The Hanover Insurance Group®

Hanover Risk Solutions

What Businesses Can Do to Reduce the Risk of Identity Theft

Identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. According to a survey by Javelin Research, identity theft losses to businesses and financial institutions in 2015 totaled nearly $15 billion. The report, "2016 Identity Fraud: Fraud Hits an Inflection Point" also found that 13.1 million Americans were victims of identity fraud in 2015. In 2015, the United States (U.S.) switched to a credit/debit card microchip, which is designed to reduce in-person fraud and the profitability of counterfeit card operations. Fraudsters have reacted by moving away from existing card fraud to focus on new account fraud. This drove a 113-percent increase in incidences of new account fraud, which now accounts for 20 percent of all fraud losses. The U.S. Federal Trade Commission (FTC) provides the following information to help businesses reduce their risk of identity theft:

- Keep valuable customer data, such as credit card or bank account numbers, in a secure location that is not readily visible to others who may have access to the premises.
- Shred or destroy paperwork no longer needed, such as bank machine receipts, receipts from electronic and credit card purchases, utility bills, and other documents from customer transactions that contain personal and/or financial information.
- If part of the business involves online transactions, check regularly to see whether someone has set up a "spoof site" in the name of the business. If a spoof site is found, identify the web hosting service or Internet service provider the spoof site is using and contact that service or provider immediately.
- If the business has a website that customers can use to order merchandise or enter personally identifiable information, have your information technology staff check regularly to ensure that there are no security "holes" through which others can improperly access customer data. This includes all upgrades of software used on your site. Security holes are sometimes inadvertently created as current programs are upgraded or patched but may expose customer data for long periods of time if they are not found and fixed promptly.
- Implement a fraud prevention and detection program. Online businesses, which often depend on credit cards for payment, should consult the financial institutions with which they have merchant relationships, and the major payment card associations as appropriate, to learn what programs or mechanisms may be most suitable for their businesses.
- Online merchants should be especially vigilant because when they handle "card-not-present" transactions, they may be held financially responsible for a fraudulent transaction even when the card issuer has approved that transaction.

continued ▸

- A variety of financial service providers, including depository institutions, credit card issuers, and brokerages, provide their customers with the option to receive notifications of suspicious activity. These notifications can often be received through email or text message, making some notifications immediate, and some go so far as to allow their customers to specify the scenarios under which they want to be notified so as to reduce false alarms.
- Merchants who conduct business face-to-face with their customers should establish a policy of requiring more than one form of identification when a customer is paying by check or credit card. In any event, all card-present merchants need to take all necessary steps to ensure, for each consumer transaction involving a payment card, that the card, the cardholder, and the transaction are legitimate.

If the business has become a victim of identity theft, take three immediate steps. First, contact the financial institution with which there is a merchant relationship. Second, report the matter to the local police. Police authorities often will take reports even if the crime ultimately may be investigated by another law enforcement agency. In addition, the police report may be useful in dealing with your financial institution or other businesses about the identity theft. Third, report the identity theft case immediately to the appropriate government organization, such as the Federal Trade Commission (FTC), and the fraud department of any of the three major credit bureaus (i.e., Equifax, Experian, or Trans Union).

At least 47 states have enacted legislation requiring customer notification of security breaches involving personal identification. The FTC also requires that certain businesses report data breaches. For a listing of states, see http://www.ncsl.org/default.aspx?tabid=13489. Also, the Better Business Bureau offers *5 Steps to Better Business Cybersecurity* https://www.bbb.org/council/for-businesses/cybersecurity/.

To learn more about Hanover Risk Solutions, visit hanoverrisksolutions.com

Why The Hanover?

The Hanover is a leading Property and Casualty insurance company dedicated to achieving world-class performance. Our commitment is to deliver the products, services, and technology of the best national companies with the responsiveness, market focus, and local decision making of the best regional companies. This powerful combination has been a proven success since our founding in 1852, and is backed by our financial strength rating of "A" (Excellent) from A.M. Best.

The Hanover Insurance Group®

The Hanover Insurance Company
440 Lincoln Street, Worcester, MA 01653

hanover.com

171-0944 (6/17) LC 13-119