Data Breach! Don't Become the Next Target

By Brenda Eaden, identity theft prevention and compliance expert

Odds are, you will or maybe already have been a victim. You may not even know it.

As more retailers utilize technologically advanced retail systems, both online and in store, customers are growing more and more at risk for having their personal information hijacked.

In fact, the headlines have recently been inundated with high-profile retailers facing significant financial and customer relations nightmares as a result of breaches of confidential files such as customers credit card numbers, Social Security numbers and other personal information.

One such retailer, popular mass merchant Target, was forced to face the consequences of a painful data breach late last year when the company reported hackers stole more than 70 million of its customers' payment-card data. Now, almost two months later, the company is still scrambling to mitigate lawsuits, gain back customer loyalty and prevent future attacks.

While we all say it will never happen to us, the reality is it could if you don't protect yourself and your store. With all the advantages and necessities technology brings, it also presents a whole new set of risks.

We hope this article helps you and your team better navigate through the often-intimidating world of technology security and compliance.

Two Common Breaches

Let's briefly cover the two types of breaches your business should be concerned about and may encounter. Identity theft is the first, and what we refer to as the *frontal attack*—most often occurring when an individual's personal identifiable information (PII) or business information is used to illegally obtain goods without authorization.

Identity thieves are getting more brazen in their methods of stealing business names, executive credentials and credit history to open accounts. One would think this isn't possible, but it happens more often than you'd think. According to the FBI, more than $8 billion is lost or stolen from small businesses every year.

The second, more high-profile, type of attacks involve network system data breaches. This type of breach defines Target's recent blunder. Unfortunately, a simple apology doesn't fix it, either. It will take months to learn all the details and the full extent of these breaches. But one thing is certain: Target will likely feel the brunt of the aftermath due to lost customer confidence for a long time to come.

And while Target has been the, forgive me, target of many headlines lately, it's not the only one. Other notable retailers such as TJMaxx, DSW, Barnes & Noble, and Zappos are still bearing the scars of stolen information. Lesser-known retailers are also battling the same fight without the financial resource reserves to combat their breach, or multiple breaches in some cases. Smaller businesses are hit hardest by the recovery process and the arduous task of rebuilding customer trust and confidence, which affects the bottom line.

Where Is My Company and Customers at Risk of Identity Theft?

So where is your store at risk? There are three common ways you could be leaving yourself vulnerable to a breach.

1. **Untrained employees.** If your staff is not fully trained on identity theft prevention—especially as it relates to safeguarding sensitive customer information—they can make a mistake that leads to an identity theft incident.
2. **Rogue employees.** Unfortunately, there are times when a trusted employee can turn into an identity thief. Financial duress, disagreements with company policy, conflicts with members of your staff or temptation can lead an employee to compromise customer data.
3. **Vendors.** Many businesses store customer information electronically. If you outsource your network maintenance and computer support to a third-party, or if you use a service to do your customer billing, you run the risk that your data could be compromised.

A well-thought-out identity theft prevention program can mitigate these risks because it contains policies and procedures that address these areas of vulnerability. It forces your team to stop and ask, "Where are we exposed—and how can we shore up these discovered areas to the best of our ability?" By addressing the weaknesses in your theft prevention practices, you reduce your exposure to a potentially devastating identity theft event affecting your customers as well as your business.

> "By addressing the weaknesses in your theft prevention practices, you reduce your exposure to a potentially devastating identity theft event affecting your customers as well as your business."

The Use of Technology Exposes Your Store

Few retail businesses can sustain growth without the use of technology. It allows for speed of transacting business activities and banking and expedites receipt of revenues—the speed customers demand when they want product and services delivered as quickly as possible and use bank cards and commercial credit as methods of payment. With the necessity and convenience of technology comes with it inherent risks.

Compounding security challenges is the necessity for a business to have an online presence in the same way it once did when Yellow Pages were the primary tool for marketing and commerce.

Hackers have figured out ways to capture trusted websites, even government sites, and expose visitors to a host of hidden malware, which most often is undetectable by even the industry's best anti-virus programs.

"I'm not very techie." We hear this all the time. It is vital your network administrator explain your risks and what processes are in place to protect your hardware business from exposure to outside system intrusions and hackers.

If you outsource the maintenance of your network and computers, again, carve out some time to have your vendor educate you on how it is protecting your business. Remember, if something happens, the business's key executives will be held responsible and liable even if an employee may have been negligent.

Industry Breach Data

We are not going to saturate you with a lot of data minutiae, but industry analysts provide stats which should make every retailer sit up and take notice.

There's no pretty way to package breaches and the fallout in a way that provides a false sense of security—or supports the "head buried in the sand" mentality that "It's not going to happen to me."

The data speak for themselves. According to Verizon's 2013 Data Breach Investigations Report, one key takeaway is "While the sophistication of attacks is growing, most breaches could still be easily prevented."

Interestingly enough, Verizon also states of the 47,000-plus security incidents analyzed and 621 confirmed data breaches studied, 78 percent of the breaches employed tactics and techniques they rate were in the low

On Track with ID Theft Compliance

Preventing identity theft is crucial to your business. It gives customers confidence that their sensitive data is safe, and it offers your officers and shareholders protection against a damaging identity theft event. With identity theft seemingly in the headlines every day, it makes more sense than ever to comply with federal and state laws and put a protection program in place for your company.

Here's a checklist that can get you started on your own identity theft prevention program:

- Understand state identity theft and breach laws in addition to federal Red Flags Rule
- Understand the requirements for implementing an ITPP
- Write an ITPP that is legally compliant
- Make changes to make handling of sensitive customer data more secure, both physically and electronically
- Train employees (part-time and full-time) and all contractors on ITPP policies and procedures. This includes written signoff that they completed training
- Implement a process to make sure your company is compliant at all times (including changes that stem from amendments to state and federal laws)
- Get written confirmation from contractors and service providers who handle your sensitive business information that they are compliant with applicable laws

(basic methods, little or no customization or resources required) to very low (the average person could have done it) category of skill range. However, Verizon goes on to say "The simplicity of attacks doesn't take anything away from their effectiveness or impact. Even well-known techniques can be used to devastating effect."

According to the 2013 Trustwave Cyber Security Breach Report, retail ranks No. 1 in the top industries compromised. The primary targets of cybercriminals in 2012 were retailers by a whopping 45 percent. One of the reasons the report cites is "The main focus of organizations operating in these spaces is customer service, not data security."

Other contributing factors to this continuing trend: There's a misconception that these organizations are not a target. In practically all of Trustwave's 2012 investigations, this statement was made in just about every case: "Why me?" The answer can only be because you have something worth taking that is not protected.

Customer Expectations

Identity theft and data breaches aren't just about monetary risk. What's also at stake is your reputation. When customers shop at your hardware store, they expect and assume you are protecting their private information and you are in full compliance with state and federal identity theft laws. If you're not—and if their data is stolen—it can destroy their confidence in you. Without warning, the repeat business you've counted on to grow and expand can evaporate overnight.

> "Once a prevention program is in place that meets the test of the law, you may need to make changes in the way you handle and store customer information, both physically and electronically."

So how do you protect your business and valued customers? It starts with compliance.

Your Best 'Two-Pronged' Protect & Defend Strategy

Compliance is your best two-pronged strategy and ensures employees charged with handling customer information are formally trained to protect and defend your operations.

One would be naïve if the belief is every identity theft event or data breach can be easily thwarted. But all is not lost. If your hardware business is compliant with state and federal identity theft laws and is truly compliant with the Payment Card Industry Data Security Standard (PCI DSS), then this two-pronged approach will provide the protection your business needs to prevent the preventable. As part of your best practices, it also acts as your defense should an identity theft or breach event occur.

Are You Fully PCI DSS Compliant?

There is no shortcut to PCI DSS compliance. This was painfully discovered by Heartland Payment Systems, the fifth largest payment processor in the United States, when it took up permanent residence in the news for quite some time back in 2009. Their historical breach from an undetected network intrusion resulted in the data theft from 130 million credit cards.

Heartland CEO Robert Carr later conducted a webinar sharing his cautionary tale of the dangers businesses face contracting with the least expensive PCI compliance vendor and ending up with mediocre PCI audits. Carr went on to say, "The auditors have contracts with clients that essentially absolve themselves of gross negligence. The false reports we got for six years, we have no recourse. No grounds for litigation."

Yes, in 2009 he cast a disparaging light on Heartland's PCI vendor's compliance auditors' competence for failing to flag key attack vectors, but resorting to blame for a company of its size did little to dampen the backlash and string of lawsuits which later ensued. But the reality is the buck stopped with him.

So what is your litmus test for ensuring you are fully PCI DSS compliant? The first place we recommend you start is understanding the basics. You can download a free copy of the PCI DSS Quick Reference Guide from www.HardwareBizCompliance.com. There is a host of information provided in the guide to help you understand the requirement standards. Once you go through the guide, you are better prepared to ask questions and discuss your store's data security with the network administrator and your PCI compliance vendor.

If you are not PCI compliant, do not delay in bringing your store up to date. Every day you ignore this obligation or are not sure you are fully compliant with the standards, you leave your business and customers open to huge financial risk.

If you need help, the PCI Security Standards Council can provide you with a list of approved security consultants and vendors.

Compliance Isn't an Option— It's Required by Law

Compliance with state and federal identity theft laws is not optional. If your business engages in any of these activities:

- accepts credit and debit cards;
- collects bank account information;
- records customer address, phone numbers, business license numbers and/or Social Security numbers;
- reports account information to a credit bureau directly or indirectly through a third-party firm

you are required to be fully compliant with all state and federal identity theft and breach laws.

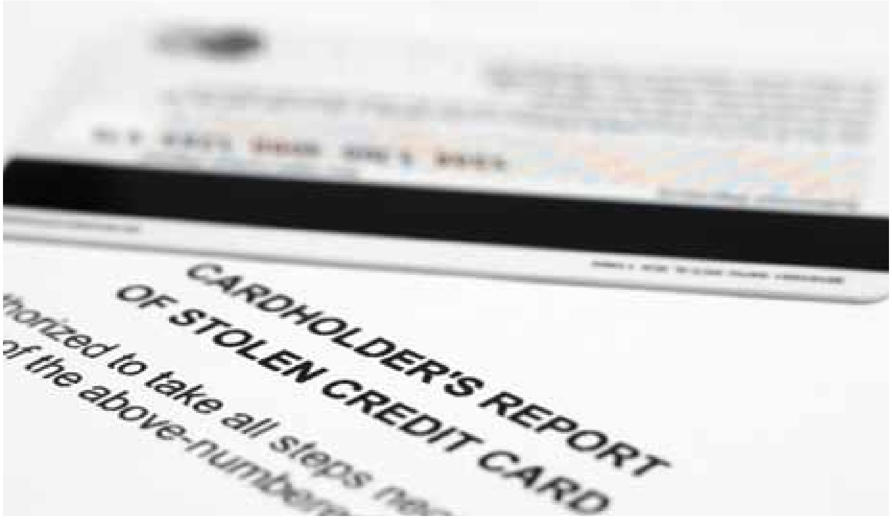
Getting Started with Compliance

If your company has not yet implemented an Identity Theft Prevention Program (ITPP), this is a great time to start the process. It begins with understanding identity theft and breach laws—not only in the states in which you do business, but federal requirements as well. If you don't know where to find these laws, an experienced identity theft prevention consultant can be of great help.

Next, you need to develop a program. A quick online search will turn up dozens of templates for an identity theft prevention program. Just be careful. A number of these templates are only appropriate for companies that have a low risk of identity theft. They may not fit your kind of business. Also, larger companies collecting and handling sensitive customer information will need to develop a comprehensive protection program far beyond an online template.

Once a prevention program is in place that meets the test of the law, you may need to make changes in the way you handle and store customer information, both physically and electronically. You will also need a regimen to train part-time and full-time employees about your program and prevention procedures. Additionally, to ensure you have deployed a sound program, contractors and service providers should be included in your prevention training.

Finally, you will need to have a process that keeps your compliance procedures current and in full force at all times.



Compliance Confusion

Many businesses are under the misconception that if customer personal information is outsourced to a third-party firm, they don't have to comply with identity theft laws. This is definitely not the case! If you handle customer information including collection of sensitive information on applications—in your store or direct customers to a third-party for account processing —you are also required to follow the laws as well.

In addition, your store has to comply with the federal Red Flags Rule law if you report customer information to any credit bureau, whether by you or a third-party firm you hire. The *Red* Flags Rule was enacted to detect the warnings signs (or "red flags") of identity theft. This law requires you to develop a written ITPP—a playbook that helps your company detect, prevent and mitigate identity theft.

If you don't have an ITPP in place and are not compliant with other identity theft laws, you could be subject to fines—including those levied against your third-party vendors. Non-compliance also opens your business up to civil and class action lawsuits. No one wants to face that!

All businesses that accept bank cards have to agree to a set of rules established by the bank card industry (also known as PCI DSS). Be careful! Don't mix up PCI compliance with identity theft compliance. Although there is some overlap, being PCI compliant does not mean you are compliant with federal and state identity theft and breach laws—including the Red Flags Rule.

With a sound ***two-pronged protection and defense program*** in place, you'll know you're safeguarding your vital business assets from the threat of identity theft and data breaches, restoration hassles, fines for non-compliance, and potential litigation. Putting a formal Identity Theft Prevention Program (ITPP) in place and ensuring you are fully Payment Card Industry Data Security Standards (PCI DSS) compliant is more than good business. It's great protection for you and for your customers.

Brenda Eaden is a leading expert and speaker on identity theft prevention and compliance and has been instrumental in crafting state and federal laws to ensure protection for businesses. She founded IDTELi, LLC, a leading developer of business solutions focused on the prevention of identity theft and provides businesses with education, current information on the laws and cost-effective tools designed to help businesses easily become compliant with state and federal identity theft laws.

For more information on identity theft and compliance, visit www.HardwareBizCompliance.com, call 503-388-6200 or email info@HardwareBizCompli.com.