HOW TO PROTECT YOUR BUSINESS AND YOUR CUSTOMERS FROM DATA FRAUD

ABOUT VISA USA

Visa USA is a leading payments brand and the nation's largest payments system, enabling banks to provide their consumer and business customers with a wide variety of payment alternatives tailored to meet their evolving needs. Visa USA is committed to increasing the choice, convenience, acceptance and security of Visa payments for all stakeholders—financial institutions, cardholders and merchants. In the United States, more than 521 million Visa-branded cards have been issued by our 13,320 financial institution customers. Visa products generated nearly $1.8 trillion in total volume in the United States through March 2007 and enjoy unsurpassed acceptance around the globe. For more information, visit www.visa.com.

Risky Behavior

A survey by NFIB, conducted in partnership with Visa USA, found that most small businesses are engaging in activities that could put their customer information at risk.

37% of card-accepting businesses knowingly store customer card numbers

24% store customer Social Security numbers

28% store customer bank account numbers or copies of their checks

52% keep at least one of these sensitive pieces of information

57% don't see securing customer data as something that requires formal planning

61% have never sought out information about how to properly handle and store customer information

PROTECTING DATA IS GOOD BUSINESS

What's at Stake?

Few business owners can also claim to be security experts. However, with high-tech fraudsters growing ever-more sophisticated, it's important to clearly understand the nature of the threats that face us and take the necessary steps to protect our businesses and our mutual customers.

Indeed, as a small-business owner, you take all the necessary precautions to protect your storefront. But did you know that criminals are seeking more than what's physically inside your business? Increasingly, they also want to rob your customers of their financial data. Leaving customer and employee data unprotected is like locking your jewelry in a safe but leaving the combination on top.

Data is the currency most coveted by criminals today. Whether the target is payment card information, Social Security numbers or personnel files, data theft is a full-time occupation for a new breed of criminal. Small businesses are now being targeted by these sophisticated and relentless criminals, who may be operating from down the street or half a world away.

When security is breached, thieves rob your business of its reputation and steal your customers' trust. In fact, a March 2007 survey by Javelin Strategy & Research found a strong link between a consumer's perception of a retailer's reputation for protecting card account information and the consumer's willingness to shop there. Only 20 percent surveyed said they would likely continue shopping at a store if they learned it had a data breach that may have compromised their card account information, while 78 percent said they would be unlikely to continue to shop there.

Besides the loss of customer goodwill, a breach may result in unflattering media headlines, fines from merchant banks or government regulatory agencies, or exposure to potential litigation.

Rank Your Risk Level: Four Simple Questions

1. Do you accept payment cards through a computer-based payment application or an application that is directly connected to the Internet (as opposed to a stand-alone dial-up terminal)?
2. Do you have multiple systems connected to your payment application, and do any of them have Internet access?
3. Do you use wireless Internet access at your business?
4. Does your business have an e-commerce component?

ARE YOU A TARGET?

Gauge Your Risk for Data Fraud

Your risk exposure depends on the way you operate your business. If you answered "yes" to any of these questions to the left, it's time to get smart about your company's data security practices. However, even if you answered "no" to all of these questions, your business may still be vulnerable to data thieves. Visa has developed a list of four key vulnerabilities that small businesses should be aware of to help ensure they won't be victimized by fraudsters:

1 Storing Magnetic Stripe Data (and other sensitive data)

The magnetic stripe on the back of payment cards contains two tracks of encoded payment data, also called "track data," that could be used by thieves to create counterfeit cards and commit other forms of fraud. This sensitive cardholder data from the magnetic stripe is received by point-of-sale (POS) systems when a merchant swipes a payment card. POS systems often store this sensitive data post-authorization without the small business owner's knowledge, in violation of Visa rules.

In addition to magnetic stripe data storage, Visa has also observed compromises involving other prohibited-to-store data, such as the CVV2 value and PIN data. CVV2 is the three-digit number on the signature panel on the back of the card used for telephone and e-commerce transactions. The PIN is entered by a consumer for debit transactions, and encrypted PIN blocks are created by the PIN Entry Device for debit transactions.

2 Missing or Outdated Security Patches

Hackers are constantly attempting to exploit known software vulnerabilities, as well as uncover unknown deficiencies in commercially available software products. Product vendors respond with frequent fixes in the form of software updates or patches. It's crucial that all relevant software updates or patches be applied as soon as possible to minimize the risk of compromise.

3 Vendor-Supplied Default Settings and Passwords

Hardware and software products come packaged from vendors with preset passwords and settings. Default passwords and settings are easily guessed and often are well publicized in hacker chat rooms. Once an attacker accesses one of these systems, security mechanisms can easily be turned off, databases can be accessed, and any evidence of an intrusion can be eliminated.

4 Uncontrolled Access to Sensitive Customer Information

Small-business owners face the threat of sensitive customer data simply walking off. Data files, paper files and laptops are all portable. Without controls in place, this information can quickly disappear.

TAKE ACTION TO PROTECT YOUR BUSINESS AND YOUR CUSTOMERS

It's smart business for you to invest the time and resources necessary to protect payment card data and other sensitive customer information. At stake is nothing less than your good name and the trust your customers place in you and your business. Several studies have indicated that the costs associated with mitigating a data breach far exceed the costs of sound security investments.

Waiting on the sidelines is not an option. Since June 2001, Visa USA's Cardholder Information Security Program (CISP) has been mandated for all merchants and service providers that store, process or transmit Visa cardholder data. Under CISP, Visa enforces compliance with the industry-wide Payment Card Industry Data Security Standard (PCI DSS), which enables members and merchants to implement a single security program across all payment brands. Outlined below are the key security standards as well as details particularly relevant to you as a small-business operator.

Know and Comply with PCI DSS. If you accept card payments, you must comply with the PCI DSS, which sets requirements for protecting sensitive transaction information. The standard, supported by major payment card brands, has been in place since 2004 and provides effective tools to protect against cardholder data exposure and compromise. It consists of 12 basic requirements for safeguarding account data, supported by more detailed sub-requirements. (See chart on page 7.) You can find the PCI DSS in its entirety or learn more about the CISP at www.visa.com/cisp.

Validate Your PCI Compliance. In addition to adhering to the PCI DSS, your business may also have to validate its compliance with the standard. Validation requirements are determined by a merchant's Visa transaction volume over a 12-month period. Most small businesses are considered a Level 4 category. For more information about validation requirements for small businesses, consult your bank or see www.visa.com/cisp.

Prioritize Your Approach to Cardholder Data Security. Consider the risk-prioritized steps on the following pages: 1) eliminate prohibited data, 2) protect stored data and 3) secure the environment in accordance with the PCI DSS.

STEP 1 Eliminate Prohibited Data

Check Your POS Systems. Small businesses that use commercially available POS systems or payment software should contact their vendors to determine whether the systems they use store prohibited data after transaction authorization.

- Ask your POS or payment software vendor (or reseller/integrator) to confirm that your software version does not store magnetic stripe data, CVV2, PINs or encrypted PIN blocks. If it does, these data elements must be removed immediately, including any historical data that has been stored in database or log files.

- Ask your payment software vendor to share a list of files written by the application and a summary of the contents of those files to verify prohibited data is not stored.

- Confirm with your payment processor that all cardholder data storage is necessary and appropriate for the transaction type.

- Verify that your POS software version has been validated as compliant with the Visa Payment Application Best Practices (PABP) program. Visa created the PABP program to facilitate compliance with the PCI DSS by establishing minimum standards for payment applications. A list of PABP-compliant applications is available at www.visa.com/pabp.

Minimize Data Storage. It is permissible to store the following data from the magnetic stripe: cardholder's name, primary account number, expiration date and service code. These values, which should only be stored if needed, must be protected in accordance with the PCI DSS. Small businesses can limit the damage from a compromise by not storing magnetic stripe data, CVV2 and PIN blocks. Small businesses can also decrease their risk by only storing cardholder data if it is needed to perform business functions. If you don't need it, don't store it!

STEP 2 Protect Stored Data

Encrypt or Truncate Your Data. Small businesses should evaluate whether they must retain full account numbers after a transaction has been authorized. In many cases, small businesses may be able to fulfill their business requirements on some or all of their systems by retaining only a truncated portion of the account number, such as the first six and last four digits. Small businesses that must electronically store full account numbers for business needs must render the account number unreadable through other means, such as encryption. Additionally, account numbers transmitted over public networks, such as the Internet or wireless, must be encrypted during transmission using technology such as SSL.

STEP 3 Secure the Environment

Replace Missing or Outdated Security Patches. When it comes to updating security patches, speed is the name of the game. Many vendors now offer automated alert services that provide prompt notification to their clients. Some vendors also provide automated patching mechanisms. If a patch cannot be applied immediately, other controls to reduce this risk should be implemented, and monitoring of all affected systems should be increased. Small businesses should establish software upgrade policies and procedures to ensure patches are reviewed and installed in a timely manner.

Check Your Settings and Passwords. Hardware and software products come packaged from vendors with preset passwords and settings. Any default or blank settings and passwords should be changed prior to deployment. Passwords should comply with current industry standards for storing passwords. Any default settings should be modified immediately.

Prevent Employee Fraud Scams. Your business policies should be designed to prevent fraud scams involving collusive employees. As part of this, physical access to information, whether it resides in a computer or a file drawer, should be restricted. Only those employees with a business need should be permitted access. Whenever possible, account numbers should be encrypted or scrambled during transaction processing. Unauthorized electronic equipment—such as personal laptop computers—that can be used to steal or replicate account information should not be allowed in the workplace.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

BUILD AND MAINTAIN A SECURE NETWORK	1 **Install and maintain a firewall configuration** to protect data 2 **Do not use vendor-supplied defaults** for system passwords and other security parameters
PROTECT CARDHOLDER DATA	3 **Protect stored data** 4 **Encrypt transmission of cardholder data** and sensitive information across public networks
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	5 **Use and regularly update** anti-virus software 6 **Develop and maintain** secure systems and applications
IMPLEMENT STRONG ACCESS CONTROL MEASURES	7 **Restrict access** to data based on business necessity 8 **Assign a unique ID** to each person with computer access 9 **Restrict physical access** to cardholder data
REGULARLY MONITOR AND TEST NETWORKS	10 **Track and monitor** all access to network resources and cardholder data 11 **Regularly test** security systems and processes
MAINTAIN AN INFORMATION SECURITY POLICY	12 **Maintain a policy** that addresses information security

HELPFUL RESOURCES

While small businesses often lack in-house support for securing their customers' private information, there are many online resources available to help.

For more information on Visa's Cardholder Information Security Program (CISP) and the Payment Card Industry Data Security Standard (PCI DSS), visit www.visa.com/cisp.

The Payment Card Industry Security Standards Council (PCI SSC) provides a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. To learn more and see how your business can contribute to the effort, visit www.pcisecuritystandards.org.

For a list of POS payment applications compliant with Payment Application Best Practices, go to www.visa.com/pabp.

Not every small-business owner can be a security expert. Outside vendors can help. See the "Resources" page at www.pcisecuritystandards.org.

To learn more about ways your business can strengthen its data security practices, e-mail Visa at AskVisaUSA@Visa.com.

SIMPLE STEPS TO SAFEGUARD CONFIDENTIAL BUSINESS INFORMATION

Apply These Simple Steps Today

In addition to complying with the card companies' data security requirements, small-business owners should take precautions to safeguard all types of sensitive business and customer information:

Empty the mailbox. Never leave outgoing or incoming mail in pickup boxes overnight. This is your best defense against possible off-hour mail snoops.

Watch the fax. A document sitting on the fax waiting for pickup is an open invitation for prying eyes. Try to stand by the fax machine to receive sensitive information as soon as it comes in.

Send e-mail sparingly. When sending sensitive information via e-mail, encrypt it first—or don't send it at all. There's always the possibility of interception or an accidental electronic distribution.

Make copies carefully. Private matters can go public fast when juicy stuff gets left behind. When making copies of sensitive documents, remember to grab your originals off the copy machine.

Use the shredder. Always shred sensitive information before dumping it in the trash bin. If you can't shred, use receptacles designed for sensitive paper disposal.

Leave discreet voice-mail messages. You never know who's standing within earshot of someone's work area, so avoid leaving a detailed voice-mail message if it involves sensitive information.

Protect your onsite ID. Play it safe with your ID badges, office keys and building-entry codes. Protect them as you would your own credit cards and cash.

Keep things private in public. When you're in a public place, think twice before discussing proprietary information or any details about sensitive projects. You never know who's listening.

Identify strangers. Don't make it easy for an outsider to pull an inside job. If you see an unfamiliar face roaming around your office, step up and ask if you can assist. Make your presence known.

Be careful with your documents. Remove all sensitive materials from your work area when you're not using them or at the end of the day. Be sure to lock them in the appropriate file cabinets, desk drawers, etc.

Note what's on your screen. Those account numbers and financial details on your computer screen are intended for your eyes only! To keep it that way, use a glare screen to minimize easy information access.

Limit cell phone conversations. Anyone can listen in on your cell phone conversations. All it takes is a good ear and a decent scanner. Avoid sharing any sensitive information over a cell phone.