



Deterring Identity Theft

CHALLENGES AND OPPORTUNITIES FOR BUSINESSES

The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year.

Identity theft complaints increased 22 percent from 2007 to 2008 (Javelin 2009 Identity Fraud Survey Report)

The average consumer costs of identity fraud were \$496 per incident in 2008 (Javelin 2009 Identity Fraud Survey Report)

Industry estimates put the total cost of identity fraud at \$48 billion in 2008 (2009 Javelin Strategy & Research)

A business can be affected by direct losses resulting from fraudulent transactions. Regardless of the goods or services it sells, a business collects, stores and uses sensitive customer information. Businesses can be affected by identity theft in several ways.

Most businesses keep customer and employee information in their files, including Social Security numbers, credit card numbers or other account data. Identity thieves can use this information to co-opt customers' existing accounts or open fraudulent accounts. Businesses are expected to protect information entrusted to them. Regulatory, legal and financial consequences may result.

The fact that many businesses are also employers introduces additional challenges. Employee records are a lucrative source of data for identity thieves. Employee and applicant information may be accessed and misused anywhere along the way while it is being acquired, validated, stored, transmitted or destroyed.

Businesses affected by a security breach experience loss of time and money while repairing damage.

› **The changing regulatory landscape**

The types of regulations that govern information security, privacy and identity theft differ based on many factors including the data businesses collect, how credit is issued, and which payment methods are used in the state or country where the business operates.

Federal and state laws may require a business to notify individuals if their information has been disclosed in an unauthorized way by a security breach. Other remedial steps may include the replacement of credit cards or accounts or credit monitoring — all at a cost to your business.

deter

Data security requirements from the credit card association, known as Payment Card Industry Standards, establish the level of data protection your business needs to incorporate in its operating plans.

Evolving health care privacy and security standards may apply if your business provides services to health care providers and has access to patient information.

If your business extends credit, which can be as simple as allowing deferred payments by your customers, your business must implement a formalized Identity Theft Prevention Program under the Red Flags Rule. Businesses that issue credit are required to maintain adequate and reasonable procedures to detect, prevent and mitigate identity theft.

A big cost of a security breach is the damage to your business's image and loss of your customer's trust.

► **Actions you can take to protect your business and your customers:**

Many small businesses do not have an information security plan. Steps can be taken to protect your business:

- Add and update physical and technical safeguards about information protection.
- Educate employees and define your business approach to identity theft and information security.
- Collect and retain only essential data on employees and applicants.
- Determine all places where employee and customer personal information is found, how long it is retained and who has access.
- Verify the information is securely stored and used, with access granted on a need-to-know basis.
- Protect the data on your computer systems with firewalls, encryption, anti-spyware and anti-virus technologies.
- Ensure all computers are logged off and all personal information is properly secured after hours. Information stored on laptops should be password protected and encrypted.
- Be aware of state laws on payment card information storage and retention. Some state laws require businesses to truncate payment card information included on customer's receipts.
- Be careful when transmitting information via e-mail or on websites. Ensure that you use Secure Socket Layer (SSL) or another secure connection to protect payment card information.
- Make employees aware of social engineering scams targeting business and personal information. More than half of business PC users receive at least one phishing e-mail per day.
- Position work stations and computer screens so personal information cannot be seen by employees or customers who may randomly be in the vicinity.

- Temporary employees and contractors with access to employee and/or customer information should be subject to screening and trained in security practices and expectations.
- Ensure hard drives have been destroyed, degaussed or scrubbed and all documents have been removed before selling or discarding used computers, file cabinets and other office equipment.
- Periodically confirm document destruction practices. Discarded documents and magnetic media containing employee or customer data should be shredded or otherwise properly destroyed.
- Establish procedures for handling and resolving customer disputes concerning the accuracy of credit bureau reports.

In addition to being familiar with your obligations under industry guidelines and federal statutes, contact your state's Attorney General's Office to identify additional requirements and protections that may exist under state laws.

Many organizations, including the Better Business Bureau and the Federal Trade Commission, have created materials and tools designed to help businesses with information security, privacy and identity theft.

Additional Resources:

www.ftc.gov/idtheft • www.ftc.gov/infosecurity • www.OnGuardOnline.gov