Visa E-Commerce Merchant Guide to Risk Management

Tools and Best Practices for
Building a Secure Internet Business

VISA®

Table of Contents

About This Guide 1

Section 1: Understanding the Basics 3

What Every E-Commerce Merchant Should Know About Handling Visa Transactions 5

Approaching Risk From a Strategic Perspective 7

Online Transaction Processing – From Start to Finish 8

A Brief Look at Chargebacks 12

Section 2: E-Commerce Risk Management Best Practices 15

Fifteen Steps to Managing E-Commerce Risk 17

E-Commerce Start-Up 20

1. Know the Risks and Train Your Troops 21

2. Select the Right Acquirer and Service Provider(s) 23

Web Site Utility 26

3. Develop Essential Web Site Content 27

4. Focus on Risk Reduction 32

Fraud Prevention 36

5. Build Internal Fraud Prevention Capability 37

6. Use Visa Tools 39

7. Apply Fraud Screening 45

8. Implement Verified by Visa 50

9. Protect Your Merchant Account From Intrusion 54

Visa Card Acceptance 55

10. Create a Sound Process for Routing Authorizations 56

11. Be Prepared to Handle Transactions Post-Authorization 57

Cardholder Information Security Program 58

12. Safeguard Cardholder Data Through CISP Compliance 59

Chargeback and Loss Recovery 62

13. Avoid Unnecessary Chargebacks and Processing Costs 63

14. Use Collection Efforts to Recover Losses 65
15. Monitor Chargebacks.....66
Section 3: Special Considerations for Travel Merchants 67
Airlines.....69
Car Rental Companies 73
Cruise Lines.....75
Hotels.....78
Travel Agencies 81
Section 4: Resources 85
Online Support and Information 87
Visa Materials for E-Commerce Merchants 89
Appendices 91
Appendix A. Glossary 93
Appendix B. Checklist for Success 97
Appendix C. E-Commerce Merchant
Fraud Reduction Tools Quick Lookup 103

About This Guide

Introduction

To help e-commerce merchants build and maintain a secure infrastructure for payment card transactions, Visa has created the *E-Commerce Merchants' Guide to Risk Management*.

This guide was originally developed using the findings from a 1999 study of nine leading U.S. e-commerce merchants. Since then, it has been updated to reflect the evolution and expansion of the e-commerce marketplace. 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 already in place in the e-commerce programs studied. Others are recommendations based on Visa's payment industry experience.

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 still weighing the benefits and challenges of the Internet marketplace, this guide can 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. By finding the best ways to control risk in the early stages of your program, you will 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 can help you identify areas for improvement and explore advanced tactics for reducing risk exposure, as well as improving profitability as your Internet volume continues to grow.

How This Guide is Organized

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

Section One: Understanding the Basics — If you're just starting out as an e-commerce merchant or in the early stages of your program, you might want to take a few minutes to review this section. Here you'll find the background details you need in order to better understand what's required when it comes to maximizing information security and minimizing Visa card payment risk. The section also 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.

Section Two: E-Commerce Risk Management Best Practices — From setting up your e-commerce program, to developing your web site content and functionality, to establishing data security and fraud control tools, 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 Three: Special Considerations for Travel Merchants — In addition to the overall risk management practices discussed in Section Two, there are a number of industry-specific risk management "how-to's" that can be adopted by airlines, car rental companies, cruise lines, hotels, and travel agencies. This section highlights the industry-specific best practices.

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

Appendices — Includes a glossary of terms commonly used in the e-commerce market today, an *E-commerce Merchant Fraud Reduction Tools Quick Look-up*, and a checklist summary of the best practices discussed in this guide.

For More Information

To learn more about e-commerce risk management, contact your Visa Acquirer. 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 which 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 Every E-Commerce Merchant Should Know About 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-not-present 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 and cardholder signature. E-commerce merchants, however, can minimize their fraud exposure with the proper Internet-specific risk management infrastructure.
- **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 lets the Issuer make a more informed authorization decision.
- **must be in compliance with Visa's Cardholder Information Security Program (CISP).** To achieve compliance, all merchants and their service providers must adhere to the Payment Card Industry (PCI) Data Security Standard which offers a single approach to safeguarding sensitive data for all card brands. *For more information about Visa CISP compliance and the PCI Data Security Standard, refer to the best practices on pages 58-61 of this guide.*
- **must never store Card Verification Value 2 (CVV2) data.** For information security purposes, *Visa U.S.A. Inc. Operating Regulations* prohibit merchants from storing CVV2 data.

BITS AND BYTES

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

- ✔ **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.

- ✔ **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.
  - Include any required taxes in the total transaction amount. Do not collect taxes separately in cash.
  - Deposit transactions only for your own business.
  - Deposit Visa transaction receipts within five calendar days of the transaction date. For card-not-present transactions, the transaction date is the ship date, not the order date. Transactions deposited more than 30 days after the original transaction date may be charged back to you.
  - Deliver the merchandise or services to the cardholder at the time of the transaction. For card-not-present transactions, cardholders should be informed of delivery method and tentative delivery date. Transactions cannot be deposited until goods or services have been delivered.
  - Make refund and credit policies available to online customers through clearly visible links on the home page.
  - **NEVER** impose any surcharge on the Visa transaction.
  - **NEVER** use the Visa card/account number to collect other debts or dishonored checks.

Approaching Risk From a Strategic Perspective

E-Commerce Risk – The Good...

For merchants who have decided to move beyond the traditional "brick and mortar" storefront, there are many opportunities to enhance customer relationships, attract new customers, and increase sales revenue.

...The Bad...

Along with the opportunities, however, come a greater level of risk and stronger need for strategic actions to help effectively control fraud and better safeguard cardholder account information.

...and The Necessary

Unlike merchants who operate in the physical world, you do not have face-to-face contact, a card-in-hand, or an actual signature. You also don't have a physical door with a lock and key...or a security guard posted 24/7 for protection. Cyber-thieves know all of this and are always on the look-out for merchants who have hung up a virtual shingle, but have let their risk management guard down.

It's up to you to understand the unique issues of running a virtual storefront and take a strategic approach to proactively address these issues and position your business for success.

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

Settlement ------- Once a product/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 third-party processors to provide any of these services, which is typically the case. An Acquirer is often referred to as the "merchant bank."

A Merchant Processor can route an electronic transaction through the payment network for authorization, clearing, and settlement on behalf of the Acquirer.

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.

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 e-commerce merchant's site.

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

Payment Gateway is a service that allows an e-commerce merchant to connect to the Acquirer (or its merchant processor) to complete a bankcard transaction in real-time.

Service Provider can include any third-party payment support entity (e.g., Web host, shopping cart, payment processors, fulfillment houses, etc.). This term is also used to describe a payment gateway alliance.

The Online Transaction Lifecycle

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

Authorization

❶ The Cardholder orders goods from e-commerce merchant by entering Visa card payment information into the web site form, as prompted.

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

❷ 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 merchant processor).

❸ The Acquirer (or merchant processor) electronically sends the authorization request to VisaNet.

❹ VisaNet passes the request on to the Issuer.

❺ The Issuer approves or declines the transaction.

The authorization response is routed back through the same channels.

REAL-TIME VS. BATCH AUTHORIZATION PROCESSING

E-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

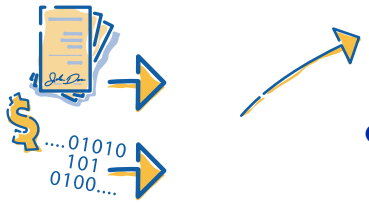
It is up to the e-commerce merchant to apply the right kinds of tools and controls to help verify the cardholder's identity and the validity of the transaction. Appropriate action can help an e-commerce merchant reduce fraudulent transactions and the potential for customer disputes. Here is a brief look at the Visa tools you can use to verify the legitimacy of the Visa cardholder and the card.

TOOL	DESCRIPTION
Address Verification Service (AVS)	Allows e-commerce merchants to check a Visa cardholder's billing address with the Issuer. AVS provides merchants with a key indicator that helps verify whether or not a transaction is valid.
Card Verification Value 2 (CVV2)	Is a three-digit number imprinted on the back of Visa cards to help validate that the customer has a genuine card in his/her possession and that the card account is legitimate. CVV2 is required on all Visa cards.
Verified by Visa	Validates a cardholder's ownership of an account in real-time during an online Visa card transaction. Verified by Visa authentication occurs **prior** to the authorization request process. When the cardholder clicks "buy" at the checkout of a participating merchant, the merchant server recognizes the registered 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.
CyberSource Advanced Fraud Screen enhanced by Visa	A real-time risk management tool that evaluates the risk associated with individual transactions and provides merchants with risk scores. You use the scores as an additional means to identify potentially fraudulent orders.

For more information about AVS, CVV2, and CyberSource Advanced Fraud Screen enhanced by Visa, refer to the best practices covered on pages 39–49 of this guide. For additional details about Verified by Visa and associated best practices, see pages 50 through 53.

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.



❶ Once the goods/services have been shipped or delivered, the merchant then "captures" and batches the related transactions for settlement. The batch is electronically submitted to the Acquirer (or merchant processor).

❷ The Acquirer (or merchant processor) electronically submits the transaction data to Visa for settlement.

❸ VisaNet electronically submits the transaction data to the Issuer and then facilitates settlement by paying the Acquirer for the transaction and debiting the Issuer account.

❹ The Acquirer typically receives funds for a transaction within 24 hours. The merchant is usually credited within 48 hours of settlement, or as stated in the merchant agreement.

❺ The Issuer posts the transaction to the cardholder account and sends a monthly statement to the cardholder.

A Brief Look at Chargebacks

What is a Chargeback?

With millions of Visa transactions generated worldwide everyday, it is inevitable that a few will become "chargebacks." A chargeback is a transaction that is returned as a financial liability by the Issuer to the Acquirer (and most often, to the merchant). Chargebacks can occur for a variety of reasons, including:

- ✔ Customer-disputed transactions
- ✔ Fraud
- ✔ Authorization issues
- ✔ Inaccurate or incomplete transaction information
- ✔ Processing errors

Most chargebacks begin when a cardholder notifies his or her Issuer that there is a transaction problem on the monthly billing statement. When this happens, the Issuer may request an explanation of the problem from the cardholder. Once the Issuer receives the necessary information, the first step is to determine whether a chargeback situation truly exists. If the Issuer determines that a chargeback right applies, the Issuer can resolve the disputed transaction by sending the transaction back to the Acquirer.

Merchants who use Verified by Visa are protected from certain fraud-related chargebacks on all consumer Visa cards—credit or debit, domestic, or international—whether or not the Issuer or cardholder is participating in Verified by Visa.

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.

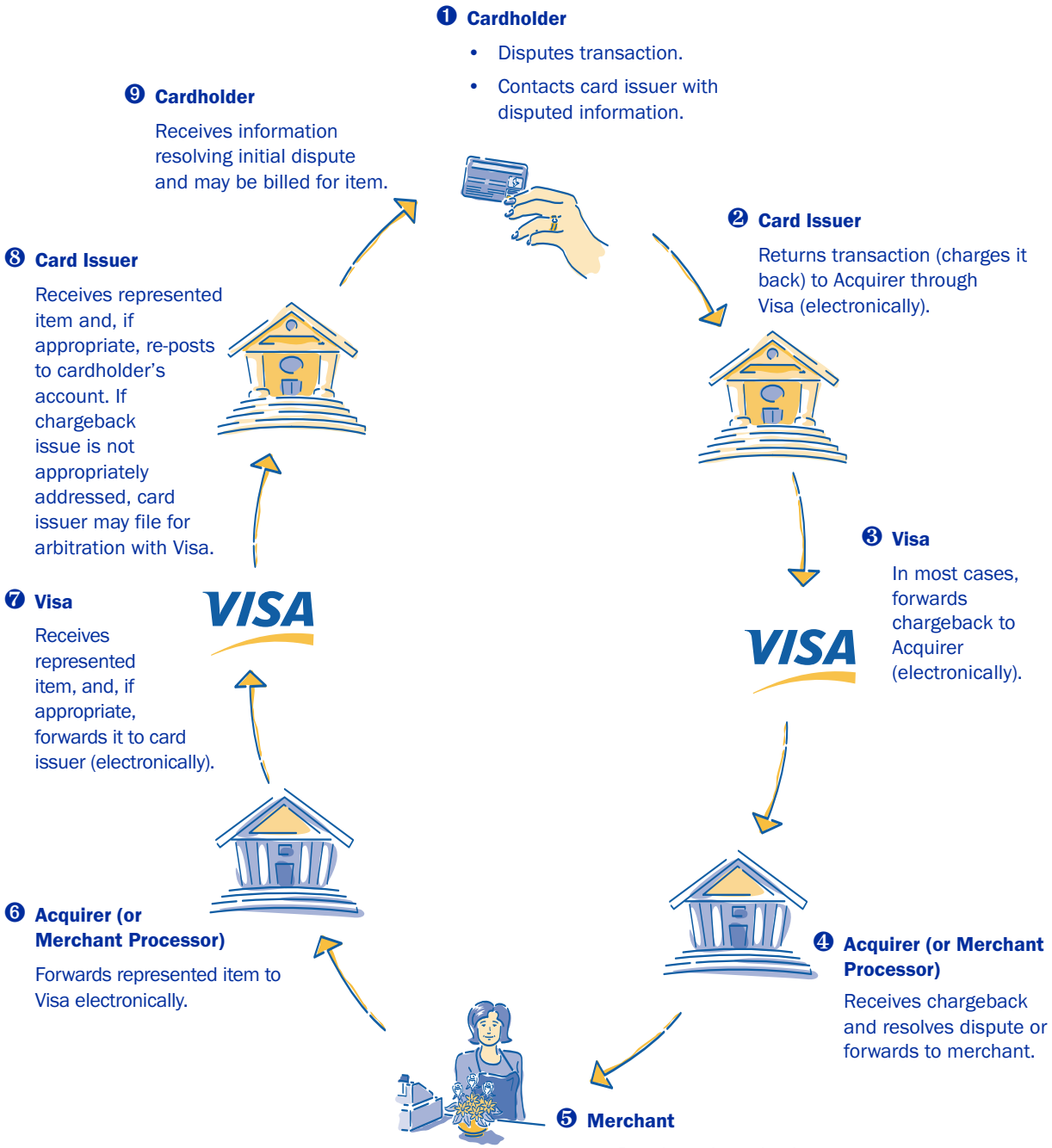
The merchant must then send the transaction receipt copy to the Acquirer who sends it on to the Issuer.

QUICK TIP

When a sales draft request is not fulfilled in a timely manner, 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 Chargeback Lifecycle

The diagram below illustrates the key actions that Issuers and Acquirers can typically take in a customer-dispute situation.



Section 2 E-Commerce Risk Management Best Practices

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

❶ Know the risks and train your troops

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.

❷ Select the right Acquirer and service provider(s)

If you have not yet launched an electronic storefront, you need to partner with a Visa Acquirer 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. The bottom line is — does the service provider have what it takes to keep your cardholder data safe and minimize fraud losses?

Web Site Utility

❸ Develop essential web site content

When designing your web site, you should always keep operational needs and risk factors foremost in mind. Key areas to consider are privacy, reliability, refund policies, and customer service access.

❹ 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 through such actions as highlighting required transaction data fields and verifying Visa card and customer data that you receive through the Internet.

FIFTEEN STEPS TO MANAGING E-COMMERCE RISK

Fraud Prevention

❺ Build internal fraud prevention

By understanding the purchasing habits of your web site 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.

❻ 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.

❼ 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.

❽ Implement Verified by Visa

VERIFIED by VISA

Verified by Visa is the tool that 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 personal Visa cards with limited exceptions. They also benefit by settling at a reduced interchange rate.

❾ 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 the associated fraud risks.

Visa Card Acceptance

❿ Create a sound 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.

⓫ 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.

FIFTEEN STEPS TO MANAGING E-COMMERCE RISK

Cardholder Information Security Program

⓬ Safeguard cardholder data through CISP compliance

Visa's *Cardholder Information Security Program (CISP)* 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. CISP compliance can help you protect the integrity of your operations and earn the trust of your customers.

Chargeback and Loss Recovery

⓭ 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.

⓮ 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.

⓯ Use collection efforts to recover losses

You can often recover unwarranted chargeback losses through a well-thought through collections system.

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, as well as the basic usage of the tools and technologies 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 Troops
- → 2. Select the Right Acquirer and Service Provider(s)

1. Know the Risks and Train Your Troops

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 risk of 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 the chargeback process. Follow your Acquirer's processing instructions to avoid chargebacks related to authorizations and sales draft requests.

- Work with your Acquirer to develop an understanding of the various reasons for chargebacks, particularly in regard to the following:
  - 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.

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 don'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 bankcard 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 web site. ◆ 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.

BITS AND BYTES

Unauthorized use fraud involves a perpetrator who illegally obtains an 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-not-present 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 which 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, and web site cloning scams.

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

When selecting an Acquirer and your service provider(s), you need to carefully look at several important factors, particularly those related to risk management. Here are some essential best practices:

Acquirer

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.

- **Choose an Acquirer with robust e-commerce capabilities.** Carefully review the services, capabilities, and benefits of the Visa Acquirers in your market and partner with the one that will best meet your e-commerce needs. Be sure the Acquirer offers:
  - expertise in e-commerce platforms and security measures, particularly transaction data encryption and secure storage of cardholder information.
  - technical solutions or partnerships with service providers that support your unique Internet business needs and system requirements.
  - risk management tools to avoid or minimize fraud losses, such as Address Verification Service (AVS), Card Verification Value 2 (CVV2), Verified by Visa, velocity checks, and fraud-scoring technologies.

    For more information, refer to "Use Visa Tools" on pages 39 through 49 of this guide.
  - transaction identification using the Electronic Commerce Indicator (ECI).
- When selecting an Acquirer for participation in Verified by Visa, ensure the Acquirer or merchant processor can incorporate the required 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 supports Visa's *Cardholder Information Security Program (CISP)* requirements.** Although security can never be completely guaranteed, the CISP requirements for e-merchants can help significantly reduce the ability of hackers to gain access to proprietary data.

BITS AND BYTES

A good Acquirer:

- provides merchants with Visa rules, standards, and training.
- monitors merchant activities to ensure Visa regulation compliance.
- knows how to support e-commerce business.

BITS AND BYTES

Visa merchants and service providers who process or store cardholder data and have access to that information on the Internet must comply with Visa's *Cardholder Information Security Program (CISP)* requirements. *For specific details, refer to "Safeguard Cardholder Data Through CISP Compliance" on pages 58 through 61, of this guide.*

Acquirer *(continued)*

- **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-not-present, which means you can be held responsible for a charge the cardholder claims he/she did not commit, 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.
  - timeframes for providing additional documentation to your Acquirer in order to fulfill a sales draft request or represent a chargeback.

Service Provider

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 the Visa's Cardholder Information Security Program (CISP).** To ensure protection for Internet transactions, partner with service providers who comply with Visa CISP 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 Visa CISP compliance and the PCI Data Security Standard, refer to the best practices on pages 58-61 of this guide.
- **If you are using a payment gateway, make sure the business has registered as an Agent with Visa.** Check 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.

KEY POINT TO REMEMBER

To achieve compliance, all merchants and their service providers must adhere to the Payment Card Industry (PCI) Data Security Standard which offers a single approach to safeguarding sensitive data for all card brands. A list of CISP-compliant service providers can be found at *www.visa.com/cisp*.

What the Acquirer Will Expect of You

Acquirers often require e-commerce merchants to meet specific standards before they open an account and officially set up their site for business. Listed below are some of the basic requirements e-commerce merchants may need to meet.

Credit Performance/Finance History

In addition to reviewing the merchant's application, Acquirers also check the merchant's financial stability and credit history by reviewing Dun & Bradstreet (or a similar service) and credit bureau reports, financial statements, and income tax returns for the business and its owners.

Business and Owner Profiles

Application forms for e-commerce merchants typically ask for detailed business plans, descriptions of merchandise or services, and copies of all relevant marketing materials.

Acquirers usually conduct a thorough background check on all business principals. Personal credit reports are scrutinized, and addresses verified. If appropriate, a criminal background check is also performed.

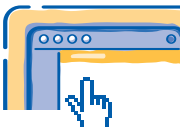
Adherence to Visa's Cardholder Information Security Program (CISP)

To ensure information is being properly safeguarded, Acquirers will ask the merchant and, if applicable, the merchant's service provider to demonstrate compliance with Visa's CISP requirements.

Site Inspections

An Acquirer may conduct a site inspection, which usually includes a merchant's warehouse, as well as office facilities. Shipping, billing, and return policies are carefully reviewed to make sure that no customer is billed before merchandise is shipped. An Acquirer may also "shop" prospective merchants by having one of their own employees place and then return an order. If shipment and delivery are handled by a fulfillment house or other third-party agent, complete information on this firm will also be requested and a site inspection performed. Acquirers may also conduct an inspection of an Internet Service Provider's (ISP's) physical and logical controls, as well as CISP compliance.

Web Site 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 Web Site Content
- → 4. Focus on Risk Reduction

3. Develop Essential Web Site 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 "in's" and "out's" 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 web site visitors through links on your homepage.** 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 web site.**
  - Another way to allay customer concerns about providing personal data is to display a privacy "seal-of-approval" on your web site homepage.
  - To obtain this seal, you need to apply to a major privacy program, such as TRUSTe or the Better Business Bureau's BBBOnLine Privacy.

QUICK TIP

If you need assistance, TRUSTe, an independent privacy organization, has a "wizard" you can use to create a customized privacy policy for your site. It is available at **http://www.truste.org/wizard.**

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 web site visitors through lists on your home page.
- **Create an FAQ page that includes questions and answers on how customers can protect themselves shopping online.**
- **If using Verified by Visa, add the logo on your home, security information, and checkout pages to promote reliable and secure on-line 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.*

Information Security *(continued)*

- **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 web site and in 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 web site offer reliable protection from unauthorized access and give cardholders the safest way to make purchases over the Internet.

Payment Choice

- **Offer the customer clear payment choices**
  - Provide your customers with a clear choice of payment brands. Confusion can often occur when customers believe they're paying with one payment brand, but the transaction is processed using another brand. For example, a customer who selects payment by Visa should always have that choice honored. Options such as "Debit" and "Credit" may be misleading and may have different meanings depending upon the customer's understanding. Selection of a payment brand provides a clear choice to the customer.
  - Display a menu or radio button that presents all of the payment brand options and allows the customer to make an informed choice as shown in the example to the right.
  - **If the customer indicates that he or she wants to pay with a Visa card, make sure the choice is honored.** A merchant is allowed to steer the customer to other forms of payment, but cannot confuse or mislead the customer or omit important information in the process. In other words, the choice is ultimately the customer's. A transaction can only be processed as something other than Visa if the customer has selected another form of payment. However, if a customer chooses Visa, it must be processed as a Visa transaction.

KEY POINT TO REMEMBER

Cardholder protections and promotional benefits associated with the Visa brand may not be available to a cardholder if that cardholder selects Visa as a payment option, but the transaction is not processed in accordance with his or her choice.

Billing Information

Product Description

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

KEY POINT TO REMEMBER

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

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 customers of any goods or service delivery delays.**
- **Consider not providing the tracking number if selling higher fraud risk merchandise and 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 bankcard statement (i.e., the service provider name and amount). This will reduce the risk of confusion when the statement arrives.
- **Encourage cardholders to retain a copy of the transaction.**

KEY POINT TO REMEMBER

Never bill the customer until the merchandise has been shipped.

Digital Content Policies

- **Implement a policy that the cardholder will not be billed until the web site 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

- **Inform potential customers of the currency used for purchases on web sites.** Currency must be clearly stated, especially if the unit of currency is not unique, for example, a dollar could be an Australian, New Zealand, Hong Kong, or U.S. dollar.

KEY POINT TO REMEMBER

Merchants cannot convert transaction amounts into a different currency. Equivalent amounts in other currencies may be shown, but they must be clearly labeled as being listed for information only and subject to variation in accordance with the customer's cardholder agreement.

Country of Origin

- **Declare your address information and country of merchant domicile on the web site.** Check with your Acquirer to ensure your declaration is made in accordance with the *Visa U.S.A. Inc. Operating Regulations* and local law.

Refunds and Credits

- **Establish a clear, concise statement of your refund and credit policy.**
  - Make this statement available to web site visitors through links on your homepage.
  - Provide "click through" acceptance for important elements of the policy — for example, when purchasing tickets to a sporting event, customers click on a button to acknowledge that tickets are non-returnable unless the event is postponed or cancelled.

QUICK TIP

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 providing them with a prompt response, you can help avoid downstream customer disputes and subsequent chargebacks.
  - Display e-mail "Contact Us" options on your web site and make them prominent and easily accessible.
  - To facilitate efficient internal processing of customer responses, provide different e-mail contacts for product/service information, customer support, and back order/shipping information.
- **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.

QUICK TIP

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.

- **Establish e-mail inquiry response standards and monitor staff compliance.**
  - Establish a standard timeframe for responding to 100 percent of e-mail inquiries – for example, 24 hours. Use shorter timeframes 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 web site.**
  - 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.

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 will customers 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—such as grammar school name, place of birth—and 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 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 web site 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 web sites 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.
  - Identify the field that requires completion in the return message 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 Orders

- **Develop controls to avoid duplicate transactions.** Duplicate orders can lead not only to higher processing costs, but also 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 outsort these for review to ensure that they are not duplicates.
  - Send e-mail messages to customers to confirm whether a duplicate order was intentional.

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.
- **Display only the last four digits when showing a card number to a repeat customer at your web site.** This practice 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.

BITS AND BYTES

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 – for example, a Visa cardholder enters a wrong number or transposes digits – and then receives an authorization decline.

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 by customers and often 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 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 since 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.

High-Risk International Address Screening ***(continued)***

- Capture and translate the Internet Protocol (IP) address to identify the computer network source.
  - Use a geolocation 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.

Fraud Prevention

The reality of the e-commerce environment is that we don't live in a perfect world. 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 the associated losses. Given this reality, you just can't make a leap of faith when it comes to accepting payments online. That's the bad news! 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 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 the 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 the 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.** You can ensure and improve the effectiveness of your fraud control group by monitoring such areas as:
  - 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 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.***

BITS AND BYTES

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.

Internal Negative File *(continued)*

  - 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 amount.
  - 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 it during the authorization process.

QUICK TIP

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.

BITS AND BYTES

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 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.

Card Verification Value 2 (CVV2)

CVV2 may be printed in a separate box to the right of the signature panel by early to mid-2006.

- **Work with your Acquirer to implement CVV2.** Ask your Acquirer for a copy of the *Merchant Guide to Card Verification Value 2 (CVV2)*, or order this book directly through Visa Fulfillment. (*Refer to Section 4: Resources for order information.)*
- **Use Visa's CVV2 code to verify the card's authenticity.**
  - Ask the customer for the last three numbers on the back of the Visa card.
  - Provide an option for the customer to enter a code signifying the CVV2 is not legible, such as 000.
  - Send one of the following CVV2 presence indicators along with other required authorization data (i.e., account number, expiration date, and transaction amount).

    The CVV2 presence indicator is an important tracking mechanism that allows merchants to better understand the characteristics of non-face-to-face transactions.

QUICK TIP

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.**

IF:	SEND THIS INDICATOR TO THE CARD ISSUER:
You have chosen not to submit CVV2	0
You have included CVV2 in the authorization request	1
Cardholder has stated CVV2 is illegible	2
Cardholder has stated CVV2 is not on the card	9

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

RESULT:	ACTION:
M – Match	Complete the transaction (taking into account all transaction characteristics and any questionable data).
N – No Match	View the "No-Match" as a sign of potential fraud and take it into account along with the authorization response and any other data available to you. Potentially hold the order for further notification.
P – CVV2 request not processed	Resubmit the authorization request.

RESULT:	ACTION:
S – CVV2 should be on the card, but cardholder has reported to the Merchant that there is no CVV2	Consider following up with your customer to verify that he or she checked the correct card location for CVV2. All valid cards are required to have CVV2 printed on the back.
U – Issuer does not support CVV2.	Evaluate all available information and decide whether to proceed with the transaction or investigate further. Uncertified card issuers lose chargeback rights for Fraudulent Mail Order/ Telephone Order (MO/TO) transactions when CVV2 is included in the authorization message.

- **Take appropriate action if you receive an approval, but still suspect fraud.**
  - Call the customer with any questions,
  - Ask for additional information (e.g., bank name on front of card), or
  - Separately confirm the order by sending a note to the customer's billing address.
- **Contact your Acquirer to report suspicious activity.**
- **To prevent CVV2 from being compromised, NEVER keep or store a Visa card's CVV2 code once a transaction has been completed.** Such action is prohibited and could result in fines.

Address Verification Service (AVS)

- **Work with your Acquirer to implement AVS.** Several options are available to you for connecting to AVS, depending on your card-not-present 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. (*Refer to Section 4: Resources for order information*.)
- **Use AVS to verify the cardholder's billing address (street number and zip code).**
  - Ask the customer for the billing address as it appears on the monthly statement.
  - Submit the address with the authorization request. The Issuer will return an AVS result with the authorization response.

Address Verification Service (AVS) *(continued)*

- **Research all AVS partial matches.** AVS provides a response with the results of the attempted address match. A "partial match" indicates that the compared billing addresses have the same zip code or the same numeric values in the street address, but not both.
  - Evaluate AVS partial matches to date and assess historical risk.
  - Contact the Issuer for high-risk transactions to determine whether the name, address, and telephone number given by the cardholder match the corresponding elements for that customer in the Issuer's file.
- **Evaluate AVS no-matches carefully.** An AVS "no-match" is typically a strong indicator of fraud. However, a no-match may be legitimate if a customer has recently moved and not given an updated address to the Issuer. To research a no-match, do the following:
  - Call the customer to verify that the given telephone number belongs to the individual who placed the order, the address given is the correct billing address and whether the cardholder has recently moved.
  - Contact the Issuer to determine whether the name, address, and telephone number given by the customer matches the corresponding elements for the cardholder in the Issuer's file.
  - Use directory assistance or Internet search tools to contact the individual at the billing address and confirm that he or she initiated the transaction.
- **Ensure that the AVS response is incorporated into the fraud scores used.** For many third-party fraud-screening services today such as the *CyberSource Advanced Internet Fraud Screen enhanced by Visa*, the AVS result code is a critical component of the scoring system. *For details, refer to "Apply Fraud Screening" on pages 45 through 49 of this guide.*
- **Evaluate fraud rates by AVS result and product type.**
  - Review actual fraud experience stratified by the AVS result so you can tailor your AVS review strategies to prevent future losses.
  - Develop transaction review criteria based on the results on your fraud analysis.

Your Acquirer may modify the AVS result codes shown here to make them more 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."

Check with your Acquirer for specific AVS result code definitions.

U.S. AVS Result Code Definitions

CODE	DEFINITION	EXPLANATION
Y	Exact Match	Street address and 5- or 9-digit ZIP Code match
A	Partial Match	Street address matches, ZIP Code does not
Z	Partial Match	Zip Code matches, street address does not
N	No Match	Street address and ZIP Code do not match
U	Unavailable	Address information is unavailable for that account number, or the card issuer does not support AVS
*G	Global	Address information not verified for International transaction
R	Retry	Issuer authorization system is unavailable, retry later

**U.S. merchants use the "G" result code to identify internationally-issued cards.*

International AVS Result Code Definitions

ADDRESS VERIFICATION RESULT CODE VALUES	DEFINITIONS
A	Street addresses match. The street addresses match; the postal codes do not match or the request does not include the postal code
B	Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code)
C	Street address and postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code)
D	Street address and postal codes match
G	Address information not verified for International transaction
I*	Address information not verified for International transaction
M*	Street addresses and postal codes match
N	No match. Neither the street addresses nor the postal codes match
P	Postal codes match. Street address not verified due to incompatible formats (Acquirer sent both street address and postal code)
U	Address information is unavailable for that account number, or the card issuer does not support AVS

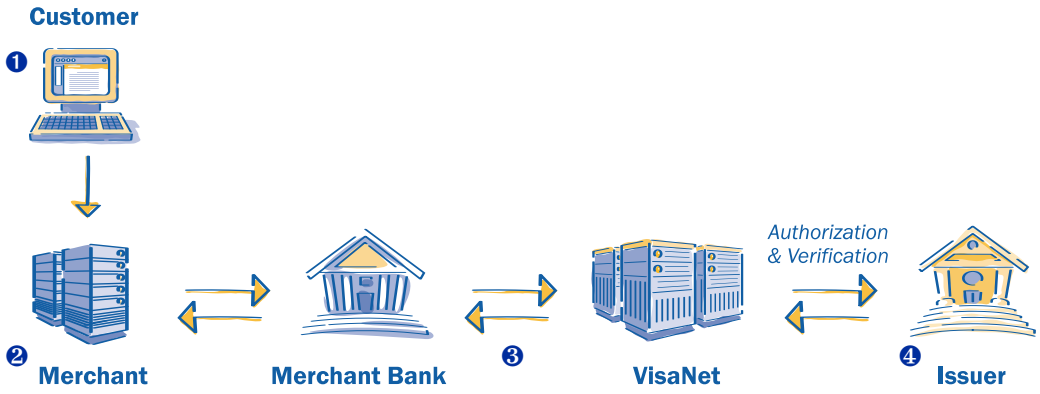
**These codes are currently reserved, in anticipation of Visa Operating Regulations changes.*

AVS PROCESSING AT A GLANCE

AVS With an Authorization Request

You may process AVS requests the same way you process authorizations, that is, either on a real-time basis or in a batch mode using an electronic terminal or personal computer. Real-time requests typically are used for transactions during which the customer waits on-line for a response. The batch mode is geared more toward low-cost processing in which no immediate response is required.

The authorization and address verification process is illustrated and explained below.



1. Customer contacts you to place an order.
2. Your system confirms the usual order information including the merchandise description, price, the Visa account number, card expiration date, and shipping address.

   Your system then prompts the customer for one new piece of information: the billing address (street address and ZIP Code) for the card being used. (The billing address is where the customer's monthly Visa statement is sent for the card being used.)
3. The cardholder's billing address and the transaction information are entered into your authorization request. Both requests are sent at the same time to Visa via the Acquirer.
4. The Issuer makes an authorization decision separately from the AVS request. At the same time, it compares the cardholder billing address sent with the billing address it has for that account. It then returns both the authorization response and a single character alphabetic code indicating the address verification results. Your merchant processor may modify these AVS codes to make them more self-explanatory.

AVS Without an Authorization Request

You may also send an address verification request without an accompanying authorization request if, for example:

- you want to verify the customer's billing address before you request an authorization, or
- you sent an AVS and an authorization request earlier and received an authorization approval, but an AVS "try again later" response.

7. Apply Fraud Screening

Today, there are a wide variety of fraud-screening services 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 the following:

Screening for High-Risk Transactions

- **Implement fraud-screening tools to identify high-risk transactions.**
  - 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).
  - 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.
- **Treat international IP addresses as higher risk.** 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. 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.
- **Treat non-U.S. transactions as higher risk.** Transactions that involve cards issued outside of the U.S. 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.

Screening for High-Risk Transactions *(continued)*

- Be on the lookout for customers who use anonymous e-mail addresses.
- Use a third-party fraud scoring for non-U.S. 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 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.**

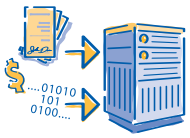
12 Signs of Possible Internet Fraud

When more than one of the following indicators is present in a transaction, it may indicate potential fraud. E-commerce merchants need not be concerned when only one of these signs is present, but when several appear in an Internet purchase, they must take care to avoid becoming a victim of fraud.

- **First-time shopper:** Criminals are always looking for new victims. They usually hit a merchant once and don't go back a second or third time.
- **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchases. Of course, the size of "normal" orders vary from merchant to merchant.
- **Orders consisting of several of the same item:** Having multiples of the same item increases criminals' profits.
- **Orders made up of big-ticket items:** These items have maximum resale value and therefore maximum profit potential.
- **Orders shipped "rushed" or "overnight":** Crooks aren't concerned about extra delivery charges. They want their fraudulently obtained items as soon as possible for the quickest possible resale. This also includes the purchase of large dollar gift cards sent overnight or for "rush" delivery.
- **Orders from Internet addresses at free e-mail services:** These services have no billing relationships with their users, which in turn means no audit trail or verification that a legitimate cardholder has opened the account.
- **Orders shipped to an international address:** A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the United States. AVS can validate addresses in the United Kingdom, but other non-U.S. addresses cannot be verified.
- **Transactions on similar account numbers:** Fraudsters often use account numbers that have been generated with software available on the Internet, such as CreditMaster.*
- **Orders made on multiple cards but shipped to a single address:** These orders can also be characteristic of a software-generated account number or may have been made using a batch of stolen cards.*
- **Multiple transactions on one card over a very short period of time:** Criminals often attempt to run up purchases on a single card until the account is closed.*
- **Multiple shipping addresses:** In a similar fraud scenario, multiple transactions are charged to one card or similar cards that have a single billing address but multiple shipping addresses. This situation could be a sign of some organized activity, rather than one individual at work.*
- **Multiple cards from a single IP address.** The Internet Protocol (IP) address identifies the computer in a network from which an order has been made. In this instance, fraud indicators may include multiple orders using different names, addresses, and card numbers, but coming from one IP address.*

* *Requires regular monitoring of your business transactions. Ideally, you should have a database or account history files against which to compare individual sales for possible fraud.*

Third-Party Fraud Screening



- **Develop a fraud score internally, or use third-party tools for fraud-scoring—such as CyberSource Advanced Fraud Screen enhanced by Visa—to better target the highest risk transactions requiring additional verification.**
- **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 web site "click-through" patterns
    - AVS results
    - CVV2 results
    - Verified by Visa results

What's *CyberSource Advanced Fraud Screen enhanced by Visa*?

CyberSource Advanced Fraud Screen enhanced by Visa complements and improves the detection capabilities of other risk tools — such as card authorization, Visa Address Verification Service (AVS), and Card Verification Value 2 (CVV2). The fraud score predicts the likelihood of a fraudulent transaction by referencing thousands of unique high– and low-risk profiles, comprised of account, merchant, transaction, and global data. A returned risk score typically takes less than two seconds — in real-time. *CyberSource Advanced Fraud Screen enhanced by Visa* calculates the risk score using a combination of neural networks, rules-based modeling, and Visa hybrid fraud technologies to produce the most accurate assessment of potential risk available.

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 merchant processor.
    - Confirm name, address and telephone number associated with the card number.
    - Request whether recent address change or alternative address, as appropriate.
  - Call the cardholder as necessary to confirm the transaction, resolve any discrepancies, and let the cardholder know that you are performing this confirmation as a protection against fraud.

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 the following:

Work with your Acquirer

- **Work with your Acquirer to implement Verified by Visa.**
  - Assess whether Verified by Visa is right for your web site.
  - To learn more about this service, visit ***www.visa.com/verifiedmerchants*** and download the *Visa Merchant Implementation Guide*.
- **Evaluate the benefits of Verified by Visa.** These include:
  - **Increased security and revenue growth** — By improving online security with Verified by Visa, cardholders who currently browse the Internet will become more confident purchasers, possibly increasing sales volume for participating Merchants.
  - **Reduced fraud and chargeback processing expense** — Merchants who use Verified by Visa are protected from fraud-related chargebacks on all personal Visa cards-credit or debit, domestic, or international—whether or not the Issuer or cardholder is participating in Verified by Visa, with limited exceptions. Attempted Issuer chargebacks for fraud on Verified by Visa transactions will be rejected in most cases, resulting in chargeback expense reduction as well as reduced fraud.
  - **Interchange benefit** — Verified by Visa transactions that meet processing requirements settle at an interchange rate that is lower than a standard e-commerce transaction. Pricing of Visa services is determined independently by Acquirers. Check with your Acquirer for more information.

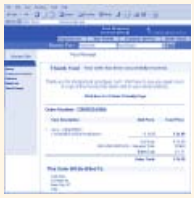
Verified by Visa At a Glance

Verified by Visa enables Issuers to validate the identity of their activated Visa cardholders during online payment transactions.

❶ At a participating merchant site, the Visa cardholder clicks “buy” at the checkout. Software installed on the merchant server recognizes eligible Visa cards, initiating the next steps.

❷ A Verified by Visa page appears within the merchant frame showing the merchant URL. If the cardholder has previously activated their card, he or she will be prompted to enter the password previously created. There is also a “forget password” option to enable a cardholder to establish a new password if forgotten. If the cardholder has not previously activated, the Issuer may prompt the cardholder to activate their card. If the Issuer does not participate in Verified by Visa, no cardholder interaction occurs. However, the merchant still qualifies for certain fraud liability protection; the merchant receives an Attempted Authentication response with authentication data to be submitted in the authorization as proof of qualification for chargeback protection for the transaction.

❸ The Issuer validates the cardholder's identity for activated cards and sends a response to the merchant on the results of the authentication. If authentication fails, the merchant should request payment by alternate means.



❹ After the authentication process is complete, the merchant includes the authentication data received from the Issuer in the authorization request through VisaNet for authorization processing.

Ensure Transaction Qualification

- **Ensure the Acquirer or processor is providing the authentication results and ECI in the authorization message to obtain fraud chargeback protection.**
  - This can be an issue when a second authorization is obtained, such as a split shipment.
- **Monitor percentage of settled transactions that are authenticated or attempts, to identify potential processing problems.**
  - 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.

BITS AND BYTES

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

Perform Transaction Fraud Screening

Verified by Visa has proven to be an effective fraud prevention tool, but 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 45 through 49 of this guide.**
- **Continue to utilize fraud screening tools for Verified by Visa transactions.** There are important reasons for this best practice:
  - **Keeping fraud out of the payment system** — No one except the crook benefits when fraud occurs. At a minimum, your customers or potential customers are inconvenienced and may become wary of using your site.
  - **Providing protection from processing errors** — Transactions believed to have qualified for chargeback liability protection may not qualify due to processing errors. These are typically discovered after the fact and can result in merchant losses.

BITS AND BYTES

In a typical **account takeover** case, a perpetrator gains access to the account information of a valid cardholder either by stealing a monthly statement from the cardholder's mail box or by some other illegal means. Posing as the cardholder, the perpetrator then contacts the Issuer to request a change of address and an additional card in a second name. At this time or soon after, the perpetrator may also request a Personal Identification Number (PIN) for making cash withdrawals at ATMs.

Once in possession of the new card, the perpetrator is able to charge merchandise or obtain cash advances on the legitimate cardholder's account.

**Acceptance costs are determined independently by Acquirers. Check with your Acquirer for details.*

- **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 my 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.

Additional Operational Considerations

- **If using Verified by Visa, add the logo on your home, security information, and checkout pages to promote reliable and secure on-line shopping.** Use one of the following two approaches:
  - **Activate Now** — This is the preferred approach that guides your customers directly to an activation page where they can activate their Visa cards without leaving your site.
  - **Learn More** — This approach directs your customers to a service description page (hosted on your site) where they can read more about Verified by Visa and activate their cards. Be sure to provide clear, easy-to-understand instructions on how Verified by Visa works. *Your Merchant Toolkit includes a "Learn More" page that details the Verified by Visa program.*
- **Do not submit an authorization request for Verified by Visa transactions that fail authentication.**
  - Immediately display a message or page to communicate to the cardholder that the purchase will not be completed with the card that failed.
- **Provide an easy, simple recovery mechanism to cardholders that fail Verified by Visa authentication.**
  - Offer an immediate opportunity for the cardholder to enter a new payment card number and click to try again, or
  - Present a button that, when clicked, presents a new page that allows the cardholder to easily reinitiate the purchase.

9. Protect Your Merchant Account From Intrusion

Unauthorized persons appear to be gaining entry to e-merchant accounts via shopping-cart or payment gateway processor systems. The intruders are attacking e-commerce merchants using weak or generic passwords. Once a password is compromised, the 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 therefore — are 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 (e.g., CreditMaster).
  - multiple transactions on a single card over a very short period of time.
- **Monitor your batches.**
  - Know what time your transactions are settled and review your transactions before settlement occurs.
  - If you use Address Verification Service (AVS) or Card Verification Value 2 (CVV2), look for transactions that may have been submitted without an AVS or CVV2 in the authorization record.

Passwords

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

Information Security Efforts

- **Ensure the requirements of Visa's *Cardholder Information Security Program (CISP)* are in place.**

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 Sound Process for Routing Authorizations
- → 11. Be Prepared to Handle Transactions Post-Authorization

10. Create a Sound Process for Routing Authorizations

The authorization process must be well managed since it has a significant impact on risk, customer service, and operational expense. Best practices include the following:

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 — such as 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 web site 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 U.S.A. Inc. Operating Regulations* and helps protect you from chargebacks due to no authorization.

11. Be Prepared to Handle Transactions Post-Authorization

If an online transaction is approved by the Issuer, you should 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

- **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 it 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.

Cardholder Information Security Program

All e-commerce merchants must take extra care to safeguard their cardholder data and improve their front-line defense to avoid internal and external security compromises. That's where Visa's *Cardholder Information Security Program (CISP)* requirements come in.

Mandated since June 2001, the program is intended to protect Visa cardholder data—wherever it resides—ensuring Members, merchants, and service providers maintain the highest information security standard.

Steps Covered...

→ 12. Safeguard Cardholder Data Through CISP Compliance

12. Safeguard Cardholder Data Through CISP Compliance

Before consumers and businesses order goods and services online, they want assurance that their account information is "cybersafe." That's what the Visa U.S.A. Cardholder Information Security Program (CISP) is all about. As the name implies, its primary purpose is to help establish security procedures to protect cardholder information in all payment security channels.

PCI Data Security Standard

To maintain the highest level of due care, all merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs.

Using the PCI Data Security Standard as its framework, Visa provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard consists of 12 basic requirements.

PCI DATA SECURITY STANDARD	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure applications
Implement Strong Access Control Measures	7. Restrict access to 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

To protect the interest of your Visa customers, follow these best practices.

Adhere to CISP Requirements	• **Work with your Acquirer to understand your information security role and what's required of you and your service providers in regard to CISP compliance.** • **Train employees on CISP compliance basics.** – Use available Visa tools and materials to train your staff on CISP compliance. – Make sure all service providers are fully compliant and the contracts between you specify CISP compliance as a condition of doing business.
Avoid CVV2 Data Storage	• **Do not store Card Verification Value 2 (CVV2) data.** – For information security purposes, *Visa U.S.A. Inc. Operating Regulations* prohibit merchants from storing CVV2 data.
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, other liability, such as to consumers, may also arise.
Taking Immediate Action	• **If you have experienced a suspected or confirmed security breach, 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 Visa systems.

Taking Immediate Action *(continued)*

- **Alert all necessary parties of a suspect or confirmed security breach immediately.** This includes:
  - Internal information security group and Incident Response Team, if applicable
  - Your Legal department
  - Your Acquirer
  - Visa Fraud Control Group at (650) 432-2978
  - Local FBI Office

  Note: Visa and/or the Acquirer will contact the merchant or service provider to discuss the compromise and go over the steps that must be followed to demonstrate ability to prevent future loss or theft of transaction information, consistent with the CISP requirements.
- **Provide the compromised Visa accounts to Visa Fraud Control Group within 24 hours.** Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that **all potentially compromised accounts are provided**. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.
- **Within four business days of a reported compromise, provide an incident report document to Visa and/or depending on the level of risk and data elements obtained, undergo an independent forensic review and complete a compliance questionnaire and vulnerability scan as determined by Visa.**

Contact Information

For more information about Visa CISP compliance, visit ***www.visa.com/cisp***.

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

- **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 and reduce chargebacks, 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

QUICK TIP

By supplying details of the sales transaction in question, you may be able to resolve the request and avoid a chargeback.

QUICK TIP

An Issuer may charge a transaction back if a sales draft is not received within 30 days of a request to the Acquirer. By fulfilling sales draft requests promptly, you can avoid such chargebacks and their associated costs.

Avoiding Chargebacks *(continued)*

- **Provide timely responses to sales draft requests.**
  - Work with your Acquirer to design and implement a timely, efficient process for fulfilling sales draft requests.
  - Investigate facsimile fulfillment by your Acquirer, if this is appropriate for the goods or services that you provide.

Representment Rights

- **Know your AVS and CVV2 representment rights.**

Card-not-present merchants should be familiar with the chargeback representment rights associated with the use of AVS and CVV2. Specifically, your Acquirer can represent a charged-back transaction if you:

- received an AVS positive match 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 delivery.
- submitted an AVS query during authorization and received a "U" response from a U.S. Issuer. This response means the issuer is unavailable or does not support AVS.
- submitted a CVV2 verification request during authorization and received a "U" response from a U.S. Issuer. This response means the issuer does not support CVV2.

BITS AND BYTES

Even though an Acquirer has the right to represent on a merchant's behalf under the circumstances described here, it is no guarantee that the disputed items will be accepted.

If you believe you have AVS or CVV2 representment rights on a charged-back transaction, work with your Acquirer to ensure that all supporting evidence for representment is submitted.

- **Know your Verified by Visa representment rights.**

Merchants that participate in Verified by Visa are protected from unauthorized use chargebacks, in most cases. If you are a Verified by Visa merchant and received a fully authenticated or attempted authentication response from the Issuer and provided the authentication data in the authorization request, you retain representment rights. This even applies to "unauthorized use" chargebacks.

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 first steps 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 to 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.

General best practices for chargeback monitoring include:

- **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.**
- **Track card-present and card-not-present chargebacks separately.** If your business combines traditional retail with Internet transactions, track the card-present and card-not-present chargebacks separately. Similarly, if your business combines MO/TO and Internet sales, these chargebacks should also be monitored separately.

VISA CHARGEBACK MONITORING PROGRAMS

Visa monitors all merchant chargeback activity on a monthly basis and alerts Acquirers when any one of their merchants has excessive chargebacks. In most instances, merchants with a chargeback rate of 1 percent or greater may be considered excessive.

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 be required to work with your Acquirer to develop a detailed chargeback-reduction plan.

Visa may impose financial penalties on Acquirers that fail to reduce excessive merchant-chargeback rates. The extent of your liability for excessive charge-backs and fees should be detailed in your merchant agreement.

Visa also monitors international sales and chargebacks through the *Global Merchant Chargeback Monitoring Program*.

Section 3 Special Considerations for Travel Merchants

Airlines

Web Site Utility

- **Clearly display your change fee policy and pricing.** You can reduce customer inquiries and disputes by informing your customers in advance of the terms and conditions of your change fee policy and the amounts of fees that will be assessed if booked itineraries are changed. This information should be prominently displayed on your web site so that customers can review it before purchasing tickets.
- **Display refund rules on both your booking and confirmation pages.** This practice can help you preserve customer relations in cases where customers cancel their flights. By showing refund rules on your confirmation page, as well as your booking page, you can educate customers about the refund policy prior to ticket purchase and then reinforce this policy after the booking has been made.
- **Use e-tickets in all eligible markets and ensure risk control.** E-tickets enable you to lower processing costs while meeting the needs of Internet users seeking greater convenience. It is a good business practice to use e-tickets in all eligible markets unless there is a ticket on another carrier that does not offer this option. However, since e-tickets are not mailed to the billing address which is checked by the Address Verification Service (AVS), they create a higher level of risk exposure than traditional paper tickets. You can control this risk by requiring the customer at the time of travel to present the Visa card that was used to purchase the e-tickets. This practice gives you a face-to-face opportunity to validate the cardholder and card prior to travel. To avoid customer dissatisfaction, be sure to clearly communicate this policy to customers at the time of ticket reservation and purchase.
- **Determine whether or not to allow third-party sales and establish appropriate polices.** Allowing third parties to purchase tickets for airline travelers increases sales, but also increases risk. For example, a criminal could use the information from a legitimate card to obtain a ticket in his or her own name.
  - If you decide to allow third-party sales through the Internet, establish policies to protect your airline from risk – for example, you might require third-party purchasers to have the same surname as the ticket recipient or to accompany the ticket recipient during travel.
  - If you decide not to allow third-party sales through the Internet, establish procedures to direct third-party purchasers to your physical sales offices.
- **Require customers to use a password to book award travel.** If you offer award travel programs, you need to protect your customers and your airline from unauthorized use of award miles. By requiring customers to use a password or Personal Identification Number (PIN) to access and select award travel, you can tighten control of benefits distribution.

Web Site Utility *(continued)*

- **Lock out account access after multiple failures to enter the correct password.** A web site visitor with several incorrect password entries may be an indicator of risk. For example, a criminal could be trying to guess a legitimate customer's password and gain unauthorized access to the customer's account. You can control this risk by locking out account access after a certain number of incorrect password attempts.
  - Determine the number of incorrect password attempts – for example, five unsuccessful attempts will automatically lock out access to personal account information.
  - Establish a method for legitimate customers to verify their personal security information and regain access to their accounts after they have been locked out.
  - Use an automated e-mail message to inform the legitimate customer of the lock out and the method for regaining account access.
- **Capture, verify, and retain e-mail addresses.** During the reservation and sales process, ask the customer to provide an e-mail address. This vital link between you and the customer can then be stored with other data in the booking record and customer profile for future communications. Be sure to verify each e-mail address that you receive since an invalid e-mail address may be an indicator of risk.
- **Capture and retain Internet Protocol (IP) addresses.** It is important to know the IP addresses of the Internet Service Providers (ISPs) from which your customers make purchases. With a database of these addresses, you can develop fraud-screening tools based on transaction characteristics.
- **Determine whether or not to require a Visa card presentment at the time of travel.** You can effectively manage risk by asking customers at the time of travel to present the Visa card that was used to purchase tickets through the Internet. However, this practice can lead to extreme dissatisfaction among customers who do not carry the card or are not aware of the policy.
  - If you decide to **require** Visa card presentment, be sure that this policy is clearly communicated to customers at the time of ticket reservation and purchase.
  - If you decide **not to require** Visa card presentment, use other fraud-screening procedures instead – for example, you might require the customer at the time of travel to present identification with an address that matches the billing address.

- **Deliver paper tickets only to the billing address.** This practice – especially when combined with Visa's Address Verification Service (AVS) screening – can significantly reduce the risk of losses resulting from ticket purchases made with stolen Visa cards.
- **Require a waiting period of at least four to six hours between ticket purchase and flight time.** Tickets purchased just before a flight may indicate fraud risk. To protect your airline from potential losses, you need adequate time to verify the validity of the customer and Visa card before travel begins.

Visa Card Acceptance

- **Clearly disclose all terms and conditions of the sale.** Before making the decision to buy, your customers should know all of the terms and conditions of the booking at hand. Always tell your customers the following details:
  - The amount of the fee
  - How the fee will appear on the cardholder statement (in total or billed separately)
  - When the fee will be billed
  - What name will appear on the cardholder statement

  By clearly disclosing this information, you can ensure quality of service and avoid unnecessary customer disputes later. For best results, require the customer to "click and accept" the disclosure statement displayed on your site.

Fraud Prevention

- **Screen higher-risk bookings.** This practice can help you detect and prevent fraud before it happens. Be sure to screen bookings with such characteristics as:
  - Third-party purchase
  - First or business class tickets
  - e-tickets or tickets not delivered to billing address
  - Date of travel less than six days after ticket purchase
  - Customer not enrolled in frequent-flyer program
- **Use AVS to confirm billing addresses for paper ticket sales.** AVS can add significant value to your fraud control efforts by confirming whether the Visa card billing address matches the address given by the ticket purchaser. Remember, however, that AVS fraud chargeback rights do not apply to e-ticket sales or cases where paper tickets are not mailed to the billing address.

BITS AND BYTES

If you receive an Address Verification Service (AVS) "positive match" for a paper ticket transaction authorization and the billing and ticket mailing addresses are the same, your Acquirer has the right to represent a fraud chargeback. This right, however, does not carry over to e-tickets because they are not mailed to a billing address that is checked by AVS. Since e-tickets present a higher level of risk, it is still a sound business practice to use AVS to verify the cardholder's address with the Issuer.

Fraud Prevention *(continued)*

- **Track fraud by ticket source.** This practice can help you identify your airline's greatest areas of risk exposure and develop strategies to reduce risk in these areas. When tracking fraud, compare it to the volume of tickets sold by source, such as the Internet, central reservations, ticket counters, and travel agencies.

Car Rental Companies

Web Site Utility

- **Require web site "membership" to book car reservations.** By requiring renters to become members of your web site service, you can collect additional customer data that can help you assess risk. When establishing member profiles:
  - verify the customer data that you collect before you store it.
  - ensure that strong security measures — such as secure data storage and limited employee access — are in place to protect sensitive customer data.
- **Capture and retain reasons for car rentals.** During the reservation booking process at your web site, ask the customer to identify the reason for the car rental — such as business travel, leisure travel, car repair, or weekend excursion. You can then maintain this information in the customer history, as well as the booking record. Rental reason data can help you facilitate risk assessment. For example, a rental due to a car repair is typically lower risk than a walk-up leisure travel rental.
- **Capture, verify, and retain e-mail addresses.** During the reservation booking process, ask the customer to provide an e-mail address. Be sure to verify each e-mail address that you receive since an invalid e-mail address may be an indicator of risk.
- **Issue rental reservation confirmation numbers.** This Visa requirement helps assure customers that their rental reservations were successful and will be honored on the date of car pick-up. Be sure that your reservation systems are integrated to support inquiries from customers who may contact you later to confirm their reservations.
- **Require a waiting period of at least four hours between rental reservation and car pick-up for new customers.** To protect your company from risk exposure, you need adequate time to verify the validity of the Visa cardholder and his or her card before car rental service begins. This is especially important for new customers who have no track record with your company.

Visa Card Acceptance

- **Obtain an incremental authorization approval if the car rental period is extended.** In some cases, a customer with a rental car may wish to extend the rental period beyond the time frame of the original agreement. When this occurs, you need to obtain an incremental authorization approval for the additional transaction amount or amounts that will be generated by the car rental extension.
  - Follow standard authorization procedures to obtain an approval for the incremental transaction amount(s).
  - If you receive a "decline" response, contact the customer and request an alternate payment method for the amount that was not approved.
- **Settle only for the cumulative approved authorization amount if an incremental authorization was declined.** Good settlement practices will help you minimize chargebacks, processing costs, and potential losses when Issuers decline incremental authorization requests for car rental extensions.
  - Submit a settlement transaction for the total approved authorization amount and do not include any amount(s) that received an authorization decline.
  - Obtain alternate payment means for the declined incremental amount(s).
- **Submit an authorization reversal if the originally approved authorization amount exceeds the actual car rental cost.** In some cases, the actual cost of a rental car may be less than the amount you previously estimated for the authorization approval. To complete settlement and to avoid tying up the customer's credit, you need to submit an authorization reversal for the difference between the authorization amount and the actual rental agreement.
- **Understand and apply the final authorization and 15 percent rule.** At the end of the car rental period, authorization is required in the following instances:
  - If there was no previous authorization, authorize the total transaction amount.
  - If there was a previous authorization, and the actual final transaction amount is more than the previous authorization amount, you need to apply the "15 percent rule" to determine whether or not an additional authorization is required. To do this:
    - add 15 percent to the previously authorized amount.
    - compare the total (sum of authorization amount plus 15 percent) to the actual transaction amount.

    If the actual transaction amount is more than the total, **an additional authorization is required for the difference between the original authorization and final transaction amount**.

Cruise Lines

Web Site Utility

- **Require web site "membership" to book cruise reservations.** By requiring customers to become members of your web site service, you can collect additional data that can help you assess risk. When establishing member profiles:
  - verify the customer data that you collect before you store it.
  - ensure that strong security measures — such as secure data storage and limited employee access — are in place to protect sensitive customer data.
- **Capture, verify, and retain e-mail addresses.** During the cruise booking process, ask the customer to provide an e-mail address. Be sure to verify each e-mail address that you receive since an invalid e-mail address may be an indicator of risk.
- **Issue cruise reservation confirmation numbers.** This Visa requirement helps assure customers that their cruise reservations were successful and will be honored on the date of the trip. Be sure that your systems are integrated to support inquiries from customers who may contact you later to confirm their reservations.
- **Issue a cancellation code to the cardholder.** In accordance with the Visa reservation service requirements, you must provide a cancellation number when a cruise is properly cancelled. Always advise the cardholder to retain his or her cancellation code.
- **Clearly display your change fee policy and pricing.** You can reduce customer inquiries and disputes by informing your customers in advance of the terms and conditions of your change fee policy and the amounts of fees that will be assessed if booked itineraries are changed. This information should be prominently displayed on your web site so that customers can review it before purchasing tickets.
- **Display refund rules on both your booking and confirmation pages.** This practice can help you preserve customer relations in cases where customers cancel their cruises. By showing refund rules on your confirmation page, as well as your booking page, you can educate customers about the refund policy prior to ticket purchase and then reinforce this policy after the booking has been made.

- **Determine whether or not to allow third-party sales and establish appropriate polices.** Allowing third parties to purchase tickets for cruise passengers increases sales, but also increases risk. For example, a criminal could use the information from a legitimate card to obtain a ticket in his or her own name.
  - If you decide to **allow third-party sales** through the Internet, establish policies to protect your business from risk – for example, you might require third-party purchasers to have the same surname as the ticket recipient or to accompany the ticket recipient during travel.
  - If you decide **not to allow third-party sales** through the Internet, establish procedures to direct third-party purchasers to your physical sales offices.
- **Capture and retain Internet Protocol (IP) addresses.** It is important to know the IP addresses of the Internet Service Providers (ISPs) from which your customers make purchases. With a database of these addresses, you can develop fraud-screening tools based on transaction characteristics.

Visa Card Acceptance

- **Obtain an incremental authorization approval for onboard charges.** In some cases, you may need to obtain an incremental authorization approval for the additional transaction amount(s) generated for onboard incidentals.
  - Follow standard authorization procedures to obtain an approval for the incremental transaction amount(s).
  - If you receive a "decline" response, contact the customer and request an alternate payment method for the amount that was not approved.
- **Settle only for the cumulative approved authorization amount if an incremental authorization was declined.** Good settlement practices will help you minimize chargebacks, processing costs, and potential losses when Issuers decline incremental authorization requests for cruise extensions.
  - Submit a settlement transaction for the total approved authorization amount and do not include any amount(s) that received an authorization decline.
  - Obtain alternate payment means for the declined incremental amount(s).
- **Submit an authorization reversal if the originally approved authorization amount exceeds the actual cruise cost.** In some cases, the actual cost of a cruise may be less than the amount you previously estimated for the authorization approval. To complete settlement and to avoid tying up the customer's credit, you need to submit an authorization reversal for the difference between the authorization amount and the actual cruise agreement.
- **Understand and apply the final authorization and 15 percent rule.** When the customer checks out at the end of a cruise, authorization is required in the following instances:
  - If there was no previous authorization, authorize the total transaction amount.

Visa Card Acceptance *(continued)*

- If there was a previous authorization, and the actual final transaction amount is more than the previous authorization amount, you need to apply the "15 percent rule" to determine whether or not an additional authorization is required. To do this:
  - add 15 percent to the previously authorized amount.
  - compare the total (sum of authorization amount plus 15 percent) to the actual transaction amount.

  If the actual transaction amount is more than the total, **an additional authorization is required for the difference between the original authorization and final transaction amount**.

- **Clearly disclose all terms and conditions of the sale.** Before making the decision to buy, your customers should know all of the terms and conditions of the booking at hand. Always tell your customers the following details:
  - The amount of the fee
  - How the fee will appear on the cardholder statement (in total or billed separately)
  - When the fee will be billed
  - What name will appear on the cardholder statement

  By clearly disclosing this information, you can ensure quality of service and avoid unnecessary customer disputes later. For best results, require the customer to "click and accept" the disclosure statement displayed on your site.

Fraud Prevention

- **Screen higher-risk bookings.** This practice can help you detect and prevent fraud before it happens. Be sure to screen cruise line bookings with such characteristics as:
  - Passenger name different from cardholder name
  - Date of travel less than six days after ticket purchase
- **Use AVS to confirm billing addresses.** AVS can add significant value to your fraud control efforts by confirming whether the Visa card billing address matches the address given by cruise ticket passenger.
- **Participate in Verified by Visa.** This service can help prevent fraud and protect against fraudulent "unauthorized use" chargebacks.

Hotels

Web Site Utility

- **Require web site "membership" to book hotel reservations.** By requiring customers to become members of your web site service, you can collect additional data that can help you assess risk. When establishing member profiles:
  - verify the customer data that you collect before you store it.
  - ensure that strong security measures — such as secure data storage and limited employee access — are in place to protect sensitive customer data.
- **Capture, verify, and retain e-mail addresses.** During the hotel reservation process, ask the customer to provide an e-mail address. Be sure to verify each e-mail address that you receive since an invalid e-mail address may be an indicator of risk.
- **Issue hotel reservation confirmation numbers.** This Visa requirement helps assure customers that their hotel reservations were successful and will be honored on the date of the trip. Be sure that your systems are integrated to support inquiries from customers who may contact you later to confirm their reservations.
- **Issue a cancellation code to the cardholder.** In accordance with the Visa reservation service requirements, you must provide a cancellation number when a hotel room is properly cancelled. Always advise the cardholder to retain the cancellation code.
- **Clearly display your cancellation policy and pricing.** You can reduce customer inquiries and disputes by informing your customers in advance of the terms and conditions of your cancellation policy and the amounts of fees that will be assessed if booked hotel reservations are changed. This information should be prominently displayed on your web site so that customers can review it before making reservation commitments.
- **Display refund rules on both your booking and confirmation pages.** This practice can help you preserve customer relations in cases where customers cancel their hotel reservations. By showing refund rules on your confirmation page, as well as your booking page, you can educate customers about the refund policy prior to hotel room purchase and then reinforce this policy after the booking has been made.
- **Capture and retain Internet Protocol (IP) addresses.** It is important to know the IP addresses of the Internet Service Providers (ISPs) from which your customers make purchases. With a database of these addresses, you can develop fraud-screening tools based on transaction characteristics.

Visa Card Acceptance

- **Obtain an incremental authorization approval if the hotel accommodation timeframe has been extended or if the customer has incurred incidental charges.** In some cases, a customer may wish to extend their stay beyond the time frame of the original agreement. When this happens, you need to obtain an incremental authorization approval for the additional transaction amount(s) that will be generated by the extension.
  - Follow standard authorization procedures to obtain an approval for the incremental transaction amount(s).
  - If you receive a "decline" response, contact the customer and request an alternate payment method for the amount that was not approved.
- **Settle only for the cumulative approved authorization amount if an incremental authorization was declined.** Good settlement practices will help you minimize chargebacks, processing costs, and potential losses when Issuers decline incremental authorization requests for hotel extensions and/or incidental charges.
  - Submit a settlement transaction for the total approved authorization amount and do not include any amount(s) that received an authorization decline.
  - Obtain alternate payment means for the declined incremental amount(s).
- **Submit an authorization reversal if the originally approved authorization amount exceeds the actual hotel accommodation cost.** In some cases, the actual cost of the hotel accommodations may be less than the amount you previously estimated for the authorization approval. To complete settlement and to avoid tying up the customer's credit, you need to submit an authorization reversal for the difference between the authorization amount and the actual hotel reservation agreement.
- **Understand and apply the final authorization and 15 percent rule.** When the customer checks out, authorization is required in the following instances:
  - If there was no previous authorization, authorize the total transaction amount.
  - If there was a previous authorization, and the actual final transaction amount is more than the previous authorization amount, you need to apply the "15 percent rule" to determine whether or not an additional authorization is required. To do this:
    - add 15 percent to the previously authorized amount.
    - compare the total (sum of authorization amount plus 15 percent) to the actual transaction amount.

    If the actual transaction amount is more than the total, **an additional authorization is required for the difference between the original authorization and final transaction amount**.

Visa Card Acceptance *(continued)*

- **Clearly disclose all terms and conditions of the sale.** Before making the decision to book a hotel room, your customers should know all of the terms and conditions. Always tell your customers the following details:
  - The cancellation policy
  - How the "No Show" fee will appear on the cardholder statement (in total or billed separately)
  - When the "No Show" will be billed
  - What name will appear on the cardholder statement

  By clearly disclosing this information, you can ensure quality of service and avoid unnecessary customer disputes later. For best results, require the customer to "click and accept" the disclosure statement displayed on your site.

Fraud Prevention

- **Use AVS to confirm billing addresses.** AVS can add significant value to your fraud control efforts by confirming whether the Visa card billing address matches the address given by the customer.

Travel Agencies

E-Commerce Start-up

- **Recognize your potential sales agent liability.** Understanding your risk exposure can help you take appropriate steps to minimize it, and protect your agency from losses associated with customer disputes and fraud. As a sales agent of an airline, for example, your agency may be liable for the entire amount of an airline ticket if it is disputed by the customer or purchased with a stolen account number. To mitigate risk, you need to establish e-commerce policies and procedures that address the following factors:
  - An approved authorization request indicates that the account is in good standing. However, the response is not proof that the legitimate cardholder is making the purchase, nor is it a guarantee of payment. In most cases, therefore, airlines are liable for fraudulent "card-not-present" transactions even when they were approved by the Issuer.
  - Even if a travel agency is not a Visa merchant subject to Visa regulations, the airline partner is. In most fraud-related cases, the airline transfers financial liability to the travel agency partner as part of the contractual agreement.

Web Site Utility

- **Require web site "membership" to book airline tickets and other travel services such as hotel accommodations and car rentals.** By requiring customers to become members of your web site service, you can collect additional customer data that can help you assess risk. When establishing member profiles:
  - Verify the customer data that you collect before you store it.
  - Ensure that strong security measures – such secure data storage and limited employee access – are in place to protect sensitive customer data.
- **Capture and retain Internet Protocol (IP) addresses.** It is important to know the IP addresses of the Internet Service Provider (ISPs) from which your customers make purchases. With a database of these addresses, you can develop fraud-screening tools based on transaction characteristics.

Web Site Utility *(continued)*

- **Display a web site notice that the customer's billing addresses will be verified.** If you access Address Verification Service (AVS) offline, you may encounter address verification failures long after your customer has completed booking. By letting customers know that the billing address will be verified, you can prepare them to understand potential address inquiries later. This web site notice should clearly state that airline tickets cannot be issued until the customer's billing address has been verified by the Issuer.
- **Require a waiting period of at least four to six hours between ticket purchase and flight time.** Tickets purchased just before a flight may indicate fraud risk. To protect your company from potential losses, you need adequate time to verify the validity of the customer and payment card before travel begins.

Visa Card Acceptance

- **Ensure that your agency name and toll-free telephone number or URL address appear on the cardholder statement with your airline partner's name.** Customer inquiries and disputes can be avoided if your travel agency name and contact information are included in the merchant descriptions that appear on the billing statements of your customers. Work with your airline partners and Acquirer to ensure that cardholder statements give your customers an easy way to recognize their bookings with your agency and an easy way to reach you when they have questions.
- **Clearly disclose all terms and conditions of the sale.** Before making the decision to buy, your customers should know all of the terms and conditions of the booking at hand. Always tell your customers the following details:
  - The agency fee will be billed separately from the reservation fee (airline ticket charge, hotel charge, etc.)
  - The amount of the fee
  - When the fee will be billed
  - What name will appear on the cardholder statement

  By clearly disclosing this information, you can ensure quality of service and avoid unnecessary customer disputes later. For best results, require the customer to "click and accept" the disclosure statement displayed on your site.

QUICK TIP

A travel agency booking made with a Visa card involves not only the agency and its customer, but also the airline that issued the ticket and the financial institution that issued the card. Your Visa card acceptance practices need to address the potential consumer confusion that can result from a single transaction with multiple participants.

Fraud Prevention

- **Queue large-value bookings for fraud review.** High-dollar transactions may increase your exposure to fraud and customer disputes. You can mitigate risk and its associated costs by reviewing this type of booking carefully before settling with your airline partner. For best results, queue large transactions for review and call the cardholders involved to verify booking data.
- **Track key fraud characteristics.** To ensure effective fraud control, you need to track known fraud transactions, identify all key characteristics of these bookings, and store the information in an ever-growing database that you can use to make risk assessments. Focus on such characteristics as:
  - Passenger names, addresses, and telephone numbers
  - Cardholder names, addresses, and telephone numbers
  - E-mail addresses, Internet Protocol (IP) addresses, and Internet Service Providers (ISPs)
  - Transaction times, amounts, air carriers, classes of service, and travel itineraries
- **Screen higher-risk bookings.** This practice can help you detect and prevent fraud before it happens. Be sure to screen bookings with such characteristics as:
  - Passenger name different from cardholder name
  - First or business class tickets
  - Electronic tickets or tickets not delivered to billing address
  - Date of travel less than six days after ticket purchase

Section 4 Resources

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 web site, 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 web site privacy.

The E-Commerce Market Today

- **BBB*Online*** – An array of resources provided by the Better Business Bureau to assist consumers and businesses interested in e-commerce: **http://www.bbbonline.com/**
- **CommerceNet Electronic Resources** – Broad range of information on establishing Internet commerce web sites and conducting business over the Internet: **http://www.commerce.net/resources/**
- **Shop.Org** – Trade association for e-commerce retailers. Includes information on sponsored conferences, research, and other resources provided by the association: **http://www.shop.org/**
- **U.S. Government E-Commerce Policy** – Summary of Federal Government e-commerce policies and initiatives, with references to other available resources: **http://www.ecommerce.gov/**
- **Visa Home Page** – Starting point to access a wide range of information provided by Visa: **http://www.usa.visa.com/**

Web Site Privacy

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

Fraud Prevention

- ***CyberSource Advanced Fraud Screen enhanced by Visa*** – The first tool of its kind to use updated purchase activity from both online and in-store purchasing profiles and trends on a continuous basis — resulting in a highly accurate fraud-detection and scoring system. To reliably assess the rank order of risk on any purchase order, *CyberSource Advanced Fraud Screen enhanced by Visa* employs Visa's patent-pending, encrypted, distributed-scoring technology. The service provides subscribing merchants with a risk score indicating the likelihood of a fraudulent transaction. For more information contact your Acquirer or CyberSource at **http://www.cybersource.com/**
- **Verified by Visa** – Through the simple Verified by Visa checkout process, Issuers confirm their registered Visa cardholder's identities in real-time during transactions at participating merchant sites. With Verified by Visa, merchants initiate the authentication process. When the Visa cardholder clicks "buy" at checkout, software installed on the merchant server recognizes registered Visa cards and the Verified by Visa screen automatically appears on the cardholder's desktop. The cardholder simply enters his password to verify his identity. For more information, contact your Acquirer or refer to **http://www.usa.visa.com/verifiedmerchants**

Address Validation

- **US Postal Service City/State/ZIP Code Verification** – Web tool to validate a combination of city, state and ZIP code: **http://www.usps.com**

Social Security Number Validation

- **Social Security Administration SSN Verification** – Features guidelines on how to verify SSN/EIN. This cannot be done directly via the Internet, but entails a phone call with instructions provided on the web site: **http://www.ssa.gov/employer/ssn.html**
- **Social Security Number Death Index** – No-charge search tool to identify deceased Social Security Numbers: **http://www.ancestry.com/ssdi/advanced.html**

Merchant Risk Council

- **Merchant Risk Council** – The Merchant Risk Council establishes the fundamentals and standards of good practices for e-commerce merchants in an effort to identify industry trends of common interest and become a voice in the payments industry. Its pursuit of new technology in the Internet industry helps enable e-commerce merchants to guard against fraudulent activity, and positively influence customer perception of online ordering security. For further details, visit **http://www.merchantriskcouncil.org**

Visa Materials for E-Commerce Merchants

All of the resources below are available in print and can be ordered through Visa Fulfillment Center at 1-800-VISA-311.

Card Acceptance and Chargeback Management Guide for Visa Merchants

The *Card Acceptance and Chargeback Management Guide 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 sales staffs with accurate, up-to-date information on processing Visa transactions, while minimizing risk of loss from fraud and chargebacks. Materials in the book are targeted at both card-present and card-not-present merchants and their employees, and include requirements and best practices for doing business online.

Item # VBS 02.01.04

Visa Card Verification Value 2 (CVV2) Merchant Guide

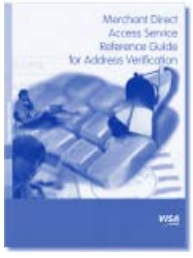
This four-page brochure provides a detailed look at the CVV2 process. It includes instructions on how to use CVV2 in conjunction with other fraud protection tools such as Verified by Visa to maximize security and protect against fraud.

Item # VRM 04.02.05

Merchant Guide to Visa Address Verification Service (AVS)

This 16-page guide describes AVS, Visa's risk management service for card-not-present transactions. Targeted at MO/TO and Internet merchants, the guide explains how to maximize the fraud-reduction benefits of AVS and also covers recent system enhancements and dial-up access.

Item # VBS 10.20.04



Merchant Direct Access Service Reference Guide for Address Verification

This eight-page guide offers step-by-step procedures for accessing MDAS and requesting an address verification for a mail-order or telephone-order transaction.

Item # VBS 07.02.01

Protect Your Virtual Storefront Against Fraud

This three-fold brochure is a fast and easy reference for Internet merchants. It contains best practices to help prevent fraud and fraud-related losses for online transactions.

Item # *VBS 01.04.01*

Merchant Best Practices for Recurring Transactions

This brochure contains merchant tools and best practices for effectively handling recurring transactions. Step-by-step procedures cover all aspects of the recurring-transaction life cycle, from initial setup to handling customer-dispute chargebacks.

Item # *VBS 04.21.04*

Visa USA Merchant Catalog

Visa has assembled this catalog of tools and materials specifically to help merchants in key areas such as card acceptance and fraud-prevention procedures. This assortment of brochures, manuals, flyers, leaflets, videos and online training tools will assist brick-and-mortar, card-not-present, and business to business merchants.

Item # *VBS 07.09.04*

Appendices

Appendix A. Glossary

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

Acquirer — A financial institution with which a merchant contracts to accept Visa cards for payment of goods and services, and with which the merchant deposits its Visa card transactions. Also known as a *merchant bank*.

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 of a variety of 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 — Takes place at the time the transaction occurs. It is the process by which an Issuer approves (or declines) a Visa card purchase.

AVS — See *Address Verification Service*.

Card-not-present (CNP) — An environment where a transaction is completed under both of the following conditions:· cardholder is not present and card is not present. Transactions in this environment include mail/phone order transactions as well as Internet transactions.

Card Verification Value 2 (CVV2) — A three-digit value that is printed on the back of a Visa card, provides a crypto graphic check of the information embossed on a card, and assures the merchant, Acquirer, and Issuer that the card is in possession of the cardholder. CNP merchants should ask the customer for the CVV2 to verify the card's authenticity. For information security purposes, merchants are prohibited from storing CVV2 data.

Chargeback A processed bankcard transaction that is later rejected and returned to the 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.

Cardholder Information Security Program (CISP) A Visa program that provides e-commerce merchants with standards, procedures, and tools for data protection.

Cookie A special text file created by a web site service and written onto the computer hard drive of a web site visitor. The Internet relies upon a computer language called Hypertext Transfer Protocol (HTTP) to let users access Web pages. Since 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 or anything about the user's previous visits. Cookies allow the server to retain information about a visitor or a visitor's actions on its web site 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" typically let customers fill virtual shopping carts with more than one selection before checking out. Also known as Web browser cookies.

Copy request See *sales draft request*.

Cryptography The advanced process of encoding and decoding data to prevent unauthorized parties from reading it while it travels over the Internet. Also known as encryption/decryption.

CVV2 See *Card Verification Value 2.*

CyberSource A third-party service provider offering a range of services for e-commerce merchants, including payment processing, global tax calculation, distribution control, and fulfillment messaging as well as Internet fraud screening. CyberSource and Visa offer the *CyberSource Advanced Fraud Screen enhanced by Visa* (see below).

CyberSource Advanced Fraud Screen enhanced by Visa A real-time fraud-detection service that examines transactions generated from online stores. It estimates the level of risk associated with each transaction and provides merchants with risk scores, enabling them to more accurately identify potentially fraudulent orders.

Decryption The process of decoding, or unscrambling, data that was encrypted to prevent unauthorized parties from reading it during Internet transmission.

ECI See *Electronic Commerce Indicator*.

Electronic Commerce Indicator (ECI)	A transaction data field used by e-commerce merchants and Acquirers to differentiate Internet merchants from other merchant types. Use of the ECI in authorization and settlement messages helps e-commerce merchants meet Visa processing requirements, and enables Internet transactions to be distinguished from other transaction types. Visa requires all e-commerce merchants to use the ECI.
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 which 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 likeliness of an individual transaction being fraudulent.
Internet Protocol (IP) Address	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 card to cardholders, and with which each cardholder has an agreement to repay the outstanding debt on the card. Also known as a *consumer bank*.
Mod 10 check	A mathematical algorithm for checking the validity of Visa card numbers. By performing a Mod 10 check, e-commerce merchants can verify that a card number entered by a customer has a numerically valid structure. However, a Mod 10 check does not ensure that this card number has a legitimate account associated with it.

Payment gateway An Acquirer's link between its e-commerce merchants and the global VisaNet transaction processing system. The payment gateway receives encrypted transactions from the merchant server. The gateway then authenticates the merchant, decrypts the payment information, and sends this data through VisaNet to the Issuer for authorization. When an Issuer response is returned through VisaNet, the gateway encrypts the payment data again along with the response and sends this back through the Internet to the merchant server. The payment gateway thus supports merchant and cardholder authentication, the safe transmission of payment data, and the authorization and capture of e-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.

Sales draft request A request by an Issuer to an Acquirer for a copy or facsimile of a sales order in question. The Acquirer either fulfills this request directly or forwards it to the merchant for fulfillment. Also known as a copy request. This is often a first step prior to chargeback and indicates some initial question about the transaction on the cardholder's part.

Secure Sockets Layer (SSL) An established industry standard that encrypts the channel between a Web browser and Web server to ensure the privacy and reliability of data transmitted over this channel. SSL does not, however, provide ways to validate the identities or banking accounts of the parties exchanging this data.

SSL See *Secure Sockets Layer.*

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" at checkout of a participating merchant, the merchant server recognizes the registered 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 Issuer confirms the consumer's identity.

Appendix B. Checklist for Success

E-Commerce Start-Up

❶ Know the risks and train your troops

- ❒ Be aware of the risk of selling on the Internet.
- ❒ Understand the chargeback process.
- ❒ Train your employees in e-business risk management.

❷ Select the right Acquirer and service provider(s)

- ❒ Choose an Acquirer with robust e-commerce capabilities.
- ❒ Make sure the Acquirer supports *Visa's Cardholder Information Security Program (CISP)* requirements.
- ❒ Understand the terms and conditions of your Acquirer contract.
- ❒ Research the service provider (e.g., webhost, shopping cart, payment processors, fulfillment houses, etc.) business.
- ❒ Make sure your service provider can ensure maximum security for cardholder data received.
- ❒ Partner with a risk-focused service provider.

Web Site Utility

❸ Develop essential web site content

- ❒ Develop a clear, concise statement of your privacy policy and make it available to web site visitors through links on your homepage.
- ❒ Register with a privacy organization and post a "seal of approval" on your web site.
- ❒ Create a page that educates customers about your site's information security practices and controls.
- ❒ Create an FAQ page that includes questions and answers on how customers can protect themselves shopping online.
- ❒ If using the Verified by Visa service, add the logo on your home, security information and checkout pages, to promote reliable and secure on-line shopping.
- ❒ Avoid the use of e-mail for transactions.
- ❒ Offer the customer clear payment choices.
- ❒ Make sure your goods or services are accurately described on your web site. Include photos where possible

Web Site Utility

❸ Develop essential web site content *(continued)*

- ❒ 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.
- ❒ Develop an e-mail response to customers of any goods or service delivery delays.
- ❒ Consider not providing the tracking number if selling higher fraud risk merchandise and not allowing redirection of the shipment.
- ❒ Develop a description of your billing practices terms and conditions and make them available to customers at the time of the online purchase.
- ❒ Encourage cardholders to retain a copy of the transaction.
- ❒ Inform potential customers of the currency used for purchases on web sites.
- ❒ Declare your address information and country of merchant domicile on the web site.
- ❒ Establish a clear, concise statement of your refund and credit policy.
- ❒ Clearly display your recurring transaction disclosure statement on the screen.
- ❒ Provide an e-mail inquiry option.
- ❒ Develop an e-mail inquiry response policy.
- ❒ Establish e-mail inquiry response standards and monitor staff compliance.
- ❒ Offer local and toll-free telephone customer service support and display your phone numbers on your web site.

❹ Focus on risk reduction

- ❒ Make effective use of permanent Web browser cookies to recognize and acknowledge existing customers.
- ❒ Establish ways to assist customers who forget their passwords.
- ❒ Establish transaction data fields that can help you detect risky situations, and require the customer to complete them.
- ❒ Highlight the data fields that the customer must complete.
- ❒ Edit and validate required data fields in real-time to reduce risk exposure.
- ❒ Develop controls to avoid duplicate transactions.

❹ Focus on risk reduction *(continued)*

- ❒ Display only the last four digits when showing a card number to a repeat customer at your web site.
- ❒ Check the validity of the customer's telephone number, physical address, and e-mail address.
- ❒ Screen for high-risk international addresses.

Fraud Prevention

❺ Build internal fraud prevention

- ❒ Establish a formal fraud control function.
- ❒ Track fraud control performance.
- ❒ Establish and maintain an internal negative file.
- ❒ Use the internal negative file to screen transactions.
- ❒ Establish transaction controls and velocity limits.
- ❒ Modify transaction controls and velocity limits based upon transaction risk.

❻ Use Visa tools

- ❒ Ask the customer for both a card type and an account number, and make sure that they match.
- ❒ Require the cardholder to enter the card expiration date or select it from a pull-down window.
- ❒ Work with your Acquirer to implement CVV2.
- ❒ Use Visa's CVV2 code to verify the card's authenticity.
- ❒ Take appropriate action if you receive an approval, but still suspect fraud.
- ❒ Contact your Acquirer to report suspicious activity.
- ❒ To prevent CVV2 from being compromised, NEVER keep or store a Visa card's CVV2 code once a transaction has been completed.
- ❒ Work with your Acquirer to implement AVS.
- ❒ Use AVS to verify the cardholder's billing address (street number and zip code).
- ❒ Research all AVS partial matches.
- ❒ Evaluate AVS no-matches carefully.
- ❒ Ensure that the AVS response is incorporated into the fraud scores used.
- ❒ Evaluate fraud rates by AVS result and product type.

Fraud Prevention

❼ Apply fraud screening

- ❒ Implement fraud-screening tools to identify high-risk transactions.
- ❒ Treat international IP addresses as higher risk.
- ❒ Require shipping address to match billing address for higher risk transactions.
- ❒ Screen for high-risk shipping addresses.
- ❒ Treat non-U.S. transactions as higher risk.
- ❒ Thoroughly scrutinize or restrict shipping merchandise to foreign addresses.
- ❒ Use prior cardholder purchases as a favorable factor to apply less restrictive screening and review when cardholder information has not changed.
- ❒ Develop a fraud score internally, or use third-party tools for fraud-scoring—such as CyberSource Advanced Fraud Screen enhanced by Visa—to better target the highest risk transactions requiring additional verification.
- ❒ Perform internal fraud screening before submitting transactions for third-party scoring.
- ❒ Evaluate the costs and benefits of third-party scores for low-risk transactions.
- ❒ Establish cost-effective thresholds for determining which suspect transactions to review.
- ❒ Establish cost-effective procedures for verifying purchase activity.

❽ Implement Verified by Visa

- ❒ Work with your Acquirer to implement Verified by Visa.
- ❒ Evaluate the benefits of Verified by Visa.
- ❒ Ensure the Acquirer or processor is providing the authentication results and ECI in the authorization message to obtain fraud chargeback protection.
- ❒ Monitor percentage of settled transactions that are authenticated or attempts, to identify potential processing problems.
- ❒ Perform fraud screening.
- ❒ Continue to utilize fraud screening tools for Verified by Visa transactions.
- ❒ Work with your Acquirer on a timely basis regarding alerts of high fraud rates.

❽ Implement Verified by Visa *(continued)*

- ❒ If using Verified by Visa, add the logo on your home, security information, and checkout pages, to promote reliable and secure on-line shopping.
- ❒ Do not submit an authorization request for Verified by Visa transactions that fail authentication.
- ❒ Provide an easy, simple recovery mechanism to cardholders that fail Verified by Visa authentication.

❾ Protect your merchant account from intrusion

- ❒ Conduct daily monitoring of authorizations and transactions.
- ❒ Monitor your batches.
- ❒ Change the password on your payment gateway's system regularly.
- ❒ Ensure the requirements of *Visa's Cardholder Information Security Program (CISP)* are in place.

Visa Card Acceptance

❿ Create a sound process for routing authorizations

- ❒ Implement a fraud-focused authorization routing sequence when a customer initiates a transaction.
- ❒ Use the correct Electronic Commerce Indicator (ECI) for all Internet transactions.
- ❒ Obtain a new authorization if the original expires.

⓫ Be prepared to handle transactions post-authorization

- ❒ Issue an e-mail order confirmation for approved transactions.
- ❒ Review declined authorizations and take appropriate actions.
- ❒ Track order decline rates.

Cardholder Information Security Program

⓬ Safeguard Cardholder data through CISP compliance

- ❒ Work with your Acquirer to understand your information security role and what's required of you and your service providers in regard to CISP compliance.
- ❒ Train employees on CISP compliance basics.
- ❒ Do not store Card Verification Value 2 (CVV2) data.
- ❒ Know your liability for data security problems.
- ❒ If you have experienced a suspected or confirmed security breach, take immediate steps to contain and limit exposure.

⓬ Safeguard Cardholder data through CISP compliance *(continued)*

- ❒ Alert all necessary parties of a suspect or confirmed security breach immediately.
- ❒ Provide the compromised Visa accounts to Visa Fraud Control Group within 24 hours.
- ❒ Within four business days of a reported compromise, provide an incident report document to Visa and/or depending on the level of risk and data elements obtained, undergo an independent forensic review and complete a compliance questionnaire and vulnerability scan upon Visa's discretion.

Chargeback and Loss Recovery

⓭ Avoid unnecessary chargebacks and processing costs

- ❒ Act promptly when customers with valid disputes deserve credits.
- ❒ Provide data rich responses to sales draft requests.
- ❒ Provide timely responses to sales draft requests.
- ❒ Know your AVS and CVV2 representment rights.
- ❒ Know your Verified by Visa representment rights.

⓮ Use collection efforts to recover losses

- ❒ Use e-mail collection messages and letters as first steps toward collecting low-dollar amounts.
- ❒ 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.

⓯ Monitor Chargebacks

- ❒ Track chargebacks and representments by reason code.
- ❒ Include initial chargeback amounts and net chargebacks after representment.
- ❒ Track card-present and card-not-present chargebacks separately.

Appendix C. E-Commerce Merchant 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-not-present 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 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-not-present 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 (VBV) 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" at the checkout of a participating merchant, the merchant server recognizes the registered 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.

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.*	These files allow you to make use of the details of your own history with fraudulent transactions or suspected fraud. You can create them by recording 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 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. This lets you avoid the manual handling of low-risk transactions.
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 outsort 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 charge-backs in your own environment. Transactions with higher risk characteristics or from higher risk sales channels should be routed for fraud review. These 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 using different names, addresses, and card numbers, but coming from same Internet Protocol (IP) address • Negative renewal options • Free-trial offer periods • Continuity programs

TOOL	DESCRIPTION
Velocity Monitoring *Automated velocity monitoring can help reduce risk exposure and 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.*	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 on same card used 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 using different names, addresses, and card numbers, but coming from one IP address. • Frequency of orders from same URL.
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.*	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 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—such as *CyberSource Advanced Fraud Screen enhanced by Visa*—can be used to better target the highest risk transactions requiring additional verification.

TOOL	DESCRIPTION
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.*	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 geolocation 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.
E-mail Confirmations *Simple verification steps can help alert you to data entry errors by customers and often uncover fraudulent attempts.*	You should 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 outsorted 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 bankcard fraud risks.*	You should conduct daily monitoring of authorizations and transactions to check for • Authorization-only transactions. An unusual number could indicate testing. • Large number of transactions followed by offsetting credits. • Transactions on similar account numbers. This could indicate 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 web site/digital content has been accessed.* Consumers often sign-up for free-trial access to merchant sites with 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 since the service was never used. Merchants that implement controls to prevent billing these customers can reduce the number of disputed transactions.

TOOL	DESCRIPTION
PC Fingerprinting	PC Fingerprinting applications provide the geographical location of the Internet Protocol (IP) address of every online customer. You can use the IP information and compare it to the billing address and even the billing phone number to identify any riskier transactions (i.e., cardholder's billing information locates customer in CA and fraudster 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 and when it is received. You should also to return the merchandise to track the time from when the goods are sent back until a credit is processed. Delays in shipping or issuing credit can increase chargebacks.

 VRM 04.01.05