HARDWARE Retailing

Nuts and Bolts of Recent Retail Breaches

by Brenda Eaden - March 14, 2014 - From the Experts

Retail data breach and identity theft concerns have heightened since the December 2013 announcement Target was attacked by hackers and bank card information for more than 100 million of its customers were stolen—this followed by the recent announcement that retailer Neiman Marcus also experienced a similar breach where a million of its customers had their information stolen.

At first blush it seemed the hackers were only able to extract the minimal information contained on bank card magnetic strips. Not a surprise to industry experts, but later it was learned hackers obtained other nonpublic personal identifiable information that could lead to identity theft.

The media frenzy continues to amp up attacking retailers for not doing enough to ensure proper protection of customers' personal information and bank cards.

Riding on the coattails of recent breach news, the blame game is heating up between banks and retailers. As they battle over who absorbs the losses incurred, consumers are upset and are demanding justice, which boils down to seeking financial restitution and satisfaction through legal channels.

There seems to be a trend of filing lawsuits even if the claimant hasn't incurred any financial damages due to breaches. Claimants argue enough hasn't been done to protect their information, and notification was slow in coming. The risks do not stop with stolen bank cards. Damage can rear its ugly head later if identity thieves obtained access to enough information to duplicate someone's identity.

Although pinpointing the exact origination of the theft is difficult to prove given the myriad places bank cards are used, every breached retailer becomes a target. Defense is very costly, not only financially but the damage to a retailer's name most certainly results in lost customers and revenue.

New Legislation Coming Down the Pike

Due to accelerated recent concerns and demands by consumers and consumer advocates for Congress to "do something and do more" to force retailers and banks to protect personal information, the response has been swift by lawmakers.

In January 2014, Senators Tom Carper (D-De.) and Roy Blunt (R-Mo.) reintroduced legislation to protect consumers from identity theft and fraud. The Data Security Act of 2014 would help better protect consumers from identity theft and account fraud and establish clear and consistent rules nationally for public and private institutions to follow to prevent and respond to data breaches.

The bill would require entities such as financial institutions, retailers, and federal agencies to better safeguard sensitive information, investigate security breaches and notify consumers when there is a substantial risk of identity theft or account fraud. These new requirements would apply to businesses that take credit or debit card information, data brokers that compile private information, and government agencies that possess nonpublic personal information.

The Data Security Act would better protect consumers by replacing the current patchwork of state laws and establish one set of national standards. Today, 49 states and U.S. territories have enacted laws governing data security and data breach notification standards. Inconsistent and conflicting state-by-state standards force public and private entities to comply with multiple regulations, leaving many consumers in a confusing web of regulation depending on the state.

We may see the length of time it typically takes a bill to be enacted into law and enforced by the Federal Trade Commission shorter than usual in direct response to increased pressure put upon lawmakers.

More Industry Change Is Coming!

The conversation about "chip and pin" is growing hotter than ever and is gaining traction. Pressure is being felt for the banking industry to follow this type of signature technology in the U.S. which has been adopted for years by countries abroad.

For those not familiar with chip and pin smart card technology, EMV stands for Europay, MasterCard and Visa, a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card-capable point of sale terminals and ATMs, for authenticating credit and debit card transactions.
U.S. banks and retailers face an October 2015 deadline imposed by payment networks Visa Inc and MasterCard to switch to new cards that use computer chips to store information rather than magnetic strips.

Not a "Techie"? No Excuse! Time to Bone Up!

Lots of storeowners talk about their lack of technical knowledge and why should they know more. They pay trusted partners to put processes and systems in place to protect their businesses. There is a list of compelling reasons. The most important one is the financial livelihood of the store.

Given the threat landscape, it is highly advisable to invest time with your system administrators to learn in layman's terms just how your system is protected. Ask them to help you clearly understand the areas of

weaknesses that could potentially leave systems open and exposed to hacking and how the protections they've put in place are keeping your business as safe as possible from outside intrusions.

What's At Stake for Your Hardware Business?

Compromised customer information isn't the only vulnerable area where attacks occur. Businesses are also at risk of being hit and incur financial loss.

"Small businesses may find funds frozen for some time, resulting in an inability to pay vendors, employees and meet other operating needs. Imagine a small business that needs to make payroll with its funds frozen for a two-week investigation—that could be devastating." said Jani Gode, vice president and division manager of the risk management and payments group at SightSpan Inc., a Mooresville, N.C.-based global management consulting group and financial crimes solution provider.

Businesses could also be affected more harshly because it may be easier to hide fraudulent transactions on a business account versus a consumer account, Gode said. Businesses also typically have many more transactions and each transaction amount could be much higher, she noted.

It is critical for storeowners to take stock in all processes governing how customer and business information is handled internally, and in some cases externally. Owners should know first-hand how sensitive data is collected, stored, accessed, shared and disposed.

This is not an option—it's required under the federal "Red Flags Rule." Noncompliance with state and federal identity theft prevention laws puts owners and customers at huge financial and emotional risk. It is also important to ensure your business is meeting current Payment Card Industry Data Security Standards known as PCI DSS.

Not sure if you are compliant? To help you determine your compliance status, you may want to visit ***www.HardwareBizCompliance.com*** *to obtain information.*

Bottom line: Those charged with the responsibility of maintaining the health and vitality of your hardware business should be hands-on when it comes to knowing how all the security pieces work and fit together because when all is said and done, being ***aware and prepared*** is your best defense.