Contact: Donald Scarinci
Tel: 201-806-3386
DonaldScarinci@Yahoo.com

Seven Things Businesses Can Do About Identity Theft

If you have ever had your credit card compromised, you understand the havoc that identity theft can create. Now imagine if that happened to your business.

Given the harm it can do to your reputation and bottom line, business identity theft should be on the radar of all companies. Of course, if the security breach involves customer data, the legal risks only multiply.

What should businesses look out for?

Business identity theft can take a variety of forms. Much like identity theft targeting individuals, criminals attempt to steal a legitimate business identity by gaining access to its bank accounts and credit cards, as well as other sensitive company information. They then often use the stolen information to secure lines of credit using the stolen business entity.

In other cases, imposters will pose as a look-alike or sound-alike business in an attempt to steal customers from a reputable business. A recent NPR article details the story of a Tennessee pest control business that fell victim to identity theft. The owner of the business opened the local phone book to discover three other "AAA Pest Controls," none of which were affiliated with his company.

Phishing attacks are also common. Many businesses have reported receiving emails that purport to be from official agencies and organizations like the Better Business Bureau, the Secretary of State's Office, or even the Securities and Exchange Commission. The emails often contain viruses programed to access and steal confidential business information. Because the emails appear to come from a trusted source, businesses often fail to detect the scam until after their information is compromised.

According to the National Association of Secretaries of State, inactive companies have also been frequent targets during the economic downturn. Because owners frequently stop monitoring the shuttered business, scammers are able to file fake reports with state business filing offices, or manipulate online business records, in order to change its registered address or appoint new officers/change its registered agent information.

What can businesses do to protect themselves?

Here are seven simple things businesses can do to protect themselves against identity theft:

1. Enroll in a credit monitoring service to monitor credit reports.
2. Review business accounts, bills, credit card statements for signs of suspicious activity on a regular basis.
3. Limit which employees can file required documents with state regulators and have access to that information.
4. Make computer security a priority and require all employees to change their password quarterly.
5. Invest in a good firewall to require outside email servers to identify themselves in order to deliver emails to employees on the network.
6. Restrict access to the company's sensitive information, including account numbers and passwords.
7. Create a procedure for shredding documents before disposing of them in the trash.

If you have been the victim of business identity theft, it is often a good idea to consult with an experienced business attorney who can help you put out the fire, including pursuing the individuals responsible and minimizing the damage to your business reputation.

This article was originally written by Donald Scarinci and published on blog.martindale.com on April 26, 2012.
http://blog.martindale.com/seven-things-businesses-can-do-about-identity-theft