

IDENTITY THEFT

Name: Class/Block: Date:

SIMON'S SITUATION

When Simon lost his wallet, he thought it was a pain. He had over \$50 in it, and his driver's licence and bank card. The next day he called the bank to replace the card, and applied for a new driver's license.

A few months later, at a roadside driving check, the police asked him to step out of his car and placed him under arrest. That's when he found out that someone had been using his identity to buy expensive jewellery and sound equipment. One store charged him with forgery, and the police became involved.

It took months of letter-writing, phone calls and explanations to convince the police, his bank, the collection agencies and credit bureaus that someone else using his ID was responsible for the crime and the debts.

MELISSA'S MESS

At first, Melissa was surprised when she got an email from her bank saying that the security department had detected suspicious activity on her account. It asked her to go to a special web page to confirm her account information and password. It's lucky the bank caught the problem on time, she thought as she entered the correct information.

But she was more surprised the next day when she went to pay for a movie with her debit card – it was rejected. She checked her bank balance and found her account was empty. All her savings were gone. She was furious when she called the bank to ask what it did with her money.

The bank said she had spent the whole amount in online purchases, using her password. Melissa said she had not bought anything online, but the bank said she was responsible if anyone used her password. Melissa was lucky, because she still had the email asking for her password. The bank said that she was the victim of an online fraud called phishing, and agreed to refund her account. But it took many pages of paperwork and several months to get the problem cleared up.

DANIEL'S DILEMMA

Daniel was popular and had many friends on his networking page. It was a great way to keep in the loop and let friends know about his birthday party. So naturally when he moved into his own place, he posted his new address and phone number.

But it wasn't long before Daniel started getting unwelcome messages in the mail – bills from stores he didn't shop at. Credit card bills from card companies he didn't use. And the more he ignored them, the more threatening they became. When he finally phoned to tell them they had the wrong guy, he found out they had his name, address, even his birthday. And many of them wouldn't believe it wasn't really him until they compared his signature with the one setting up all the new accounts.

IDENTITY THEFT (cont'd)

Daniel had to file a police report saying that someone was using his name and address. The officer said they probably got all his personal information from his networking page. It took months of paperwork to sort out all the false charges, and some of the stores refused to change the reports on his credit record. He was so careless, he was a bad risk, they said.

THERESA'S TROUBLES

Theresa first noticed her magazine subscription was late. Then she noticed she wasn't getting her mail. She contacted Canada Post to ask what happened. She found out that someone had asked Canada Post to divert her mail. For ID, someone had used a drivers' licence that Theresa thought she'd lost.

Soon after, she found that someone had received a credit card in her name. And a department store credit card. Bills addressed to her were mounting up, but they weren't being paid.

Theresa was lucky – she was able to pay her own bills before her electricity or cellphone were cut off. But she didn't feel so happy when she had to start contacting all the stores that were sending her bills. She also had to convince the credit card company that she wasn't responsible for the bills in her name.

Identity theft is a new type of crime, but it's growing fast. It happens when someone obtains your personal information and uses it without your knowledge to make purchases and commit crimes such as fraud. Police say Canada has over 20,000 cases of identity theft a year, and the number is growing.

Identity thieves build up a profile using pieces of information, such as a Social Insurance Number and a date of birth. With two pieces of ID, they can apply for banking services, or change the address on existing accounts. When they build up an identity, they can take over accounts, transfer bank balances, apply for loans and credit cards, and purchase items.

Most internet users have seen "phishing" emails – messages from scammers trying to gain confidential information such as a password by pretending to be a legitimate email or website. Fraud artists can also look through your garbage or recycling box for bank cheques, insurance forms, pre-approved credit card applications, tax forms and other bits of personal information. New computers and photocopying machines make it easier for thieves to copy or modify documents and create identities. With more people posting personal information on social networking sites like Myspace, Facebook and Bebo, scammers can often find all the personal details they need to set up a phony identity.

Some scammers post ads for jobs, asking applicants to send copies of documents like social insurance cards, birth certificates and driver's licences. Others use phony websites that ask for personal information to establish an account or to "verify" an existing account.

IDENTITY THEFT (cont'd)

WHAT CAN YOU DO TO PROTECT YOURSELF FROM IDENTITY THEFT?

Here are some tips:

- Don't give out your Social Insurance Number, birth date, or other personal or employment data except to a reputable agency.
- Don't throw any identifying information, like bank statements or credit card offers, in the garbage or recycling box. Shred or cut them up.
- Never leave receipts at bank machines, bank wickets, trash cans or gasoline pumps.
- Pick up your mail as soon as possible.
- Watch for late bills and mistakes in your monthly statements.
- Review your bank statements to make sure that all the transactions are yours.
- Don't carry more ID than you need, and don't leave ID in your vehicle.
- Report lost or stolen identification and debit or credit cards to the card issuer and Canada's credit bureaus (Equifax Canada at www.equifax.ca and TransUnion Canada at www.transunion.ca).
- Check your credit rating annually to ensure it is accurate and up-to-date. (You can request a free copy by mail. Agencies may charge a fee for requests by internet.)
- Report identify theft to the police as soon as you are aware of it.

Security online

- Don't give out personal information over the phone or internet.
- Don't post personal or employment details on social networking sites like Myspace, Facebook and Bebo.
- Check the security and privacy settings on networking sites and limit personal access to trusted friends.
- Share your personal webpages only with trusted friends.
- Don't write down PINs or passwords, and choose difficult passwords.
- Never give your PINs to friends or post them online.
- Don't use personal data like addresses or phone numbers in your passwords.

For more information about frauds and scams, visit the Canadian Anti-Fraud Centre website (www.antifraudcentre.ca).