

A decorative graphic consisting of a white square with a yellow swoosh on the top left and a blue swoosh on the bottom right, positioned to the right of the main title.

Global Visa Card-Not-Present Merchant Guide to Greater Fraud Control

Protect Your Business and Your Customers with
Visa's Layers of Security





Millions of Visa cardholders worldwide make one or more purchases every day online, over the phone, or through the mail—where there is no card available.

For Visa® merchants who operate in the card-not-present environment, there are a large number of opportunities to enhance customer relationships, attract new customers, and increase sales revenue. There are, however, some additional fraud risk challenges. Card-not-present merchants are perfect targets for payment card scams simply because there's no face-to-face customer contact, no tangible card, and no physical signature on the sales draft.

Today's scam artists are savvy. They understand the payment structure and the security processes involved with each type of transaction. They're constantly coming up with different ways to circumvent the system, and they are always on the look out for vulnerable merchants who are susceptible to fraud.

Whether you are a merchant who does business online, over the phone, or through the mail, security should be a top priority. That's why Visa has developed a "layered approach to security" in the card-not-present environment. This approach offers both merchants and consumers multiple security checkpoints. When you accept Visa cards for payment, you have access to a variety of services* that can help you prevent fraud and ensure that you and your customers are better protected.

With tools like Verified by Visa® (VbV), Card Verification Value 2 (CVV2), Address Verification Service (AVS), CyberSource Advanced Fraud Screen (AFS) enhanced by Visa, and the Payment Card Industry (PCI) Data Security Standard (PCI DSS), you can be confident that your business is offering the highest level of protection to your customers when they make online, phone or mail order purchases from you. To reduce exposure to fraud risk and minimize associated losses, you need to start with the right combination of fraud prevention and detection tools and controls.

*Service availability varies by region. To learn more about the tools and business practices covered in this document, consult with your merchant bank. The information contained in this document is intended only as a reference for merchants and is not a definitive set of instructions.

Notice: The information furnished herein by Visa is CONFIDENTIAL and shall not be duplicated, published, or disclose in whole or part, or used for other purposes, without the prior written permission of Visa.

What Is A Layered Security Approach for Card-Not-Present Merchants?

Visa fraud prevention and detection tools are designed to compliment each other and work together as multiple services that can help merchants better combat fraud.

- **Address Verification Service (AVS)** verifies the credit card billing address of the customer who is paying with a Visa card. The merchant includes an AVS request with the transaction authorization and receives a result code (separate from the authorization response code) that indicates whether the address given by the cardholder matches the address in the issuer's file. A partial or no-match response may indicate fraud risk.
- **Card Verification Value 2 (CVV2)** is a three-digit code that is printed on the signature panel of all Visa cards. Telephone order and Internet merchants use CVV2 to verify that the customer has a legitimate Visa card in hand at the time of the order. The merchant asks the customer for the three-digit code and sends it to the issuer as part of the authorization request.
- **Verified by Visa (VbV)** offers an extra level of security for online transaction authentication. It is an innovative service that verifies cardholder identity in real-time so customers can shop more confidently. Also, Internet merchants can accept Visa cards with peace of mind while authenticating a cardholder's identity at the time of purchase.
- **CyberSource Advanced Fraud Screen (AFS) enhanced by Visa** is designed for Internet merchants who want to use third-party screening. It is an effective fraud-screening program that suspends processing if a transaction:
 - Matches data stored in the merchant's internal negative files.
 - Exceeds velocity limits and controls.
 - Generates an AVS mismatch or CVV2 no match.
 - Matches other high-risk attributes (customized by the merchant).
- **The Payment Card Industry (PCI) Data Security Standard (DSS)** is intended to help protect Visa cardholder data—wherever it resides—ensuring that customers, merchants, and service providers maintain the highest information security standard. As mandated by Visa, all issuers, merchant banks, agents, merchants, and service providers that store, process, or transmit cardholder data are required to comply with PCI DSS.



The Right Combination of Tools at the Right Time

The chart below highlights Visa's layers of security by business type.

Merchant	VbV	CVV2	AVS	AFS	PCI DSS
Internet	✓	✓	✓	✓	✓
Telephone Order		✓	✓		✓
Mail Order			✓		✓

Other Fraud Prevention Solutions

Third party vendor fraud prevention solution providers offer a combination of leading technology and innovative tools for detection and prevention of fraud within the various card-not-present channels. These solutions are designed to help merchants protect their customers and brand by reducing fraud losses and making the Internet a safer place to conduct business. To obtain a list of third party fraud prevention solution providers, contact your merchant bank.

Fraud Prevention for Card-Not-Present Merchants: Start-to-Finish

Mail order/telephone order, and Internet merchants must verify—to the greatest extent possible—the cardholder’s identity and the validity of the transaction. **Basic fraud control actions include these key actions:**

- **Obtain an authorization.** Avoid using a \$1 authorization to verify if the account is in good standing.
- **For Internet transactions, use VbV to authenticate the cardholder’s identity at the time of purchase.** Do not submit an authorization request for VbV transactions that fail authentication.
- **Ask the customer for card expiration date and include it in your authorization request.** An invalid or missing expiration date can be an indicator that the person does not have the actual card in hand.
- **If participating in the CVV2 service, obtain the CVV2 three-digit code from the cardholder.** An issuer-validated CVV2 code is a good indicator that the card is genuine.
- **Where available, verify the cardholder’s billing address via the AVS.** This helps to validate the cardholder’s billing address directly with the issuer.
- **Submit the authorization request with the cardholder’s billing address and necessary CVV2 code information.** VisaNet® will return a CVV2 and AVS result codes with the authorization.
- **Perform internal screening or use a third-party tool to screen for questionable transaction data or other potential warning signs indicating “out of pattern” orders.** Route transactions with higher risk characteristics for fraud review.

If You Suspect Fraud:

- 1 Ask the customer for day/evening phone numbers, then call the customer with any questions.
- 2 Ask for additional information (e.g., bank name on front of card).
- 3 Separately confirm the order by sending a note via the customer’s billing address, rather than the “ship to” address

Report suspicious activity to your merchant bank.

12 Potential Warning Signs of Card-Not-Present Fraud

Stay alert for the following fraud indicators. When more than one of the following statements is true during a card-not-present transaction, fraud might be involved. Follow up, just in case.

- 1 **First-time shopper:** Criminals are always looking for new merchants to steal from.
- 2 **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
- 3 **Orders that include several varieties of the same item:** Having multiples of the same item increases criminal’s profits.
- 4 **Orders made up of “big-ticket” items:** These items have maximum resale value and therefore maximum profit potential.
- 5 **“Rush” or “overnight” shipping:** Criminals want their fraudulently obtained items as soon as possible for the quickest possible resale and aren’t concerned about extra delivery charges.
- 6 **Shipping outside of the merchant’s country:** There are times when fraudulent transactions are shipped to fraudulent criminals outside of the home country.
- 7 **Transactions with similar account numbers:** May indicate the account numbers used have been generated using software available on the Internet.
- 8 **Shipping to a single address, but transactions placed on multiple cards:** Could involve an account number generated using special software, or even a batch of stolen cards.
- 9 **Multiple transactions on one card over a very short period of time:** Could be an attempt to “run a card” until the account is closed.
- 10 **Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses:** Could represent organized activity, rather than one individual at work.
- 11 **For online transactions, multiple cards used from a single IP (Internet Protocol) address:** More than one or two cards could indicate a fraud scheme.
- 12 **Orders from Internet addresses that make use of free e-mail services:** These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

Card Verification Value 2—The Three-Digit Code

What

CVV2 is an important three-digit security feature for merchants who accept Visa cards as payment over the telephone or online. Located on the back of all Visa cards, the CVV2 code consists of the last three digits either printed on the signature panel or on a white box to the right of the security panel.



In the card-not-present sales environment, CVV2 is an excellent tool for verifying that the customer has a legitimate Visa card in hand at the time of the sales order.*



How

CVV2 works as follows:

- 1 The customer contacts the merchant to place an order.
- 2 The merchant asks the customer for the CVV2 three-digit code and sends it to the card issuer as part of the authorization request.
- 3 The card issuer checks the CVV2 code to determine its validity, then sends a CVV2 result code back to the merchant along with the authorization decision.
- 4 Before completing the transaction, the merchant evaluates the CVV2 result code, taking into account the authorization decision and any other relevant or questionable data.

CVV2 Without An Authorization Request

A merchant may also verify CVV2 without an accompanying authorization request by using the \$0 Account Verification Message**, which is available in all regions.

Why

Merchants who use CVV2 benefit in a number of ways:

Enhanced Fraud Protection

Because card-not-present merchants are at greater risk for stolen account number schemes, they need to be diligent in their fraud control efforts. CVV2 can help a merchant differentiate between good customers and fraudsters who operate anonymously. It allows merchants to make a more informed decision before completing a non-face-to-face transaction.

Reduced Chargebacks

Using CVV2 potentially reduces fraud-related chargeback volume. Reduced fraud-related chargebacks translate into maximized profitability.

Improved Bottom Line

For card-not-present merchants, fraudulent transactions can lead to lost revenue and can also mean extra processing time and costs, which often narrow profit margins. CVV2 complements the merchant's current fraud detection tools to provide a greater opportunity to control losses and operating costs.

*In certain markets, CVV2 is required to be present for all card-not-present transactions.

**For more information regarding the \$0 Account Verification Message, contact your merchant bank.

CVV2—Three-Digit Code

After obtaining the card CVV2 Result Code, account number, and card expiration date:

- 1 Send one of the following CVV2 presence indicators along with other required authorization data (i.e., account number, expiration date, and transaction amount).

If:	Send this Indicator to the Card Issuer:
You have chosen not to submit CVV2	0
You included CVV2 in the authorization request	1
Cardholder has stated CVV2 is illegible	2
Cardholder has stated CVV2 is not on the card	9



- 2 After receiving a positive authorization response, evaluate the CVV2 result code and take appropriate action based on all transaction characteristics.

Result	Action
M - Match	Complete the transaction (taking into account all transaction characteristics and any questionable data).
N - No Match*	View the “No-Match” as a sign of potential fraud and take it into account along with the authorization response and any other questionable data. Potentially hold the order for further verification.
P - Not Processed	View the “Not Processed” as a systemic technical problem or the request did not contain all the information needed to verify the CVV2 code. Resubmit the authorization request.
S - CVV2 should be on the card	Consider following up with your customer to verify that he or she checked the correct card location for CVV2. All valid cards are required to have CVV2 printed either in the signature panel or on a white box to the right of the signature panel.
U - Issuer does not participate in the CVV2 service	Evaluate all available information and decide whether to proceed with the transaction or investigate further.

*In some markets, if the transaction is approved, but the CVV2 response is a no match, the merchant is protected against fraud chargebacks.

Address Verification Service (U.S., Canada, and United Kingdom)

What

AVS allows card-not-present merchants to check a Visa cardholder's billing address with the card issuer. An AVS request includes the billing address (street address and/or zip or postal code). It can be transmitted in one of two ways: (1) as part of an authorization request, or (2) by itself. AVS checks the address information and provides a result code to the merchant that indicates whether the address given by the cardholder matches the address on file with the issuer.

AVS can only be used to confirm addresses in the United States, Canada, and the United Kingdom. In other countries, card issuer participation in AVS is optional.

How

AVS Processed as Part of an Authorization Request

The AVS request can be processed either on a real-time basis or in a batch mode using an electronic terminal or personal computer. Real-time requests are typically used for transaction situations where the customer must wait online for a response. The batch mode is geared more toward low-cost processing in which no immediate response is required as is usually the case with mail orders.

AVS Processed As Part of Account Verification Request

A merchant may also send a stand-alone AVS request without an accompanying authorization request by using the \$0 Account Verification Message,* which is available in all regions. For example:

- The merchant wants to verify the customer's billing address before requesting an authorization, or
- The merchant sends an authorization request with AVS data and receives an authorization approval, but also receives an AVS "try again later" response.

When AVS is processed as part of an authorization request, or without it using account verification, AVS works as follows:

- 1 The customer contacts the merchant to place an order.
- 2 The merchant:
 - Confirms the usual order information.
 - Asks the customer for the billing address (street address and/or zip or postal code) for the card being used. (i.e., the address is where the customer's monthly Visa statement is sent for the card being used.)
 - Enters the billing address and the transaction information into the authorization request system and processes both requests at the same time.
- 3 The issuer makes an authorization decision separately from AVS request and compares the cardholder billing address sent with the billing address for that account. The issuer then returns both the authorization response and a single character alphabetic code result that indicates whether the address given by the cardholder matches the address on file with the card issuer.

Why

Merchants who use AVS to verify cardholder information benefit in a number of ways.

Minimized Fraud

The value of AVS as an indicator of potential fraud has been amply demonstrated in Visa studies. Since the person fraudulently using a card is not likely to know the cardholder's billing address for that card account, a "no match" AVS result can be a key predictor of potential fraud.

Reduced Chargebacks

Using AVS potentially reduces fraud-related chargeback volume. Reduced fraud-related chargebacks translate into maximized profitability.

Improved Bottom Line

For card-not-present merchants, fraudulent transactions can lead to lost revenue and can also mean extra processing time and costs, which often narrow profit margins. AVS complements the merchant's current fraud detection tools to provide a greater opportunity to control losses and operating costs.

*For more information regarding the \$0 Account Verification Message, contact your merchant bank.

Address Verification Service (U.S., Canada, and United Kingdom)

AVS Result Codes

One of the following AVS result codes will be returned to the merchant indicating the issuer's response to the AVS request. A merchant's bank may modify these single character alpha AVS codes to make them more self-explanatory—for example, a "Y" response may be shown as an "exact match" or as a "full match," while an "N" response may be shown as a "no match."



Code	Definition	Code Applies to	
		Domestic	Cross-border
A	Street addresses match. The street addresses match but the postal or ZIP codes do not, or the request does not include the postal or ZIP code.	✓	✓
B	Street addresses match. Postal or ZIP code not verified due to incompatible formats. (Merchant bank sent both street address and postal or ZIP code.)	✓	✓
C	Street address and postal code or ZIP code not verified due to incompatible formats. (Merchant bank sent both street address and postal or ZIP code.)	✓	✓
D	Street addresses and postal or ZIP codes match.		✓
F	Street addresses and postal codes match. Applies to U.K.-domestic transactions only.	✓	
G	Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, or Visa performed address verification on behalf of the issuer and there was no address.		✓
I	Address information not verified.		✓
M	Street addresses and postal and ZIP codes match.		✓
N	No match. Merchant bank sent postal or ZIP code only, or street address only, or both postal or ZIP code and street address.	✓	✓
P	Postal or ZIP codes match. Merchant bank sent both postal or ZIP code and street address, but street address not verified due to incompatible formats.	✓	✓
R	Retry. System unavailable or timed out. Issuer ordinarily performs address verification but was unavailable. Visa uses code R when issuers are unavailable.	✓	
U	Address information is unavailable for that account number, or the card issuer does not support.	✓	
Y	Street address and postal and ZIP code match.	✓	
Z	Postal or ZIP codes match, street addresses do not match or street address not included in request.	✓	✓

Please contact your merchant bank for further questions on AVS result codes.

Address Verification Service (U.S., Canada, and United Kingdom)

Guidelines for Using Domestic and Cross-border AVS Result Codes

While Visa cannot recommend any particular approach, the following general guidelines are drawn from card-not-present industry practices and may be helpful. Merchants should establish their own policy regarding the handling of transactions based on AVS result codes.

Domestic	Cross-border	Definition	Explanation	Action(s) to Consider
Y F*	DM	Exact Match	Both street address and ZIP or Postal Code match.	Generally speaking, you will want to proceed with transactions for which you have received an authorization approval and an "exact match."
A	B	Partial Match	Street address matches, but ZIP or Postal Code does not.	You may want to follow up before shipping merchandise. The issuer might have the wrong ZIP or Postal Code in its file; merchant staff may have entered the ZIP or Postal Code incorrectly; or this response may indicate a potentially fraudulent situation.
Z	P	Partial Match	ZIP Code matches, but street address does not.	Unless you sent only a ZIP or Postal Code AVS request and it matched, you may want to follow up before shipping merchandise. The issuer may have the wrong address in its file or have the same address information in a different format; the cardholder may have recently moved; merchant staff may have entered the address incorrectly; or this response may indicate a potentially fraudulent situation.
N	N	No Match	Street address and ZIP or Postal Code do not match.	You will probably want to follow up with the cardholder before shipping merchandise. The cardholder may have moved recently and not yet notified the issuer; the cardholder may have given you the shipping address instead of the billing address; or the person may be attempting to execute a fraudulent transaction. "No match" responses clearly warrant further investigation.

AVS result codes and explanation provided here are meant to give you enough information to make your own determination of what works best for you. How one merchant treats these codes may be different than the way another merchant may choose to interpret them.

* United Kingdom

On ZIP or Postal Code only requests and P.O. Box addresses, issuers may respond either with a "Y" (Exact Match) or a "Z" (Partial Match — ZIP Code/Postal Code Matches).

Verified by Visa

What

Visa's security strategy is built on the belief that the most effective way to address the multiple types of fraud is to employ multiple layers of security and fraud protection. Verified by Visa (VbV) was designed to serve as one of these "multiple layers of security" by providing cardholder authentication for online transactions. Based on the 3-D Secure protocol, the VbV service verifies the authenticity of cardholders to participating merchants. It allows cardholders to choose a password through their card issuer, and use it to authenticate themselves while making a purchase. This helps ensure that their card number cannot be fraudulently used at an Internet merchant web site.

Cardholders sign up for the VbV service through their issuing financial institution and choose their own personal password to authenticate themselves online.

Merchants offering VbV to their customers must incorporate a software module called a Merchant Plug-In (MPI), as part of their e-commerce server application. Merchants who opt to implement VbV should use PCI compliant vendors and payment solutions.

How

VbV Activation

To use VbV, consumers must first activate their existing card(s). There are a number of ways they may do this:

- Card issuers typically provide an online activation site.
- Visa, card issuers, and participating merchants may display "Activation Anytime"* banners or buttons that enable cardholders to activate their Visa card.
- Cardholders may also activate during the shopping experience, where available.

If the cardholder chooses to activate during shopping, he or she provides information to their Visa card issuer for identification purposes. The cardholder then creates a password. On future purchases at participating online stores, the cardholder's Verified by Visa password will be required during checkout, reducing fraudulent use of the card.

- 1 Cardholder uses Visa card to make purchase
- 2 Cardholder enters authentication information requested by their issuing date
- 3 Cardholder creates password
- 4 Cardholder completes purchase

* Activation Anytime is only available in the U.S.



VbV Shopping

Once VbV is activated, a consumer's card is automatically recognized when used for purchases at participating online stores. The consumer is asked for their password; the password is verified; and the transaction is completed.

- 1 After activating their card, cardholder shops at participating stores
- 2 Cardholder submits password at checkout
- 3 Cardholder identity is confirmed and they're done!

Why

Internet merchants who use VbV experience several key benefits.

Reduced Chargebacks

VbV can reduce the risk of fraud and chargeback costs—with minimal impact to the current transaction process. Merchants who use VbV are protected from fraud-related chargebacks on all personal Visa cards—credit or debit, U.S., or non-U.S. country—whether or not the issuer or cardholder is participating in VbV with limited exceptions.

Lowered Transaction Fees

Depending upon processing arrangements with financial institution and payment provider, you could qualify for a lower transaction discount fee on Internet transactions that use VbV, compared to those transactions that do not. Not all merchant categories are eligible for a lower interchange rate as part of their VbV implementation.

Boosted Consumer Confidence

VbV meets consumer concerns regarding safety and protection, which are important factors in a consumer's choice of where to shop online.

Easy Implementation

Merchant Plug-In software is easily installed and can be readily integrated into existing e-commerce systems.

Verified by Visa



Merchant Chargeback Protection

- If the cardholder is successfully authenticated, the merchant is protected from fraud-related chargebacks, and can proceed with authorization using Electronic Commerce Indicator (ECI) of '5'.*
- If the card issuer or cardholder is not participating in Verified by Visa, the merchant is protected from fraud-related chargebacks, and can proceed with authorization using ECI of '6'.*
- If the card issuer is unable to authenticate, the merchant is **not** protected from fraud-related chargebacks, but can still proceed with authorization using ECI of '7'. This condition occurs if the card type is not supported within VbV or if the cardholder experiences technical problems.

Note: Liability shift rules for VbV transactions may vary by region. Please check with your merchant bank for further information.

*A VbV merchant identified by the Merchant Fraud Performance (MFP) program may be subject to chargeback Reason Code 93: Merchant Fraud Performance Program.

VbV Processing Actions

If you are a VbV merchant:

- **Add the VbV logo on your home, security information, and checkout pages to promote reliable and secure online shopping.** Use one of these two approaches:
 - **Activation Anytime***—This is the preferred approach that guides your customers directly to an activation page where they can activate their Visa cards without leaving your site.
 - **Learn More**—This approach directs your customers to a service description page (hosted by your site) where they can read more about VbV and activate their cards. Be sure to provide clear instructions on how VbV works. *Your merchant toolkit includes a "Learn More" page that details the VbV program. The merchant toolkit is available on www.visa.com.*
- **Add a pre-authentication message on the checkout page to inform customers that they may be asked to activate their Visa card for VbV.**
- **Complete the authentication process.** Provide the authentication data in the VisaNet authorization request as appropriate.
- **If authentication fails, request payment by alternate means.**
 - Quickly display a message or page to communicate to the cardholder that the purchase will not be completed with the card that failed.
 - Offer an immediate opportunity for the cardholder to enter a new payment card number and try again, **or**
 - Present a button that, when clicked, opens a new page that allows the cardholder to reinitiate the purchase.
- **Do not submit an authorization request for VbV transactions that fail authentication.**

* Activation Anytime is only available in the U.S.

CyberSource Advanced Fraud Screen Enhanced by Visa

What

Today, there are a wide variety of fraud-screening technologies and practices available to help merchants assess the risk of a transaction in real time and increase the likelihood that they are dealing with a legitimate customer with a valid Visa card. Fraud-screening tools can be developed internally or acquired from third parties like AFS.*

AFS evaluates the risk associated with individual transactions and provides Internet merchants with risk scores. These scores can be used as an additional means to identify potentially fraudulent orders; therefore, improving a merchant's ability to:

- Accurately detect fraud and maximize sales
- Deliver a more positive online shopping experience to customers

It is the first system to utilize updated purchase activity on a continuous basis, making it a better fraud detection and scoring system.

Merchants establish their own risk threshold. This is the risk level at which their systems will automatically accept, reject, or suspend the order. Thresholds can be set uniquely for every product and order type.

How

Every time a cardholder clicks the **Buy** button on a web site using AFS, the transaction is immediately evaluated based on over 150 order variables using sophisticated risk modeling techniques. Running 24 hours a day, seven days a week, the service uses the world's largest database of global fraud and payment-card usage patterns, including online and offline transactions. Risk scores are calculated using a combination of neural networks, rules-based modeling, and Visa hybrid fraud technologies.

AFS works as follows:

- 1 Upon receipt of an order, the merchant's system sends a request for assessment to CyberSource.
- 2 CyberSource checks and compares key order data variables for fraud risk using order attributes, worldwide transaction histories, and global payment card usage patterns.
- 3 The risk score is calculated indicating a probability of risk (0-99) in two seconds.
- 4 The score (and associated risk profile and information codes, where applicable) are sent back to the merchant system(s) where a decision is made to accept, reject, or review the order on the bases of the score received.

* AFS is not available in all regions. Please check with your merchant bank for further information.

Why

Merchants who implement AFS experience several important benefits.

Increased Sales Conversion

Merchants generate more order approvals as a result of improved risk assessment accuracy.

Improved Customer Satisfaction

Valid order processing is increased due to the automated fraud scoring system. This, in turn, allows customers to receive goods and services in a timely manner.

Reduced Costs

AFS can lower direct and indirect costs associated with the management of fraudulent transactions.

Direct Costs	Indirect Costs (Chargeback Related)
Loss of product	Customer service staff time
Order shipping and handling costs	Cash management and discount rates

For more information about AFS, visit www.cybersource.com.

Payment Card Industry Data Security Standard

What

The PCI DSS is intended to help protect Visa cardholder data—wherever it resides—ensuring that customers, merchants, and service providers maintain the highest information security standard. It offers a single approach to safeguarding sensitive data for all card brands. PCI DSS compliance is required of all entities that store, process, or transmit Visa cardholder data.

As mandated under the **Visa Cardholder Information Security Program (CISP)** which is U.S. based effort and the **Account Information Security (AIS)** program which is implemented in non-U.S. countries, all Visa clients, merchants, and service providers must adhere to the PCI DSS.



The PCI DSS consists of twelve easy-to-remember basic requirements supported by more detailed sub-requirements.

Build and Maintain a Secure Network

- 1 Install and maintain a firewall configuration to protect cardholder data
- 2 Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- 3 Protect stored cardholder data
- 4 Encrypt transmission of cardholder data across open, 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 cardholder data by business need-to-know
- 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

How

Separate and distinct from the mandate to comply is the validation of compliance. It is an ongoing process that helps ensure the safety and security of Visa cardholder data (wherever it is located), and holds all Visa members accountable for verifying that their merchants and all supporting service providers adhere to the PCI DSS requirements.

Visa has prioritized and defined levels of CISP and AIS compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the Visa System by merchants and service providers. For specifics about the validation requirements, visit www.visa.com or contact your merchant bank.

Why

By complying with PCI DSS requirements, merchants not only meet their obligations to the Visa payment system, but also:

Consumer Trust in the Security of Sensitive Information

Customers seek out merchants that they feel are “safe.” Confident consumers are loyal customers. They come back again and again, as well as share their experience with others.

Minimized Direct Losses and Associated Operating Expenses

Appropriate data security protects cardholders, limits risk exposure, and minimizes the losses and operational expense that stem from compromised cardholder information.

Maintained Positive Image

Information security is on everyone’s mind...including the media’s. Data loss or compromise not only hurts customers, it can seriously damage a business’s reputation.

For more information, contact your merchant bank or visit www.pcisss.org

Payment Card Industry Data Security Standard

Sensitive Data Storage and Security

All stored sensitive cardholder account information must comply with the PCI DSS and *Visa Operating Regulations*.

To protect sensitive customer information from compromise merchants that store, process, or transmit cardholder data must:

- Keep all material containing account numbers—whether on paper or electronically—in a secure area accessible to only selected personnel.
- Render cardholder data unreadable, both in storage and prior to discarding.
- Never retain full-track, magnetic-stripe data and CVV2 data subsequent to transaction authorization. Storage of track data elements in excess of name, account number, and expiration date after transaction authorization is strictly prohibited.
- Use payment applications that comply with the PCI Payment Application Data Security Standard (PA-DSS). A list of validated payment applications is available at www.pcissc.org.

Protect Your Cardholders and Your Business

- Work with your merchant bank to understand your information security and what's required of you and your service provider(s) in regard to PCI DSS compliance.
- Train your employees on compliance basics.
- Know your liability for data security problems. Many merchant banks today are providing contracts that explicitly hold merchants liable for losses resulting from compromised card data if the merchant (and/or service provider) lacked adequate data security. Other liability, such as to consumers, may also arise.
- If you experience a suspected or confirmed security breach, take immediate steps to contain and limit exposure.
- Alert all necessary parties of a suspected or confirmed security breach immediately.
- Provide any compromised Visa accounts to your merchant bank within 24 hours.



Resources and Tools for Card-Not-Present Merchants

Visa offers a number of risk management materials as part of its merchant education program. Current publications that are geared toward card-not-present merchant needs are available as downloadable PDF files.

Materials for merchants that support U.S. domestic transactions are available at <http://usa.visa.com/merchants>.

To access global merchant publications for your region, click the **Global Sites** link at the bottom of the screen.

This will take you to the **Visa Global Gateway** where you can select a country or region.

Click "Global Sites" to visit regional web sites



<http://usa.visa.com/merchants>

Select a country



www.visa.com/globalgateway/

Glossary of Terms

Address Verification Service (AVS)	A risk management tool that enables a merchant to verify the billing address of a customer presenting a Visa card for payment. The merchant includes an AVS request with the transaction authorization and receives a result code indicating whether the address given by the cardholder matches the address in the issuer's file. A "Partial" or "No Match" may indicate fraud risk.
Authentication	Involves the verification of the cardholder and the card. At the time of authorization, to the greatest extent possible, the e-commerce merchant should use fraud prevention controls and tools to validate the cardholder's identity and the Visa card being used.
Authorization	The process by which an issuer approves (or declines) a Visa card purchase takes place at the same time as the transaction.
Card-not-present	An environment where a transaction is completed and both the cardholder and the card are not present. Transactions in this environment include mail/phone order transactions and Internet transactions.
Card Verification Value 2 (CVV2)	A three-digit value that is printed on the back of a Visa card, provides a cryptographic check of the information embossed on a card, and assures the merchant, merchant bank, and issuer that the card is in possession of the cardholder. Card-absent merchants should ask the customer for the CVV2 to verify the card's authenticity. For information security purposes, merchants are prohibited from storing CVV2 data.
Chargeback	A processed bankcard transaction that is later rejected and returned to the merchant bank by the issuer for a specific reason, such as a cardholder dispute or fraud. The merchant bank may then return the transaction to the merchant, which may have to accept the dollar loss unless the transaction can be successfully represented to the issuer.
CyberSource Advanced Fraud Screen (AFS) enhanced by Visa	A real time fraud detection service that examines transactions generated from online stores. It estimates the level of risk associated with each transaction and provides merchants with risk scores, enabling them to more accurately identify potentially fraudulent orders.
Electronic Commerce Indicator (ECI)	A transaction data field used by e-commerce merchants and merchant banks to differentiate Internet merchants from other merchant types. Use of the ECI in authorization and settlement messages helps e-commerce merchants meet Visa processing requirements and enables Internet transactions to be distinguished from other transaction types. Visa requires all e-commerce merchants to use the ECI.
Expiration date	The date after which a bankcard is no longer valid, embossed on the front of all valid Visa cards. The "Good Thru" date is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.
Fraud scoring	A category of predictive fraud detection models or technologies that may vary widely in sophistication and effectiveness. The most efficient scoring models use predictive software techniques to capture relationships and patterns of fraudulent activity, and to differentiate these patterns from legitimate purchasing activity. Scoring models typically assign a numeric value that indicates the likelihood that an individual transaction will be fraudulent.
Issuer	A financial institution that issues Visa cards to cardholders, and with which each cardholder has an agreement to repay the outstanding debt on the card. Also known as a <i>consumer bank</i> .
Merchant bank	A financial institution or merchant bank that contracts with a merchant to accept Visa cards as payment for goods and services and enables the use of Visa cards as a form of payment. Also known as a merchant bank.
Payment Card Industry (PCI) Data Security Standard (DSS)	A set of requirements established by the Payment Card Industry to protect cardholder data. These requirements apply to all members, merchants, and agents that store, process, or transmit cardholder data.
Verified by Visa (VbV)	A Visa Internet payment authentication system that validates a cardholder's ownership of an account in real time during an online payment transaction.

