First Data
beyond the transaction

First Data Market Insight

Why You Should Care about Payment Security

Introduction

Recent news stories have been filled with reports of high profile merchant data breaches and compromises of cardholder and personal information. In a confidential report to the retail and financial sector, the U.S. Federal Bureau of Investigation warned merchants to expect more cyber attacks as criminals seek to replicate the success of these attacks and exploit weaknesses in payment systems with new tools and techniques.

You may think what's going on with these attacks is far removed from your business—that your shop is too small to be of interest to cyber thieves. This kind of thinking can promote a false sense of security.

The fact is, criminals will go after whatever targets are available to them. They continually seek the path of least resistance, and see many small businesses as easy targets. Though breaches at major retail chains grab all the headlines, Visa reports that most events occur at small merchant locations. In 2011, for example, 97 percent of the payment breaches detected in the U.S. happened to small merchants, with restaurant franchises being the leading merchant category impacted.[1] Ingrid Beierly of the Cyber Security and Investigations group within Visa, Inc., warns that cyber criminals are attracted to the remote access business model that is commonly implemented at small and franchise merchant locations. Beierly says this is a contributing factor in the increasing number of cyber intrusions Visa is seeing.[2]

A National Retail Federation study revealed that about a million small businesses a year report being a victim of fraud.[3] Statistics like these don't make the news headlines because they aren't tied to tens of millions of customers being affected in a single breach, but they are serious numbers nonetheless.

Why PCI compliance is not a guarantee of security

By now, every merchant that accepts credit and debit cards knows (or should know) about the Payment Card Industry Data Security Standard (PCI DSS). It is an industry information security standard created by the leading card brands to increase protection of cardholder data 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, achieving PCI DSS compliance is not a guarantee that your shop will be immune to a breach—especially as threats grow ever more sophisticated. Many retailers that have validated PCI compliance have still suffered a data breach.

Beyond
the transaction℠

Why You Should Care about Payment Security

If PCI compliance is not a guarantee of payment data security, why make the effort and incur the expense? First, non-compliance is not an option if you want to continue to accept the major brands of credit and debit cards for your customers' convenience. More importantly, adherence to the recommended security guidelines is an ongoing process designed to minimize your risk of a data breach. As the forms of data compromise become ever more sophisticated, it becomes more difficult for an individual merchant to stay ahead of the vast array of threats. The PCI DSS continues to evolve to guide retailers in putting in place the most appropriate measures to protect their businesses against the evolving threat landscape.

A breach is costly in many ways

For any size retailer, a data breach is costly in many ways. The most obvious losses are financial in nature. The cost of a data breach for a Level 4 merchant (i.e., with less than 1 million card transactions annually) averages $36,000 and can reach or exceed $50,000.[4] If your business were to suffer a breach, your actual cost would be determined by factors such as:

- **Notification of customers** – Most states require that the state attorney general as well as customers be notified if their financial information may have been compromised in a data breach. Depending on the number of customers and their locations, the process of sending notifications may cost thousands of dollars.
- **Credit monitoring for affected customers** – You may be required to provide up to a year's worth of credit monitoring services to customers affected by your breach.
- **A mandatory forensic examination** – The regulations of PCI DSS require that a merchant that is even suspected of having a data breach undergo a forensic examination to determine if a breach has actually occurred and, if so, to what extent. This examination can last several days and may require the shutdown of your POS during that time.
- **Card replacement costs** – Card issuers may require that you pay the cost of reissuing debit and credit cards of those customers whose data has been compromised. These fees can range from $3 to $10 per card.
- **PCI compliance fines** – The card associations may levy fines against your business, depending on the nature of the offense that led to the breach, and whether or not the cards have been used in actual fraud cases. Such fines for small merchants can range from $5,000 to $50,000 or more.
- **Liability for fraud charges** – Many merchants assume they have no liability for the fraudulent use of payment cards after a data breach. This is not necessarily the case; lawsuits may impose liability on your business under certain circumstances. Your regular business insurance would not necessarily cover this type of liability (check with your insurance provider to determine exact coverage limitations).

Your reputation is at stake

The direct costs outlined above are just the start; the ensuing loss of reputation and loss of customer trust can be quite damaging as well.

In a Ponemon Institute study on measuring the loss of brand and business reputation after a data breach, 76 percent of the executives whose companies had experienced a customer data breach said the event had a significant or moderate impact on the business' reputation. What's more, it can take a year or longer to restore reputation and brand image after a breach.[5] Can your business sustain a year of business drop-off due to a bad public image? Many small merchants in this situation could not survive.

Why You Should Care about Payment Security

Consumers absolutely do expect you to protect their financial data. In a recent poll of American shoppers, 88 percent of the 1,060 people surveyed place the burden of protecting the data on retailers who are collecting it.[6] Consumers who use their payment cards at your establishment place a high level of trust in your business, and that trust can be broken with just one breach event.

If you experience a breach, credit and debit card companies such as Visa®, MasterCard®, American Express® and others can refuse to do further business with you. Are you prepared to have a cash-only business? How many of your customers would reduce the value of their ticket or take their business elsewhere if they can't use their payment cards?

Conclusion

There are numerous reasons why you should care about payment security. Probably the top reason is to preserve the integrity and viability of your business. A data breach has the potential to do costly or even irreparable harm to a small merchant.

Electronic payment systems can be complex but securing them doesn't have to be. Today there are so many resources and innovative solutions to help you bolster your payment card security. The first step is recognizing that your business can be vulnerable to a breach, even if you have passed a PCI compliance assessment or audit. The next step is to discuss your business specifics with your merchant acquirer.

First Data partners with merchants of every size to mitigate possible cyber attacks and secure consumers' transactions from start to finish. First Data has the expertise and innovative solutions to keep your business protected and to ensure PCI compliance. Click here to learn more about First Data's security and compliance solutions or contact your Business Consultant today to find out what First Data can do for your business.

Why You Should Care about Payment Security

Sources

1. Ingrid Beierly, Sr. Business Leader, Cyber Security and Investigations, Visa, Inc., "Cardholder Data Compromise Trends and Security Best Practices," June 2012
2. Ibid.
3. Survey of small businesses conducted by First Data and the National Retail Federation, 2010
4. Robert Halsey, "The Real Cost of Data Breach," published on www.PCIcomplianceguide.org, April 2009
5. "Reputation Impact of a Data Breach," U.S. Study of Executives & Managers, Ponemon Institute Research Report, Sponsored by Experian Data Breach Resolution and independently conducted by Ponemon Institute LLC, November 2011.
6. Associated Press – GfK poll of American consumers, January 17, 2014

Beyond the transaction℠

9254 0314