



Ask SCORE for Business Advice

Safeguarding Your Customers

By Tina Dettman-Bielefeldt

Consumers are growing increasingly cautious about providing personal information. Identity theft has become a staggering problem with a new victim every three seconds. To date, statistics estimate that there have been 10 million victims with estimated losses totaling \$50 billion. Of special concern to businesses is that the single largest identity theft case involved information obtained from major retailers.

In spring 2007, TJX, the parent company of T J Maxx, Marshalls, and HomeGoods, disclosed the theft of information from about 45.7 million credit and debit cards. Hackers accessed information from other retailers, as well, including Barnes & Noble, Sports Authority, BJ's Wholesale Club, OfficeMax, Boston Market, Forever 21, and DSW. The Justice Department, who announced earlier this month that the case has been cracked, estimated that the fraud reached into the tens of millions of dollars. For the retailers, the costs have also been substantial.

TJX Companies reported last year that it had already spent \$256 million trying to clean up the mess. The costs including fixing the company's computer system, notifying consumers, dealing with lawsuits and investigations, and other claims associated with the theft.

Meanwhile, 11 people have been indicted including the ringleader, Albert Gonzalez, one of the U.S. Secret Service's own informants. Gonzalez has been charged with computer fraud, wire fraud, aggravated identity theft and conspiracy. Unfortunately for the retailers involved, the investigation also includes them.

Almost immediately after the breach was disclosed, the Federal Trade Commission began investigating TJX. They questioned why information wasn't routinely deleted and if the data had been protected through encryption. In its statement, the FTC alleged that TJX failed to use "readily available security measures" to prevent hackers from stealing data off their wireless networks used to verify consumers' information. Since the incident, the company has worked closely with law enforcement and now meets all industry standards for protection of customer data.

New laws have also been enacted, and businesses need to be aware of their responsibilities under these laws. Robert Jahnke, SCORE volunteer and owner of a company that sells prepaid legal services, said that businesses must be able to prove that

they have procedures in place to protect information. Failure to comply with the Fair and Accurate Credit Transaction Act (FACTA), and the Gramm-Leach-Bliley Safeguard Rule could result in fines up to \$1,000,000 per occurrence and up to 10 years in jail for executives. Businesses can also be subject to litigation.

FACTA provides that companies that haven't taken "appropriate measures" to safeguard information from identity theft can be sued and face not only civil, but criminal penalties. Simply put, if data aiding an identity theft originates from a security breach at your business, you could be sued, fined, or become a defendant in a class-action lawsuit by affected parties.

The issue for small businesses then becomes compliance. Next week, we'll look at steps all businesses need to implement.

If you'd like further information on business concerns, contact the Green Bay Chapter of SCORE "Counselors to America's Small Business." Visit www.greenbayscore.org or call Cindy Gokey at 920-496-8930 for information.

Tina Dettman-Bielefeldt is co-owner of DB Commercial Real Estate in Green Bay and Chapter Chairman for the Green Bay SCORE group.