First Data Market Insight

First Data
beyond the transaction

What You Can Do to Prevent a Payment Card Data Breach

A Breach of Payment Data Could Have a Significant Impact on Your Business

We understand that data security may be low on your list of priorities for your business—but it shouldn't be. A breach of payment card information is a serious situation that can not only cost your business tens of thousands of dollars, it can also impact your business in variety of ways that can be difficult to recover from.

You may not have heard about small merchants experiencing data breaches. However, while these events rarely make the news, it doesn't mean that it doesn't happen every day. Many incidents simply go unreported, but many others are discovered by third parties such as card issuers, payment associations and even law enforcement agencies.

> Data breaches "already are happening among smaller employers. It's not happening with any lower frequency than the Targets you're reading about."
>
> — **John Rose**, security expert and senior partner at The Boston Consulting Group.[1]

The fact is, your business is at risk. Small merchants are key targets to thieves who see such businesses as unprotected and easier to breach. Even though the volume of electronic payment data that passes through small merchants' POS systems is relatively small, it is the easier path for a cyber-thief who can quickly break through if the data is poorly protected.

- **A National Retail Federation study** revealed that about a million small businesses a year report being a victim of fraud.[2]
- **According to Trustwave** research, 90% of data breaches impact small merchants. A 2012 Trustwave security report indicates that Retail (45%), Food and Beverage (24%), and Hospitality (9%) are the top three compromised industries.[3]

Did you know you're liable if your business incurs a breach of payment data? Many merchants believe they have a "safe harbor" from liability if they undergo and pass a PCI assessment or audit. This simply isn't true, although compliance with PCI can help to reduce your liability.

Your business could be impacted by a payment card data breach in numerous ways:

- **Substantial fees and fines** that could potentially total in the tens of thousands of dollars or more.
- **A forensic examination** is required under PCI regulations for merchants even just suspected of having a breach to dertermine if a breach has actually occurred, and, if so, to what extent. According to Verizon Business, a small business examination may run in the range of $20,000 to $50,000.[4]
- **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.
- **The value of your reputation** and brand could decline as much as 15% to 30%[5], depending on the type of information lost. Customer confidence can make or break a business.
- **Loss of time and money** by you and your employees who will have to manage and resolve a variety of issues associated with recovering from a data breach.

[1]Heesun Wee, "How the threat of cybercrime is heightened for Main Street," CNBC, January 27, 2014
[2]Survey of small businesses conducted by First Data and the National Retail Federation, 2010
[3]Trustwave SpiderLabs, "Trustwave Global Security Report 2012"
[4]Chris Novak, Managing Principal, Verizon Business, "Crisis Data Breach Response: Computer Forensic Services"posted on August 27, 2012
[5]Ponemon Institute LLC, "Reputation Impact of a Data Breach," October 2011

What You Can Do to Prevent a Payment Card Data Breach

- **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).

Protecting electronic payment data is the responsibility of your business—not on the merchant service provider. There are four steps you can take right now to prevent a breach and protect your business.

Understand the Nature of the Data Your Business Uses

When a customer swipes a credit or debit card, or a cashier types in the account number, the data enters your point-of-sale (POS) system. The data is highly vulnerable at this stage because most often it is in plain text (i.e., not encrypted). If the data is intercepted by a cyber-thief, it can be replicated onto fake cards and used for fraudulent purposes.

> Intruders use various types of malicious software to steal cardholder data, including key loggers, packet sniffers and memory scrapers.

The card data typically gets encrypted only at the time that your POS system forwards it to your acquiring bank. From that point on it is out of your hands.

Cyber-thieves know this and they specifically target capturing unencrypted data still in your system. If they can gain entry into your POS system – which is not difficult – they can install malicious software (malware) that makes a copy of customers' account information and sends it digitally out of your business. This technique has been used in both large and small merchant data breaches. Consider this: If some of the country's largest retailers with all of their sophisticated data security resources can lose data to cyber-thieves, your business can. too.

Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals. 74% of attacks on retail, accommodation, and food services companies target payment card information.[6]

What you can do: You should never actually store or keep cardholder data. This is explicitly prohibited by PCI DSS, and you do not need this data for returns, chargebacks or any other type of transaction. You should never use real cardholder data for sales reporting, marketing analysis or any other back office purpose.

Next, you can deploy a solution that protects the sensitive cardholder data the moment it is swiped or entered. For example, First Data's TransArmor solution uses a combination of encryption and tokenization technology to protect and remove payment card data completely from your merchant environment, so your systems never hold the actual card numbers from the transactions you process. The solution removes the need for you to store card data by replacing it with a randomly assigned number, called a "token." In doing so, the TransArmor solution minimizes your risk by reducing the scope of PCI compliance, thus shifting the burden of protecting cardholder data from you to First Data.

You can use the token number, just like the actual cardholder number to manage business functions and generate sales and marketing reports. But, the token can never be used to initiate a fraudulent purchase, even if a criminal is able to steal it.

Encryption and Tokenization Work Together for Maximum Protection

Encryption is the process of using algorithmic schemes to transform plain text information into a non-readable form called ciphertext. A key (or algorithm) is required to decrypt the information and return it to its original plain text format. Encryption of either the data itself or the transmission path the data takes along the network, or both, can vastly reduce the vulnerability of the data, which in turn reduces a merchant's business risks.

In the process of tokenization, actual cardholder data is used in a payment transaction and, once the transaction is authorized, this very sensitive data is sent to a centralized and highly secure server called a "vault" where it is stored securely. At the same time, a random unique number called a token is generated and returned to the merchant's systems for use in place of the cardholder data. The vault manager maintains a reference database that allows the token number to be exchanged for the real cardholder data if it is needed again for, say, a chargeback. Meanwhile, the token number, which cannot be monetized, can be used in various auxiliary business applications as a reliable substitute for the real card data.

[6]Verizon 2014 PCI Compliance Report

What You Can Do to Prevent a Payment Card Data Breach

Follow the PCI DSS Guidelines to Secure Your Payment Environment and Maintain Continuous Compliance

The Payment Card Industry Data Security Standard (PCI DSS) was enacted in 2004 to increase merchants' controls around cardholder data to reduce credit card fraud and its exposure. Your business must validate compliance annually, typically by a self-assessment questionnaire (SAQ) even if your company handles a small volume of payments.

As of January 2014, all merchants should be following the guidelines of PCI DSS 3.0, which has 12 requirements omprised of more than 400 controls and subcontrols.[7]

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 be helpful to consult with a security specialist to implement all the protective measures that your business needs. Afterward, it's important to have an independent Qualified Security Assessor validate your PCI compliance status. Such an assessment is required annually anyway.

88.9% **of organizations** failed their PCI baseline assessment the first time around.[8]

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. This set of data security guidelines 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. In 2013, just 11.1% of all companies complied with every requirement outlined in the security guidelines.[9]

What you can do: Begin with a service like First Data's PCI Rapid Comply to verify your PCI compliance status. PCI Rapid Comply is a "help-based" web application that can be used to complete the annual SAQ quickly and easily. After you answer just a few "pre-SAQ" questions, the PCI Rapid Comply solution can direct you to the SAQ version that is right for your business and help pre-populate the appropriate SAQ questions with accurate answers. This process streamlines your self-assessment, making it easier and quicker for you to complete it with accuracy.

Additional features of PCI Rapid Comply help you maintain your PCI compliance. There is integrated and completely automated vulnerability scanning for merchants that are required to perform quarterly scans. The solution also offers a customized remediation or "fix it" plan to help identify any steps you need to take to become compliant. After achieving PCI certification, you will receive customized Information Security and Incident Response Policies based on the specific SAQ document you completed.

Don't Forget Your eCommerce Store

If you offer an online channel for customers to purchase goods and services, you must ensure the security of customers' cardholder data over the Web. As a small merchant, the best way to do this is to engage a trusted gateway service like First Data Global Gateway e4 to handle all of the work of accepting online transactions. The card data will never hit your own website, and thus it will never be a security issue for you. Business-to-consumer (B2C) e-Commerce sales are expected to reach $482.6 billion in North America in 2014.[10]

Take Small – But Critical – Measures to Secure Your Systems

Many times, data breaches happen because someone has been careless or has overlooked something simple. Check your environment and be sure you have taken care of these simple things:

- Do not use the computers that run your POS system for any other purpose, especially for checking email or "surfing the Web." These types of activities are prime vectors for allowing malware onto your computer through phishing and drive-by malware drops.
- Security researchers at McAfee Labs identified 200 new malware samples per minute, or more than three new threats every second, during 2013, with a marked upswing in point-of-sale attack vectors in the final quarter.[11]
- If you allow remote access into your business computer systems, secure it with a strong password, and absolutely do not use the default password that came with the remote access software. If you really don't need remote access, disable it completely.

[7]Thor Olavsrud, "5 Ways to Improve Your PCI Compliance Program," CIO magazine, February 27, 2014
[8]Verizon 2014 PCI Compliance Report
[9]Verizon 2014 PCI Compliance Report
[10]eMarketer, "Global B2C Ecommerce Sales to Hit $1.5 Trillion This Year Driven by Growth in Emerging Markets," February 3, 2014
[11]Finextra, "Cybercrime-as-a-service comes of age with POS hacks – McAfee," March 11, 2014

What You Can Do to Prevent a Payment Card Data Breach

- Change all of the default credentials of your POS system and other Internet-facing devices your business uses. Implement a firewall with strong access controls to protect your POS system.
- Vendor default passwords provide the easiest entry into a business system, allowing hackers to steal data and install malware.[12]
- If a third party vendor is handling any computer activities for you, ensure that your vendor is following secure practices. One of the largest retail breaches of 2013 is suspected to have originated from a third party's computers.
- Limit the number of people who have access to your POS system and make sure they are trained on security procedures.
- Buy or lease your computer equipment from reputable sources and be aware that secondhand equipment may come preconfigured with malware like a keystroke logger or memory scraper.
- Above all, focus on protecting the cardholder data under your control. Do not store the data and use encryption and tokenization technologies to protect data end to end.

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 to learn about affordable, easy to deploy security solutions that can help prevent cyber attacks and better secure your customers' transactions from start to finish. Contact your Business Consultant today to find out what First Data can do for your business.

Beyond
the transaction℠

14350 0914