First Data
beyond the transaction

First Data Market Insight

Payment Card Data Breaches: What You Need to Know About Your Risk and Liability

Many small merchants are surprised to learn that they can be held liable for tens of thousands of dollars in fines and other expenses when a card data breach occurs. What you don't know can hurt you.

The owner of two small Chicago-area magazine shops received an email from his credit card processor, telling him that MasterCard had identified a compromise within his electronic point-of-sale (POS) system. The business owner called a technology consultant to check the Windows PC that ran the POS system. Sure enough, the consultant found and removed malicious software (malware) from the computer.

Over the next two months, the owner continued to receive notices about fraud stemming from information suspected of being stolen from the magazine shop's POS system. In time, MasterCard demanded that a forensic investigator be hired to do a thorough review of the system. The owner hired an investigator from the information security company Trustwave, and he discovered malware that captured the card data at the POS before it was even sent to the payment processor. The malware sent the captured data via the Internet to a person in Russia who sold or used it to commit fraud. This had been going on for at least a year without anyone knowing about the problem. The stunned owner of the two shops couldn't believe a cyber-criminal would come after a business as small as his.

The source of the breach was traced to remote access software the merchant used occasionally to connect to his computer system from outside his shop. This program could be used by anyone who knew – or guessed – the password, which wasn't a very strong one. Pointing a finger of blame at the merchant, the shop owner's card processor claimed the breach was the result of the lack of basic security on the merchant's part.

The owner was required to pay for the forensic investigation and upgrades to his POS system technology. A year later he was still paying off more than $22,000 in expenses his business incurred—a huge chunk of his already thin profit margin. The owner talked to the police and the Secret Service, the federal agency that investigates hacking attacks, but they offered little help.[1] But as bad as this was, it could have been worse. Issuing banks could have required this business owner to pay the cost of replacing consumers' compromised credit cards, and he could have faced hefty fines and lawsuits from his payment processor and other parties in the payment process. These types of incidents are more prevalent than ever, even though many small business owners who have been impacted by data breaches are understandably reluctant to share their experiences.

A YEAR LATER HE WAS STILL PAYING OFF MORE THAN

$22k

IN EXPENSES HIS BUSINESS INCURRED

1 Geoffrey A. Fowler and Ben Worthen, "Hackers Shift Attacks to Small Firms," The Wall Street Journal, July 21, 2011

Beyond the transaction℠

Payment Card Data Breaches: What You Need to Know About Your Risk and Liability

Your Business Is at Risk

Could something like this happen to you? Absolutely. Businesses like yours experience a data compromise every day. It can be as simple as a stolen receipt from a trash can, or as sophisticated as a ring of cyber-criminals hacking into computer systems. In fact, it happens more often than you may think. Consider that:

- Verizon reports that 40% of the confirmed breaches it investigated in 2012 were companies with fewer than 1,000 employees. Companies with fewer than 100 employees represent the single largest segment of breach victims. [2]
- Trustwave analyzed 691 data breaches in 2013 and found that Retail was the top industry compromised, making up 35 percent of the attacks investigated. POS breaches made up 33% of the total investigations.[3]
- The Ponemon Institute survey of small businesses throughout the United States found that 55% of those responding have had a data breach, almost all involving electronic records, and 53% had multiple breaches.[4]
- Almost one-third of U.S. small businesses surveyed by the Ponemon Institute had a cyber attack in 2012.[5] The technology security company Symantec Corporation confirmed this figure, stating that 31 percent of the cyber attacks committed in 2013 were aimed at companies with fewer than 250 employees.[6]

53%
OF SMALL BUSINESSES HAD MULTIPLE BREACHES

31%
OF CYBER ATTACKS IN 2012 WERE AIMED AT COMPANIES WITH FEWER THAN 250 EMPLOYEES

Recently, in another First Data Market Insight, we illustrate just how vulnerable small merchants are to thieves who view small businesses as prime targets with weak defenses. Even though the volume of electronic payment data that passes through small merchants' POS systems is relatively small, it is low hanging fruit to a cyber-thief who doesn't have to work hard to obtain that poorly protected data. Data breaches "already are happening among smaller employers. It's not happening with any lower frequency than the Targets you're reading about," according to John Rose, a security expert and senior partner at The Boston Consulting Group.[7]

In the case described above, a thief used a default password to log in to the store's administrative remote access software. He was able to gain entry into the POS system and plant malware that collected the unencrypted primary account number (PAN) from the credit and debit cards swiped at the store counters. This stolen data was sent out over the Internet connection without anyone's knowledge for at least a year.

Security experts consider the effort behind this type of attack to be very low and unsophisticated. In fact, 78% of intrusions rate as "low" or "very low" on the VERIS difficulty scale, meaning they require no special skills or resources.[8] Making matters worse, the malware used in many thefts of this nature is readily available in the underground world of cyber-crime. Anyone can buy it for a song and get it going from their parents' basement—and they do.

2 Verizon 2013 Data Breach Investigations Report
3 2014 Trustwave Global Security Report
4 Ponemon Survey for Hartford Steam Boiler (HSB), June 2013
5 Ponemon Survey for Hartford Steam Boiler (HSB), June 2013
6 Symantec Corporation, 2013 Internet Security Threat Report
7 Heesun Wee, "How the threat of cybercrime is heightened for Main Street," CNBC, January 27, 2014
8 Verizon 2013 Data Breach Investigations Report

Beyond the transaction℠

Payment Card Data Breaches: What You Need to Know About Your Risk and Liability

But your business isn't vulnerable, is it? When you print a customer's receipt after an electronic transaction, only the last four digits of the PAN are on the receipt. That means a thief can't get the full card number from your system, right? Wrong. What's on the receipt is not indicative of the actual data in your POS system. Most likely the full PAN – the account number that thieves covet and steal – is passing through your system in clear text format before it is passed off to your payment processor. This data is extremely vulnerable at this point, and you are completely responsible for protecting it while it is in your possession. Your business is at risk of a data breach if your measures to protect this data are inadequate.

DATA IS EXTREMELY VULNERABLE AND YOU ARE COMPLETELY RESPONSIBLE FOR PROTECTING IT

Your Liability in the Event of a Payment Card Data Breach

By now, every merchant that accepts credit and debit cards likely knows about the Payment Card Industry Data Security Standard (PCI DSS). It is an industry security standard created by the leading card brands to increase protection of cardholder information and reduce fraud. All merchants – even small ones – are required to comply or risk losing the ability to accept many brands of payment cards.

Your own business has probably undergone, at minimum, a PCI self-assessment via questionnaire (SAQ) or perhaps even an audit conducted by an external Qualified Security Assessor (QSA). Passing an assessment or audit validates that your business is following industry best practices to protect against a data breach. However, PCI compliance – when actually achieved and sustained – does not equal security. Moreover, the vast majority of merchants of all sizes don't comply with all 12 requirements of PCI DSS. In 2013, just 11.1% of all companies complied with every requirement outlined in the security guidelines.[9] PCI DSS is designed to help your business reduce vulnerability and mitigate risk, but it doesn't mean you are risk-free and it doesn't protect you against liability in the event of a breach.

11.1%

OF COMPANIES COMPLIED WITH THE 12 PCI DSS REQUIREMENTS

In the event of a payment data breach, your business could face liability from several different groups, including:

- Associations will require you to undergo a forensic examination of your POS system.
- Your acquiring bank, which may pass along hefty fines and other fees assessed by the card associations. Your acquirer also may withhold payments to your account to cover losses from fraud.
- Credit card issuers, which may require you to cover the cost of reissuing cards to customers who have been affected.
- Government agencies such as state attorneys general or the Federal Trade Commission, which may file suit for your failure to adequately protect consumers' information. You may also be required to send out breach notices as well as to provide credit monitoring to all consumers whose information may have been compromised.
- Individual customers whose information is compromised by the breach may sue, especially if they personally sustain financial losses or experience other hardship.

9 Verizon 2014 PCI Compliance Report

Beyond the transaction℠

12202 0614

Payment Card Data Breaches: What You Need to Know About Your Risk and Liability

It's worth repeating: undergoing or even passing a PCI compliance assessment does not provide "safe harbor" from liability, although it may help to minimize your liability.

A Breach Could Have a Significant Impact on Your Business

In another recent First Data Market Insight, we outlined the numerous ways your business can be impacted by a payment card data breach:

- Substantial fees and fines that could potentially total in the tens of thousands of dollars or more.
- Loss of customer confidence and trust.
- Damage to your brand and good business reputation, especially as word travels quickly through social media and online review services like Yelp.
- Considerable time that you and other employees will have to devote to dealing with and recovering from the breach event.
- Loss of payment card privileges, meaning your business will not be permitted to accept debit and credit card payments if the card associations refuse to do business with you.
- Costs to upgrade or replace your POS system and associated security measures (e.g., firewall, anti-virus/anti-malware software).

It's not inconceivable that a breach can put you out of business, for a short time or for good. In another small-business example, cyber-criminals hacked into the computerized cash register of a restaurant in Bellingham, Washington. An unknown number of customers had their cardholder information stolen, and some of that data was used to run up fraudulent charges. The business owner received a Common Point of Purchase letter from an Association stating that 22 cards were used at the restaurant had subsequent fraudulent charges at other merchant locations.

IT'S NOT INCONCEIVABLE THAT A BREACH CAN PUT YOU OUT OF BUSINESS

A forensic investigation was demanded of the merchant's POS system. The business was tied up for weeks with the investigation and associated activity. The forensic team found that there had been unauthorized access to the payment application. This particular application had previously been flagged on an alert as one that improperly stores cardholder data—but the merchant was unaware of the issue.

The forensic investigation and other expenses exceeded $12,000. What's more, the restaurant's payment processor dropped the business. As a result of the unplanned expenses and the inability to accept customers' payment cards, the restaurant was out of business for several months. The owner said the cyber-attack "cost me my dream." [10]

10 Geoffrey A. Fowler and Ben Worthen, "Hackers Shift Attacks to Small Firms," The Wall Street Journal, July 21, 2011

Payment Card Data Breaches: What You Need to Know About Your Risk and Liability

What You Can Do to Protect Your Business

Now that you know you do have liability as well as risk, it's important to do what you can to protect the payment information in your possession in order to protect your business. The first step to take is to become and remain compliant with PCI DSS. If you follow these prescribed measures for data security, you'll vastly reduce your risk of a data breach, and possibly reduce your liability in the event of a breach.

The PCI Security Standards Council is the official source for everything you need to learn about PCI DSS. Some of the requirements are quite technical, so it may benefit you to consult with a security specialist to implement all the protective measures. Afterward, it's important to have an independent Qualified Security Assessor validate your PCI compliance status. Such an assessment is required annually anyway.

While the PCI DSS guidelines are quite thorough, there are additional security measures you can implement to vastly improve your security long-term. Two technologies in particular address many vulnerabilities in the payment process: encryption and tokenization.

Encryption changes card numbers from plain text information into a non-readable form called ciphertext. A software key is required to decrypt the information and return it to its original plain text format. Tokenization is the process of substituting a token (or alias) as a replacement for a real credit card number. Your merchant service provider can advise you on how to use these technologies in your payment system to greatly reduce your risk of a data breach by rendering the data in your system unreadable and unusable by cyber-thieves.

One more component of safety that is designed to help prevent the fraudulent use of cards at the POS is chip and PIN technology. Make sure you have the equipment and processing capabilities to accept the new EMV cards that issuers are beginning to distribute to their customers. These cards can generate a one-time code for each transaction, making them more secure than traditional magstripe cards.

Conclusion

As a successful merchant, you want to focus on serving your customers and expanding your business. You don't want to lose sleep over concerns about data breaches and liabilities that can harm your business.

First Data has a range of security solutions for merchants. Talk to your First Data Business Consultant today to learn about affordable, easy-to-deploy security solutions that can help protect against potential cyber attacks and secure your customers' transactions from start to finish.

First Data®

Beyond the transaction℠