Identity theft on the rise

While it can't be prevented, proactive steps can be taken

INTERVIEWED BY DENNIS SEEDS

FRANK A. SUPONCIC, CPA, CFE, CFF
Partner
Skoda Minotti

(440) 449-6800
fsuponcic@skodaminotti.com

WEBSITE: For more information about how Skoda Minotti can help your business, visit www.skodaminotti.com.

Insights Accounting & Consulting is brought to you by **Skoda Minotti**

A few years ago, identify theft was likely the result of losing a purse or wallet, or having mail stolen. The recent explosion of database hacking has made security precautions all the more important.

"It is not a matter of if you are going to be a victim of identity theft — it's a matter of when," says Frank A. Suponcic, a partner at Skoda Minotti. "Think of the 80 million people at Anthem whose records were accessed — identity theft affects everyone."

In January, it was discovered that hackers had accessed the database of Anthem Inc. The information stolen included customer Social Security numbers and other data.

If hackers can breach high profile organizations, including federal agencies, they can break into smaller businesses' databases. Fraudulent income tax refund filings have shot up in the last few years, which indicates how sophisticated identity thieves are becoming.

"Data breaches today are the biggest threat to identity security," Suponcic says.

Smart Business spoke with Suponcic about identity theft and how it can be minimized.

How much of a threat is identify theft?

People have to realize that they are vulnerable, and they can never prevent identity theft. No agency can guarantee that it will protect a person's credit. The only thing that can be done is to be proactive and to mitigate the damage.

How can individuals be proactive in protecting their identity?

Anything that contains a Social Security number gives a thief carte blanche to impersonate someone in order to obtain new credit and make additional fraudulent transactions.

Every lawful U.S. citizen is allowed to receive one free credit report each year from each of the three credit reporting bureaus: Experian, Equifax and Trans Union. All three must be checked because the information can be radically different between the bureaus.

People should always use care when sharing information, especially on social media sites. Identity thieves are good at putting puzzles together. If someone's birthday is on Facebook, it gives a thief another piece to stealing that person's identity since birthdates are a common security question.

What is the No. 1 thing a business should do to prevent identity theft?

How the company protects its database is critical. There are regulations on how the information has to be protected, but there are a lot of businesses that don't take the threat seriously. Companies should develop a vendor management program. When sensitive information is shared with a vendor, the company has an obligation to know how their customer's data is being secured.

What tests should be conducted on a company database?

A company should have an IT risk assessment, including a vulnerability assessment, and then penetration testing. IT professionals will attempt to hack into a company's database during a penetration test — to gain unauthorized access to personal data, credit card information and Social Security numbers.

The purpose is to educate the business on whether or not its database is vulnerable and improve any weaknesses that may have been identified. A company needs to think about shoring up any deficiencies to protect client data and to protect its good name. An organization wants to avoid being smeared as a result of negligence because it failed to protect its data.

The economic effect that companies such as Target, which suffered a data breach in 2013, and Anthem, both which were victims of database hackers, is beyond the dollars to clear it up. The company image, and brand, could be damaged long term.

What other measures can businesses take to secure information?

Businesses are including only the last four digits of customer Social Security numbers in their documents. Organizations also have to be cognizant of what is thrown out. A good practice is to shred discarded paperwork that contains any customer or patient information.

A business has a responsibility to protect its databases and should never let its guard down. The threat that a data breach can happen is real. ●