HARDWARE Retailing
IN THE MAGAZINE • LATEST NEWS •

Chaos or Compliance: Protecting Your Business from Identity Theft

by Brenda Eaden - December 2, 2013 - From the Experts, Web Exclusives

It is no secret that identity theft continues to plague our personal and professional lives. It leads the list of consumer privacy concerns and has ranked as the No. 1 consumer complaint to the Federal Trade Commission for the past 13 years in a row.

Businesses large and small are vulnerable to identity thieves who are determined to steal sensitive financial information. Businesses opening commercial accounts are at particular risk due to the collection and handling of customer banking and business information.

Fortunately, there are steps you can take to protect your business and your customers. December is National Identity Theft Prevention and Awareness Month: A great time to step back, evaluate your company's approach to managing and securing confidential customer information, and take steps to make sure your hardware business is in proper compliance with the law.

Customer Expectations

Identity theft isn'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 your store can evaporate overnight.

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.

Where Is My Company At Risk?

Compliance with the laws becomes a critical part of your hardware business security and helps to address areas in the company that would otherwise be overlooked and open to attack.

There are three common ways identity theft is able to strike at your company.

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 computer support to a third-party or if you use a service to do your customer billing, you run the risk of your data being 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 that up 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.

Getting Started with Compliance

If your company has not yet implemented an Identity Theft Prevention Program, this is a great time to start the process. It begins with understanding identity theft and breach laws—not only in the states you do business in, 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 for your hardware store. 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 small 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 put a process in place 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 that 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 Identity Theft Prevention Plan (ITPP)—a playbook that helps your company detect, prevent and mitigate identity theft.

If you don't have an ITPP in place and if you're 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 known as Payment Card Industry Data Security Standards 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.

Conclusion

Preventing identity theft is crucial to your business. It offers your customers the 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

With a sound prevention program in place, you'll know that you're safeguarding your vital business assets from the threat of identity theft, restoration hassles, fines for non-compliance, and potential litigation. Putting a formal Identity Theft Prevention Program (ITPP) in place is more than good business. It's great protection for you and for your customers.

Brenda J. Eaden is president and CEO of IDTELi and a provider of cost-effective identity theft prevention compliance tools and consulting services for the hardware industry. For more information, visit www.HardwareBizCompliance.com or email Info@HardwareBizCompliance.com.

Read more posts by Brenda Eaden