on the browser, or make sure the URL begins with "https://".
- Chain letters and phony investment schemes try to win your confidence with false promises of incredible returns—they're only after your personal and/or credit information.
- Teach children to keep their identities confidential in chat rooms, bulletin boards or newsgroups. Help them learn to choose screen names that do not identify them, and to understand that any information they exchange on the Internet is not private.
- Look into encryption, firewalls and virus protection for your computer.