Visa Data Security

Tips and Tools for Small Merchant Businesses

Protect Your Cardholder Data, Your Customers, and Your Business

Consumer trust in the security of sensitive information is more critical than ever. When customers hand you their Visa payment card or provide you with their account information, they expect you to safeguard that data. Keeping that trust is essential to fraud reduction and customer service.

1. **Don't store any cardholder data that is not needed to run your business.** Ask your merchant processor if you can use alternative data, rather than the full cardholder account number to respond to chargebacks and other customer inquiries.
2. **Ensure all printed copies containing full cardholder account number (paper receipts, orders, invoices, etc.) are physically secured.**
3. **Know who has access to your business computers, including any vendors who may need to connect to it remotely for maintenance purposes.** If you use vendors that have access to your customers' data, make sure they are protecting that information.
4. **Destroy any physical or electronic records containing full cardholder account numbers when it is no longer needed for business purposes.** Take the necessary steps to destroy it responsibly.
5. **If you use a computer at your business to handle cardholder data or facilitate payment card transactions, make sure you have an anti-virus program installed and it is updated regularly.** If possible, do not use your computer for any function that is not business-related. This includes web surfing or accessing web-based e-mail accounts.

Maintain a Solid Front-Line Defense Against Data Theft

If you are a merchant who . . .

. . . uses a standalone, dial-up terminal:

- Ensure both the customer receipt and your merchant receipt do not include the full account number or expiration date.
- Work with your merchant processor to program the terminal to only show the last four digits of the account number and to hide the expiration date.

. . . uses an IP-based terminal, wireless terminal, or payment application connected via the Internet:

- Make sure your Internet connection has a firewall installed. This firewall must be properly configured so that it does not allow any unauthorized computer access or traffic.
- Have an Approved Scan Vendor perform network vulnerability scans on your Internet connection at least every three months. You can check with your merchant processor to learn if they have a preferred vendor they would like you to use to perform the scans.

. . . uses a payment application connected via the Internet:

- Ask your payment application vendor or merchant processor if the payment application you are using is compliant with the Payment Application Data Security Standard (PA-DSS). You may also check the website — *https://www.pcisecuritystandards.org/security_ standards/vpa/* — to learn if the payment application has been validated against this standard. If the payment application is not PA-DSS compliant, it may need to be upgraded.
- Make sure you have installed anti-virus and anti-malware programs on any computer system that contains your payment applications. Update these programs regularly.
- Change any IDs and passwords supplied by the payment application vendor to ones that are unique and hard-to-guess.
- Create a unique ID and hard-to-guess password for every employee accessing the computer system and/or the payment application.
- If you have vendors that access your computer systems remotely, ensure they are using secure access protocols and they are protecting any data within their control.

. . . accepts card-not-present transactions (mail order/telephone order/fax order/e-mail order/internet order):

- Do not store the three-digit number on the back of Visa payment cards (CVV2) in any format.
- Do not request the CVV2 number on mail-order forms or billing forms.

Who's Doing What to Safeguard Data in the Payment System?

All participants in the payment system play a major role in upholding the highest information security standards and protecting Visa cardholder data, wherever it resides.

ROLE	RESPONSIBILITY
Visa Is a card brand that is accepted at merchants around the world who display the Visa logo.	• Works with merchant banks to ensure merchants and service providers protect cardholder data according to the Payment Card Industry Data Security Standard (PCI DSS). • Manages the Account Information Security (AIS) Program, formerly known as the Cardholder Information Security Program (CISP) in the U.S. to drive PCI DSS compliance.
A **Merchant Bank** (also known as acquiring bank) is a financial institution that establishes accounts for merchants, allowing the merchants the ability to accept payment cards.	• Ensures a merchant is PCI DSS compliant. • Establishes the compliance validation requirements for their Level 4 merchants*, including direct receipt of any validation documentation from the merchant.
An **Independent Sales Organization (ISO)** is a third-party agent that partners with merchant banks to establish and manage merchant accounts on behalf of the merchant banks. ISOs may also be referred to as merchant service providers when they offer financial transaction processing services.	• May also manage PCI DSS compliance programs on behalf of the merchant bank and establish the compliance validation requirements for their Level 4 merchants.
A **Merchant** is a seller of goods or services that agrees to accept Visa payment cards.	• Protects cardholder data according to the PCI DSS.
A **Third-Party Agent/Service Provider** may offer processing services, fulfillment services, loyalty programs, call center services, etc.	• Must be registered as a Third-Party Agent of Visa. • Must be PCI DSS compliant. • Validated Level 1 service providers are listed on Visa's Global List of PCI DSS Validated Service Providers.
The **Payment Card Industry Security Standards Council (PCI SSC)** is an independent organization that maintains responsibility for management of payment card industry security standards including the PCI Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), PIN Transaction Security (PTS).	• Manages and maintains the tools merchants and service providers use to validate compliance with the security standards, including Self-Assessment Questionnaires (SAQ) which are used by many small merchants to validate PCI DSS compliance. • Answers questions regarding the SAQs and intent of the standards. • Manages the Qualified Security Assessor (QSA) Program. • Manages the Approved Scan Vendor (ASV) Program.
A **Qualified Security Assessor (QSA)** is a third-party security company approved by the PCI SSC to provide compliance validation and data security consulting services.	• Provides independent security assessments of a company's cardholder data processing environment. • May contract with merchant banks or ISOs to provide data security compliance programs, education and customer support.
An **Approved Scan Vendor (ASV)** is a third-party security company approved by the PCI SSC to perform network vulnerability scans.	• Performs network vulnerability scans according to the PCI DSS requirements.

* Visa defines Level 4 merchants as those who process less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually.

Link and Learn More About Visa Cardholder Data Security

For quick and easy access to Visa data security tools for merchants, visit the Visa Data Security website at ***www.visa.com/cisp***. Here, you'll find a list of the most current resources available for download, including the following:

- Visa PCI DSS Data Security Compliance Program Overview
- Visa's Business Guide to Data Security
- Global List of PCI DSS Validated Service Providers
- Visa List of PABP Validated Payment Applications
- What To Do If Compromised
- Responding To A Data Breach
- Alerts, Bulletins, Best Practices, Third Party Media Articles and Webinars

To find out more about PCI DSS requirements, check out these additional websites:

Visa and the Better Business Bureau's national education initiative to help small businesses address data security	*http://www.bbb.org/data-security/*
PCI Security Standards Council	*https://www.pcisecuritystandards.org/index.shtml*
Qualified Security Assessors (QSAs)	*https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf*
Approved Scan Vendors (ASVs)	*https://www.pcisecuritystandards.org/pdfs/asv_report.html*
List of Validated Payment Applications	*https://www.pcisecuritystandards.org/security_ standards/vpa/*