Tough New Security Measures In Payment Processing:

Can Small And Mid-sized Companies Keep Up?

By: Kristin Los

Many home improvement retailers are looking forward to revenue growth opportunities this year as more and more Canadians opt to renovate over buying new homes. But as retailers and wholesalers work to adjust their merchandise strategies, they also need to keep up with regulatory requirements for payment processing, especially around credit card security.

Mastercard and Visa now hold Canadian merchants liable for fraudulent transactions that may have been avoided with chip technology. This means merchants not using PIN pads in their stores and that fall victim to fraud will, in most cases, have to pay for it.

Can Be Costly

For small and mid-sized retailers that don't have chip and pin technology, this can be costly. Any fraudulent transactions that take place with counterfeit cards, lost cards, stolen cards, or cards-not-received will be considered fraud that could have been prevented and thus the merchant must absorb the cost of the fraud.

Companies that stay up-to-date with their payment processing systems won't have to worry. Their providers should have added PIN pads to their stores by the March deadline, depending on the plan they have in place.

If you don't already have PIN pads in your stores, you should contact your payment processor or POS provider immediately and discuss your next steps to reduce your exposure to this fraud liability.

Small retailers should take special note of the PCI Security Standards Council's standards as they are a well-known target of data thieves.

Started in 2006, the council is an open global forum that was founded by the five major payment brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The council establishes and manages payment security standards for merchants around the world.

While the standards are good news for the consumer, they have been met with mixed reactions from merchants who must figure out how to ensure each one of their stores is compliant.

Retailers that rely on custom providers for their POS software may find that what once looked like the cheaper option may turn out to be more expensive in the long run. Custom-built systems need to be updated manually every time a new standard emerges and with custom-built solutions you don't have the benefit of spreading the cost of research and development out over many retailers.

Preliminary Steps

Retailers that wish to follow the council's guidelines can take preliminary steps by doing the following:

◆ Ensure you aren't storing unencrypted credit card numbers anywhere. This includes written numbers kept in a filing cabinet and spreadsheets or documents kept on a computer.

◆ If you do wish to store credit card numbers, they must be encrypted according to the guidelines established by council and strict security rules must be followed. Not storing credit card numbers lowers the number of regulations you must observe.

◆ Keep your anti-virus software up to date.

◆ Check the serial numbers on your PIN pads every day. Thieves have been known to swap out PIN pads with a dummy PIN pad, add a skimming device that steals card data, and replace the dummy PIN pad with the now corrupt PIN pad. This is especially important if your PIN pads are not physically locked down.

◆ Secure any networks used to perform third-party processing for your credit cards by a firewall.

◆ Keep the computer used for card processing in a locked room.

If you do experience a security breach or a stolen PIN pad, you should contact your acquirer and your local police immediately.

Least Amount Of Pain

Those retailers that have council-validated payment applications will feel the least amount of pain through transitional periods, as they will have made incremental, regular payments to a vendor to ensure their systems remain PCI-compliant. This is generally easier to manage than large capital investments in short intervals, which can hurt all-important cash flow for small and mid-sized retailers.

Making POS systems fully PCI security standards compliant is long, difficult, and expensive work. It requires rigorous testing from internal developers, external auditors, and banks. Retailers can find a complete list of vendors that have completed this process and received validation by the PCI Standards Council online at its website.

In these times of complex technology and security, it's best to leave the technology up to the experts and let home improvement retailers focus on what they do best: serving their customers. You'll sleep better knowing you've got the proverbial brick house securing your data, and not the straw one. ❖

Kristin Los is a product manager, hardware and building supplies solutions, at ProfitMaster Canada's GFI Solutions Group Inc.