The Real Cost of Identity Theft

By Terri A. Kamoto

Online fraud and cyber related crimes are on the rise, affecting more lives and costing individuals and businesses more money each year. According to the US government, over 10 million Americans are the victims of identity theft each year. And with major company data breaches and recent cyber attacks on the general population this past year, people are concerned with cyber security and protecting their private information.

The three most common items exposed or stolen in a businesses data breach are: credit card numbers, bank account information and social security numbers. When this sensitive information is compromised you are far more likely to suffer from an identity fraud incident.

For some, identity theft is an inconvenience which can be quickly resolved to restore their identity. For victims of cyber security crimes, recovering their identity can cost thousands of dollars, cause damage to their credit score, disqualify them for loans and even employment and take months of legal battles to resolve. Some consumers have even been arrested for crimes committed by someone using their identities and have had to prove that they were not guilty.

What is Identity Theft

Identity theft is a form of theft, deception, scam, or crime resulting in the loss of personal data, including names, D.O.B., phone numbers, passport or license info, credit card numbers, usernames

and passwords, bank account access, Social Security numbers, health insurance files, financial aid forms and tax IDs, which are then used without permission to commit fraud and other crimes.

How is Identity Theft Committed?

There are many ways to become the victim of identity fraud and everyday hacker criminals are hatching new ways to steal your information. On the street someone might steal wallet or purse, go through your trash, maybe steal your mail. In an office a corrupt worker might steal your information from files they have access to. But online there are infinite ways to steal someone's identity. For example, a virus sent to your computer can steal private information, a skimming device can wirelessly steal your account numbers and passcode right from a device attached to an ATM, someone could hack your old cellphone or a hacker might gain access to files in a poorly secured commercial database.

Everyone has personal information floating around the internet. And while most of us are familiar with direct attacks on our privacy, fewer of us understand the extent and reach of identity theft these days. Potentially, every business and government entity you give your information to is at risk for a cyber security threat or data breach themselves.

How Much Does Identity Theft Cost?

According to the latest Javelin Strategy & Research Report, identity theft is costing Americans an estimated **$54 billion dollars**. The cost goes beyond dollar and cents though, since some cases can cost victims time and peace of mind.
It can take the average identity theft victim *months* and *years* to resolve with courts, creditors and government agencies. And for some it can mean recuperating more than lost money but rebuilding their legal status. Not to mention the time it takes to recuperate confidence for submitting applications on loans and credit cards or trusting your knowledge to bet on stocks again.
That is the **REAL** cost of identity theft. At some point, everyone will be financially affected by cyber security threats, but is is how we are able to get through to the other side of financial despair and rebuild not only our safety net but our emotional outlook towards the future.

Take Steps to Protect Yourself From Costly Identity Theft & other Cyber Threats

Prevention

- Protect your computer and smartphone with strong, up-to-date security software.
- Ensure operating system updates are installed.
- Use strong passwords with uppercase letters, numbers AND symbols (Pa$$w0rd)
- Do not search on secure websites (banks, emails, etc.) or provide personal information such as SSN or account numbers from computers on public networks
- Use only reputable websites to purchase good and services online, and look for the*locked* icon next to the URL.

Detection

- Monitor your bank accounts and credit card statements weekly.
- Monitor your credit report to ensure there is no unauthorized activity. By law you have the right to three free credit reports per year from the main credit bureaus: Experian, Transunion, and Equifax.
- Opt-in for any notifications or protections offered by your financial institution

Solutions

- Educate yourself and stay up-to-date on the latest scams or global cyber security threats.
- Freeze your accounts and credit cards immediately if you feel you information has been accessed.
- Consider available insurance protections – **Identity Theft Insurance** for individuals or**Cyber Security and Data Breach Insurance** for businesses.

Speak with a security professional, trusted financial advisor, insurance broker and legal counsel to ensure you are taking precautions to prevent becoming a victim of identity theft or cyber crime. Continue to monitor and improve your security measures. And if you become the victim, take steps quickly to stem your losses and regain your peace of mind.