

TIP OF THE MONTH APRIL 2010

LEARNING ABOUT IDENTITY THEFT -1

Identity theft is one of the fastest growing criminal activities in North America. A recent study by **Javelin Strategy and Research** reported that 11.1 million adults – one in every 20 U.S. adults – have been victims of identity fraud in the United States in 2009. That figure is up 12 percent over 2008 and is 37 percent ahead of 2007.

Once a thief gets hold of your personal information (national insurance number, bank and credit card account numbers, your income, name, address and phone numbers) he has a goldmine of information to use as a means to rip you off big time!

How Identity Theft Occurs

Skilled identity thieves use a variety of ways to gain access to your personal information. For example, they may get information from businesses or other institutions by stealing it while they're on the job; bribing an employee who has access to these records; hacking these records; and conning information out of employees. Or:

They may steal your wallet or purse.

They may steal your personal email or the phone by saying they're from a legitimate company and claiming that you have a problem with your account. This practice is known as "**phishing**" online, or "**pretexting**" by phone.

They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "**skimming**." They may swipe your card for an actual purchase, or attach a device to an ATM machine where they may enter or swipe your card.

They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "**dumpster diving**."

They may steal personal information they find in your home.

They may steal your mail, including bank and credit cards statements, credit card offers, and new checks.

They may complete a "change of address form" to divert your mail to another location.

Once identity thieves have your personal information, they may use it to commit fraud or theft. For example:

They may call your credit card issuer to change the billing address on your account. The imposter then runs up charges on our account. Because the bills are being sent to a different address, it may be some time before you realize there's a problem.

They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts eventually damage your credit.

They may establish phone or wireless service in your home.

They may open a bank account in your name and write bad checks on the account.

They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.

They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

They may buy a car by taking out an auto loan in your name.

They may get identification such as a driver's license issued with their picture, in your name.

They may give your name to the police during an arrest. If they don't show up for the court date, a warrant for arrest is issued in your name.

TO BE CONTINUED!

Feel free to email us at dataprotection@bahamas.gov.bs.

Remember, we welcome your complaints and are happy to address your data protection (privacy) concerns!