identity theft

how to protect your identity and safeguard your future

EDITORIAL | JACK FOSTER

No individual or company is immune to the threat of identity theft. The importance of those words was driven home when two **Agency Sales** readers recently reported "near misses" for having their identities stolen.

In the first case a vigilant company accountant noticed some unusual online banking activities. The agency owner and the bank were notified and a potential financial disaster was averted.

Second, an equally wary bank employee noticed what she thought were "suspicious" checks being written on an agency account.

Arguably, instances such as these are merely the tip of the iceberg, but they give credence to the advice offered by law enforcement officials, security experts and banks regarding the importance of companies closely guarding their financial records and personal/personnel information.

Consider the following figures provided by the Better Business Bureau to gauge the impact of identity theft in this country:

- Approximately nine million people in the United States have their identities stolen annually.
- On average identity theft cost victims approximately $6,000.
- It will take the average identity theft victim 40 hours to resolve the problem.
- In the United States identity theft cost is approximately $50 billion annually.
- 65% of identity theft information is gained via offline methods rather than online methods.
- The most common sources of identity theft are from lost wallets, theft of paper mail and dishonest family and friends.
- Only 15% of identity theft victims discover the identity theft by proactive measures.
- The state with the highest rate of identity theft is California, followed by New York.

A Growing Industry

Any doubt that these figures are accurate can be put to rest by the fact that identity protection consultants, products and services seem to be cropping up all over the place. Two of the more prominent companies offering such protection provide what they call "proactive theft protection" — for a fee. In their national advertising campaigns they offer news, blogs, advice, service guarantees and promises to reduce junk mail.

In addition, local, state and federal law enforcement agencies are keeping taps on the growing ID theft industry and many police departments now have computer crimes units.

When asked if any type of business or individual is more apt than another to fall victim to identify theft, Lieutenant Joe Donohue of the New York State Police maintains that it depends upon how the company looks at and deals with technology.

Donohue, who is assigned to the computer crime unit of the New York State Police in Albany, New York, says that it doesn't matter whether a company is large or small, it's all about their attitudes concerning technology. "For instance," he says, "I can recall one company that had a problem primarily because they hadn't come to terms with the difference between operating in the 'real' world vs. the 'virtual' world. In this case, the company's long-distance phone system had been hacked into and the perpetrator was using their phone lines to run up huge charges in long-distance fees overseas. Now, here's where I mean not getting past the 'real' world. The first instinct they followed to solve the problem was to place a guard at the door of the room where the company's central phone system was located. Their first thought was that the perpetrator needed proximity. They just couldn't get their arms around the fact the hacker had done his job remotely and didn't need to have a physical presence near the phone system. That's what I mean about the difference between the 'real' and the 'virtual' world."

"In the U.S., identity theft cost is approximately $50 billion annually."

Coming to terms with the impact of the "virtual" world is a point that's emphasized on a number of websites that provide tips on how to avoid identity theft. One of the most readable and useful sites is that of the Wachovia Corporation, the third largest banking chain in the United States, headquartered in Charlotte, North Carolina. In addition to detailing a number of methods that thieves employ to steal identities, the bank offers a number of steps wary consumers should take if they become victims of ID theft or other forms of Internet fraud:

Steps to Follow

Contact banks and credit card issuers. Immediately contact your bank(s) and credit card issuer(s) to:

- Put holds on your account(s).
- Stop payments placed on missing checks.
- Get your Personal Identification Numbers (PINs) and Online Banking Passwords changed.
- Open new account(s) as appropriate.

Include all accounts impacted. Be sure to indicate to the bank or issuer all the cards and/or accounts potentially impacted, including your ATM card(s), Check Cards and credit cards.

Review with rigor. Review all recent transactions and electronic authorizations on your account linked to stolen cards, including checking, savings, money market, credit, home equity and other types of accounts.

Look out for change requests. Ensure that no one has requested an address change, title change, PIN change or ordered new cards or checks to be sent to another address.

File a police report with your local police department and provide the facts and circumstances surrounding your loss. After filing, obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the investigation.

File a report with the Federal Trade Commission.

Security Checklist

When you know what to look for, it's not all that difficult to make simple changes in your life that protect you from fraud and identity theft.

- ✓ Learn how to safeguard your information, increase your awareness and become proactive about detecting fraud.
- ✓ Learn ways to watch for fraud and identity theft online and offline, as well as how to help prevent fraud for business accounts.
- ✓ Safeguard important information both off and online.
- ✓ Learn all you can about ID theft and Internet scams.
- ✓ Monitor your credit. Regularly reviewing your credit report alerts you to any suspicious activity, so you can take control as soon as possible.
- ✓ Learn about the availability of fraud protection resources.
- ✓ Learn how to work with the department of motor vehicles, the U.S. Postal Service, and other resources that can aid you with fraud protection.

Finally there are many websites devoted to providing guidance on the subject of identity theft. A few of them are:

- The FTC's portal — **www.ftc.gov**/bcp/edu/microsites/idtheft/ — a one-stop national resource where visitors can be brought up to date on the problem of identity theft and other information to help deter, detect and defend against the problem.
- **www.scambusters.org** — a website dedicated to assisting visitors in protecting themselves from Internet scams and identity theft threats.
- **www.wachovia.com**/securityplus/page/0,,10957_10970,00.html — the aforementioned banking website that offers a number of tips on the problem.
- **www.identitytheftrefuge.com**/internet-identity-theft.htm — covers employee theft, phishing scams and online fraud.

"It's important to have a **company-wide network security plan** [and] ensure that you have someone in your company that regularly monitors your system."

Keep a record. Maintain a written chronology of what happened, what was lost and the steps you took to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person you spoke with, and any relevant report or reference number and instructions.

Stay vigilant. Continue to perform a thorough review and inventory of bank activity and/or items that may have been stolen from you. If you later discover additional fraud items or missing articles, be sure to contact the respective police agency, bank, credit card issuer or commercial establishment to update your initial report.

Employ Internal Security

Following up on the steps offered by the bank, Lieutenant Donohue stresses internal security steps that must be taken. "It's important to have a company-wide network security plan. But that's not enough just to have a plan. Back up that effort by ensuring that you have someone in your company that regularly monitors your system."

Donohue isn't done yet. "Treat any company online identifications and passwords with the greatest amount of security. Don't share passwords with anyone. In addition, be sure that your employees change their passwords with regularity. A failure to do so is one of the greatest assets that hackers can take advantage of. Among the recommendations I've seen are to change passwords every 30 to 60 days."

In stressing the importance of changing passwords, Donohue uses the analogy of steps taken to make a car thief's life more difficult. "The car thief is always looking for the easiest score. He doesn't want to have to overcome any hurdles placed in front of him as he plans to jump in the car and quickly drive away. Often he'll rattle the door handles of cars until he finds one that is unlocked or not equipped with a car alarm. So too is it with the Internet ID thief. He doesn't want to deal with firewalls, virus scanners or companies that have a security plan in place. Do anything and everything you can to make their jobs more difficult and secure the integrity of your information." asm