VISA E-COMMERCE MERCHANTS' GUIDE TO RISK MANAGEMENT

VISA

TOOLS AND BEST PRACTICES FOR BUILDING A SECURE INTERNET BUSINESS

Visa E-Commerce Merchants' Guide to Risk Management

Tools and Best Practices for Building a Secure Internet Business

Table of Contents

About This Guide

Introduction

To help e-commerce merchants address the emerging and rapidly growing digital and hard goods markets from a global perspective, and maintain a secure infrastructure for payment card transactions, Visa has revised and updated the *E-Commerce Merchants' Guide to Risk Management*.

The purpose of this guide is to recommend a set of "best practices" that your business can use to manage e-commerce risk. Some of these practices cover policies, procedures, and capabilities currently in place in the e-commerce merchant marketplace. Others are recommendations based on Visa's payment industry experience and key learnings from its Global Card-Absent initiative.

This guide focuses on the core e-commerce merchant best practices used worldwide, taking into consideration, however, that processing dynamics may differ by country or geography.

Since this guide was first published, a large number of third party service providers have emerged to offer assistance in the mitigation of e-commerce fraud. A few of these providers have been included for further insight and consideration in your overall fraud mitigation planning

Key Points

Visa is a public corporation that works with financial institutions that issue Visa cards and/or sign merchants to accept Visa cards for payment of goods and services. Visa provides card products, promotes the Visa brand, and establishes the rules and regulations governing member participation in Visa programs. Visa also operates the world's largest retail electronic payment network to facilitate the flow of transactions between members.

Who Will Benefit from This Guide

This guide is a valuable planning tool for merchants at any stage of the e-commerce life cycle. This includes:

- ✔ **Merchants that are considering an e-commerce program.** If you are weighing the benefits and challenges of the Internet marketplace, this guide will help you assess your needs, resources, and expectations by identifying key risk issues that must be addressed and proven solutions that you can adapt to your unique operational environment.
- ✔ **Merchants that have just launched an e-commerce program.** If your e-commerce business is new, this guide will help you evaluate your efforts to date and ensure that you have sound operating practices in place from the outset. Finding the best ways to control risk in the early stages of your program, will allow you to set the foundation for future growth.
- ✔ **Merchants with established e-commerce programs.** If your business is already an active participant in the Internet marketplace, this guide will help you identify areas for improvement, explore advanced tactics for reducing risk exposure, and improve profitability as your Internet volume continues to grow.

How This Guide is Organized

Depending on your current e-commerce experience, you can either use this guide sequentially as a step-by-step planning tool, or move directly to any of the topics listed below:

Section 1: Understanding the Basics. If you're just starting out as an e-commerce merchant or are in the early stages of your program, take a few minutes to review this section. Here you'll find the background details you need to better understand what's required when it comes to maximizing information security and minimizing Visa card payment risk. In addition, this section helps demystify some e-commerce payment concepts and offers a simple explanation of online Visa card transaction processing—what it is, how it works, and who's involved. This section also includes a brief look at the nine top fraud schemes that are most impactful to today's e-commerce merchant.

Section 2: E-Commerce Risk Management Best Practices. This section identifies the best ways to reduce risk exposure when selling your goods and services through the Internet. These recommendations are organized by functional area and include practical step-by-step details to facilitate your e-commerce planning and management efforts. The best practices in this section apply to all e-commerce merchants and their service providers.

Section 3: Resources. This section of the guide offers a comprehensive listing of useful risk management resources available online and in print.

Section 4: Appendices. In this section you'll find two key resources: an *E-commerce Merchant Fraud Reduction Tools Quick Look-up*, and a glossary of terms commonly used in the e-commerce market today.

For More Information

To learn more about e-commerce risk management, contact your Visa acquirer or payment processor. If your current acquirer does not yet offer Internet support or if you do not yet accept Visa cards for payment, contact a Visa acquirer in your market with an established e-commerce program.

Note: *The information in this guide is offered to assist you on an "as is" basis. This guide is not intended to offer legal advice, or to change or affect any of the terms of your agreement with your Visa acquirer or any of your other legal rights or obligations. Issues that involve applicable laws (e.g., privacy issues, data export), or contractual issues (e.g., chargeback rights and obligations) should be reviewed with your legal counsel. Nothing in this guide should replace your own legal and contract compliance efforts.*

Section 1 Understanding the Basics

What's Covered

- Handling Visa Transactions
- Approaching Risk from a Strategic Perspective
- Online Transaction Processing—From Start to Finish
- A Brief Look at Chargebacks
- Nine Top Fraud Schemes Every E-Commerce Merchant Should Know

Handling Visa Transactions

✔ All e-commerce merchants:

- **Must authorize their Visa transactions.** If account funds are available and a card has not been reported lost or stolen, the transaction will most likely be approved by the issuer. For e-commerce merchants, it is important to remember that an authorization is not proof that the true cardholder is making the purchase or that a legitimate card is involved.
- **Are subject to Visa's card-absent chargeback rules and regulations.** An e-commerce merchant can be held financially responsible for a fraudulent transaction, even if it has been approved by the issuer. This is because there is a greater chance of fraud due to the absence of a card imprint, no cardholder signature, and no individual present. E-commerce merchants can minimize their fraud exposure with the proper Internet-specific risk management infrastructure.

> **Key Points**
>
> In the e-commerce environment, the shipment date is considered to be the transaction date. As such, e-commerce merchants have up to seven days to obtain an authorization prior to the transaction date.

- **Are eligible to participate in Verified by Visa.** This important service improves transaction security by authenticating the cardholder and obtaining protection against chargebacks from fraud. In addition, customers enjoy a safer place to shop and transaction discount fees are lower in many cases.
- **Must enter an accurate Electronic Commerce Indicator (ECI) for all Internet transactions.** When entered as part of the authorization and settlement message, the ECI identifies the transaction as "e-commerce." This allows the issuer to make a more informed authorization decision.
- **Must be in compliance with the Payment Card Industry (PCI) Data Security Standard (DSS).** To achieve compliance, all merchants and their service providers (including third party agents) must adhere to the PCI DSS requirements, which offer a single approach to safeguarding sensitive data for all card brands. *For more information about PCI DSS, refer to the best practices on pages 63-67 of this guide.*

> **Key Points**
>
> A third party agent:
>
> - Is an entity that is *not* defined as a VisaNet processor, but instead provides payment-related services (directly or indirectly) to a member, and/or stores, processes or transmits cardholder data.
> - Must be registered by all Visa members that are utilizing their services directly or indirectly.

- **Must never store Card Verification Value 2 (CVV2)* data.** The storage of CVV2 is strictly prohibited subsequent to authorization.

✔ **Visa's operating rules apply to all e-commerce businesses that accept Visa cards.** In adhering to these policies and principals, e-commerce merchants should do the following:

- **Accept all Visa credit cards and all Visa debit cards, or both, depending on which Visa card acceptance option you have chosen.** Visa cards must be honored regardless of the dollar amount of the purchase.
- **Display the Visa logo on the merchant website, depending on the card acceptance option you choose.**
- **Include any required taxes in the total transaction amount.** Do not collect taxes separately in cash. *Among other things, this policy reflects the needs of Visa cardholders who must have written records of the total amount they pay for goods and services, including taxes.*
- **Deposit transactions only for your own business.** Depositing transactions for a business that does not have a valid merchant agreement is called "laundering" and it is not allowed. Laundering is a form of fraud associated with high chargeback rates and the potential for accommodating illegal activity.
- **Deposit your Visa transaction receipt as specified by your acquirer.** Generally, transaction receipts must be deposited within three business days of the transaction date, with some exceptions. The sooner you deposit transaction receipts with your acquirer, the sooner you get paid. Transactions deposited more than 30 days after the original transaction date may be charged back to you. For card-absent transactions, the transaction date is the merchandise **ship date**, not the order date.
- **Deliver the merchandise or services to the cardholder at the time of the transaction.** Cardholders expect immediate delivery of goods and services unless other delivery arrangements have been made. For card-absent transactions, cardholders should be informed of delivery method and tentative delivery date. Transactions cannot be deposited until goods or services have been shipped.
- **For a delayed delivery, obtain where applicable two authorizations: one for the deposit amount and one for the balance amount.** Some merchandise, such as a custom-covered sofa, requires delivery after the transaction date. In these delayed-delivery situations, the customer pays a deposit at the time of the transaction and agrees to pay the balance upon delivery of the merchandise or services.

*In certain markets, CVV2 is required for card-absent transactions.

- Make refund and credit policies available to online customers through clearly visible links on your website's home page.
- **NEVER** use the Visa card/account number to collect other debts or dishonored checks.

✔ Issuers have 120 days from the central processing date (CPD) to charge back transactions in which the cardholder claims to have not participated. This means that fraudulent activity can end up posing a significant risk to the e-commerce merchant long after the transaction has been processed.

Online Transaction Processing—From Start to Finish

Starting with the Fundamentals

A key to understanding online Visa card payments is to first know these three core processing actions:

Authorization Takes place at the time the transaction occurs. It is the process by which an issuer approves (or declines) a Visa card purchase.

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 fraud detection tools to validate the cardholder's identity and the Visa card being used.

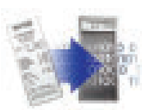
Settlement Once a product or service has been shipped or delivered to the customer, the e-commerce merchant can initiate the settlement of a transaction through their acquirer and trigger the transfer of funds into the merchant account.

Who Does What?

Besides you and your customer, several other parties participate in an online Visa card transaction. Here's a quick look at the different players typically involved.

An issuer is a financial institution that maintains the Visa cardholder relationship. It issues Visa cards and contracts with its cardholders for repayment of transactions.

An acquirer is a financial institution that contracts with merchants to accept and process Visa cards for payment of goods and services. An acquirer may contract with VisaNet processors to provide any of these services, which is typically the case. An acquirer is often referred to as the "merchant bank."

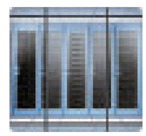


VisaNet® is a collection of systems that supports the electronic transmission of all Visa card authorizations between acquirers and issuers and facilitates the settlement of funds.

VisaNet processor (also referred to as a payment processor) is a member, or Visa-approved nonmember that is directly connected to VisaNet, that provides authorization, clearing, or settlement services for merchants and/or members.

A cardholder is an authorized user of Visa payment products. In order to make an online purchase, the cardholder must use a web browser to interact with the

An e-commerce merchant is an authorized acceptor of Visa cards for the electronic payment of goods and services.



A service provider stores, processes, or transmits Visa account numbers on behalf of a member's merchant. A service provider is defined by Visa as a third party agent that has a direct relationship with a merchant (instead of the acquirer). Function examples include providing such services as online shopping carts, payment gateways, hosting facilities, data storage, authorization, and/or clearing and settlement messages.

A service provider can also include a fraud detection solution vendor (e.g., CyberSource) who offers a combination of leading technology and innovative tools for fraud mitigation.

The Online Transaction Life Cycle

The following example illustrates real time processing for an online Visa card transaction. Processing events and activities may vary slightly depending on your acquirer and/or payment processor relationship, service provider needs, business requirements, and the systems used.

Authorization

1 The cardholder orders goods from an e-commerce merchant by entering Visa card payment information into the website form, as prompted.

For merchants participating in Verified by Visa, the cardholder authentication step occurs prior to authorization processing. (See next page for further details.)

2 The information is encrypted and transmitted via the Internet to the merchant server.

The payment gateway receives the encrypted information from the merchant server. The information is formatted and transmitted to the acquirer (or VisaNet processor).

3 The acquirer (or VisaNet processor) electronically sends the authorization request to VisaNet.

4 VisaNet passes the request on to the issuer.

5 The issuer approves or declines the transaction.

The authorization response is routed back through the same channels.

Real Time vs. Batch Authorization Processing

E-commerce merchants who do not process Visa transactions in real time typically download their transactions from their server within 24 hours of the purchase/service request. They then batch the transactions and submit them for authorization using a point-of-sale (POS) terminal or PC program. If the order is declined, the merchant must notify the customer via e-mail or by telephone.

Authentication and Fraud Reduction

It is up to the e-commerce merchant to apply the right tools and controls to help verify the cardholder's identity and the validity of the transaction. Appropriate action can help an e-commerce merchant reduce fraudulent transactions and the potential for customer disputes.

Visa Fraud Prevention Tools

Here is a brief look at the Visa tools you can use to verify the legitimacy of a Visa cardholder and card.

TOOL	DESCRIPTION
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. Merchants are prohibited from retaining CVV2 data subsequent to transaction authorization.
Verified by Visa	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 that the issuer authenticates the cardholder's identity at the time of purchase.

For more information about CVV2 and AVS, refer to the best practices on pages 47-50 of this guide. For additional details about Verified by Visa and associated best practices, see pages 56-58.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

Authentication and Fraud Reduction

(continued)

Cardholder Data Protection

The **Payment Card Industry (PCI) Data Security Standard (DSS)** is intended to help protect Visa cardholder data—wherever it resides—ensuring that 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.

Other Card-Absent Fraud Detection Tools

To supplement the effective use of your own data, Visa's fraud prevention tools, third party data feeds/services, and fraud detection solution vendors such as CyberSource offer a combination of leading technology and innovative tools for fraud mitigation within the various card-absent 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.

CyberSource Risk Management Solutions provide the following fraud detection for organizations of all sizes.

- **Decision Manager (DM) and Managed Risk Services** by CyberSource enable mid-size to large companies to detect fraud more accurately, review transactions 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.

> To obtain a list of third party fraud prevention solution vendors, contact your acquirer or payment processor.

The Right Combination of Tools at the Right Time

These Visa fraud prevention and detection tools are designed to complement each other and work together to help merchants better combat fraud.

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

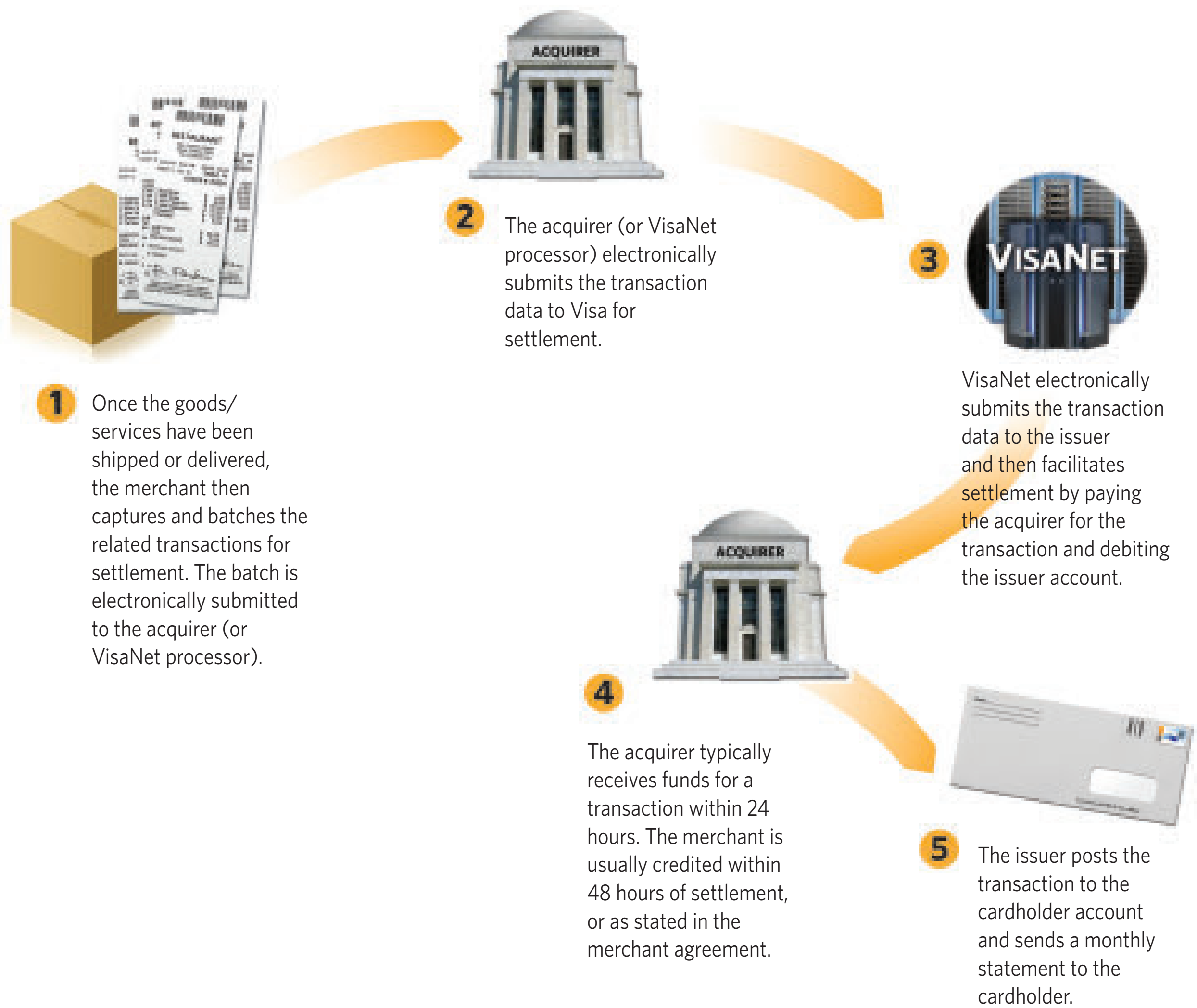
	VISA CARD-ABSENT FRAUD PREVENTION TOOLS				FRAUD DETECTION SERVICES
	VERIFIED BY VISA	CVV2*	AVS**	PCI DSS	DM/AFDS
Internet	✔	✔	✔	✔	✔
Telephone Order		✔	✔	✔	✔
Mail Order			✔	✔	✔

*In certain markets, CVV2 is required for card-absent transactions.

**AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

Settlement

The process illustrated below offers a "big picture" view of the Visa card payment settlement events that can take place. The process may vary slightly depending on your technology requirements and the service providers you use.



A Brief Look at Chargebacks

What is a Chargeback?

A chargeback is a transaction that a card issuer returns to an acquirer as a financial liability and which, in turn, an acquirer may return to a merchant. In essence, it reverses a sales transaction:

- The card issuer subtracts the transaction dollar amount from the cardholder's Visa account. The cardholder receives a credit and is no longer financially responsible for the dollar amount of the transaction.
- The card issuer submits a chargeback through VisaNet to the acquirer for the dollar amount of the transaction.
- The acquirer will, most often, deduct the transaction dollar amount from the merchant's account. The merchant loses the dollar amount of the transaction.

For merchants, chargebacks can be costly. You can lose the dollar amount of the transaction being charged back and incur your own internal costs for processing the chargeback. Since you control how your employees handle transactions, you can prevent many unnecessary chargebacks by simply training your staff to pay attention to a few details.

Why Chargebacks Occur

The most common reasons for chargebacks include:

- Customer disputes
- Fraud
- Processing errors
- Authorization issues

Although you probably cannot avoid chargebacks completely, you can take steps to reduce or prevent them. Many chargebacks result from avoidable mistakes, so the more you know about fulfillment procedures and proper transaction-processing procedures, the less likely you will be to inadvertently do, or fail to do, something that might result in a chargeback.

Of course, chargebacks are not always the result of something merchants did or did not do. Errors are also made by acquirers, card issuers, and cardholders.

Key Points

From the administrative point of view, the main interaction in a chargeback is between a card issuer and an acquirer. The card issuer sends the chargeback to the acquirer, which may or may not need to involve the merchant who submitted the original transaction. This processing cycle does not relieve merchants of the responsibility of taking action to remedy and prevent chargebacks. In most cases, the full extent of your financial and administrative liability for chargebacks is spelled out in your merchant agreement.

What is a Sales Draft Request?

When cardholders do not recognize transactions on their Visa statements, they typically ask their issuer for a copy of the related transaction receipt to determine whether the transaction is theirs. If necessary, the issuer sends a sales draft request to the acquirer, who either fulfills the request or forwards it to the merchant for fulfillment.

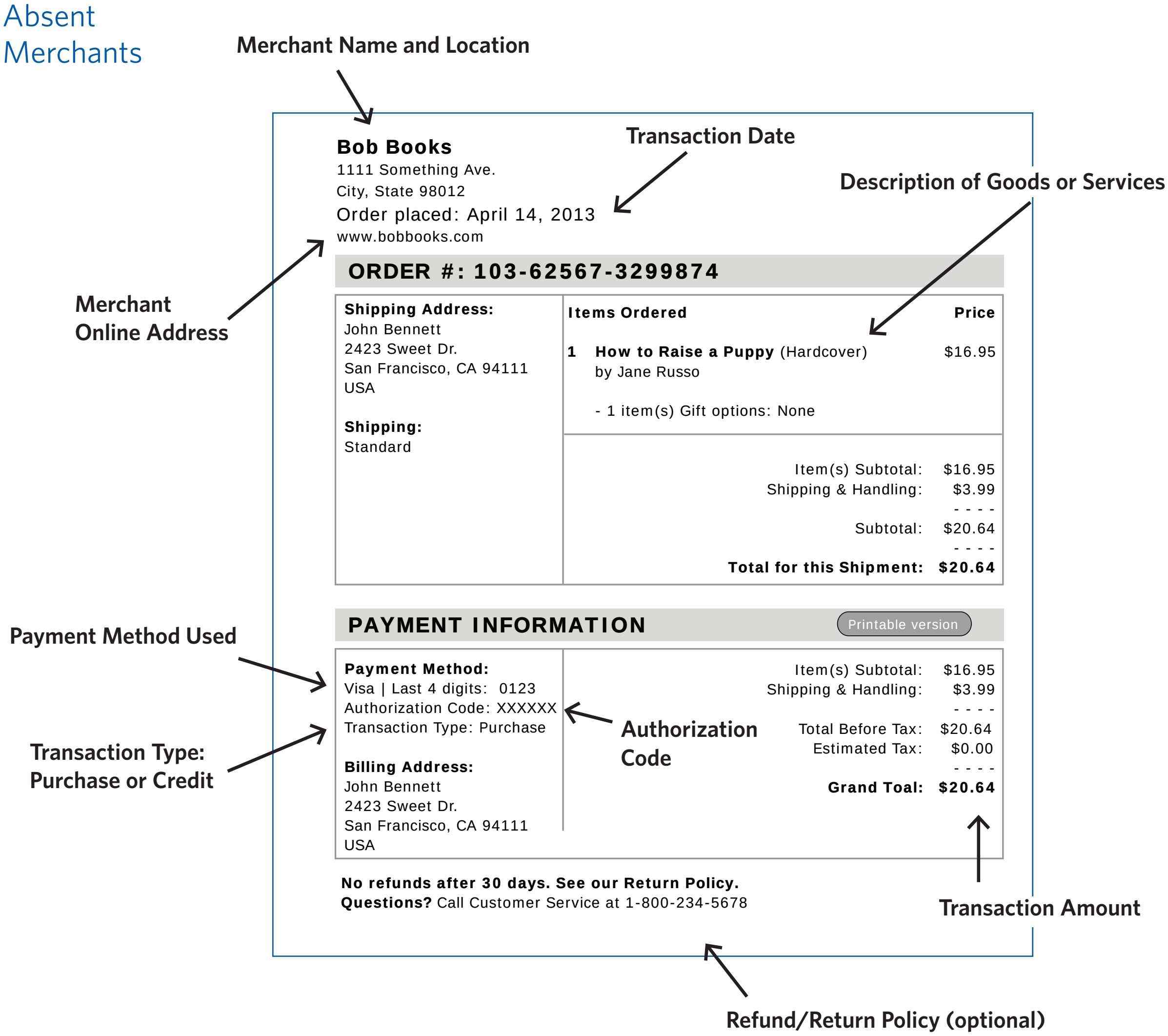
> **Quick Tip**
>
> When a sales draft request is not fulfilled in a timely manner, or if the copy is illegible or it does not contain all of the required data, it almost always results in a chargeback. It is in your best interest to respond promptly to a sales draft request.

The merchant must then send the transaction receipt copy to the acquirer who sends it on to the issuer.

Transaction Receipt Requirements for Card-Absent Merchants

The following are the Visa requirements for all manually printed transaction receipts in the card-absent environment.

Manual Transaction Receipts



Bob Books
1111 Something Ave.
City, State 98012
Order placed: April 14, 2013
www.bobbooks.com

ORDER #: 103-62567-3299874

Shipping Address:	Items Ordered	Price
John Bennett 2423 Sweet Dr. San Francisco, CA 94111 USA	1 **How to Raise a Puppy** (Hardcover) by Jane Russo - 1 item(s) Gift options: None	$16.95
Shipping: Standard	Item(s) Subtotal: Shipping & Handling: Subtotal: **Total for this Shipment:**	$16.95 $3.99 - - - - $20.64 - - - - **$20.64**

PAYMENT INFORMATION Printable version

Payment Method: Visa | Last 4 digits: 0123 Authorization Code: XXXXXX Transaction Type: Purchase **Billing Address:** John Bennett 2423 Sweet Dr. San Francisco, CA 94111 USA	Item(s) Subtotal: Shipping & Handling: Total Before Tax: Estimated Tax: **Grand Toal:**	$16.95 $3.99 - - - - $20.64 $0.00 - - - - **$20.64**

No refunds after 30 days. See our Return Policy.
Questions? Call Customer Service at 1-800-234-5678

The Chargeback Life Cycle

The diagram below illustrates the key actions that issuers and acquirers typically take in a customer dispute situation.

1. Cardholder

- Disputes transaction.
- Contacts card issuer with disputed information.

2. Card Issuer

Reviews eligibility of transaction for chargeback. If appropriate, returns transaction (charges it back) to merchant's acquiring bank through Visa (electronically).

3. Visa

- Electronically screens chargeback for technical criteria compliance.
- If appropriate, forwards chargeback to merchant's acquiring bank (electronically).

4. Acquirer

Receives chargeback and resolves issue, or forwards to merchant.

5. Merchant

- Receives chargeback.
- If appropriate, and under certain conditions, can re-present chargeback to its acquiring bank.
- If conditions aren't met, merchant may have to accept chargeback.

6. Acquirer

Forwards re-presented item to Visa.

7. Visa

- Electronically screens re-presentment for technical criteria compliance.
- If appropriate, forwards re-presentment to card issuer (electronically).

8. Card Issuer

Receives re-presented item and, if appropriate, re-posts to cardholder's account. If chargeback issue is not appropriately addressed, card issuer may submit dispute to Visa.

9. Cardholder

Receives information resolving initial dispute and may be re-billed for item or receives credit.

Arbitration

If the card issuer disputes a representment from the acquirer, the card issuer may file for arbitration with Visa. In arbitration, Visa decides which party is responsible for the disputed transaction. In most cases, Visa's decision is final and must be accepted by both the card issuer and the acquirer. During arbitration, the Visa reviews all information/documentation submitted by both parties to determine who has final liability for the transaction.

Compliance

Members may submit a compliance case to Visa for review if members incur a loss and a valid chargeback or representment is unavailable.

Nine Top Fraud Schemes Every E-Commerce Merchant Should Know

As technology becomes more sophisticated and accessible, new opportunities for fraud arise. In a recent study* involving 81 e-commerce merchants, CyberSource® partnered with the Merchant Risk Council (MRC) to survey its members on the top fraud attacks that were most impactful to them in terms of frequency of attack and revenue. The results yielded these top nine fraud schemes—shown here in ranked order.

1. Clean Fraud
2. Account Takeover
3. Friendly Fraud
4. Identity Theft
5. Affiliate Fraud
6. Re-Shipping
7. Botnets
8. Phishing, Pharming, and Whaling
9. Triangulation

Constant and consistent vigilance is key to mitigating e-commerce fraud. It could be a year, a month, or a week, but eventually fraudsters will identify the path of least resistance. The only way to counter the fraud threat is through effective fraud management, consistently monitoring and updating fraud prevention configurations as fraud schemes change.

For merchants, chargebacks can be costly. You can lose the dollar amount of the transaction being charged back and incur your own internal costs for processing the chargeback. Since you control how your employees handle transactions, you can prevent many unnecessary chargebacks by simply training your staff to pay attention to a few details.

*Survey of Merchant Risk Council members conducted in 2012.

1. Clean Fraud	Clean fraud is a transaction that passes a merchant's typical checks and appears to be legitimate, yet is actually fraudulent. For instance, the order has valid customer account information, an IP address that matches the billing address, accurate AVS and card verification number, etc.
2. Account Takeover	Account takeover is a type of identity fraud where criminals attempt to gain access to a consumer's funds by adding their information to the account (for instance, adding their name as a registered user to the account, changing an e-mail or physical address). Once armed with cardholder information, such as payment and bank account numbers, as well as other personal data, criminals can successfully pose as the actual account cardholder and make online purchases.
3. Friendly Fraud	Friendly fraud occurs when a merchant receives a chargeback because the cardholder denies making the purchase or receiving the order, yet the goods or services were actually received. In some instances, the order may have been placed by a family member or friend that has access to the buyer's cardholder information.
4. Identity Theft	Identity theft is the fraudulent acquisition and use of sensitive personal information, such as National Identification numbers (e.g., Social Security Numbers), passports, and driver's licenses. This information enables a skilled thief to assume an individual's identity and conduct numerous crimes.
5. Affiliate Fraud	Affiliate fraud scams involve the fraudulent use of a company's lead or referral programs to make a profit. For instance, fraudsters may submit phony leads with real customer information, or inflate web traffic in order to increase their payout before the merchant is aware of the scam.
6. Re-Shipping	A common re-shipping scam involves fraudsters that recruit an innocent person (referred to as a mule) to package and re-ship merchandise purchased with stolen credit cards. Since the mule has a legitimate shipping address, the merchant would have no reason to suspect fraud. The fraudsters then ask the unsuspecting individual to re-package and send the goods to them.
7. Botnets	A botnet is a network of infected machines controlled by a fraudster (the "botmaster") to perpetrate a host of crimes. In the case of e-commerce, the infected device could be used with stolen payment and identity information, and appear as though the transaction were originating from a location that reasonably matches the credit card in use. In this way, infected computers appear to be "good", when in fact they are not.

8. Phishing, Pharming, and Whaling

Phishing is the practice of sending seemingly official e-mails from legitimate businesses to steal sensitive personal information from customers, such as account log-in details, passwords and account numbers.

Pharming re-directs website traffic to an illegitimate site where customers unknowingly enter their personal data.

Whaling is a variation of phishing, but targets or "spears" a specific subset of consumers, customers, or employees. Fraudsters send tailored messages that appear as though they originate from within the targeted entity's organization, sent by another staff member, known business partner, or other trusted party.

9. Triangulation

Triangulation enables fraudsters to steal credit card information from valid customers, typically through online auctions, ticketing sites, or online classified ads. A fraudster posts a product online at a severely discounted price, which is purchased by a customer using a valid credit card. The fraudster uses other stolen payment credentials to purchase and ship the product from a legitimate website to the customer. Neither the merchant nor the customer suspects anything, yet both have been duped. In the meantime, the fraudster now has access to the unsuspecting buyer's credit card number and can continue to steal and amass other credit card numbers using the same scheme.

In all of these cases, effectively combating fraud can be distilled into three points: data, intelligence, and action. Merchants need to gain access to as much relevant data as possible, work to develop fraud intelligence through thorough analysis of that data, and then act swiftly to shut the fraud schemes down, adopting a layered approach to security.

Section 2

E-Commerce Risk Management Best Practices

What's Covered

- Fifteen Steps to Managing E-Commerce Risk
- E-Commerce Start-Up
- Website Utility
- Fraud Prevention
- Visa Card Acceptance
- Payment Card Industry Data Security Standard
- Chargeback and Loss Recovery

Fifteen Steps to Managing E-Commerce Risk

The following steps have been identified as those that are most important to managing e-commerce risk. These steps serve as a general framework for the best practices presented in this section.

E-COMMERCE START-UP	
1. Know the risks and train your staff	Your exposure to e-commerce risk depends on your business policies, operational practices, fraud prevention and detection tools, security controls, and the type of goods or services you provide. Your entire organization should have a thorough understanding of the risks associated with any Internet transaction and should be well-versed in your unique risk management approach.
2. Select the right acquirer/ payment processor and service provider(s)	If you have not yet launched an electronic storefront, you need to partner with a Visa acquirer/payment processor that can provide effective risk management support and demonstrate a thorough understanding of Internet fraud risk and liability. You also want to take a good, hard look at any service provider before you sign a contract. Bottom line? Does the service provider have what it takes to keep your cardholder data safe and minimize fraud losses?

WEBSITE UTILITY	
3. Develop essential website content	When designing your website, keep operational needs and risk factors foremost in your mind. Key areas to consider are privacy, reliability, refund policies, and customer service access.
4. Focus on risk reduction	Your sales order function can help you efficiently and securely address a number of risk concerns. You can capture essential Visa card and cardholder details by highlighting required transaction data fields and verifying the Visa card and customer data that you receive through the Internet.

Fifteen Steps to Managing E-Commerce Risk

FRAUD PREVENTION	
5. Build internal fraud prevention	By understanding the purchasing habits of your website visitors, you can protect your business from high-risk transactions. The profitability of your virtual storefront depends on the internal strategies and controls you use to minimize fraud. To avoid losses, you need to build a risk management infrastructure, robust internal fraud avoidance files, and intelligent transaction controls.
6. Use Visa tools	To reduce your exposure to e-commerce risk, you need to select and use the right combination of fraud prevention tools. Today, there are- a number of options available to help you differentiate between a good customer and an online thief. Key Visa tools include Address Verification Service (AVS)*, Card Verification Value 2 (CVV2)**, and Verified by Visa.
7. Apply fraud screening	Fraud-screening methods can help you minimize fraud for large-purchase amounts and for high-risk transactions. By screening online Visa card transactions carefully, you can avoid fraud activity before it results in a loss for your business.
8. Implement Verified by Visa	The tool Verified by Visa can create the most significant reduction in merchant risk exposure by increasing transaction security through cardholder authentication and by providing chargeback protection against fraud. E-commerce merchants who work with their acquirers to implement Verified by Visa are protected from certain fraud-related chargebacks on all Consumer and Commercial cards with limited exceptions. If applicable, E-commerce merchants may receive a reduced interchange rate.
9. Protect your merchant account from intrusion	Using sophisticated computers and high-tech smarts, criminals are gaining access to shopping cart and payment gateway processor systems, attacking vulnerable e-commerce merchant accounts, and making fraudulent merchant deposits. By taking proactive measures, you can effectively minimize this kind of cyber attack and its associated fraud risks.

VISA CARD ACCEPTANCE	
10. Create a secure process for routing authorizations	Before you accept Visa cards for online payment, you must ensure that you have a secure and efficient process in place to submit authorization requests through the Internet.
11. Be prepared to handle transactions post-authorization	There are a number of steps you can take to deal effectively with approved and declined authorizations before you fulfill an order. The idea here is to apply appropriate actions that best serve your business and the customer.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

Fifteen Steps to Managing E-Commerce Risk

CARDHOLDER INFORMATION SECURITY PROGRAM	
12. Safeguard cardholder data through PCI DSS compliance	The Payment Card Industry (PCI) Data Security Standard (DSS) provides e-commerce merchants with standards, procedures, and tools for data protection. For maximum security, you need reliable encryption capabilities for transaction data transmissions, effective internal controls to safeguard stored card and cardholder information, and a rigorous review of your security measures on a regular basis. PCI DSS compliance can help you protect the integrity of your operations and earn the trust of your customers.

CHARGEBACK AND LOSS RECOVERY	
13. Avoid unnecessary chargebacks and processing costs	For your business, a chargeback translates into extra processing time and cost, a narrower profit margin for the sale, and possibly a loss of revenue. It is important to carefully track and manage the chargebacks that you receive, take steps to avoid future chargebacks, and know your representment rights.
14. Use collection efforts to recover losses	You can often recover unwarranted chargeback losses through a well-thought through collections system.
15. Monitor chargebacks	Merchants with chargeback monitoring mechanisms are in a better position to spot excessive chargeback activity, identify the causes, and proactively bring chargeback rates down by applying appropriate remedial actions.

E-Commerce Start-Up

When establishing an e-commerce site, there are a number of risk management start-up strategies to consider. You can position your business for long-term success by training your staff in the importance of risk management, and educating them on the basic usage of the tools and technologies that you employ. You should also take the necessary time up front to ensure sound relationships with your acquirer and service provider(s).

Steps Covered

1. Know the Risks and Train Your Staff
2. Select the Right Acquirer and Service Provider(s)

1. Know the Risks and Train Your Staff

The cost of Internet fraud and/or security breaches make it imperative for merchants to clearly understand the risks of doing business online. Your entire organization should have a thorough working knowledge of the fraud and chargeback risks associated with any Internet transaction. They should also be well versed in your unique risk management approach. Consider these best practices when getting your business off the ground:

Risk Awareness

- **Be aware of the risks involved in selling on the Internet.** The more you know about the different kinds of risks involved, the better you will be at fine-tuning your business policies, operational practices, fraud prevention tools, and security controls. *(Listed on the next page are some of the typical types of risks that e-commerce merchants encounter.)*
- **Understand your direct responsibility for taking action to remedy and prevent chargebacks.** Follow your acquirer's processing instructions to avoid chargebacks related to authorizations and sales draft requests.
- **Work with your acquirer and/or payment processor to develop an understanding of the various reasons for chargebacks.** This is particularly important in regards to:
  - Transaction authorization requirements
  - Expired authorization rules for unshipped goods
  - Time limits for fulfilling sales draft requests
  - Cardholder disputes
  - Fraudulent use of account numbers
- **Know your rights to resubmit transactions that have been charged back for fraud reasons.**
- **Use Verified by Visa to substantially reduce fraud chargeback risk exposure.**

Key Point

In most cases, the full extent of your financial and administrative liability for chargebacks is spelled out in your merchant agreement.

Training

- **Train your employees in e-business risk management.** You can implement all of the controls you need to deter fraud, minimize customer disputes, and protect your site from hacker intrusions, but they won't mean much without proper employee training.

  To be truly effective, your entire staff should:
  - Have a thorough understanding of the fraud risk and security issues involved in an Internet transaction.
  - Know the chargeback rules and regulations for Internet transactions.
  - Be well versed in your risk management policies and procedures.

Typical Risks for E-Commerce Merchants

AREA	RISK POSSIBILITIES
Fraud	• Customer uses a stolen card or account number to fraudulently purchase goods/services online. • Family member uses payment card to order goods/services online, but has not been authorized to do so. • Customer falsely claims that he or she did not receive a shipment. • Hackers find their way into an e-commerce merchant's payment processing system and then issue credits to hacker card account numbers.
Account Information Theft (Cyber-Thieves)	Hackers capture customer account data during transmission to/from merchant. • Hackers gain access to service provider's unprotected payment processing systems and steal cardholder account data.
Account Information Theft (Physical Site)	• Unauthorized individual accesses and steals cardholder data stored at merchant or service provider site and fraudulently uses or sells it for unauthorized use or identity theft purposes. • Unscrupulous merchant or service provider employee steals cardholder data and fraudulently uses or sells it for unauthorized use or identity theft purposes. • Dumpster-divers steal unshredded account information from trash bins at merchant or service provider location.
Customer Disputes and Chargebacks	• Goods or services are not as described on the website. • Customer is billed before goods/services are shipped or delivered. • Confusion and disagreement between customer and merchant over return and refund. • Customer is billed twice for the same order and/or billed for an incorrect amount. • Customer doesn't recognize the merchant name on statement because merchant uses a service provider to handle billing. • Goods or services are billed without customer approval.

Key Points

Unauthorized use fraud involves a perpetrator who illegally obtains the account number of a valid cardholder to purchase goods and services from a legitimate Mail Order/Telephone Order (MO/TO) or Internet merchant. The card and number are valid but the "use" is not. Card-absent fraud is typically carried out to obtain high-priced but easily resold goods (e.g., computers, electronic items, jewelry, etc.) via the mail or standard shipping. There are a number of ways that criminals can get their hands on valid Visa account numbers. Some of the most common scenarios include system hackings, account number generation software, internal compromises, discarded receipts, deceptive solicitations, phishing schemes, and website cloning scams.

2. Select the Right Acquirer/Payment Processor and Service Provider(s)

When selecting an acquirer, payment processor, and/or your service provider(s), you need to carefully consider several important factors, particularly those related to risk management. Here are some essential best practices:

Acquirer/ Payment Processor Selection

The acquirer plays a key role in your e-commerce success by enabling you to accept Visa cards through the Internet and by ensuring the secure and efficient processing of the sales volume that results.

- **Ensure that the selected acquirer/payment processor can incorporate the required Verified by Visa authentication results in the authorization message.** This can pose a challenge in cases of split shipments when additional authorizations are obtained after the initial authorization.
- **Make sure the acquirer/payment processor support Visa's *Payment Card Industry (PCI) Data Security Standard (DSS)* requirements.** Although security can never be completely guaranteed, the PCI DSS requirements for e-merchants can help significantly reduce the ability of hackers to gain access to proprietary data.
- **Understand the terms and conditions of your acquirer contract.** Be sure that you read and understand all of the contract provisions, particularly in such areas as holding funds and chargeback liability. For best results, you should know:
  - The length of time and conditions under which your deposits may be held.
  - Your liability for fraudulent transactions. Remember, Internet transactions are classified as card-absent, which means you can be held responsible for a charge the cardholder claims he/she did not make, even if the authorization was approved by the issuer.
  - Your liability for losses resulting from compromised card data.
  - The nature and causes of chargebacks, including customer disputes, fraudulent activity, and technical issues.
  - Time frames for providing additional documentation to your acquirer in order to fulfill a sales draft request or represent a chargeback.

  For more information about the PCI DSS requirements, refer to the best practices on pages 63-67 of this guide.

Service Provider Selection

The service provider(s) you choose can help you successfully manage Internet payments and security risks, or leave you out on a limb to deal with fraudulent transactions and excessive chargebacks.

- **Research the service provider business.** Check your service provider's risk management track record and ability to perform to your expectations and industry requirements.

- **Make sure your service provider is in compliance with PCI DSS requirements.** To ensure protection for Internet transactions, partner with service providers who comply with Visa PCI DSS requirements and use:
  - Reliable transaction encryption capabilities to safeguard Internet data transmissions.
  - Effective internal security controls to protect stored data.
  - Rigorous review and testing of data security on a regular and ongoing basis.

  For more information about the PCI DSS requirements, refer to the best practices on pages 63-67 of this guide.

- **If you are using a third party to provide such merchant services such as online shopping carts, payment gateways, hosting facilities, data storage, authorization and/or clearing and settlement messages, make sure the business has been registered through your acquirer as a third party agent with Visa.** If you are not sure, confirm with your acquirer.
- **Partner with a risk-focused service provider.** If you are using a payment gateway for real time payment processing, work with a service provider who:
  - Has experience in online authentication.
  - Offers high-quality reliable fraud prevention options.
  - Follows payment industry risk management best practices.
  - Offers risk management support 24/7.

Website Utility

When building an e-commerce business, you need to establish a set of policies that clearly communicate where you stand on consumer privacy and information security, how billing and shipping will be handled, and what is involved in terms of credit refunds. In addition to being subject to legal requirements, full disclosure in these areas can help eliminate any customer misunderstandings and avoid unnecessary customer disputes. Another critical step in terms of risk reduction is to "design in" ways to capture pertinent card and cardholder details as part of the sales order process.

Steps Covered

3. Develop Essential Website Content
4. Focus on Risk Reduction

3. Develop Essential Website Content

The more a customer knows about your e-commerce business, the better! Unfortunately, customers aren't mind readers, so you can't expect them to enter your site knowing the basic "ins" and "outs" of the operation; particularly when it comes to policies covering privacy, billing, shipping, and refunds. To avoid any customer misunderstandings and downstream disputes, follow these best practices:

Privacy

- **Develop a clear, concise statement of your privacy policy and make it available to website visitors through links on your home page.** This practice may be subject to legal requirements. To allay customer concerns about providing personal data, your privacy policy should define:
  - What customer data is collected and tracked
  - With whom this information is shared, and
  - How customers can opt out
- **Register with a privacy organization and post a "seal of approval" on your website.**
  - Another way to allay customer concerns about providing personal data is to display a privacy "seal-of-approval" on your website home page.
  - To obtain this seal, you need to apply to a major privacy program such as TRUSTe or the Better Business Bureau's BBBOnLine Privacy.

Information Security

- **Create a page that educates customers about your site's information security practices and controls.**
  - Explain how card payment information is protected:
    - During transmission
    - While on your server, **and**
    - At your physical work site
  - Make the page available to all website visitors through lists on your home page.
- **Create an FAQ page that includes questions and answers on how customers can protect themselves when shopping online.**
- **If using Verified by Visa, add the logo to your home page, security information page, and checkout pages to promote reliable and secure online shopping.** Be sure to include clear instructions on how Verified by Visa works. *Your Merchant Toolkit includes the logo and a "Learn More" page that details the Verified by Visa program. The merchant toolkit is available on* www.visa.com.

- **Discourage the use of e-mail for transactions.** Due to misguided concerns about Internet security, some customers may send their card numbers to you by e-mail, which is a non-secure way to do business. To protect your customers and foster their loyalty, highlight security practices on your website and in any reply e-mail. Stress that:
  - E-mail is not a secure communication method and should never be used to transmit card numbers or other sensitive information.
  - The transaction encryption capabilities of your website offer reliable protection from unauthorized access and provide cardholders with the safest way to make purchases over the Internet.

Product Description

- **Make sure your goods or services are accurately described on your website.**
  - Develop clear, complete product descriptions to reduce customer disputes and dissatisfaction over the actual product received versus what is described on your website.
  - Use product images and photos, if possible.

> **Key Points**
>
> You are operating in a global market, which increases opportunities for unintended misunderstandings, miscommunication, or chargebacks. For example, if you sell electrical goods, be sure to state voltage requirements, which vary around the world.

Order Fulfillment Information

- **State time frames for order processing and send an e-mail confirmation and order summary within one business day of the original order.**
- **Provide up-to-date stock information if an item is back-ordered.**

Shipping

- **Develop a clear, comprehensive shipping policy and make it available to customers through a link on your home page and at the time of the online purchase.**
  - Explain shipping options and expected delivery.
  - Provide full disclosure of all shipping and handling fees.
- **Develop an e-mail response to inform customers of any goods or service delivery delays.**
- **Consider not providing the tracking number if you are selling higher fraud risk merchandise and are not allowing redirection of the shipment.** Online merchants have discovered fraudsters using the correct billing address and shipping to that address, then redirecting the merchandise. This practice could be applied selectively, based on merchandise type and amount

Billing Practices

- Develop a description of your billing practices terms and conditions and make them available to customers at the time of the online purchase.
  - Explain to customers when their Visa cards will be billed.
  - If you use a billing service provider, let the customer know how the transaction will be reflected on their payment card statement (i.e., the service provider name and amount will be shown). This will reduce the risk of confusion when the statement arrives.
- Encourage cardholders to retain a copy of the transaction.

Digital Content Policies

- Implement a policy that the cardholder will not be billed until the website service is actually accessed via the applicable password.
- Avoid the use of negative renewal options or other marketing techniques that may create a false expectation to cardholders that the product or service is "free."
- Ensure that all terms and conditions are clear and concise. Before a sale is conducted, you must clearly communicate any special restrictions to cardholders.

Transaction Currency or Currencies

- Fully disclose to the customer on the payments page of the website, the country in which you are currently operating and inform them of the transaction currency used for the purchase. Currency must be clearly stated on payment page of website, especially if the unit of currency is not unique, (e.g., a dollar could be an Australian, New Zealand, Hong Kong, or U.S. dollar.)
- Follow "active" Dynamic Currency Conversion (DCC) choice requirements for cardholders. A merchant is required to offer the cardholder a choice to accept DCC, following proper disclosure requirements—allow the cardholder to actively choose DCC. Active choice is defined as the cardholder taking an action to indicate his or her choice to accept DCC. Keep in mind, DCC must not be offered by default or as an "opt-out" option.
  - Do not complete a DCC transaction before the cardholder has actively made his or her choice of transaction currency and honor the cardholder's choice of currency. If the cardholder decides to decline the DCC offer, allow the cardholder to complete the transaction in the merchant's local currency, using the cardholder's original payment method of choice.
- Adhere to DCC service requirements. DCC is a merchant-offered currency conversion service that is provided by acquirers (or DCC agents). It is not a Visa service. With DCC transactions, the cardholder makes a purchase decision based on a price displayed in one currency — usually, but not always, the merchant's local currency. At checkout, the merchant converts the price to the currency agreed to by the cardholder (typically the cardholder's billing currency) and usually assesses conversion-related commissions, fees, and/or mark ups over a wholesale exchange rate or government-mandated rate.

- **Ensure proper DCC disclosure.** DCC disclosures must occur at the time the DCC offer is made and before the cardholder is asked to actively choose the transaction currency. If the cardholder actively chooses DCC, the transaction receipt must include the same disclosures previously provided to the cardholder in addition to all other required DCC information.

Country of Origin

- **Disclose the permanent address of your establishment on the website.** Check with your acquirer to ensure your disclosure is made in accordance with the *Visa International Operating Regulations* and local law.

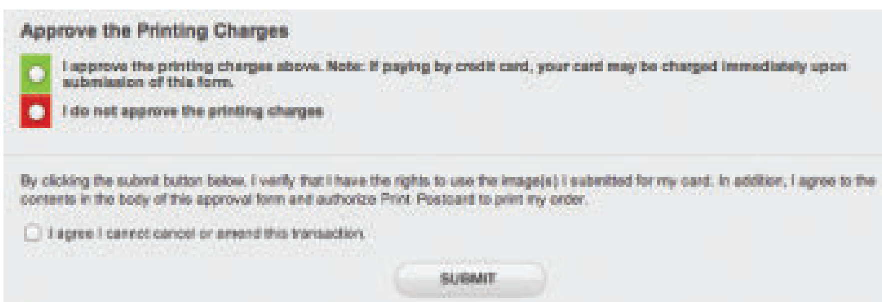
Refunds and Credits

- **Establish a clear, concise statement of your refund and credit policy.**
  - Make this statement available to website visitors through clearly visible links on your home page.
  - Provide "click through" confirmation for important elements of the policy. For example, when purchasing tickets for a sporting event, customers should be able to click on a button—"**Accept**" or "**I Agree**"—to acknowledge that they understand that the tickets are non-returnable unless the event is postponed or cancelled.

> **Key Points**
>
> Your refund and credit policy should be consistent with your business objectives and the goods or services you provide. For best results, try to find the right balance between excellent customer service and excellent risk management.

Recurring Transaction

- **Clearly display your recurring transaction disclosure statement on the screen.** Require the cardholder to "click and accept" the disclosure statement to confirm that he or she has read it.



Customer Service Access

- **Provide an e-mail inquiry option.** Your customers are likely to have questions or concerns regarding their online purchase. By offering your customers an easy way to contact you and by providing them with a prompt response, you can help avoid customer disputes and subsequent chargebacks.
  - Display prominent and easily accessible e-mail "Contact Us" options on your website.
  - To facilitate efficient internal processing of customer responses, provide different e-mail contacts for product/service information, customer support, and back order/shipping information.

Key Points

Some customers may have questions or concerns, and are not comfortable with e-mail correspondence. Though telephone customer service can be costly, it can help minimize customer disputes and preserve customer relationships that might otherwise be lost.

- **Develop an e-mail inquiry response policy.**
  - Use auto-responder e-mail programs to acknowledge receipt of e-mail inquiries and set expectations regarding the timing of complete responses.
  - Make sure that you have adequate staff in your customer service e-mail response group to provide timely and robust responses to e-mail inquiries.
- **Establish e-mail inquiry response standards and monitor staff compliance.**
  - Establish a standard time frame for responding to 100 percent of e-mail inquiries, (e.g., 24 hours). Use shorter time frames for responding to 75 percent or 95 percent of e-mail inquiries.
  - Monitor your customer service e-mail response group to ensure that these standards are met and, if necessary, add or reschedule staff to improve performance.
  - Monitor your compliance with e-mail response standards on a daily basis.
- **Offer local and toll-free telephone customer service support and display your phone numbers on your website.**
  - Provide links on your home page to a toll-free customer service number that cardholders can use to get a quick response to an inquiry.
  - Adequately staff and schedule customer service staff to respond to telephone inquiries on a timely basis.

Delivery Policy

- **Clearly state any product or service delivery policy restrictions on your website.** This is particularly important if you have geographic or other restrictions that may impact under what circumstances you will provide delivery.

4. Focus on Risk Reduction

Your sales order function should address the unique risk characteristics of your e-commerce business. Key factors to consider include how you will identify customers, what transaction data fields customers will be required to complete, what controls are needed to avoid duplicate orders, and how you will validate both the card and cardholder during an Internet transaction. Consider the best practices outlined here to reduce your risk exposure:

Passwords and Cookies

- **Make effective use of permanent web browser cookies to recognize and acknowledge existing customers.**
  - Use permanent browser cookies to retain non-sensitive cardholder information and preferences to enable repeat customers to order goods or services at your site without having to re-enter this information.
  - Use browser cookies to maintain active user sessions, but once a session expires, request that the user log in again, regardless of the computer being used.
- **Establish ways to assist customers who forget their passwords.** To help stop fraudsters in their tracks, consider either one or both of the approaches described below.
  - To verify the registered customer's identity, use customer-provided security data.
    - Ask the customer at the time of registration to select a data category question—such as their grammar school name or place of birth—and also provide the correct response.
    - If a returning customer forgets his or her password, prompt the customer to provide the correct response to the data category question selected during registration.
    - Verify the response. If it is correct, prompt the customer to reset their password.
  - Use customer-selected hints to help the customer remember the password.
    - Ask the customer at the time of registration to select a password hint.
    - Display this hint on the website if the customer enters the wrong password during log in.

Required Transaction Data Fields

- **Establish transaction data fields that can help you detect risky situations, and require the customer to complete them.** Certain transaction data fields can play an important role in helping you assess the fraud risk of a transaction. To minimize losses, define the data fields that will help you recognize high-risk transactions, and require customers to complete these fields before purchasing goods or services. Key risk data fields include the following:
  - Demographic information, such as telephone numbers, that can be validated using reverse directory look-ups.
  - E-mail address, particularly when it involves an "anonymous" service.
  - Cardholder name and billing address, which can be validated using directory look-up services.
  - Shipping name and address, particularly if this information is different from the cardholder's billing information.
  - Card Verification Value 2 (CVV2)*, especially for websites selling higher risk goods or services. However, attempt to review, rather than automatically decline, mismatches with no other risk indicators.
- **Highlight the data fields that the customer must complete.** Use color, shading, bold fonts, or asterisks to highlight the required data fields and accompany this with explanatory notes to the cardholder.
- **Edit and validate required data fields in real time to reduce risk exposure.**
  - Provide instant feedback to Internet customers when their required data fields are incorrect or incomplete.
  - Send a "correction required" message to the customer if the data in any field was not complete or not submitted in the proper format.
  - In the return message, identify the field that requires completion if a cardholder omits a required field.
  - Allow customer to page back, correct personal information, or alter the request while retaining previously entered information.

Avoiding Duplicate Numbers

- **Develop controls to avoid duplicate transactions.** Duplicate orders can lead to higher processing costs and customer dissatisfaction. Establish controls to prevent cardholders from inadvertently submitting a transaction twice.
  - Require customers to make positive clicks on order selections rather than hit the "Enter" key.
  - Display an "Order Being Processed" message to customers after they have submitted a transaction.
  - Systematically check for identical orders within short time frames and out-sort these for review to ensure that they are not duplicates.
  - Send e-mail messages to customers to confirm whether a duplicate order was intentional.

*In certain markets, CVV2 is required for card-absent transactions.

Card Information Validation

- **Implement a "Mod 10" card number check before submitting a transaction for authorization.**
  - Ask your acquirer for the "Mod 10" algorithm that lets you quickly check the validity of a card number presented for purchase.
  - Use the "Mod 10" check for all Internet transactions before submitting them for authorization.
  - Provide immediate feedback to the customer if the card number fails to pass the "Mod 10" check. For example, send a message that says: "*The Visa card number you entered is not valid. Please try again.*"
  - Do not request authorization until the account number passes the "Mod 10" check.

> **Key Points**
>
> Always use a "Mod 10" check to determine whether an entered Visa card number is valid. This simple precaution can help avoid the expense and delay that results when a cardholder enters a valid card number incorrectly, (e.g., a Visa cardholder enters a wrong number or transposes digits, and then receives an authorization decline.)

- **Display only the last four digits when showing a card number to a repeat customer at your website.** This not only reduces fraud risk, but also fosters customer confidence in your secure handling of personal information. The last four digits will give the customer enough information to identify the card and determine whether to use it or select another card for the transaction.

Cardholder Information Validation

- **Check the validity of the customer's telephone number, physical address, and e-mail address.** Simple verification steps can help alert you to data-entry errors made by customers and may also uncover fraudulent attempts.
  - Use a telephone area code and prefix table to ensure that the entered area code and telephone prefix are valid for the entered city and state. Identify mismatches and allow the cardholder to re-enter if desired. The information initially entered may be valid due to recent additions or changes in telephone area codes.
  - Use a ZIP code table to verify that the entered ZIP code is valid for the entered city and state. Allow cardholders to override alerts—the information may actually be valid due to delayed updates or erroneous data.
  - Test the validity of the e-mail address by sending an order confirmation.

High-Risk International Address Screening

- **Screen for high-risk international addresses.** Accepting transactions from certain international locations may carry high levels of risk.
  - Ask your acquirer for assistance in identifying high risk countries heavily involved in Internet fraud.
  - Test market and track fraud experience to various international locations.

- Perform additional screening and verification for higher-risk transactions, for example:
  - Obtain issuer contact information from your acquirer and call to confirm cardholder information for first-time buyers.
  - Require the billing address and shipping address to be the same.
- Capture and translate the Internet Protocol (IP) address to identify the computer network source.
  - Use a geo-location software/service to determine the IP address country.
  - Match the IP address country with the billing and shipping address country. If the countries do not match, out-sort the order for further review.

Recurring Transaction Setup and Processing

- **To set-up a recurring charge, obtain consent from the cardholder.** Include the following:
  - Transaction amount or minimum or maximum transaction amounts, if the transaction may vary
  - Frequency of the recurring charges
  - Duration of time that cardholder permission is granted
- **Ensure that all applicable state or federal laws are followed when establishing this agreement with the cardholder.** Visa recommends that the merchant consult with their own legal counsel.
- **Retain a copy of the cardholder's consent for the duration of the recurring services and provide a copy if requested by the issuer.**
- **Obtain all relevant card payment details to complete the transaction.** This includes:
  - Cardholder name and billing address
  - Card type/Account number
  - Card expiration date
  - CVV2*

Key Points

Interchange rates are set based on the authorization and processing methods used whether or not additional information is provided in the transaction record and the type of card used at the point of sale.

For security purposes *Visa International Operating Regulations* prohibit merchants from storing CVV2 data.

*In certain markets, CVV2 is required for card-absent transactions.

- **Obtain an authorization and a valid approval.**
  - Include the expiration date in the authorization request
  - Use Visa detection tools to verify the legitimacy and accuracy of the Visa cardholder and card.

TO VERIFY:	THEN:
Card information	Use Visa Account Updater (VAU)
Cardholder billing address	Use AVS* (if available)
Card authenticity	Submit CVV2** as part of the authorization request
Cardholder's authenticity online	Implement Verified by Visa

Key Points

The *Visa Account Updater (VAU)* service allows Visa merchants, acquirers, and issuers to electronically exchange the most current cardholder information, card expiration dates, account status, and more. This safety net helps merchants retain customers by reducing declined card transactions that can interrupt the payment process. (See VAU Service Best Practices on page 42.)

- **Check the authorization response and take the appropriate action based on the response.** If you receive a decline response for any reason other than "lost", "stolen", or "pick-up", you may retry the authorization if it is cost-effective for your business to do so. **Note: An authorization may be retried up to a maximum of four times within 16 calendar days of the original request.**

In determining the number and frequency of authorization attempts, merchants should take into account, among other factors, the incremental cost of retrying the authorization and the transaction amount. The *Visa International Operating Regulations* prohibit depositing a declined transaction. To view a copy of the *Visa International Operating Regulations*, visit www.visa.com.

Customer Satisfaction

- **Provide customers with a toll-free phone number, an e-mail address, and/or easy to find (and use) online procedures for cancelling recurring transactions.**
- **Train sales and customer service staff on the proper procedures for processing recurring transactions.** This is important as these transactions are particularly customer service sensitive.
- **Fully disclose all necessary transaction terms and conditions.**

Key Point

Voice plus is often used by merchants to capture the cardholder's voice or key tones as confirmation.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

VAU Service

- **Utilize the VAU service to verify that the cardholder's on-file information, account number, and/or expiration date, are correct.**
  - Keep the expiration date on file and include the expiration date in all authorization requests.
  - To reduce possible fraud, use the AVS* (if available) on every transaction.
  - Ensure that all recurring transactions are identified with a unique processing code ("50"), market-specific authorization data indicator ("B") and electronic commerce indicator ("2" for recurring or "3" for installment).
  - Notify the customer of the transaction before or at the time of billing.
  - Put proper controls in place to protect account and transaction information. All merchants must meet the Payment Card Industry (PCI) Data Security Standard (DSS) basic requirements.
  - Do not store CVV2** data.

Recurring Transaction Cancellation

- **Check customer logs daily for cancellation or non-renewal requests related to recurring transactions.** Take the appropriate action and comply in a timely manner. Notify the customer that his/her recurring payment account has been closed.
- **Process all credits promptly.** If a cancellation request is received too late to prevent the most recent recurring charge from posting to the customer's account, process the credit and notify the cardholder.
- **Flag transactions that exceed preauthorized amount ranges.** Notify customers at least ten days in advance of submitting a recurring transaction billing.
- **Check customer logs daily for customer complaints.** Pay particular attention to complaints relating to transaction amounts or failure to notify customers in advance of a recurring transaction that exceeds the preauthorized amount range. Follow up with customer.
- **Provide the cardholder with the recurring transaction cancellation number.**

> **Key Points**
>
> To minimize chargebacks and transaction processing costs, submit transaction payment information to your acquirer or payment processor in a timely manner.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

Fraud Prevention

There are plenty of cyber-thieves out there ready to pull a virtual scam or two. They operate anonymously, steal from the e-commerce merchant, and leave that business on the hook for associated losses. Given this reality, you just can't take a leap of faith when it comes to accepting payments online. The good news, however, is that today's e-commerce merchant has many options when it comes to combating card payment fraud. To protect your business, you need to build a reliable risk management system that supports robust internal negative files, intelligent transaction controls, and highly adaptive fraud detection tools.

Steps Covered

5. Build Internal Fraud Prevention Capability
6. Use Visa Tools
7. Apply Fraud Screening
8. Implement Verified by Visa

5. Build Internal Fraud Prevention Capability

To reduce losses associated with risk exposure, you must implement internal fraud detection and prevention measures and controls that make sense for your business environment. The following best practices can assist you in this area:

Risk Management Infrastructure

A dedicated fraud control individual or group can provide the direction that your business needs to deter fraud.

- **Establish a formal fraud control function.**
  - Make fraud prevention and detection your highest priority.
  - Develop day-to-day objectives that promote profitability, for example:
    - Reduce fraud as a percentage of sales.
    - Minimize the impact of this effort on legitimate sales.
  - Clearly define responsibilities for fraud detection and suspect transaction review.
  - For larger merchants, encourage fraud control group members to work closely with the chargeback group, identify causes of chargeback loss, and use this information to improve fraud prevention efforts.
- **Track fraud control performance to understand the impact of fraud on your business.** You can ensure and improve the effectiveness of your fraud control group by monitoring these areas:
  - Gross fraud as a percentage of sales.
  - Fraud recoveries as a percentage of gross fraud.
  - Timeliness in reviewing and dispositioning suspicious transactions.
  - Occurrences of complaints from legitimate customers.

Internal Negative File

- **Establish and maintain an internal negative file.** Make use of the details of your own history with fraudulent transactions or suspected fraud. By storing these details, you will gain a valuable source of information to protect you from future fraud perpetrated by the same person or group.
  - Record all key elements of fraudulent transactions such as names, e-mail addresses, shipping addresses, customer identification numbers, passwords, telephone numbers, and Visa card numbers used. *For information security purposes, all merchants are prohibited from storing Card Verification Value 2 (CVV2)* data.*

> **Key Points**
>
> When building and maintaining an internal negative file, implement procedures to ensure that only details from fraudulent transactions are stored and recorded. Information related to customer disputed transactions and/or chargebacks should not be included in your internal negative file.

*In certain markets, CVV2 is required for card-absent transactions.

   - Establish a process to remove from the file or flag information about legitimate customers whose payment data has been compromised. Criminals may use the personal data of innocent victims to commit the fraud.

- **Use the internal negative file to screen transactions.** If transaction data matches negative file data, decline the transaction, or—if warranted—out-sort the transaction for internal review and follow up with the appropriate action.

Transaction Controls

- **Establish transaction controls and velocity limits.** You can significantly reduce risk exposure by using internal transaction controls to identify high-risk transactions. These controls help determine when an individual cardholder or transaction should be flagged for special review.
   - Set review limits based on the number and dollar amount of transactions approved within a specified period of time. Adjust these limits to fit average customer purchasing patterns.
   - Set review limits based on single transaction amounts.
   - Ensure that velocity limits are checked across multiple characteristics including shipping address, telephone number, and e-mail address.
   - Adjust velocity limits as customers build history with your business. The limits should be set tighter for new customers and looser for those customers who have a solid purchasing and payment track record.
   - Contact customers that exceed these limits to determine whether the activity is legitimate and should be approved, providing that the issuer also approves the transaction during the authorization process.

> **Key Points**
>
> You can determine individual customer preferences by tracking the purchase activity of registered customers. Deviations from these patterns may be an indication of fraud.

- **Modify transaction controls and velocity limits based upon transaction risk.** Vary transaction controls and velocity limits to reflect your risk experience with selected products, shipping locations, and customer purchasing patterns.

6. Use Visa Tools

Visa offers several powerful tools that can be used to help you check for fraud during a Visa card payment authorization. To ensure safe and secure transaction processing, apply these best practices:

Card Type and Account Number

- **Ask the customer for both a card type and an account number, and make sure that they match.**
  - Offer a "card type" selection on your sales order page. The cardholder uses this feature to choose and identify a card type before entering the account number.
  - Compare the card type selected by the customer and the first digit of the entered account number to ensure a positive match. For example, if the card type is "Visa" and the account number begins with "4," the match is positive.
  - Invoke an "error message" if the first digit of the account number does not match the selected card type.
  - Enable cardholders to enter account numbers with or without hyphens, or with spaces between, or clearly designate the preferred format.

Key Points

Different types of payment cards have different account numbering systems. For example, only Visa card account numbers begin with a 4.

Card Expiration Date

- **Require the cardholder to enter the card expiration (or Good Thru) date or select it from a pull-down window.**
  - To play it safe, do not offer a default month and year for the card expiration date. The cardholder may erroneously select the default date, which will most likely differ from the actual card expiration date. Most issuers decline the transaction when this error occurs.

Key Point

An Internet order containing an invalid or missing expiration date may indicate counterfeit or other unauthorized use.

Card Verification Value 2 (CVV2)

- Work with your acquirer to implement CVV2*.
- Use Visa's CVV2 code to verify the card's authenticity.
  - Ask card-absent customers for the last three numbers in or beside the signature panel on the back of their Visa cards.
  - If CVV2 is not legible to the customer, use your external policy to determine CVV2 code acceptance that signifies that the CVV2 is not legible
  - If the customer provides a CVV2, submit this information with other transaction data (i.e., card expiration date and account number) for electronic authorization. You should also include one of the following CVV2 presence indicators, even if you are not including a CVV2 in your authorization request:

INDICATOR	WHAT IT MEANS
0	CVV2 is not included in authorization request.
1	CVV2 is included in authorization request.
2	Cardholder has stated that CVV2 is illegible.
9	Cardholder has stated that CVV2 is not on the card.

  - Evaluate the CVV2 result code you receive with the transaction authorization, and take appropriate action based on all transaction characteristics.

CVV2 RESULT CODE	RECOMMENDED ACTION
M – Match	Complete the transaction, taking into account all other transaction characteristics and verification data.
N – No Match	View a "No Match" response as a sign of potential fraud, which should be taken into account along with the authorization response and any other verification data. You may also want to resubmit the CVV2 to ensure a key-entry error has not occurred.
P – CVV2 request not processed	Resubmit the authorization request.
S – CVV2 should be on the card, but the cardholder has reported that it isn't	Follow up with the customer to verify that the correct card location has been checked for CVV2.
U – Card issuer does not support CVV2	Evaluate all available information and decide whether to proceed with the transaction or to investigate further.

Key Point

Actions taken by e-commerce merchants in response to a CVV2 "No Match," will vary by industry. Apply procedures that make sense for your particular business. Contact your acquirer to determine the appropriate CVV2 actions for your operation.

*In certain markets, CVV2 is required for card-absent transactions.

Address Verification Service (AVS)

- **Work with your acquirer to implement AVS*.** Several options are available to you depending on your card-absent transaction volume.
  - Contact your acquirer for more information and to determine which approach best meets your business needs.
  - Ask your acquirer for a copy of the *Merchant Guide to the Address Verification Service* (or order this book directly through Visa Fulfillment). (*For order information, refer to Section 3: Resources.*)
- **Use AVS to verify the cardholder's billing address (street number and ZIP code).** When a customer contacts you to place an order,
  - Confirm the usual order information.
  - Ask 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.)
  - Enter the billing address and the transaction information into the authorization request system and processes both requests at the same time.

  The card issuer will:
  - Make an authorization decision separately from AVS request and compare the cardholder billing address sent with the billing address for that account.
  - Return 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.
- **Evaluate the AVS response code and take appropriate action based on all transaction characteristics and any other verification information received with the authorization (i.e., expiration date, CVV2**, etc.).** An authorization response always takes precedence over AVS. Do not accept any transaction that has been declined, regardless of the AVS response.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

AVS Result Codes

One of the following AVS* result codes will be returned to the merchant indicating the card issuer's response to the AVS request. A merchant's acquiring 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. (Acquirer sent both street address and postal or ZIP code.)	✔	✔
C	Street address and postal code or ZIP code not verified due to incompatible formats. (Acquirer 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. Card issuer is not an AVS participant, or AVS data was present in the request but card issuer did not return an AVS result, or Visa performed address verification on behalf of the card issuer and there was no address.		✔
I	Address information not verified		✔
M	Street addresses and postal and ZIP codes match.		✔
N	No match. Acquirer 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. Acquirer 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. Card issuer ordinarily performs address verification but was unavailable. Visa uses code R when card 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 acquiring bank for further questions on AVS result codes.

Key Point

If you a complete a transaction for which you received an authorization approval and an AVS response of "U" (unavailable), and the transaction is later charged back to you as fraudulent, your acquirer may represent the item. U.S. card issuers must support AVS or lose their right to fraud chargebacks for card-absent transactions. Card issuers also lose fraud chargeback rights for "U" responses in CVV2* request situations.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

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-absent industry practices and may be helpful. Merchants should establish their own policy regarding the handling of transactions based on AVS** result codes.

U.S. CODE	INT'L CODE	DEFINITION	EXPLANATION	ACTION(S) TO CONSIDER
Y F**	D M	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 card 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 card 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.	"No match" responses clearly warrant further investigation. You will probably want to follow up with the cardholder before shipping merchandise. The cardholder may have moved recently and not yet notified the card 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.

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.

Key Points

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

* In certain markets, CVV2 is required to be present for all card-absent transactions.

** AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

*** United Kingdom

7. Apply Fraud Screening

Today, there are a wide variety of fraud-screening technologies and practices available to help you assess the risk of a transaction and increase the likelihood that you are dealing with a legitimate customer with a valid Visa card. Fraud-screening tools can be developed internally or acquired from third parties. Best practices in this area include:

Screening for High-Risk Transactions

Implement fraud-screening tools to identify high-risk transactions.

- Develop effective and timely manual review procedures to investigate high-risk transactions. The goal here is to reduce fraud as a percentage of sales and minimize the impact of this effort on legitimate sales.
- Suspend processing for transactions with high-risk attributes. This can include transactions that:
  - Match data stored in your internal negative files.
  - Exceed velocity limits and controls.
  - Generate an Address Verification Service (AVS)* mismatch.
  - Match high-risk profiles (as discussed in this section).

- **Treat international IP addresses as higher risk.** Merchants have found that international IP addresses have a substantially higher fraud rate than domestic addresses. By classifying international IP addresses as higher risk, you can require these transactions to meet higher-risk hurdles. For example, to match on Card Verification Value 2 (CVV2)** and AVS.
- **Require shipping address to match billing address for higher risk transactions.** Such transactions can include:
  - Larger transaction size
  - Type of merchandise
- **Screen for high-risk shipping addresses.** You can reduce fraud by comparing the shipping address given by the customer to high-risk shipping addresses in third party databases and in your own negative files.
  - Pay special attention to high-risk locations such as mail drops, prisons, hospitals, and addresses with known fraudulent activity.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

- **Treat international transactions as higher risk.** Transactions that involve cards issued outside of your country carry higher levels of risk. Require greater scrutiny and verification for international transactions:
  - Tighten transaction controls and velocity thresholds for these transactions to increase screening frequency.
  - Treat with high suspicion billing addresses and shipping addresses that are not the same.
  - Be on the lookout for customers who use anonymous e-mail addresses.
  - Use a third party fraud scoring for international transactions.
  - Assess risk based on such transaction factors as type of goods purchased, the amount of the transaction, and the country in which the card was issued.
  - Contact the issuer to confirm cardholder information prior to shipping goods for a high-risk transaction.
- **Thoroughly scrutinize or restrict shipping merchandise to foreign addresses.**
  - Consider curtailing shipments of merchandise to higher risk countries.
  - To help prevent fraud, thoroughly scrutinize any requests to ship merchandise to other countries.
  - Most merchants will treat U.S. military addresses that are located overseas as domestic transactions.
- **Use prior cardholder purchases as a favorable factor to apply less restrictive screening and review when cardholder information has not changed.**

Analyzing Questionable Transactions

- **Stay alert for the following fraud indicators. Any one of these factors could indicate a higher degree of fraud risk.**
  - **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
  - **Orders consisting of several of the same item:** Having multiples of the same product increases profits.
  - **"Rush" or "overnight" shipping:** Criminals want their fraudulently obtained items as soon as possible for the quickest possible resale, so they aren't concerned about extra delivery charges.
  - **Shipping outside of the merchant's country:** There are times when fraudulent transactions are shipped to fraudulent criminals outside of the home country.
  - **Inconsistencies:** Information in the order details, such as billing and shipping address mismatch, telephone area codes falling near zip codes, e-mail addresses that do not look legitimate, and irregular time of day when the order was placed.

- **Multiple transactions on one card over a very short period of time:** This could be an attempt to "run a card" until the account is closed.
- **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.
- **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.
- **For online transactions, multiple cards used from a single IP (Internet Protocol) address:** More than one or two cards could indicate a fraud scheme.
- **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.

• **Establish procedures for responding to suspicious transactions using cardholder verification calls.** Contacting customers directly not only reduces fraud risk, but also builds customer confidence and loyalty. Your verification procedures should address both the need to identify fraud and the need to leave legitimate customers with a positive impression of your company.

- Use directory assistance or Internet search tools—not the telephone number given for a suspect transaction—to find a cardholder's telephone number.
- Confirm the transaction, resolve any discrepancies, and let the cardholder know that you are performing this confirmation as a protection against fraud.

Third Party Fraud Screening

• **Perform internal fraud screening before submitting transactions for third party scoring.**

- Submit only those transactions that have passed your internal screening.
- Do not obtain fraud scores for transactions declined by the issuer or out-sorted by you for suspected fraud or other reasons.

• **Evaluate the costs and benefits of third party scores for low-risk transactions.** For many merchants, it is not cost-effective to obtain third party fraud scores for each and every online transaction. You may be able to keep costs down by eliminating low-risk transactions from third party scoring.

- Analyze your agreements with third party scoring services and determine the costs of submitting transactions to them.

- Identify transactions with fraud risk losses that are lower than the cumulative cost of obtaining third party fraud scores. Consider the following factors:
  - Dollar amount of the sale
  - Cardholder relationship—new or repeat customer
  - Type of service or goods being sold
  - Your website "click through" patterns
  - AVS* results
  - CVV2** results
  - Verified by Visa results

Use Innovative Fraud Alert Technologies

- **Consider the use of Ethoca alerts for near real-time notification from card issuers regarding confirmed fraud.** Through its relationships with Visa and a global network of card issuing banks, Ethoca is able to deliver cardholder confirmed data in the form of Alerts to effected merchants through an easy to use portal or direct link API. Ethoca Alerts are received in near real-time enabling merchants to act quickly stopping fraud and avoiding chargebacks.
- **Learn more about Ethoca's platform.** Visit www.ethoca.com or contact Sales at *sales@ethoca.com* for sales inquiries.

Key Points

E-commerce merchants are constantly dealing with the challenges and impacts of working independently from card issuing banks. The result is a significant time delay between the card issuer confirming that the transaction is fraudulent and the merchant being notified. This process can take upwards of 3-6 weeks by which time the fraudster has fled with the goods and/or the chargeback has been issued.

Ethoca is a global collaboration-based technology company serving merchants and card issuing banks in the online payment industry. It provides a single, automated, secure platform for card issuers and merchants to communicate outside of the payment authorization stream. Thousands of times a day, card issuers and merchants identify fraudulent and/or suspicious transactions that have gone undetected by the other party, resulting in financial losses and administrative costs to both. Ethoca's platform helps close the information gap between the card issuers and merchants, making this valuable information securely available in near real-time.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

Suspect Transaction Review

- **Establish cost-effective thresholds for determining which suspect transactions to review.** The manual review of transactions is time-consuming and costly, and is generally warranted only for high-risk transactions.
  - Use screening criteria that lets you avoid the manual handling of lower-risk transactions, such as those that involve:
    - Low purchase amounts.
    - Repeat customers who have a good record for at least the past 90 days and goods are sent to the same address as before.
    - An AVS* match and a shipping address that is the same as the billing address, as well as a purchase amount that is below the designated dollar threshold.
  - Ensure that all transactions with higher risk characteristics are declined or routed for fraud review, such as:
    - Hits against the negative file
    - International IP addresses
    - Foreign billing or shipping addresses

Cardholder Verification

- **Establish cost-effective procedures for verifying purchase activity.** Develop call verification procedures that address both the need to identify fraud and the need to leave legitimate customers with a positive impression of your company.
  - Use directory assistance or Internet search tools to verify the cardholder name, address and telephone number.
  - Contact issuing banks directly or through the telephone numbers provided by your acquirer.
    - Confirm name, address and telephone number associated with the card number.
    - Confirm whether the cardholder has made a recent address change or added on an alternative address, as appropriate.
  - Call the cardholder as necessary to confirm the transaction and resolve any discrepancies. Let the cardholder know that you are performing this confirmation as a protection against fraud.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

8. Implement Verified by Visa

Verified by Visa creates a significant reduction in merchant risk exposure by increasing transaction security through cardholder authentication and providing chargeback protection from fraud. Best practices include:

Work With Your Acquirer

- **Work with your acquirer to implement Verified by Visa.**
  - Assess whether Verified by Visa is right for your website.
  - To learn more about this service, visit www.visa.com/verifiedmerchants and download the *3D Secure Acquirer and Merchant Implementation Guide*.
- **Evaluate the benefits of Verified by Visa. These include:**
  - **Reduced Chargebacks.** Verified by Visa can reduce the risk of fraud and chargeback costs—with minimal impact to the current transaction process. Merchants who use Verified by Visa 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 Verified by Visa 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 Verified by Visa, compared to those transactions that do not. Not all merchant categories are eligible for a lower interchange rate as part of their Verified by Visa implementation.
  - **Boosted Consumer Confidence.** Verified by Visa 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.

Ensure Transaction Qualification

- **To obtain fraud chargeback protection, ensure that the acquirer or processor is providing the authentication results and ECI in the authorization message.**
  - This can be an issue when a second authorization is obtained, such as a split shipment.
  - Depending on the merchandise sold and your customer base, this should represent 80 percent to 95 percent of transactions. A lower percentage could indicate a processing issue and lack of fraud chargeback protection.
  - Monitor on a daily basis to identify any problems early on.

Key Points

To receive chargeback protection and the best interchange rate*, the Electronic Commerce Indicator (ECI) and results of the authentication or attempted authentication must be provided in the authorization message.

Perform Transaction Fraud Screening

Verified by Visa has proven to be an effective fraud prevention tool; however, it cannot eliminate online fraud solely on its own, particularly for Attempted Authentication (ECI = 6), for which no authentication occurs. In addition, fraud may occur on fully authenticated transactions (ECI = 5) in account takeover situations or fraudulent cardholder claims. Despite the protection from fraud chargeback liability, merchants should continue to perform fraud screening to prevent these fraud scenarios from occurring.

- **Perform fraud screening as detailed in "Apply Fraud Screening" on pages 51-56 of this guide.**
- **Continue to utilize fraud-screening tools for Verified by Visa transactions.** There are important reasons for this best practice:
  - **Keep fraud out of the payment system.** Only the crook benefits when fraud occurs. At a minimum, your customers or potential customers are inconvenienced and may become wary of using your site.
  - **Provide protection from processing errors.** Due to processing errors, transactions believed to have qualified for chargeback liability protection may not actually qualify. These errors are typically discovered after the fact and can result in merchant losses.
  - **Not exceeding Visa Fraud rate thresholds.** Visa monitors fraud levels separately for ECI 5 and ECI 6 transactions through its Risk Identification Service program (RIS). Merchants with unusually high fraud levels may be identified by RIS and may lose their chargeback protection until corrective measures are put in place.
  - **Reducing chargeback processing expense.** Under some scenarios, chargebacks for Verified by Visa transactions will not be rejected by Visa, resulting in the acquirer and merchant having to process chargebacks and representments.

Respond to Acquirer Alerts of High Fraud Rates

Visa provides warnings to acquirers of merchants that exceed fraud thresholds for ECI 5, ECI 6, and overall transactions. A merchant identified multiple times by the ECI indicator or other thresholds may be designated as a high-risk merchant, which carries with it chargeback liability for fraud transactions.

- **Work with your acquirer on a timely basis regarding alerts of high fraud rates.**
- **Identify the source of the problem and take measures to address it through more robust transaction screening, investigation and verification.**

*Acceptance costs are determined independently by acquirers. Check with your acquirer for details.

Authentication Actions for Verified by Visa Merchants

- **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 web 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 re initiate the purchase
- **Do not submit an authorization request for Verified by Visa transactions that fail authentication.**

9. Protect Your Merchant Account From Intrusion

Unauthorized persons are gaining entry to e-merchant accounts via shopping cart or payment gateway processor systems. These intruders are attacking e-commerce merchants using weak or generic passwords. Once a password is compromised, intruders then emulate the merchant and begin processing debits and credits, without the true merchant's knowledge. The fraud sales are usually similar in total to—and are therefore, offset by—the credits deposited. This is done in an attempt to circumvent detection by deposit volume monitoring. To keep your account cyber-safe, apply these best practices:

Monitoring

- **Conduct daily monitoring of authorizations and transactions.** On a daily basis, check for:
  - Authorization-only transactions. An unusual number could indicate testing for vulnerability.
  - An unusually high quantity, average size, or volume of credits. This could indicate fraud.
  - Identical transaction amounts.
  - Transactions without associated customer identification information.
  - Multiple transactions from a single Internet Protocol (IP) address.
  - Transactions on similar account numbers. This could indicate use of account number generating software.
  - Multiple transactions made on a single card over a very short period of time.
- **Monitor your batches.**
  - Know what time your transactions settle. Be sure to review your transactions before your settlement occurs.
  - If you use AVS* or CVV2**, look for transactions submitted without an AVS or CVV2 response in the authorization record.

Passwords

- **Change the password on your payment gateway system regularly.**
  - Include a combination of letters and numbers with a minimum of six characters.
  - Make sure the login ID and password are different.

Information Security Efforts

- **Ensure that the Payment Card Industry (PCI) Data Security Standard (DSS) requirements are in place.**

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

Visa Card Acceptance

For e-commerce merchants, a key step toward minimizing fraud exposure and related losses is to ensure proper Visa card acceptance. This starts with a logical and secure process for handling authorization requests and also includes the right set of fraud controls.

Steps Covered

10. Create a Secure Process for Routing Authorizations
11. Be Prepared to Handle Transactions Post-Authorization

10. Create a Secure Process for Routing Authorizations

The authorization process must be well managed because it has a significant impact on risk, customer service, and operational expense. Consider these best practices:

Routing Sequence

- **Implement a fraud-focused authorization routing sequence when a customer initiates a transaction.**
  - If you are a Verified by Visa merchant, complete the authentication process and provide the authentication data in the VisaNet authorization request as appropriate.
  - Perform internal screening for fraud, (e.g., matching the transaction against velocity parameters, high-risk locations, and internal negative files), and out-sort the transaction for review if it is unacceptable.
  - If the transaction has passed your internal check, obtain an issuer authorization that includes Address Verification Service (AVS)* and Card Verification Value 2 (CVV2)** to determine if the issuer or you will decline the transaction.
  - If you use a third party screening service, obtain a fraud score for transactions that have not yet been declined by you or the issuer.

Requirements

- **Use the correct Electronic Commerce Indicator (ECI) for all Internet transactions.** When entered into the appropriate fields of the authorization and settlement messages, the ECI identifies the transaction as e-commerce. Work with your acquirer to implement the ECI, which is required by Visa for all Internet transactions.
- **Obtain a new authorization if the original expires.** If your business sells goods through your website and if you are shipping the goods to the customer more than seven days after the original authorization, (i.e., backorder), you should obtain a **new authorization** before proceeding with the shipment. This practice is required under *Visa International Operating Regulations* and helps protect you from chargebacks due to no authorization.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

11. Be Prepared to Handle Transactions Post-Authorization

If an online transaction is approved by the issuer, consider sending a confirmation before you complete and fulfill the order. If the transaction is declined however, your procedures should specify how to handle the situation with the customer and determine whether this type of decline can be avoided in the future. Proceed in a way that best serves your customer and your business using these best practices:

Research and Review

- **Implement a fraud-focused authorization routing sequence when a customer initiates a transaction.**
- **Issue an e-mail order confirmation for approved transactions.** This practice enables you to check the validity of the cardholder's e-mail address. If the e-mail address is not valid, research the situation to determine whether the order is legitimate. You can also minimize customer disputes by sending an e-mail order confirmation that reminds the cardholder of the approved purchase and provides details about it.
- **Review declined authorizations and take appropriate actions.** In many cases, it may be worthwhile to have your customer service representatives review authorizations declined by issuers and obtain corrected information or alternate payment that may allow you to proceed safely with the sale.
  - Queue authorization declines for review and contact customers to correct problems with their cards (such as incorrect expiration date) or arrange other means of payment.
  - If the Visa information is corrected, be sure to obtain authorization approval from the issuer before completing the sale.
  - Track the success rate of your decline review strategy and modify it, as needed.
- **Track order decline rates.** This important practice can help you increase your approval rates and sales volume, and uncover potential problems related to changes in the authorization process.
  - To effectively identify trends, track order declines by reason on a daily basis.
  - Segment issuer declines versus those you decline for suspected fraud or other reasons.

Payment Card Industry Data Security Standard

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. 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.

Steps Covered

12. Safeguard Cardholder Data through PCI DSS Compliance

12. Safeguard Cardholder Data Through PCI DSS Compliance

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. More detailed information on Visa's security compliance program is available at www.visa.com. Learn about complying with the Standard, validation requirements, PIN security and key management, and more. Plus, stay current with data security with alerts, bulletins, and webinars.

Why Comply?

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.

PCI DSS Recommended Steps

The PCI DSS consists of twelve easy-to-remember steps to comply with the industry's recommended practices and to ensure transactions are conducted with confidence and ease, worldwide.

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

Protect Your Cardholders and Your Business

To protect the interest of your cardholders and your business, follow these best practices.

- **Work with your acquirer 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 acquirers 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 acquirer within 24 hours.**

Maintain Sensitive Data Storage and Security

- **Ensure that all stored sensitive cardholder account information complies 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).** The PA-DSS applies to payment application vendors. It is intended to lessen the risk of security breaches in payment applications, prevent storage of sensitive authentication data (i.e., full magnetic-stripe data, CVV2, and PIN data), and support overall compliance with PCI DSS.

  Visa's policies are intended to support these standards by ensuring merchants and service providers do not use payment applications that retain data, thereby making it easier to steal. For those doing business with Visa, that means using applications found to comply with this important data standard.

Key Points

Secure technologies such as point-to-point encryption and tokenization, when implemented in accordance with the PCI DSS, may help simplify PCI DSS compliance. 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

Learn About Your Liability

- **Know your liability for data security problems.** Many acquirers 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. Liabilities to consumers may also arise.

*In certain markets, CVV2 is required for card-absent transactions.

Taking Immediate Action

- **If you have experienced a suspected or confirmed security breach, act swiftly and take immediate steps to contain and limit exposure.** To prevent the further loss of data, conduct a thorough investigation of the suspected or confirmed compromise of information. To facilitate the investigation, do the following:
  - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords; do not log in as ROOT).
  - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
  - Preserve logs and electronic evidence.
  - Log all actions taken.
  - If using a wireless network, change SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised).
  - Be on **high alert** and monitor all systems containing cardholder data.
- **Provide all compromised Visa, Interlink, and Plus accounts to your acquirer within ten business days.** All potentially compromised accounts must be provided and transmitted as instructed by your acquirer and the Visa Investigations and Incident Management group. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information.
- **Within three business days of the reported compromise, provide an** *Incident Response Report* **document to your acquirer.**

Note: Visa, in consultation with your acquirer, will determine whether or not an independent forensic investigation will be initiated on the compromised entity.

Contact Information

For more information about PCI DSS compliance, contact your acquirer or visit www.pcissc.org.

Chargeback and Loss Recovery

For your business, a chargeback translates into extra processing time and cost, a narrower profit margin for the sale, and possibly a loss of revenue. It is important to carefully track and manage the chargebacks that you receive, take steps to avoid future chargebacks, and know your representment rights. In addition, you should also take measures to recover losses from customers who are financially liable for transactions that were charged back to your business.

Steps Covered

13. Avoid Unnecessary Chargebacks and Processing Costs
14. Use Collection Efforts to Recover Losses
15. Monitor Chargebacks

13. Avoid Unnecessary Chargebacks and Processing Costs

To minimize losses, you need an adequate chargeback tracking system, procedures in place to avoid unnecessary chargebacks, and a thorough understanding of your representment rights. Follow these best practices:

Avoiding Chargebacks

- **Do not complete a transaction if the authorization request was declined.** Do not repeat the authorization request after receiving a decline; ask for another form of payment.
- **Act promptly when customers with valid disputes deserve credits.**
  - When cardholders contact you directly to resolve a dispute, issue the credit on a timely basis to avoid unnecessary disputes and their associated chargeback processing costs.
  - Send cardholders an e-mail message to let them know immediately of the impending credit.
- **Provide data-rich responses to sales draft requests.**
  - Respond to sales draft inquiries from your acquirer with full information about the sale, and be sure to include the following required data elements:
    - Account number
    - Card expiration date
    - Cardholder name
    - Transaction date
    - Transaction amount
    - Authorization code
    - Merchant name
    - Merchant online address
    - General description of goods or services
    - "Ship to" address, if applicable
    - Address Verification Service (AVS)* response code, if applicable
  - Optionally provide additional data to help resolve inquiries, such as:
    - Transaction time
    - Customer e-mail address
    - Customer telephone numbers
    - Customer billing address
    - Detailed description of goods or services
    - Whether a receipt signature was obtained upon delivery of goods or services

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

Representment Rights for Compelling Evidence

- **Know your representment rights and requirements for submitting evidence.** Effective on or after 20 April 2013 , merchants will have a representment right to provide compelling evidence for the following chargeback reason codes:
  - Reason Code 30: Services Not Provided or Merchandise Not Received
  - Reason Code 53: Not as Described or Defective Merchandise
  - Reason Code 81: Fraud – Card-Present Environment
  - Reason Code 83: Fraud – Card-Absent Environment

Compelling evidence allows merchants to provide additional types of evidence to try and prove the cardholder participated in the transaction, received the goods or services, or benefited from the transaction.

Examples of Allowable Compelling Evidence

APPLICABLE CHARGEBACK REASON CODES	ALLOWABLE COMPELLING EVIDENCE
30, 81, 83	For a card-absent environment transaction in which the merchandise is picked up at the merchant location, any of the following: • Cardholder signature on the pick-up form • Copy of identification presented by the cardholder • Details of identification presented by the cardholder
30, 81, 83	For a card-absent environment transaction in which the merchandise is delivered, documentation (evidence of delivery and time delivered) that the item was delivered to the same physical address for which the merchant received an AVS match of "Y" or "M." A signature is not required as evidence of delivery.
30, 81, 83	For e-commerce transactions representing the sale of digital goods downloaded from a website, one or more of the following: • Purchaser's IP address • Purchaser's e-mail address • Description of the goods downloaded • Date and time goods were downloaded • Proof that the merchant's website was accessed for services after the transaction date
81, 83	For card-absent environment transactions, evidence that the transaction uses data, such as IP address, e-mail address, physical address, and telephone number, that had been used in a previous, undisputed transaction

Representment Rights Associated with Use of AVS, CVV2, and Verified by Visa

- **Know your AVS* and CVV2** representment rights.** Card-absent merchants should be familiar with the chargeback representment rights associated with the use of AVS, CVV2, and the option to provide compelling information. **Specifically, your acquirer can represent a charged-back transaction if you:**
  - Received an AVS positive match "Y" response in the authorization message and if the billing and shipping addresses are the same. You will need to submit proof of the shipping address and signed proof of delivery.
  - Submitted an AVS query during authorization and received a "U" response from a card issuer. This response means the card issuer is unavailable or does not support AVS.
  - Submitted a CVV2 verification request during authorization and received a "U" response with a presence indicator of 1, 2, or 9 from a card issuer. This response means the card issuer does not support CVV2.
  - Can provide documentation that you:
    - Spoke to the cardholder and he or she now acknowledges the validity of the transaction, or
    - Received a letter or e-mail from the cardholder that he or she now acknowledges the validity of the transaction.
- **If you believe you have AVS*, CVV2**, or compelling information representment rights on a charged-back transaction, work with your acquirer to ensure that all supporting evidence for the representment is submitted.**

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

** In certain markets, CVV2 is required to be present for all card-absent transactions.

- **Understand the Verified by Visa liability shift rules.** Verified by Visa participating merchants are protected by their acquirer from receiving certain fraud-related chargebacks, provided the transaction is processed correctly.

IF:	THEN:
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'.
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'.*
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 (i.e., commercial card products) is not supported within Verified by Visa, or if the cardholder experiences technical problems.

Key Points

Liability shift rules for Verified by Visa transactions may vary by region. Please check with your acquirer for further information.

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

14. Use Collection Efforts to Recover Losses

In some cases, customers are responsible for transactions that have been charged back to your business. To recover losses such as these, apply these best practices:

Recovery Actions

- **Use e-mail collection messages and letters as the first step toward collecting low-dollar amounts.** You often can recover unwarranted chargeback losses by contacting the customer directly through internal resources or an external collections agency. For example, if a customer claims that a transaction was fraudulent, but you have determined that the customer actually received the goods or service, contact the customer directly to recover the chargeback amount. If a cardholder letter was received as part of the chargeback documentation, try to address the customer's concerns and arrive at a mutually satisfactory solution.
- **Follow up with phone calls to those who do not respond to your initial correspondence.**
- **Outsource remaining customers with unpaid balances to a collections agency on a contingent fee basis.**

15. Monitor Chargebacks

As with copy requests, monitoring chargeback rates can help merchants pinpoint problem areas in their businesses and improve prevention efforts. However, while copy request volume is often a good indicator of potential chargebacks, actual chargeback rates and monitoring strategies vary by merchant type.

Chargeback Rates Monitoring

- **Track chargebacks and representments by reason code.** Each reason code is associated with unique risk issues and requires specific remedy and reduction strategies.
- **Include initial chargeback amounts and net chargebacks after representment.**
- **If your business combines traditional retail with card-absent transactions, track card-present and card-absent chargebacks separately.**
- **If your business combines Mail Order/Telephone Order (MO/TO) and Internet sales, monitor these chargebacks separately.**

Visa Chargeback Monitoring Program for Merchants

Visa monitors all merchant chargeback activity on a monthly basis and alerts acquirers when any one of their merchants has excessive chargebacks.

Once notified of a merchant with excessive chargebacks, acquirers are expected to take appropriate steps to reduce the merchant's chargeback rate. Remedial action will depend on merchant type, sales volume, geographic location, and other risk factors. In some cases, you may need to provide sales staff with additional training or review sessions on card acceptance procedures. In others, you should work with your acquirer to develop a detailed chargeback-reduction plan.

Visa Dispute Monitoring Program for Issuers

The Visa Dispute Monitoring Program protects and monitors the integrity of the chargeback dispute process. It ensures merchants are not negatively impacted by chargeback rule changes, and that issuers comply with the requirements outlined in the *Visa International Operating Regulations*.

The Program tracks issuer chargeback performance on a monthly basis and provides non-compliant issuers with an opportunity to research their practices or systems and make adjustments as needed.

Section 3 Resources

What's Covered

- Online Support and Information
- Visa Materials for E-Commerce Merchants

Online Support and Information

The tools presented here are available through the Internet as of the date of this publication. Whether you are a new or established merchant, you can use these "virtual" resources to learn more about the e-commerce market, ensure the security of your website, and explore the opportunities of business-to-business e-commerce.

General E-Commerce Information

The following sites offer background information about e-commerce issues, trends, and risks, as well as useful details about website privacy.

The E-Commerce Market Today

- BBBOnline – An array of resources provided by the Better Business Bureau to assist consumers and businesses interested in e-commerce: www.bbbonline.org
- CommerceNet Electronic Resources – A broad range of information on establishing Internet commerce websites and conducting business over the Internet: www.commerce.net
- Shop.org – Trade association for e-commerce retailers. Includes information on sponsored conferences, research, and other resources provided by the association: www.shop.org
- Visa Home Page – Starting point to access a wide range of information provided by Visa: www.visa.com/globalgateway

Website Privacy

- Anonymizer® – An array of Internet privacy information for consumers and businesses: www.anonymizer.com
- Electronic Privacy Information Center – Comprehensive resource and reference guide about Internet privacy issues: www.epic.org
- TRUSTe – Extensive information on ensuring privacy for web publishers and users: www.truste.org

Fraud Prevention

Fraud Detection Tools and Support

- **CyberSource Risk Management Solutions** provide fraud detection for organizations of all sizes, visit www.cybersource.com/www, or for small businesses, www.authorize.net.

The Merchant Risk Council

The Merchant Risk Council (MRC) is the world's foremost global, merchant-led trade association focused on managing payments, preventing online fraud and promoting secure e-commerce.

Each year, the MRC hosts elite conferences in Europe and America with industry leading keynote speakers, more than 200 merchant and vendor presenters, and 100 panel discussions. MRC also produces more than 75 educational webinars annually, which promote networking and year round professional development.

MRC's membership includes 365 of the world's most prominent merchants and more than 50 category testing solution providers. If you are responsible for payments or fraud prevention, the MRC is the most important community for you to join. For further details, visit www.merchantriskcouncil.org.

Key Points

Delivering bottom-line business value, MRC members have averaged a 40 percent lower fraud loss in the past four years compared to non-members.

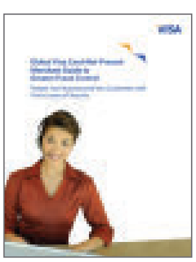
Visa Materials for E-Commerce Merchants

Visa offers a number of risk and chargeback management materials as part of its merchant education program. Current publications are geared toward the back-office needs of merchants in today's environment. To download these publications, visit www.visa.com/merchants.

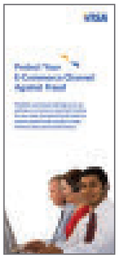
Chargeback Management Guidelines for Visa Merchants is a comprehensive manual for all businesses that accept Visa transactions. The purpose of this guide is to provide merchants and their back-office sales staff with accurate up-to-date information on minimizing the risk of loss from fraud and chargebacks. This document covers chargeback requirements and best practices for processing transactions that are charged back to the merchant.

Card Acceptance Guidelines for Visa Merchants is a comprehensive manual for all businesses that accept Visa transactions in the card-present and/or card-absent environment. The purpose of this guide is to provide merchants and their sales staff with accurate, up-to-date information and best practices for processing Visa transactions, understanding Visa products and rules, and protecting cardholder data while minimizing the risk of loss from fraud.

Improving Dispute Resolution for You is a flyer that describes the upcoming dispute resolution changes that will impact merchants in April 2013. It highlights the changes to the chargeback and retrieval request process, how these changes will impact merchants, and a list of Visa resources for merchants to use in operating their back-office dispute resolution process.



Global Visa Card-Not-Present Merchant Guide to Greater Fraud Control reviews Visa's layered approach to security in the card-absent environment. This publication offers merchants multiple security checkpoints when processing card-absent transactions. It covers best practices in detail and highlights information regarding Visa's security tools like Verified by Visa, Card Verification Value 2, Address Verification Service, and the Payment Card Industry Data Security Standard. With these tools merchants can reduce exposure to fraud risk and minimize associated losses.



Protect Your E-Commerce Channel Against Fraud is four-fold brochure designed as a "welcome" piece for internet merchants. It covers best practices to help merchants with online transactions, protect themselves against fraud, and avoid losses.

Visa Data Security Program: Keeping Cardholder Data Safe flyer provides an overview of the Visa Data Compliance Programs. It outlines the program benefits, requirements, compliance verification, what to do if compromised, and provides Payment Card Industry Data Security Standard requirements at-a-glance.

Section 4 Appendices

What's Covered

- Appendix A: E-Commerce Merchants' Fraud Reduction Tools Quick Lookup
- Appendix B: Glossary

Appendix A: E-Commerce Merchants' Fraud Reduction Tools Quick Lookup

Today's e-commerce merchant has many options for combating payment card fraud. To protect your online business and your customers, you need to build a reliable risk management system; one that uses the right combination of fraud reduction tools and, at the same time, takes into consideration your products, services, operational needs, customer service requirements and bottom line.

Fraud Prevention at the Transaction Level

TOOL	DESCRIPTION
Visa Address Verification Service (AVS)* *Studies have shown that perpetrators of fraud in card-absent transactions often do not know the correct billing address for the account they are using. Verifying the address can, therefore, provide merchants with another key indicator of whether or not a transaction is valid.*	An automated tool that enables merchants to verify the billing address (street number and ZIP code) of a customer presenting a Visa card for payment. When you include an AVS request with your transaction authorization, you will receive a result code indicating 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. Further investigation should be performed prior to proceeding with the sale.
Visa Cardholder Verification Value 2 (CVV2)** *Studies show that merchants who include CVV2 validation in their authorization procedures for card-absent transactions can reduce their fraud-related chargebacks.*	A three-digit security number printed on the back of Visa cards to help validate that a legitimate card is in the possession of the person placing the order.
Verified by Visa *Participating Verified by Visa merchants are protected from receiving certain fraud-related chargebacks.*	An online, real time service that allows you to validate that a cardholder is the owner of a specific account number. When the cardholder clicks "buy", or a similar button at the checkout of a participating merchant, the merchant's server recognizes the enrolled Visa card and the "Verified by Visa" screen automatically appears on the cardholder's desktop. The cardholder enters a password to verify his or her identity and the Visa card. The issuer then confirms the cardholder's identity.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

**In certain markets, CVV2 is required for card-absent transactions.

TOOL	DESCRIPTION
Internal Negative Files *By storing negative file details, merchants gain a valuable source of information to help protect themselves from future fraud perpetrated by the same person or group.*	Internal negative files allow you to make use of the details of your own history with fraudulent transactions or suspected fraud. To create these files, record all key elements of fraudulent transactions, such as names, e-mail addresses, shipping addresses, customer identification numbers, passwords, telephone numbers, and Visa card numbers used. If transaction data matches your internal negative file data, you should either decline the transaction or out-sort the transaction for internal review and follow up.
Internal Positive Files	It is also important to establish screening criteria to identify those repeat customers that have demonstrated a solid track record.
Suspect Transaction Analysis *To ensure effective fraud control, merchants need to analyze transactions that are reported as fraud or have resulted in chargebacks. This can help merchants adjust their risk thresholds, prevent fraud and chargebacks, and maximize the effectiveness of manual out-sort and review processes.*	Based on an analysis of your experience with selected products, shipping locations, customer purchasing patterns and sales channels, you should be able to identify the root cause of fraud or excessive chargebacks in your own environment. Transactions with higher risk characteristics or from higher risk sales channels should be routed for fraud review. These types of transactions can include: • Larger-than-normal orders. • Orders consisting of several of the same item. • Orders made up of "big-ticket" items. • Orders shipped "rushed" or "overnight". • Orders from Internet addresses at free e-mail services. • Orders shipped to an international address. • Multiple orders placed using different names, addresses, and card numbers, but coming from the same Internet Protocol (IP) address. • Negative renewal options. • Free-trial offer periods. • Continuity programs.

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

<table>
<tr><th>TOOL</th><th>DESCRIPTION</th></tr>
<tr><td>Velocity Monitoring

Automated velocity monitoring can help reduce risk exposure and can be used to identify high-risk transactions.

Merchants need to review their customer history to help establish meaningful velocity limits that are specific to their business and/or specific product lines.</td><td>Velocity checks can be implemented to monitor the frequency of card use and the number and dollar amount of transactions within a specified number of days. You should ensure that velocity limits are set and checked across multiple characteristics (including shipping address, telephone number, and e-mail address). In doing so, be sure to establish tighter control and velocity thresholds for:
Orders placed on the same card over various time periods such as hour, day, week, etc.
Frequency of orders made on multiple cards (but shipped to a single address).
Frequency of multiple orders placed using different names, addresses, and card numbers, but coming from one IP address.
Frequency of orders coming from the same URL.</td></tr>
<tr><td>Fraud Screening

Today there are a wide variety of independent companies that offer fraud-screening services and practices to help assess the risk of a transaction and increase the likelihood that a merchant is dealing with a legitimate customer with a valid Visa card.</td><td>Fraud-screening tools can be developed internally or acquired from third-parties to help identify high-risk transactions. By using proper screening criteria, you can suspend processing for transactions with high-risk attributes and set them aside or flag them for manual review. This can include transactions that:
Match data stored in your internal negative files.
Exceed velocity limits and controls.
Generate an Address Verification Service (AVS)* mismatch.
Match high-risk profiles.
Third party tools for fraud scoring can be used to better target the highest risk transactions requiring additional verification.</td></tr>
<tr><td>Global IP Address Matching

Merchants have found that international IP addresses have a substantially higher fraud rate than domestic addresses, particularly when merchants require a U.S. billing address.</td><td>In order to screen for high-risk International IP addresses, you should capture and translate the Internet Protocol (IP) address to identify the computer network source. This can be accomplished by:
Using a geo location software/service to determine the IP address country.
Matching the IP address country with the billing and shipping address country. If the countries do not match, out-sort the order for further review.</td></tr>
</table>

*AVS allows merchants to validate the cardholder's billing address with the card issuer. AVS is currently available for cards issued from Canada, the United Kingdom, or the United States.

TOOL	DESCRIPTION
E-mail Confirmation *Simple verification steps can alert you to data entry errors made by customers and uncover fraudulent attempts.*	Test the validity of an e-mail address by sending an order confirmation. If the e-mail is returned due to a bad address, the order should be out-sorted for further review. The customer may be contacted to help validate the order prior to shipment/delivery.
Account Generation and Testing Prevention *By taking proactive monitoring measures, merchants can effectively minimize cyber attacks and the associated payment card fraud risks.*	Monitor authorizations and transactions daily: • Authorization-only transactions. An unusual number could indicate testing. • A large number of transactions followed by offsetting credits. • Transactions on similar account numbers. This could indicate the use of account number generating software (e.g., CreditMaster).
Digital Content Delivery *Merchants that provide digital content media should implement controls that prevent billing consumers until the website/digital content has been accessed.*	Consumers often sign-up for free-trial access to merchant sites containing digital content media, but then never access the site. Often, they do not remember to cancel the service and assume they will not be billed because the service was never used. Merchants that implement controls to prevent billing these customers can reduce the number of disputed transactions.
PC Fingerprinting	PC fingerprinting applications provide the geographical location of the Internet Protocol (IP) address of every online customer. You can use this IP information and compare it to the billing address (and even the billing phone number) to identify riskier transactions (i.e., the cardholder's billing information locates a customer in CA and the fraudster's IP address locates him in Russia).
Test Fulfillment House Capabilities *Merchants should periodically place test orders to monitor the performance of their fulfillment centers.*	Once an order is placed, you should track the time from when the order is billed to when it is received. When merchandise is returned, you should also track the time from when the goods are sent back until a credit is processed. Delays in shipping or issuance of credit can increase chargebacks.

Appendix B: Glossary

The Internet and the e-commerce market have generated a number of new terms and acronyms. The payment card industry also has its own unique terminology. This section will help you understand some of the commonly used terms related to doing business over the Internet as a Visa merchant.

Acquirer	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 an acquirer.
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" response may indicate fraud risk.
Anonymous e-mail address	An Internet contact point assigned to a web user by any free, public domain e-mail services such as Excite, Hotmail, Juno and Yahoo. These services can be accessed from any web browser and are not specifically linked to an Internet Service Provider (ISP) account. Anonymous e-mail addresses are more difficult to trace than those linked to an ISP and have been used to make fraudulent e-commerce transactions.
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.
AVS	See *Address Verification Service.*
Card-absent	An environment where a transaction is completed under both of the following conditions: • Cardholder is not present • Card is not present
Card expiration date	See "*Good Thru*" date.
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, acquirer, 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 payment card transaction that is later rejected and returned to the acquirer by the issuer for a specific reason, such as a cardholder dispute or fraud. The acquirer 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.
Consumer bank	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 an issuer.
Cookie	A special text file created by a website service and written onto the computer hard drive of a website visitor. The Internet relies upon a computer language called Hypertext Transfer Protocol (HTTP) which allows users to access web pages. Because each request for a web page is independent of all other requests, the web page server has no memory of what pages it has sent to a user previously nor does it retain any knowledge about the user's previous visits. Cookies allow the server to retain information about a visitor or a visitor's actions on its website and to store this data in its own file on the visitor's computer. There are two types of cookies: "permanent cookies" retain information about visitors, such as log in names, addresses, and past preferences. "Sessions cookies", also known as web browser cookies, typically let customers fill virtual shopping carts with more than one selection before checking out.
Copy request	A retrieval request that is processed through an electronic documentation transfer method.
Cryptography	The advanced process of encoding and decoding data that prevents unauthorized parties from reading data as it travels over the Internet. Also known as encryption or decryption.
CVV2	See *Card Verification Value 2*.
Decryption	The process of decoding or unscrambling data that has been encrypted to prevent unauthorized parties from reading it during Internet transmission.
ECI	See *Electronic Commerce Indicator*.
Electronic Commerce Indicator (ECI)	Effective 15 March 2012, a value used in electronic commerce transactions to indicate the transaction's level of authentication and security, as specified in the applicable Verified by Visa Implementation Guide.
Encryption	An online data security method of screening data so that it is difficult to interpret without a corresponding encryption key.
Firewall	A security tool that blocks access to files from the Internet and is used to ensure the safety of sensitive cardholder data stored on a merchant server.
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.
"Good Thru" date	The date after which a payment card 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.

Internet Protocol (IP) Address	A numeric code that identifies a particular computer on the Internet. Every computer network on the Internet has a unique address that has been assigned by the Internet Service Provider (ISP). Computers require IP addresses to connect to the Internet.
Internet Service Provider (ISP)	An organization that offers an individual and businesses an Internet connection for a fee. Typically, ISPs provide this connection along with an e-mail address and a web browser.
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*.
Payment Card Industry (PCI) Data Security Standard (DSS)	A set of comprehensive requirements for enhancing payment account data security. The PCI DSS was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
Payment gateway	Effective through 14 March 2012, a system that provides electronic commerce services to merchants for the authorization and clearing of electronic commerce transactions.
Representment	A chargeback that is rejected and returned to an issuer by an acquirer on the merchant's behalf. A chargeback may be represented, or re-deposited, if the merchant or acquirer can remedy the problem that led to the chargeback, and do so in accordance with Visa's rules and regulations.
Retrieval Request	An issuer's request for a transaction receipt, which could include the original, a paper copy or facsimile, or an electronic version thereof.
Third party agent	An entity that is not defined as a VisaNet processor, but instead provides payment-related services (directly or indirectly) to a member and/or stores, processes or transmits cardholder data. A third party agent must be registered by all Visa members that are utilizing their services (directly or indirectly).
Verified by Visa	A Visa Internet payment authentication system that validates a cardholder's ownership of an account in real time during an online payment transaction. When the cardholder clicks "Buy" or a similar button at the checkout page of a participating merchant website, a Verified by Visa screen automatically appears on the cardholder's desktop. The cardholder enters a password that allows the card issuer to verify his or her identity.
VisaNet Processor	A VisaNet processor is a member, or Visa-approved nonmember that is directly connected to VisaNet, that provides authorization, clearing, or settlement services for merchants and/or members.