MANAGING THE RISK OF FRAUD

Produced by the Litigation and Dispute Resolution Division of Levi & Sinclair, LLP, Chartered Accountants
4141 Sherbrooke Street West, Suite 240, Westmount, Quebec H3Z 1B8 Tel: (514) 931-7600 Fax: (514) 931-3600

IDENTITY THEFT CAN HAPPEN TO ANYONE

PART 2

This is the second of a 3 part series on identity theft in which we present an explanation of what identity theft is, how the fraudsters can acquire your identity and what you can do to protect against becoming a victm. Lastly, should all of the above fail and you do become a victim, what to do so as to minimize your loss and exposure.

HOW YOU LOSE YOUR IDENTITY

With the heightened terror threats and increased fraudulent acts occurring in our society today, it has become more common for all of us to carry more identification and be prepared to show it to complete strangers, almost without a second thought.

But...many of these strangers may be collecting your identity information and knowingly or unknowingly making it readily available to criminals.

Next time you pass your credit card to a gas staion attendant at a strange station on the highway, consider the possibility that he is swiping the card

inside using a card reader which records the information contained on the magnetic strip of your card.

This information finds itself on fraudulent credit cards around the world in less than 12 hours and the charges begin. And yet, you hesitate to enter your credit card information on the internet for a purchase that you have initiated.

Where do you draw the line and how do you protect your identity?

We hope that by learning more about the risks you will become better able to protect your identity, and if need be, react to a threat of stolen identity.

Identity theft means one individual's personal information — a credit card number, a bank account number or Social Insurance Number — is used by another, unauthorized, person to purchase goods or services fraudulently.

RECENT MASS LOSSES OF PERSONAL DATA

More than a quarter of a million **Hotels.com** customers are now at high risk for identity theft after a password-protected laptop computer containing their credit card information was stolen from an Ernst & Young auditor's locked car in what appears to be a "random petty theft,"

This all comes on the heels of the May 2006 **Veterans Affairs** theft, wherein the unencrypted personal data of some 26.5 million veterans was stolen when a laptop was taken during a home burglary of a VA employee.The material included the veterans' Social Security numbers and dates of birth

Nearly 60,000 current and retired local public employees, most of them city and **Cook County** workers, are being notified of a possible compromise of confidential personal information, including Social Security numbers and birth dates.

The sensitive data was contained on a laptop computer stolen from the home of an employee of Nationwide Retirement Solutions

Jackson Health System informed 8,500 employees this week that their personal information may be at risk following the theft of two laptop computers seven months ago.

A computer possibly containing the names, Social Security numbers and medical information for almost 10,000 people has been stolen from the **University of Alabama at Birmingham**.

There are numerous ways that the identity thief can obtain your personal information. Here are the more common methods:

Dumpster diving: - This involves searching through your trash for information, found on bank statements, credit card applications, receipts, literally anything that has information about you upon it.

Pick Pocket: - The old favourite is still a method employed to obtain personal information. Once the thief has your driver's license or credit card, he will either use it himself or sell it to another who specialises in this type of criminal activity.

Internet Scams: - This is becoming more common and uses the internet to gather the required information simply by requesting it in bogus emails or by false hyperlinks to a website.

Phishing:- a term coined by computer hackers to describe surfers who use e-mail to fish the Internet, hoping to hook you into providing logins, passwords and credit card information. The "phisher" impersonates a legitimate company such as your own Internet service provider or financial institution. In the typical scam, an e-mail appears on your screen from a reputable company, and you're told to visit a specific site to update your account. When you click on the link, it takes you to the phisher's website. Once at the phisher's website, any personal information you enter is logged by the phiser and used to impersonate you.

Hidden Camera: - Another of the most up-to-date methods of obtaining information is by camera phone. The alert thief is always looking for an opportunity and the cash register or point of sale of any retail business is as good a place as any. Taking photographs of documentation or identification that are tendered as payment, used as verification, or simply left on display in an open purse or wallet may be the opportunity that these people have been waiting for.

College students are easier targets due to their complete integration and trust in the Internet. Many students using social networking sites like Facebook or Myspace have in plain view their telephone number, home/school addresses, and birthdays.

Computer hacker: - Personal information is not only carried in wallets or handbags, but also stored on computers. The computer savvy no longer steals it from you or waits for you to casually discard it. They simply let themselves into your computer and take it straight from the hard drive. Businesses such as America Online and Visa use their anti-identity theft software as a sales pitch to would-be customers in television advertising, demonstrating just how big a problem this form of fraud has become, and why this type of software or firewalls assist to secure your personal or business systems.

Financial Transactions: - Personal information is obtained by any kind of daily transaction legitimately entered using a credit or banking facility. The ABM is equipped with sophisticated overlays which capture the magnetically encoded information from your key-card and the PIN number you enter into the machine.

Shoulder-Surfing: - By looking over the shoulder of unsuspecting individuals, fraudsters can capture personal details. For example, you may be filling out an application form in a shop or discussing your personal details over the phone in a public place. Fraudsters also target debit or credit card receipts discarded or left behind. Many receipts still show a full (or part) card or account number, and may also show your signature.

Skimming Cards: - The technology to capture your card details is widely available - a small 'swiping' device is all that is required. When you make a genuine transaction, unscrupulous vendors can then read and store your card details and sell them on to criminals. Gas stations and restaurants are often targeted. With your card details a fraudster can purchase mail order goods, or even set up direct debits from your account. Be wary when your card goes out of sight. Check your transaction statements regularly and contact the card issuer if you spot anything suspicious.

Vishing:- Just as Internet surfers have gotten wise to the fine art of phishing, along comes a new scam utilizing a new technology. Creative thieves are now switching their efforts to "vishing," which uses Voice over Internet Protocol (VoIP) phones instead of a misdirected Web link to steal user information.

The thieves use a war dialer (software which automatically dials telephone numbers) over a VoIP system to blanket an area. A recorded message tells the person receiving the call that their credit card has been breached and to "call the following (regional) phone number immediately."

When the user calls the number, another message is played stating “this is account verification please enter your 16 digit account number.” The rest is academic.

Targeting job seekers:- This is a natural for criminals because people freely give out all kinds of personal information when applying for jobs, including names, addresses, telephone numbers, e-mail addresses — sometimes even dates of birth and Social Security numbers.

Here are some of the more common schemes thieves use to take advantage of online job seekers:

After responding to an online job ad, you’re contacted via e-mail for a phony interview. You’re asked for bank-account information so your paychecks can be direct-deposited. It’s all a ruse, and the crooks empty your bank account.

You get an e-mail from a recruiter or prospective employer requesting your personal information for a pre-employment background check. Next thing you know, your identity has been stolen.

You post your résumé with your Social Security number and other personal information. Criminals find it and use it to get credit cards and loans in your name.

Spoof letters, callers or canvassers:- Fraudsters use various tactics to harvest information directly from potential victims. They make contact in various ways. You may receive a spoof letter or fax, perhaps informing you that you are the sole benefactor to a recently deceased and very rich distant relative. Your bank details are required to transfer the funds.

You may receive telephone calls purporting to be from your bank to 'check' your personal or banking details. You may be stopped in the street by bogus canvassers and asked to take part in a 'survey' which involves divulging your personal details. Do not respond at all unless you are certain the enquiries are genuine. A legitimate enquirer won't mind you asking why they need your details.

TIPS FOR SAFE JOB-HUNTING ONLINE

♦ Think twice about telling all on your résumé. Do you really need to provide detailed personal information? Consider posting your résumé more anonymously, with an e-mail address as your primary contact point.

♦ Never provide a potential employer with your bank-account or credit-card information, a scan of your driver’s license or other ID or a detailed physical description of yourself.

♦ Never pay upfront for any job opportunity. Remember, they’re supposed to be paying you. And never forward, transfer or wire money to a prospective employer.

VISIT US

Take a moment to visit our Web Site which offers a full profile of our firm and back issues of our newsletters on business, tax and managing the risk of fraud.

.

www.levifca.com

Did You Miss ?
Part 1 - Identity Theft Explained
and
Coming this fall:
Part 3 - What to do if you become a victim.

ABOUT LEVI & SINCLAIR

LEVI & SINCLAIR is a firm of chartered accountants that traces its origin in Montreal to 1950. We pride ourselves on being more than just an accounting firm. We offer an effective blend of personalized service, experience and technological leadership, coupled with a steadfast commitment to consistently deliver excellence.

Our Chartered Accountants and Business Consultants provide advisory services on a broad range of issues to both our individual and corporate clients. The members of our firm possess unique talents, expertise and experience, giving our clients access to a knowledge base of considerable breadth and depth. Together with our support personnel, we share a commitment to developing practical solutions for the business challenges of today, and to devising strategies for tomorrow.

OUR SERVICES

Our firm takes pride in adding value to every client that we serve through our extensive expertise and proactive approach to your financial needs. We match our dedication to adding value with experience and expertise: we have experience in servicing virtually every type of industry and professional practice.

TAXATION

Our office has a strong basis in federal and provincial tax issues. Our tax group has been in existence for 50+ years and is highly qualified and experienced. Our accountants work hard to minimize your taxes, yet make sure that you fulfill your tax requirements ethically while working to add value. We can fill a variety of tax needs, both domestic and international as well as corporate and personal. Our specialties lie in tax reporting and representation, tax planning (business, personal, divorce and litigation), tax structuring of entities and transactions and tax research.

FINANCIAL

LEVI & SINCLAIR can meet all of your basic financial needs with our exemplary Accounting Services Group that can truly add value whether it's your business or your personal finances that we are reviewing. We work with business entities as well as non-profits and foundations. Our accounting services include; auditing and compilation review of financial statements, budgets and forecasts, and government reporting. We won't simply process your financial statements, our mission is to add value. We will go the extra mile to help you forecast or locate opportunities that you may be missing.

BUSINESS CONSULTING

LEVI & SINCLAIR's Business Consulting unit has proven itself as a valuable resource to businesses of all kinds. We can help you plan your future, whether you see it coming or not. We can help you bring seminal business events to life; like mergers and acquisitions, business valuation, leases and contracts, or business development plans, all of which take a huge amount of planning and attention to detail. If there are no big events on your horizon, we can still be of service by helping you to anticipate the unexpected through our forecasting, real estate projections, risk management assessments, or our feasibility studies. We look at your business and all of its many facets, to find both issues and opportunities and bring that valuable insight to you.

LITIGATION SUPPORT AND DISPUTE RESOLUTION SERVICE AREAS

- Civil and criminal Fraud Investigation
- Management and employee fraud and theft
- Identification of secret commissions and kickbacks
- Sarbanes-Oxley compliance audits
- Sarbanes-Oxley 404 audits
- Intellectual Property Litigation Support
- Training on fraud awareness and prevention
- Due Diligence Audits
- Insurance claim assistance
- Retail sales audits
- Contract dispute resolution
- Professional negligence litigation support
- Fraud prevention program design, implementation and evaluation
- Bank due diligence audits
- Employee background audits
- Financial discrepancy analysis
- Divorce litigation support
- Insurance claim quantification
- Breach of contract quantification
- Electronic Discovery and Data Recovery
- Computer forensics

CONTACT INFORMATION

LEVI & SINCLAIR SENCRL LLP

4141 Sherbrooke Street West, Suite 240
Westmount, Quebec H3Z 1B8
Tel: (514) 931-7600 Fax: (514) 931-3600
Philip C. Levi, CMC, CFE, FCA, CPA, CA•IFA
plevi@levifca.com

WITH OFFICES WORLDWIDE THROUGH MEMBERSHIP IN

INTEGRA INTERNATIONAL®
Your Global Advantage