VISA DATA SECURITY

TIPS AND TOOLS FOR
E-COMMERCE BUSINESSES

PROTECT YOUR DATA, CUSTOMERS & 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 growing your business.

5 THINGS TO REMEMBER

> *The choices you make when building your e-commerce website will determine your risk exposure as well as costs and efforts necessary to protect your business and your customers.*

1. **Don't store any cardholder data that is not needed to run your business.** Never store card verification value (CVV2, a three digit code on the back of card) after authorization and if you require Primary Account Numbers (PAN), ensure these are truncated or encrypted.
2. **Don't use generic or default passwords** that were provided by a vendor for payment application, web server or database administrator accounts and insist that strong and unique passwords are used by third parties installing or accessing your systems.
3. **Restrict the use of remote access to your systems**. If remote connectivity is required, secure remote access by turning it on only when needed, ensure that two factor authentication is used and all remote access is logged.
4. **Train employees on security basics.** Employees can be the weakest link in an organization. Establish data security policies and procedures and ensure that you provide training at least annually. Check SANS Institute for additional information and resources https://www.sans.org/security-resources/policies.
5. **Shop and compare!** Ensure that you are not receiving a discount at the cost of poor security. Use only service providers that validate compliance with the Payment Card Industry Data Security Standard (PCI DSS). Check Visa's Global Registry of Service Providers or request a compliance report directly from the entity.

IF YOU ARE A MERCHANT WHO . . .

. . . USES A FULLY MANAGED HOSTED SOLUTION

RISK
HIGHER
MEDIUM
LOWER

This is considered to be a solution with lower risk and is recommended for smaller e-commerce businesses with little or no IT knowledge or support.

You have only one service provider that offers comprehensive services including web hosting, website builder/ templates and an integrated shopping cart. Card details are entered on a service provider's payment page and you, as a merchant, do not capture, process or store card data on any of your systems.

! Ensure that the e-commerce service provider has validated PCI DSS compliance. Choosing a non-compliant service provider can put your business and your customers' data at risk. When contracting with a third party always ensure that security responsibilities are clearly defined in the service level agreements.

. . . USES CUSTOM-DESIGNED AND/OR “OFF THE SHELF” PRODUCTS

RISK
HIGHER [✓ MEDIUM] LOWER

Managing relationships with several parties requires more security consideration and due diligence. This set up may be considered a lower risk option as long as you use a redirected hosted payment page (payment page is hosted by a third party) with a PCI DSS validated provider and none of your applications (e.g. shopping cart) captures or stores card data.

You chose different providers and vendors for the various components of the e-commerce business: web hosting, website development, shopping cart and payment processing solutions. You may either buy “off the shelf” products or have systems custom built by a web developer.

- Keep your software up to date and ensure that any security patches are regularly applied. Enable automated updates where available and schedule monthly checks for all systems and applications where a manual download is required. Ensure that any vendor or supplier commits to making critical security updates when these are released.
- Verify if any of the applications, e.g. shopping cart, captures or stores card data. Use automatic card data discovery software to verify that no card data is accidently stored. All “off the shelf” applications that store, process or transmit cardholder data as part of the authorization or settlement of a payment card transaction must be compliant with the Payment Application Data Security Standard (PA-DSS). A list of validated payment applications can be found at PCI SSC website.
- Perform regular checks to confirm that the code that redirects customers to the payment page is the same as supplied by the service provider and has not been tampered with or modified.
- If using custom built software, ensure that it is correctly coded to prevent common vulnerabilities such as SQL injections.
- Have an approved vendor conduct an external vulnerability scan at least quarterly and after any significant change in the network or website and fix any vulnerabilities that have been identified. The PCI List of Approved Vendor Scanning companies can be found at PCI SSC website.
- Make sure that your web hosting company and payment gateway/payment service provider continuously validate PCI DSS compliance.

. . . CAPTURES CARD DATA ON YOUR WEBSITE

RISK
[✓ HIGHER] MEDIUM LOWER

This solution is considered higher risk and is not recommended for merchants that have limited IT and information security knowledge or resources.

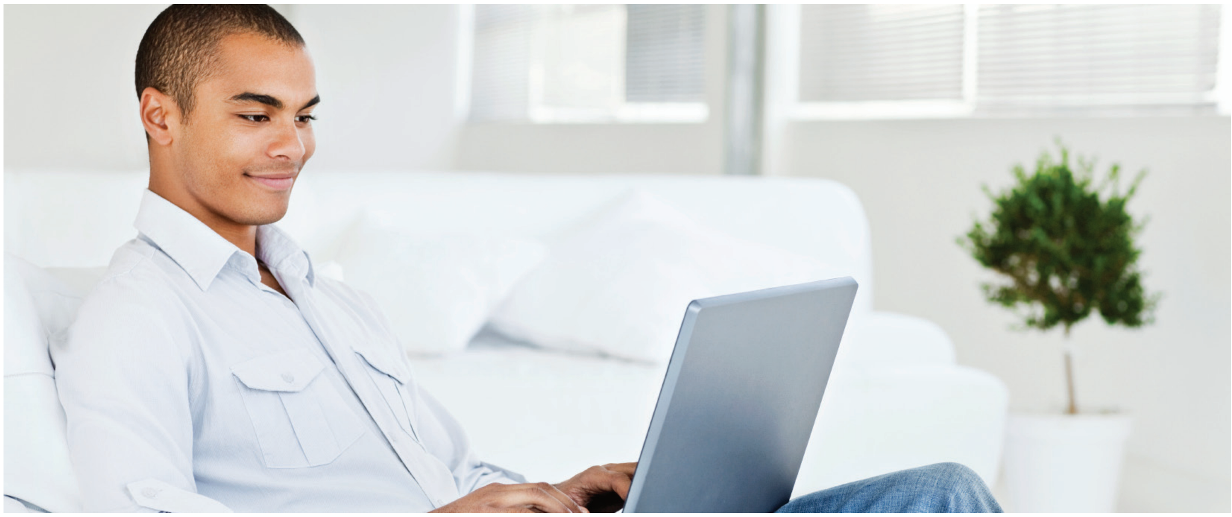
Customers enter card data on your website and transactions are processed either by entering card numbers into a standalone card terminal, web-based entry facility, or by using a payment application that is integrated within your website.

- Make sure that you only keep data that is needed to run the business. Use automatic card data discovery software to verify that no card data is accidently stored. If you require account numbers, use truncation (displaying only the first 6 and last 4 digits) or strong encryption to protect it.
- Securing the web server is critical. Hosting a site on your own requires significant data security expertise, e.g. professionally trained security and computer forensic professional. Consider outsourcing to a PCI DSS validated service provider if you don’t have appropriate resources.
- Keep your software up to date and ensure that any security patches are regularly applied. Enable automated updates where available and schedule monthly checks for all systems and application where manual download is required. Subscribe to a security alert service such as http://www.us-cert.gov/cas/techalerts/ to ensure that major security events are recognized the day they are known, and addressed immediately.
- Install a web application firewall. Web application firewalls can prevent the exploitation of vulnerability in a website by blocking the malicious request and can prevent SQL injection attacks.
- Configure firewalls to allow access to restricted services only from designated IP addresses. Ensure that the payment environment is separate from the rest of the network. Consider using a managed firewall service provider that provides ‘round the clock’ monitoring services.

For More Information
Visit the Visa
Data Security website at
www.visa.com/cisp

[continued]

Every merchant must comply with PCI DSS. Visit PCI Security Standards Council website or contact your acquirer for further details.



. . . CAPTURES CARD DATA ON YOUR WEBSITE [CONTINUED]

RISK
HIGHER
MEDIUM
LOWER

- Have an approved vendor conduct an external vulnerability scan at least quarterly and after any significant change in the network and fix any vulnerabilities that have been identified. The PCI List of Approved Vendor Scanning companies can be found at PCI SSC website.

- Use encrypted communication protocols such as SSL, SSH, and SFTP to ensure that customer data and employee passwords are protected when in transit.

- Enable remote access only as and when required and ensure that two factor authentication is used and all remote access is logged. Never allow the use of a shared password to impair your ability to match system activities with the specific individuals.

- Hire an independent assessor on a periodic basis to evaluate the overall security program at your company and ensure that all systems and business practices are designed to prevent theft and fraud.

GLOSSARY

Card discovery tools software	Automated tool that scans systems and connected networks for the presence of account data.
Merchant Bank (Acquirer)	Financial institution that establishes accounts for merchants, allowing the merchants to accept payment cards. Also responsible for ensuring a merchant is compliant with the PCI DSS.
Shopping cart	Software that enables customers to select goods, add them to a virtual shopping basket before proceeding to check out and payment. It can be bought as an "off the shelf" product or custom built by a web developer.
SQL (Structured Query Language) injection	SQL injection is one of the most frequently seen attack vectors in e-commerce environments. It is a technique used to exploit web-based applications and websites integrated with a database that uses user-supplied data in SQL queries. SQL injection attacks can occur as a result of unpatched web servers, improperly designed websites and applications, or poorly configured web and database servers. You can find more information on SQL attacks and mitigation strategies on www.visa.com/cisp.
SSL (Secure Socket Layer)	Protocol that allows secure communication between customers entering details on the website and the web or database server.
The Payment Card Industry Security Standards Council (PCI SSC)	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). The PCI SSC: ▪ 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 ▪ Manages the Qualified Resellers and Integrators (QRI) Program
Visa's Global List of PCI DSS Validated Service Providers	Visa maintains a list of PCI DSS validated service providers. Merchants should use this list as a point of reference whenever contracting with a third party, including web hosting company, payment gateway, or payment service provider. If an entity is not listed, merchants should confirm compliance directly with the entity.
Web hosting provider	A third party that allows a merchant's website to be accessible via the World Wide Web (usually by providing space on a web server, data base server, and internet connectivity).

ADDITIONAL INFORMATION AND RESOURCES

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/

SANS Institute http://www.sans.org

Visa Data Security website at www.visa.com/cisp

Visa's Global Registry of Service Providers http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf