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 the Visa card is not present.

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. According to the 12th annual Online Fraud Report by CyberSource[1], U.S. merchants lost $2.7 billion to online fraud in 2010, and over half of those surveyed indicated that fraud is getting "cleaner." In other words, it's getting harder to detect fraud, because fraudsters are becoming more sophisticated at looking like legitimate customers.

Thieves are primarily interested in two things: stealing your sensitive payment data to re-sell on the black market, and/or using that payment data to steal goods and services from you. Hackers are constantly testing your systems to identify and exploit points of weakness in your security, with increasing success. In 2010, there was a 33% increase in the number of data breaches reported by organizations, according to the Identity Theft Resource Center.[2]

Understanding the Risks with Card-Not-Present Transactions

In order to help thwart these breaches, the Payment Card Industry (PCI) Data Security Standard (DSS) is a framework that provides enhanced security around merchants' cardholder data. Consisting of twelve requirements, PCI DSS outlines the steps to take to protect sensitive payment information. By demonstrating that you are PCI DSS-compliant, customers can be more confident buying from you, assured that their cardholder data is secure.

However, not all merchant's security systems are foolproof. And if payment data is stolen, fraudsters or fraudster-controlled botnets (a network of compromised computers being used for malicious purposes) can attempt to steal as much as they can from you, using legitimate payment data. Often, the lag time it takes for you to detect the fraud results in customer chargebacks, loss of inventory, and ultimately, a hit to your bottom line. Regardless of the size of your business, you are a potential target if you're conducting business online, over the phone, or through the mail. That's why it's critical to take a multi-layered approach to fighting fraud and strengthening security.

Follow a Two-Step Fraud Detection System

A robust fraud detection system consists of two stages: an automated evaluation followed by a manual investigation process. The intent is to make as many systematic decisions as possible in order to lower your overhead costs and ensure the optimal customer experience. Only those highly suspicious orders should be sidelined for a deeper level of review by an investigator.

The first step, automated order screening, should leverage your own data, third-party fraud prevention tools (such as IP Geolocation, device fingerprinting, fraud-scoring models, velocity checks, and more), as well as a variety of services[3] made available by Visa. These include Verified by Visa® (VbV), Card Verification Value 2 (CVV2), and Address Verification Service (AVS).

Second step, orders that do not pass the first step should then be sent to your order review team for further scrutiny. Thus, it's critical that they are armed with the verification tools necessary to validate questionable orders, as well as a case management system to keep track of the orders in queue. The verification tools and the case management system enable the reviewers to process more orders more effectively and efficiently.

Ensure that your fraud management process is optimized, develop key metrics to track and analyze over a set period of time. In particular, it is extremely helpful to feed fraud chargebacks and credits back into your fraud screening process, so that you can identify fraud patterns and adjust your processes accordingly. Reporting around your order review team can also help to identify how efficiently your order review team performs, how accurate they are in detecting fraud, and where overall operations can improve.

Select the Right Tools

Comprehensive fraud prevention comes with having a complete fraud management process in place at your business. Start by using your own data, and enhance your fraud intelligence with the right combination of fraud prevention and detection tools and controls supplied by third parties or Visa. If required, third-party fraud detection solutions (such as those offered by CyberSource Risk Management Solutions) can provide deep fraud management expertise, as well as access to other fraud prevention tools. By supplementing the services provided by Visa with additional outside support, you can strengthen your defenses against sophisticated fraudsters looking for an easy mark.

---

1 CyberSource is a wholly-owned subsidiary of Visa.

2 662 in 2010 v. 498 reported in 2009; www.idtheftcenter.org

3 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.

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

Visa fraud prevention tools are designed to complement each other and work together as multiple services that can help you 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 an elevated 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. Again, the response can be used to make a risk evaluation.
- **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.
- 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. This helps to protect not only your own data, but that of your fellow merchants as well.

Card-Not-Present Fraud Detection

To supplement the effective use of your own data, Visa's fraud prevention tools, and third party data feeds/services, vendor fraud detection solution providers such as CyberSource 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 you protect your customers and brand by reducing fraud losses and making the Internet and other sales channels safer to conduct business. To obtain a list of third party fraud prevention solution providers, contact your merchant bank.

- **CyberSource Risk Management Solutions** provide fraud detection for organizations of all sizes.

- **Decision Manager (DM)** and **Managed Risk Services** by CyberSource enable mid-size to large companies detect fraud more accurately, review more efficiently, and improve control over fraud management practices.
- **Authorize.Net Advanced Fraud Detection Suite™ (AFDS)** is a set of customizable, rules-based filters and tools that help small businesses identify, manage, and prevent suspicious and potentially costly fraudulent transactions. Authorize.Net AFDS is a value-added service of the Authorize.Net Payment Gateway.

The Right Combination of Tools at the Right Time

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

	VISA CNP FRAUD PREVENTION TOOLS				FRAUD DETECTION SERVICES
	VbV	CVV2	AVS	PCI DSS	DM/AFDS
Internet	✔	✔	✔	✔	✔
Telephone Order		✔	✔	✔	✔
Mail Order			✔	✔	✔

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 the tests listed below. Keep in mind, none of these tools should be used exclusively to determine the validity of the customer or to accept or reject an order. They should be used as indicators of risk, and in combination with other fraud detectors.

- **If participating in the CVV2 service, obtain this three-digit code from the cardholder.** The purpose of CVV2 in a card-not-present transaction is to attempt to verify that the person placing the order has the actual card in his or her possession. Requesting the card verification number during a card-not-present purchase can add a measure of security to the transaction.
- **Where available, verify the cardholder's billing address via the AVS.** AVS compares numeric address data with information on file from the cardholder's card issuing bank. AVS return codes are generally available for U.S. cardholders and for a limited number of cardholders in Canada.
- **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.
- **If the customer's telephone number is supplied as part of the transaction, use area code or reverse lookup tables to verify the legitimacy and location of the phone number (these are widely available).** Similarly, postal address validation services can be used to distinguish legitimate addresses from bogus ones.
- **Leverage your own customer history data effectively.** If you have had a fraud event associated with a customer, the details of that transaction should be added to internal "negative lists." Any subsequent order that shares the same characteristics should be considered suspicious.

Many of these tests can be conducted automatically, depending on the flexibility of your technical infrastructure or your ability to connect with fraud prevention service providers. Instead of manually reviewing each order, it is typically more cost effective to perform automated internal screening or to use a third-party tool to screen for questionable transactions.

Of course, route transactions with higher risk characteristics for fraud review. Experienced fraud investigators can often distinguish a fraudulent order from a legitimate one.

11 Potential Warning Signs of Card-Not-Present Fraud

Stay alert for the following fraud indicators. Any one of these factors could indicate a higher degree of fraud risk.

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. **"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.
5. **Shipping outside of the merchant's country:** There are times when fraudulent transactions are shipped to fraudulent criminals outside of the home country.
6. **Inconsistencies:** Information in the order details, such as billing and shipping address mismatch, telephone area codes falling near zip codes, email addresses that do not look legitimate, and irregular time of day when the order was placed.
7. **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.
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 or a similar card with a single billing address, but multiple shipping addresses:** Could represent organized activity, rather than one individual at work.
10. **For online transactions, multiple cards used from a single IP (Internet Protocol) address:** More than one or two cards could indicate a fraud scheme.
11. **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.[4]

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 Zero Amount Account Number Verification Service[5], 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.

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

[5] For more information regarding the Zero Amount Account Number Verification Service, contact your merchant bank.

Address Verification Service (U.S. and Canada)

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 and Canada. 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 Zero Amount Account Number Verification Service,[6] 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.

[6] For more information regarding the Zero Amount Account Number Verification Service, contact your merchant bank.

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"[7] 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

[7] 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'.[8]
- 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'.[8]
- 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.

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**[9]**—**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.**

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

[9] Activation Anytime is only available in the U.S.

CyberSource Risk Management Solutions

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. Fraud-screening tools can be developed internally or acquired from third parties like CyberSource.

CyberSource Risk Management Solutions provide fraud detection for organizations of all sizes. Decision Manager and Managed Risk Services[10] are ideal for mid-to-large companies; Authorize.Net Advanced Fraud Detection Suite™ (AFDS)[11] is geared towards small businesses.

- **Decision Manager and Managed Risk Services** enable mid-size to large companies to detect fraud more accurately, review more efficiently, and improve control over fraud management practices, across all card brands and payment methods. Decision Manager utilizes the widest breadth of data in the market (from the specific merchant, from CyberSource's multi-merchant database, and all transactional data from Visa), and correlates the data to identify fraudulent activity.
- **CyberSource Decision Manager** comes with over 200 detectors, a powerful statistical model built with Visa, a case management system, and detailed reporting. Merchants can supplement Decision Manager with Managed Risk Services, whereby CyberSource fraud analysts provide consultation and recommendations on improving fraud management processes.
- **Authorize.Net Advanced Fraud Detection Suite (AFDS)** is a set of customizable, rules-based filters and tools that help small businesses identify, manage, and prevent suspicious and potentially costly fraudulent transactions. Multiple filters and tools work together to evaluate transactions for indicators of fraud. Their combined logic provides a powerful and highly effective defense against fraudulent transactions. Filters include transaction velocity, IP checks, address mismatches, and more. AFDS is also integrated with the Address Verification Service (AVS) and Card Verification Value 2 (CVV2). Authorize.Net AFDS is a value-added service of the Authorize.Net Payment Gateway.

Merchants that implement CyberSource Risk Management Solutions experience several important benefits.

- **Increased sales conversion:** Generate more order approvals as a result of improved risk-assessment accuracy.
- **Fewer chargebacks:** Lower direct and indirect costs associated with the management of fraudulent transactions.

  Direct costs

  - Loss of product
  - Order shipping and handling costs

  Indirect costs (chargeback-related)

  - Bank fees
  - Customer service staff time
  - Cash management and discount rates
- **Improved customer satisfaction:** Increase valid order processing due to the automated fraud screening, allowing your customers to receive goods and services in a timely manner, and reducing customer insult from incorrectly rejecting valid orders.

To learn more about the CyberSource Risk Management Solutions (for mid-size to large companies) visit *www.cybersource.com* or (for small business) *www.authorize.net*.

For a copy of the CyberSource Online Fraud Report, white papers regarding online fraud or payment security, visit *www.cybersource.com*.

For information on Authorize.Net Advance Fraud DetectionSuite, visit *www.authorize.net*.

[10] CyberSource Decision Manager and Managed Risk Services are available globally.

[11] Authorize.Net Advanced Fraud Detection Suite is available in the United States.

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.pcissc.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 International 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*. For more information about CyberSource payment security solutions addressing PCI, please visit *www.cybersource.com*

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 *www.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

www.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.
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 *consumer bank.*
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.