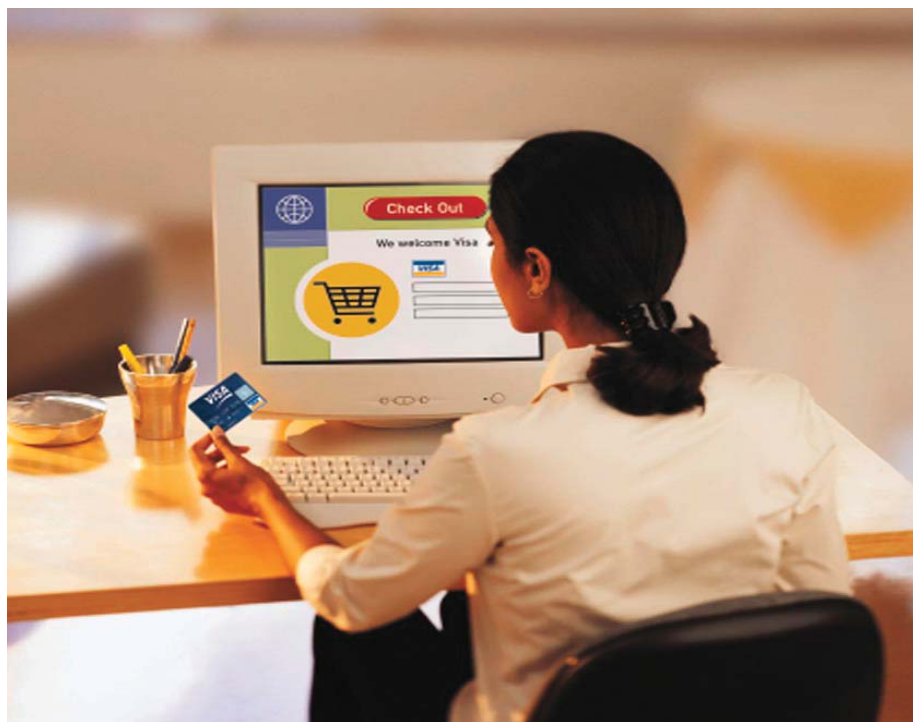


Visa Asia Pacific

# e-Commerce Merchants' Guide to Risk Management

Tools and Best Practices for Building a Secure Internet Business



# Table of Contents

About This Guide .....	3
<b>Section One: Understanding the Basics .....</b>	<b>5</b>
What Every e-Commerce Merchant Should Know About Handling Visa Transactions .....	6
Approaching Risk From a Strategic Perspective .....	7
Online Transaction Processing - From Start to Finish .....	8
A Brief Look at Chargebacks .....	12
<b>Section Two: e-Commerce Risk Management Best Practices .....</b>	<b>14</b>
Twelve Steps to Managing e-Commerce Risk .....	15
e-Commerce Start-Up .....	18
1. Know the Risks and Train Your Staff .....	19
2. Select the Right Acquirer and Service Provider(s) .....	21
Web Site Utility .....	24
3. Develop Essential Web Site Content .....	25
4. Focus on Risk Reduction .....	29
Fraud Prevention .....	33
5. Build Internal Fraud Prevention Capability .....	34
6. Use Visa Tools .....	36
7. Apply Fraud Screening .....	40
8. Protect Your Merchant Account From Intrusion .....	43
Visa Card Acceptance .....	44
9. Create a Sound Process for Routing Authorizations .....	45
10. Be Prepared to Handle Transactions Post-Authorization .....	46
Account Information Security .....	47
11. Safeguard Account Data Through AIS Compliance .....	48
Chargebacks and Processing Costs .....	50
12. Avoid Unnecessary Chargebacks and Processing Costs .....	51
<b>Section Three: Special Considerations for Travel Merchants .....</b>	<b>53</b>
Airlines, Car Rental Companies, Cruise Lines, Hotels and Travel Agencies .....	54
<b>Section Four: Resources .....</b>	<b>60</b>
Online Support and Information .....	61
<b>Section Five: Appendices .....</b>	<b>63</b>
Appendix A. Glossary .....	64
Appendix B. Checklist for Success .....	67

# 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 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 expertise and 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 and improving profitability as your Internet volume continues to grow.

---

## How This Guide is Organised

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.

**Section Five: Appendices** – Include a glossary of terms commonly used in the e-commerce market today 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 with an established e-commerce program in your market.

**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.



# 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.
- **must enter an 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.

□ **As of October 2004, 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. Section Two of this Guide discusses how Verified by Visa (a Visa tool), can protect merchants from this risk.

□ **Visa's operating rules apply to all e-commerce businesses that accept Visa cards.** In following these policies and principles, e-commerce merchants should NEVER violate Visa's rules by:

- imposing any surcharge on the Visa transaction\*
- using the Visa card/account number to collect other debts or dishonored checks.

\* Unless local law expressly permits it.

## 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 from the transaction date.

## Bits and Bytes

As a sales channel, e-commerce merchant chargebacks have been very similar to those for direct marketing and card-not-present (CNP) – between 0.20 percent and 0.30 percent of sales volume. Some e-commerce merchants with little or no fraud controls in place, however, have experienced losses of 10 percent or more.

# 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 e-commerce merchants who 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.

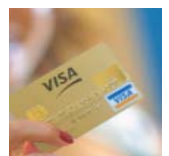
## Who Does What?

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.

**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 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."

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



**A merchant processor** can route an electronic transaction through the payment network for authorization, clearing, and settlement on behalf of the acquirer.

**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.



**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.

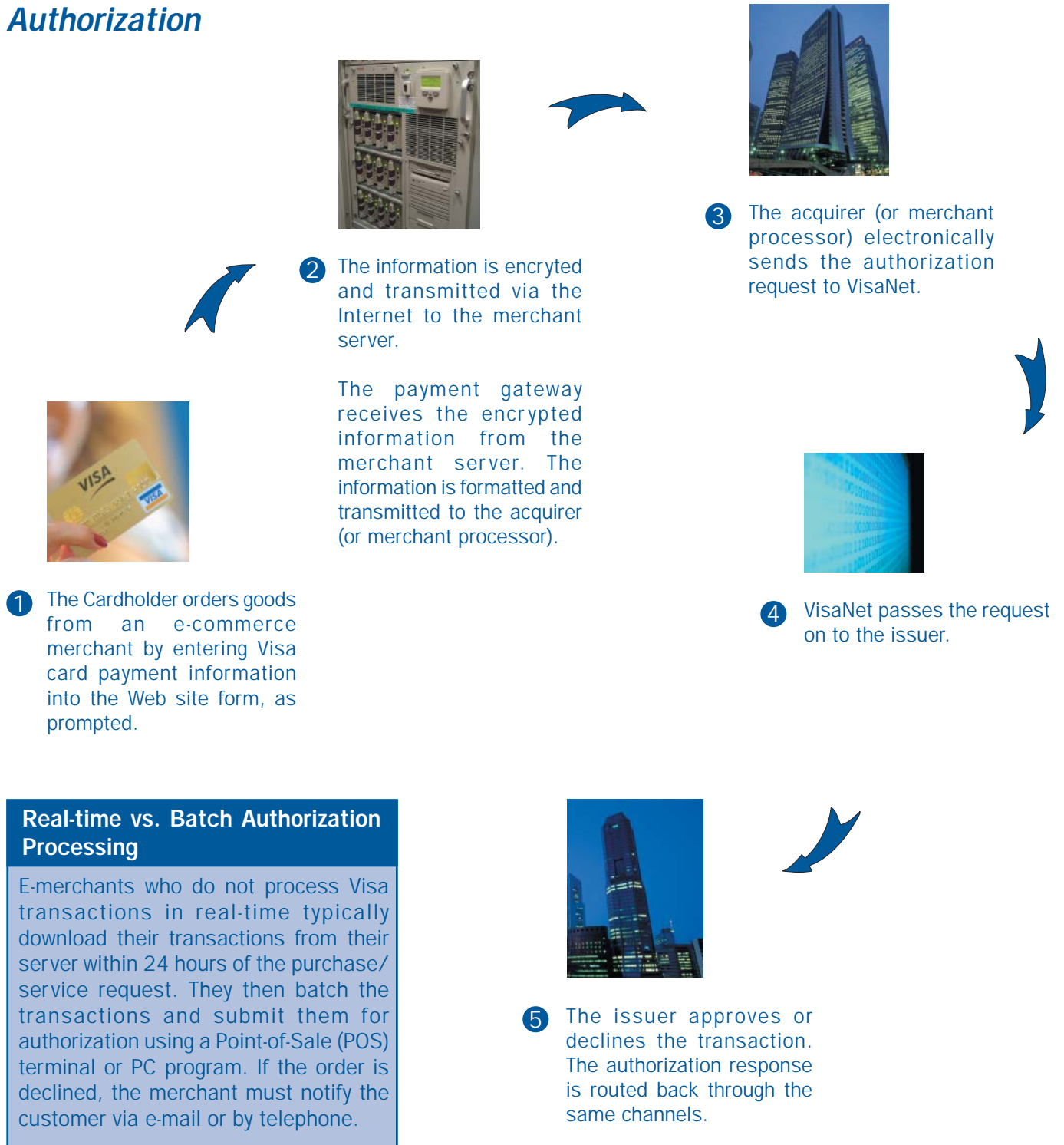
**Service provider** can include any third-party payment support entity (e.g., Web host, shopping cart, payment processors, fulfillment houses, etc.). This term is also used to describe a payment gateway alliance.



# 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



## 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.

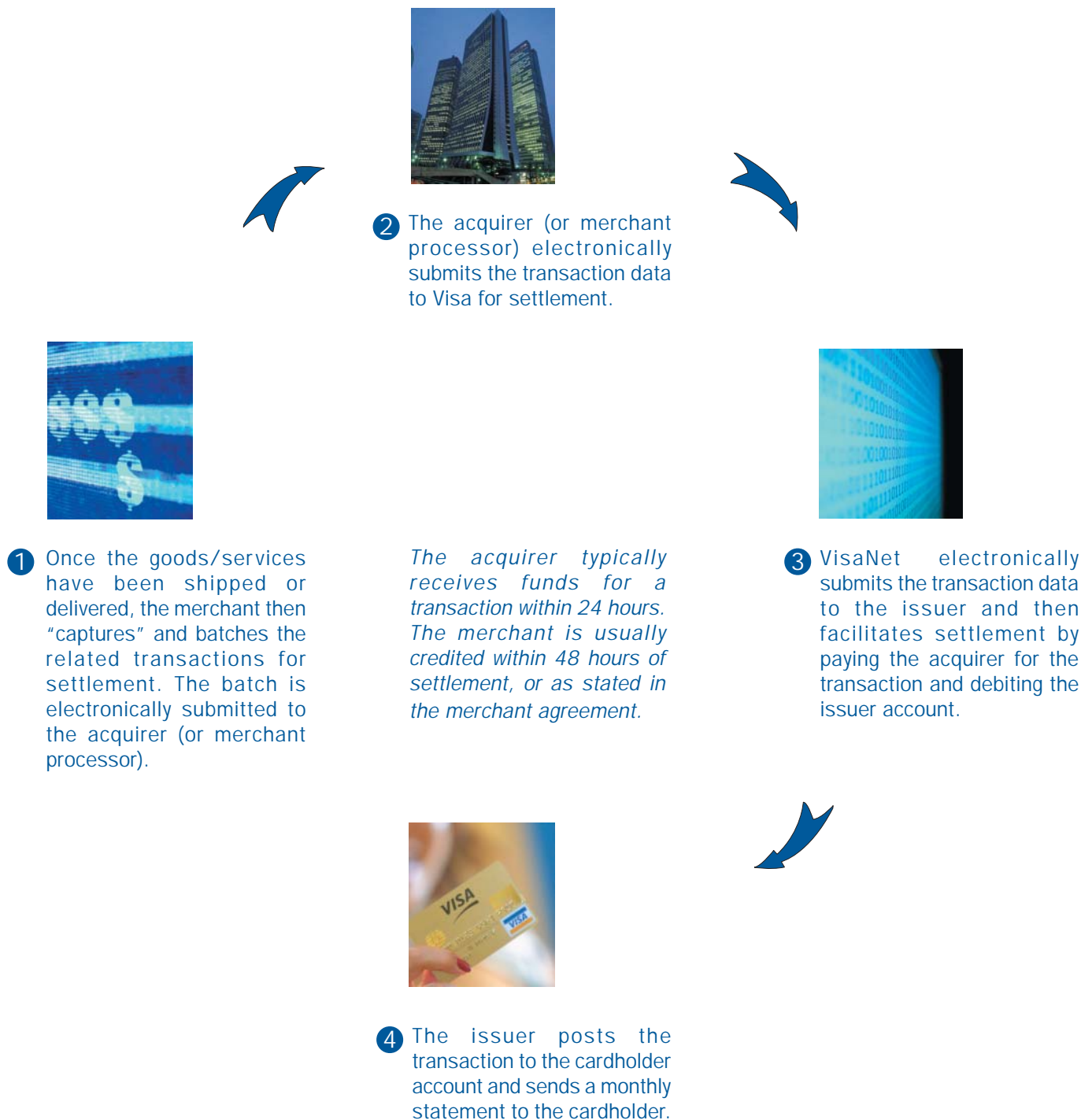
TOOL	DESCRIPTION
	<p>Verified by Visa is a tool that validates a cardholder's ownership of an account in real-time during an online Visa card transaction. When the cardholder clicks "buy" at the checkout of a participating merchant, the merchant server recognizes the registered Visa card and the "Verified by Visa" screen automatically appears on the cardholder's desktop. The cardholder enters a password to verify his or her identity. The issuer then confirms the cardholder's identity to the merchant.</p>
<p>Card Verification Value 2 (CVV2)*</p>	<p>CVV2 is a three-digit number imprinted on the signature panel of Visa cards. Merchants enabled to receive CVV2 may use it as an additional verification method. It can help validate that the customer has a genuine card in his/her possession and that the card account is legitimate. For information security purposes, merchants should never store CVV2 data (unless it is needed for recurring transaction purposes).</p>

For more information about Verified by Visa and CVV2, refer to the best practices covered on pages 37–39 of this guide.

\*At the time of publishing, the CVV2 service has limited availability in the Asia Pacific region.

## Settlement

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



# A Brief Look at Chargebacks

---

## What is a Chargeback?

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 either sending the transaction back to the acquirer, or crediting the cardholder’s account and absorbing the loss.

---

## What is a Transaction Receipt 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 transaction receipt request to the acquirer, who either fulfills the request or forwards it to the merchant for fulfillment.

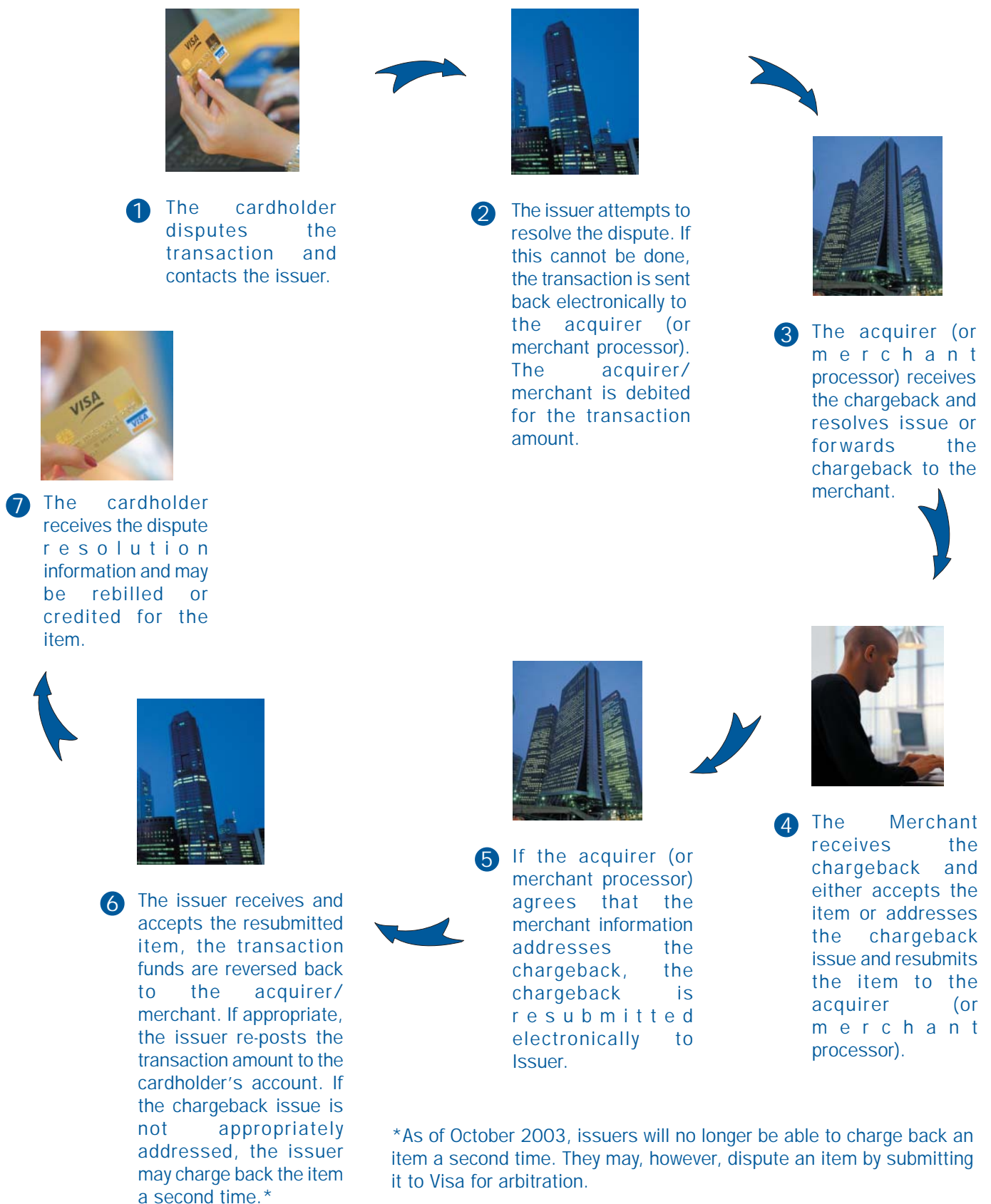
The merchant must then send the transaction receipt copy to the acquirer who sends it on to the Issuer.

### Quick Tip

When a transaction receipt request is not fulfilled in a timely manner, or the copy is illegible, it almost always results in a chargeback. It is in your best interest to respond promptly to a transaction receipt request.

# The Chargeback Lifecycle

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





# Twelve Steps to Managing e-Commerce Risk

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

---

## e-Commerce Start-up

### 1. Know the risks and train your staff

Your exposure to e-commerce risk depends on your business policies, operational practices, fraud prevention and detection tools, security controls, and the type of goods or services you provide. Your entire organization should have a thorough understanding of the risks associated with any Internet transaction and should be well versed in your unique risk management approach.

### 2. Select the right acquirer 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

### 3. 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.

### 4. Focus on risk reduction

Your sales order function can help you efficiently and securely address a number of risk concerns. You can capture essential Visa card and cardholder details through such actions as highlighting required transaction data fields and verifying Visa card and customer data that you receive through the Internet.

---

## Fraud Prevention

### 5. 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.

### 6. Use Visa tools

To reduce your exposure to e-commerce risk, you need to select and use the right combination of fraud prevention tools. Today, there are a number of options available to help you differentiate between a good customer and an online thief. Key Visa tools include Verified by Visa and Card Verification Value 2 (CVV2)\*.

### 7. Apply fraud screening

Fraud-screening methods can help you minimize fraud for large-purchase amounts and for high-risk transactions. By screening online Visa card transactions carefully, you can avoid fraud activity before it results in a loss for your business.

### 8. 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 committing merchant deposit fraud. By taking proactive measures, you can effectively minimize this kind of cyber-attack and the associated fraud risks. *Visa's Account Information Security (AIS)* standards outline the requirements for protecting your systems from intrusion - see step 11.

---

## Visa Card Acceptance

### 9. 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.

### 10. 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.

\*At the time of publishing, the CVV2 service has limited availability in the Asia Pacific region.

## Account Information Security

### 11. Safeguard account data through AIS compliance

Visa's *Account Information Security (AIS)* program 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. The AIS requirements can help you protect the integrity of your operations and earn the trust of your customers.

---

## Chargebacks and Processing Costs

### 12. 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 representation rights.

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

# 1. Know the Risks and Train Your Staff

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

---

## Risk Awareness

**Be aware of the 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 transaction receipt 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 transaction receipt requests
  - Cardholder disputes
  - Fraudulent use of account numbers.
- Know your rights to resubmit transactions that have been charged back for fraud reasons.

---

## 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
<b>Fraud</b>	<ul style="list-style-type: none"><li>• Customer uses a stolen card or account number to fraudulently purchase goods/services online</li><li>• Family member uses bankcard to order goods/services online, but has not been authorized to do so</li><li>• Customer falsely claims that he or she did not receive a shipment</li><li>• Hackers find their way into an e-commerce merchant's payment processing system and then issue credits to hacker card account numbers.</li></ul>
<b>Account Information Theft (Cyber)</b>	<ul style="list-style-type: none"><li>• Hackers capture customer account data during transmission to/from merchant</li><li>• Hackers gain access to service provider's unprotected payment processing systems and steal cardholder account data.</li></ul>
<b>Account Information Theft (Physical)</b>	<ul style="list-style-type: none"><li>• 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</li><li>• Unscrupulous merchant or service provider employee steals cardholder data and fraudulently uses or sells it for unauthorized use or identity theft purposes</li><li>• Dumpster-divers steal unshredded account information from trash bins at merchant or service provider location.</li></ul>
<b>Customer Disputes and Chargebacks</b>	<ul style="list-style-type: none"><li>• Goods or services are not as described on the Web site</li><li>• Customer is billed before goods/services are shipped or delivered</li><li>• Confusion and disagreement between customer and merchant over return and refund</li><li>• Customer is billed twice for the same order and/or billed for an incorrect amount</li><li>• Customer doesn't recognize the merchant name on statement because merchant uses a service provider to handle billing.</li></ul>

## 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 account information
- technical solutions or partnerships with service providers that support your unique Internet business needs and system requirements
- transaction identification using the Electronic Commerce Indicator (ECI)
- risk management tools to avoid or minimize fraud losses, such as Verified by Visa, Card Verification Value 2 (CVV2)\*, velocity checks, and fraud-scoring technologies. For more information, refer to “Visa Tools” on pages 36 through 39 of this guide.

- **Make sure the acquirer supports Visa’s Account Information Security (AIS) requirements.** Although security can never be completely guaranteed, the AIS requirements for e-merchants can help significantly reduce the ability of hackers to gain access to your important 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.
- underwrites responsibility.

#### 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 Account Information Security (AIS) procedures. For specific details, refer to Account Information Security on pages 47–49 of this guide.

\*At the time of publishing, the CVV2 service has limited availability in the Asia Pacific Region.

## 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 transaction receipt request or re-present 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 can ensure maximum security for cardholder data received.** To ensure protection for Internet transactions, partner with service providers who comply with Visa AIS 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.
- **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.

## **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 most e-commerce merchants need to meet.

### ***Length of Time in Business***

Most acquirers require the merchant to have been in business for at least a year or have other existing relationships with an acquirer.

### ***Credit Performance/Finance History***

In addition to reviewing the merchant's application, acquirers also need to establish the merchant's financial stability and credit history. This can be accomplished by reviewing credit bureau reports and other credit sources (e.g. Dun & Bradstreet ), financial statements, and income tax returns for the business and its owners.

Any history of personal or business bad credit or bankruptcy is a poor risk indicator, as is any derogatory history related to other businesses owned by the principals.

### ***Business and Owner Profiles***

Application forms for e-commerce typically ask for detailed business plans, samples of merchandise, 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 Account Information Security (AIS) requirements***

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 AIS requirements.

### ***Site Inspections***

Site inspections usually include 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 the Internet Service Provider (ISP) physical and logical controls, as well as AIS compliance.

## Web Site Utility

When building an e-commerce business, you need to establish a set of policies that clearly communicates 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 is required under Visa International Operating Regulations, and 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 Website homepage
  - To obtain this seal, you need to apply to a major privacy program, such as TRUSTe, the Better Business Bureau's BBBOnLine Privacy or TrustSG\*.

#### Quick Tip

If you need assistance, TRUSTe, an independent privacy organization has a Privacy Resource Guide you can use to help create a privacy policy for your site. It is available at <http://www.truste.org>

---

#### 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 links on your home page.
- **Create an FAQ page that includes questions and answers on how customers can protect themselves shopping online.**

\* Some countries have developed their own initiatives, like Singapore's TrustSG seal ([www.trustsg.org.sg](http://www.trustsg.org.sg)), to help build consumer confidence in shopping online.

## 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.
  - **Provide encryption technology for the transmission of payment data over the Internet.** It is a requirement of the Visa International Operating Regulations that merchants provide encryption technology for the transmission of payment data over the Internet. The industry encryption standard is SSL (Secure Socket Layer), 128-bit.
- 

## 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, if possible.
- 

## 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.**
- 

## Billing

- **Develop a description of your billing practices and make it 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.

---

## 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.

---

## 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.
- **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.

### 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.

## Customer Service Access (continued)

- Offer 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 cardholder information and enable repeat customers to order goods or services at your site without having to re-enter information
  - Require customers to enter their user names and passwords if they visit your Web site from a different computer.
- **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 place of birth or mother's maiden name - 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, send a separate e-mail message containing the password to the customer at the e-mail address provided at the time of registration.
  - 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.

\* Before using cookies, ensure that you will not be breaching any local privacy laws, or other laws.

---

## 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.
- **Highlight the data fields that the customer must complete.** Use color, shading, or bold fonts 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.

---

## Avoid 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 extract 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 expenses 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.
  - Validate telephone numbers using reverse directory look- ups
  - 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
  - Use a post-code table to verify that the entered post- code is valid for the entered city and state
  - Test the validity of the e-mail address by sending an order confirmation.

---

## High-Risk International Address Screening

- **Screen for high-risk international addresses.** Accepting transactions from certain international locations may carry high levels of risk.
  - Ask your acquirer for assistance in identifying high-risk countries heavily involved in Internet fraud
  - Test market and track fraud experience to various international locations
  - Perform additional screening and verification for higher-risk transactions - for example:
    - Obtain issuer contact information from your acquirer and call to confirm cardholder information for first-time buyers
    - Require the billing address and shipping address to be the same.
  - Capture and translate the Internet Protocol (IP) address to identify the computer network source.
    - Use a 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 crooks out there ready to pull a virtual scam or two. They are cyber-thieves who 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 fraud avoidance 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

## 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 Fraud Avoidance Files

- **Establish and maintain an internal fraud avoidance 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, telephone numbers, Visa card numbers used, and items purchased. **For information security purposes, e-commerce merchants should not store Card Verification Value 2 (CVV2) data\*.**
  - 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.

#### Bits and Bytes

When building and maintaining an internal fraud avoidance 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 fraud avoidance file.

\* unless required for re-curring transaction purposes. An example of a re-curring transaction is one where monthly billing occurs such as insurance payments.

- **Use the internal fraud avoidance file to screen transactions.** If transaction data matches your fraud avoidance file data, extract the transaction for internal review. 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 prior to authorization. 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 number of days. Adjust these limits to fit prior 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
  - 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
  - Do not permit cardholders to use more than one account number per purchase i.e. "split sale".
- **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.

### 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.

## 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.

#### Quick Tip

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
  - Include the expiration date as part of the authorization process.

---

## Verified by Visa

- Work with your Acquirer to implement Verified by Visa.



Verified by Visa is a new online service designed to make Internet purchase transactions safer by authenticating a cardholder's identity at the time of purchase. The goal of Verified by Visa is to create a similar level of customer trust and confidence in online shopping, as exists in the physical shopping environment.

### About Verified by Visa

#### How Verified by Visa works

1. Visa cardholders shop at participating Verified by Visa merchants, selecting items to purchase. At the checkout, the cardholder completes the required shipping and payment card information and clicks the "Buy" button.
2. Verified by Visa software installed at the merchant's site recognizes Visa Cards that are registered for Verified by Visa.
3. A Verified by Visa screen appears, and the cardholder is prompted to enter the password they created when registering for Verified by Visa.
4. The issuer validates the cardholder's identity and returns an authentication confirmation response to the merchant software. The merchant proceeds with the payment authorization.
5. The Verified by Visa screen disappears, and the cardholder views the merchant purchase confirmation screen.

#### The technology

Verified by Visa is built upon the technology platform called Three-Domain Secure (3-D Secure).

The 3-D Secure technical specifications and protocol uses Secure Sockets Layer (SSL) encryption, that is currently supported by the majority of e-commerce merchants. The 3-D Secure framework divides the authentication process according to the participants involved:

- **Issuer Domain - Issuer and cardholder.** The issuer is responsible for authenticating the cardholder during the registration process for Verified by Visa and at the time of purchase.
- **Acquirer Domain - Acquirer and Merchant.** The acquirer ensures that merchants operate in accordance with the business rules and technical requirements for the 3-D Secure service. A software module integrated into merchant websites, is used to provide the interface between the Verified by Visa service and the merchant's payment processing software.
- **Interoperability Domain - Visa-operated systems.** The issuer and acquirer Domains are connected and transaction data is routed and exchanged using 3-D Secure as the common technology platform.

## About Verified by Visa cont'd

### Benefits for Visa cardholders

Verified by Visa is intended to provide Visa cardholders with greater trust and confidence when shopping online, due to the extra security feature involved when making a purchase and the consistency of the purchasing experience. This in turn is expected to increase the cardholder's willingness to shop online, and to make purchases of higher value.

### Benefits for e-commerce merchants

The most common type of e-commerce chargebacks pertain to disputes in which the cardholder claims that they did not make the purchase. These chargebacks typically represent over half of disputes on e-commerce transactions.

Payment authentication through Verified by Visa, enables the issuer to verify the identity of the cardholder during an online purchase, regardless of in which country the Verified by Visa enabled merchant operates, thus reducing the number of disputes that a merchant receives. Verified by Visa is expected to significantly reduce disputes on e-commerce transactions, by eliminating fraudulent usage of Visa cards. This is a clear benefit for both participating e-commerce merchants and cardholders.

Verified by Visa is most effective when used along side existing risk management programs.

### Incentives for e-commerce merchants

**1. Reduced back office and support expenses** - Verified by Visa helps reduce fraudulent usage of Visa cards at participating merchants, thus reducing the number of disputes that a merchant receives.

**2. Chargeback blocking** - Transactions that meet the Verified by Visa requirements will qualify for chargeback blocking i.e. a shift in transaction liability from the e-commerce merchant to the issuer. Basically, this means that transactions may not be charged back to the merchant, if the cardholder later disputes having made the purchase. This applies to eligible (properly identified and processed) e-commerce transactions in which a Verified by Visa merchant sends an authentication request to the issuer, and the issuer returns:

- an "Authentication Confirmation" (the cardholder is registered for Verified by Visa and has been authenticated), or
- an "Attempts Response" (the cardholder is not registered for Verified by Visa)

To learn more about the Verified by Visa service, visit [www.visa-asia.com/verified](http://www.visa-asia.com/verified) or request a copy of the *Visa Merchant Implementation Guide* from your acquirer.

---

## Card Verification Value 2 (CVV2)

- **Work with your Acquirer to implement CVV2, if this service is available in your country\*.**
- **Use Visa's CVV2 code to verify the card's authenticity.**
  - Ask the customer for the last three numbers in the signature panel on the back of the Visa card (the CVV2 code)
  - Submit the CVV2 code with the authorization request. A CVV2 response will be returned with the authorization
  - Take appropriate action:
    - If you have a "match," complete the transaction (taking into account authorization and any other questionable data)
    - If you have a "no match," view this response as a sign of potential fraud and take it into account along with the authorization and any other questionable data. Hold for further verification.
- **For information security purposes, do not store CVV2 data (unless necessary for monthly recurring payments).**

### Quick Tip

Actions taken by e-commerce merchants in response to a CVV2 "no match," will vary by industry. Follow the procedures that make sense for your particular business.

\*At time of publishing, the CVV2 service has limited availability in the Asia Pacific region.

## 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
    - 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 anonymous e-mail addresses as higher risk.** Many merchants have found that anonymous e-mail addresses have a substantially higher fraud rate than e-mail accounts with large, well known Internet Service Providers (ISPs). By classifying anonymous e-mail addresses as higher risk, you can require these transactions to meet higher-risk hurdles – for example, to pass additional verification requirements.
- **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
  - Develop a policy on shipping to addresses other than the billing address.
- **Require greater scrutiny and verification for international transactions.**
  - Tighten transaction controls and velocity thresholds for these transactions to increase screening frequency
  - Treat with high suspicion billing addresses and shipping addresses that are not the same
  - Be on the lookout for customers who use anonymous e-mail addresses
  - Use third-party fraud scoring for International transactions.
  - Assess risk based on such transaction factors as type of goods purchased, the amount of the transaction, and the country in which the card was issued.
  - Contact the issuer to confirm cardholder information prior to shipping goods for a high-risk transaction.

## 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.
- **Larger-than-normal orders:** (This requires knowledge of what a “normal-sized” order is.) Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchase.
- **Orders consisting of several of the same item:** Having multiples of the same item increases the criminal’s 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 want these fraudulently obtained items as soon as possible for the quickest possible resale, and aren’t concerned about extra delivery charges.
- **Orders from Internet addresses making use of free e-mail services:** For these services, there’s no billing relationship and often 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 international addresses.
- **Transactions on similar account numbers:** This is particularly useful if the account numbers being used have been generated using software available on the internet (e.g., CreditMaster).
- **Orders shipped to a single address but made on multiple cards:** These could also be characteristic of an account number generated using special software available on the Internet, or a batch of stolen cards.
- **Multiple transactions on one card over a very short period of time :** This could be an attempt to “run” a card until the account is closed.
- **Multiple transactions on one card or similar cards with a single billing address, but multiple shipping addresses:** This could represent organized activity, rather than one individual at work.
- **Multiple cards used from a single Internet Protocol (IP) address:** More than one or two cards could well indicate a fraud scheme.

---

## Third-Party Fraud Screening

- **Use third-party tools for fraud-screening to reduce fraud for high-risk transactions.**
- **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
    - Verified by Visa results
    - CVV2 results.

---

## Manual Fraud Screening

- **Establish cost-effective thresholds for manual fraud screening.** The manual review of transactions is time-consuming and costly, and is generally warranted only for high-risk transactions. Establish screening criteria that lets you avoid the manual handling of low-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
  - a shipping address that is the same as the billing address, as well as a purchase amount that is below the designated dollar threshold.

---

## Cardholder Verification

- **Establish effective procedures for cardholder verification calls.** By contacting customers directly to investigate suspect transaction activity, you can not only reduce fraud risk, but also build customer confidence and loyalty. 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 - not the telephone number given for the suspect transaction - to find the cardholder’s telephone number
  - Confirm the transaction, resolve any discrepancies, and let the cardholder know that you are performing this confirmation as a protection against fraud.

## 8. 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 - offset 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
  - 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 Card Verification Value 2 (CVV2), look for transactions that may have been submitted without a 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 Visa's Account Information Security (AIS) requirements are in place.**  
*For details, refer to "Safeguard Account Data Through AIS Compliance," on pages 47 through 49 of this guide.*

## 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...

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

## 9. 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.**
  - First, perform internal screening for fraud - such as matching the transaction against velocity parameters, high-risk locations, and internal fraud avoidance files - and extract the transaction for review if it is unacceptable
  - If the transaction has passed your internal check, obtain an issuer authorization that includes Card Verification Value 2 (CVV2)\* to determine if the issuer or you will decline the transaction
  - Finally, 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 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. This frees you from receiving a referral response and lets the issuer make a more informed authorization decision. The ECI also helps you meet Internet transaction processing standards. 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 by Visa International Operating Regulations and helps protect you from chargebacks due to no authorization.

\*At time of publishing, the CVV2 service has limited availability in the Asia Pacific region.

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

# Account Information Security

All e-commerce merchants must take extra care to safeguard their cardholder data and improve their front-line defence to avoid internal and external security compromises. That's where Visa's Account Information Security requirements come in.

---

## Steps Covered...

→ 11. Safeguard Account Data Through AIS Compliance

## 11. Safeguard Account Data Through AIS Compliance

More and more hackers are scanning the Internet looking to attack vulnerable merchant sites and steal valuable cardholder account numbers. Because these attacks have become highly publicised, consumers and businesses are beginning to now show serious concern about information security and reliability. Before they order goods and services online, they want assurance that their account information is “cybersafe.” That’s what the Visa Account Information Security program is all about. As the name implies, its primary purpose is to help establish security procedures to protect account information in all payment security channels. To protect the interest of your Visa customers, follow these best practices:

---

### Adhere to AIS Requirements

- **Work with your acquirer to understand your information security role and what’s required of you and your service providers in regard to AIS compliance.**
  - Obtain the AIS Assessment and compliance materials from your acquirer
  - Evaluate your current level of security based on the AIS requirements established by your acquirer
  - Document and report your compliance to your acquirer.
- **Train employees on the basic AIS requirements**
  - Use available Visa tools and materials to train your staff on AIS compliance
  - Make sure all service providers are fully trained in the basic AIS requirements.

---

### CVV2 Data Storage

- **Do not store CVV2 data.**
  - For information security purposes do not store CVV2 data unless it is necessary for processing recurring payments e.g. monthly insurance payments.

---

### 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 Action if Compromised

- **If an information security breach occurs, take immediate action to contain and limit the exposure.**
  - Conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise
    - Preserve logs and electronic evidence
    - Do not access compromised systems (i.e., do not log in as ROOT)
  - Log all actions taken
  - Be on HIGH alert and monitor all Visa systems.
  - Contact and alert all necessary parties, including:
    - your security group and legal counsel
    - your acquirer
    - Visa Asia Pacific.
  - Adhere to the AIS compliance guidelines for compromised site assessment.

### The AIS requirements

At the most basic level, AIS consists of instituting and adhering to the following 15 basic requirements for protecting Visa account information. These top-level principles apply to all entities participating in the Visa payment system that process or store account information through the Internet.

1. Establish a hiring policy for staff and contractors
2. Restrict access to data on a 'need to know' basis
3. Assign each person a unique ID to be validated when accessing data
4. Track access to data, including read access, by each person
5. Install and maintain a network firewall, if data can be accessed via the Internet
6. Encrypt data maintained on databases or files, accessible from the Internet
7. Encrypt data sent across networks
8. Protect systems and data from viruses
9. Keep security patches for software up-to-date
10. Do not use vendor-supplied defaults for system passwords and other security parameters
11. Do not leave papers/diskettes/computers with data unsecured
12. Securely destroy data when it's no longer needed for business reasons
13. Regularly test security systems and procedures
14. Immediately investigate and report to Visa any suspected loss of Account or Transaction information
15. Use only service providers that meet these security standards

The *Visa Account Information Security Standards Manual* contains a complete description of these standards. To download a copy of the Standards or to find out more about the AIS requirements go to [www.visa-asia.com/secured](http://www.visa-asia.com/secured)

## 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 representation rights.

---

### Steps Covered...

→ 12. Avoid Unnecessary Chargebacks and Processing Costs

## 12. 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 representation 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 transaction receipt requests.**
  - Respond to transaction receipt 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.
  - 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 transaction receipt is not received within 30 days of a request to the acquirer. By fulfilling transaction receipt requests promptly, you can avoid such chargebacks and their associated costs.

---

## Avoiding Chargebacks (continued)

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

---

## Representment Rights

- **Know your representment rights to avoid unnecessary chargeback losses for your business.** For example, you can re-present:
  - Chargebacks for transactions with an unsupported CVV2 response in the authorization response from the issuer. If you requested a CVV2 response during authorization and received a “U” response from an issuer, it means the issuer does not support CVV2. In this situation, your acquirer has the right to re-present a fraud chargeback for that transaction on your behalf.

### Bits and Bytes

Even though an acquirer has the right to re-present on a merchant’s behalf under the circumstances described here, it is no guarantee that the disputed items will be accepted.

---

## Chargebacks Tracking

- **Track Internet chargebacks separately from non-Internet chargebacks.** If a large portion of your sales volume is from non-Internet sources, it is important to track Internet chargeback rates separately.
- **Track chargebacks and representments by reason.** Each of the chargeback reasons represents unique risk issues and requires specific risk reduction strategies.
- **Include initial amounts and net chargebacks after representment as part of your chargeback monitoring efforts.**



## Airlines, Car Rental Companies, Cruise Lines, Hotels and Travel Agencies

Special Considerations					
Airlines	Car Rental	Cruise Lines	Hotels	Travel Agents	Web Site Utility
	✓	✓	✓	✓	<p><b>Require Web site “membership” to make bookings.</b> 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:</p> <ul style="list-style-type: none"> <li>– verify the customer data that you collect before you store it</li> <li>– ensure that strong security measures, such as secure data storage and limited employee access, are in place to protect sensitive customer data.</li> </ul>
✓					<p><b>Require customers to use a password to book award travel.</b> 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.</p>
✓					<p><b>Lock out account access after multiple failures to enter the correct password.</b> 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.</p> <ul style="list-style-type: none"> <li>– Determine the number of incorrect password attempts - for example, five unsuccessful attempts will automatically lock out access to personal account information</li> <li>– Establish a method for legitimate customers to verify their personal security information and regain access to their accounts after they have been locked out</li> <li>– Use an automated e-mail message to inform the legitimate customer of the lock out and the method for regaining account access.</li> </ul>
✓		✓			<p><b>Determine whether or not to allow third-party sales and establish appropriate polices.</b> Allowing third parties to purchase travel for 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.</p> <ul style="list-style-type: none"> <li>– 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 passenger or to accompany the passenger during travel</li> <li>– If you decide not to allow third-party sales through the Internet, establish procedures to direct third-party purchasers to your physical sales offices.</li> </ul>

<i>Special Considerations</i>					
Airlines	Car Rental	Cruise Lines	Hotels	Travel Agents	Web Site Utility cont'd
✓	✓			✓	<b>Require a waiting period of at least four to six hours after purchase.</b> Purchases that occur just before travel may indicate fraud risk. To protect your business from potential losses, you need adequate time to verify the validity of the customer and Visa card before travel begins. This is especially important for new customers who have no track record with your company.
✓	✓	✓	✓		<b>Capture, verify, and retain e-mail addresses.</b> During the 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.
✓		✓	✓	✓	<b>Capture and retain Internet Protocol (IP) addresses.</b> 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.
	✓				<b>Capture and retain reasons for car rentals.</b> 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.
✓		✓	✓		<b>Clearly display your change fee policy and pricing.</b> 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 bookings are changed. This information should be prominently displayed on your Web site so that customers can review it before purchase.
✓		✓	✓		<b>Display refund rules on both your booking and confirmation pages.</b> This practice can help you preserve customer relations in cases where customers cancel their booking. By showing refund rules on your confirmation page, as well as your booking page, you can educate customers about the refund policy prior to purchase and then reinforce this policy after the booking has been made.
	✓	✓	✓		<b>Issue reservation confirmation numbers.</b> This Visa requirement helps assure customers that their reservations were successful and will be honored. Be sure that your reservation systems are integrated to support inquiries from customers who may contact you later to confirm their reservations.

					<i>Special Considerations</i>
Airlines	Car Rental	Cruise Lines	Hotels	Travel Agents	Web Site Utility Cont'd
	✓				<b>Pre-validate Visa card payment data prior to car rental.</b> Advance rental reservations help protect your company from risk exposure by giving you time to verify cardholder information and validate Visa cards before car rental service begins.
		✓	✓		<b>Issue a cancellation code to the cardholder.</b> In accordance with the Visa reservation service requirements, you must provide a cancellation number when a reservation is properly cancelled. Always advise the cardholder to retain the cancellation code.
✓					<b>Use e-tickets in all eligible markets and ensure risk control.</b> 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, 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.
✓					<b>Determine whether or not to require a Visa card be presented at the time of travel.</b> 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. <ul style="list-style-type: none"> <li>– 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</li> <li>– 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.</li> </ul>
✓					<b>Deliver paper tickets only to the billing address.</b> This practice can significantly reduce the risk of losses resulting from ticket purchases made with stolen Visa cards.

<i>Special Considerations</i>					
Airlines	Car Rental	Cruise Lines	Hotels	Travel Agents	Visa Card Acceptance
	✓	✓	✓		<p><b>Obtain an incremental authorization approval if the period is extended.</b> In some cases, a customer may wish to extend their travel 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 extension.</p> <ul style="list-style-type: none"> <li>– Follow standard authorization procedures to obtain an approval for the incremental transaction amount(s)</li> <li>– If you receive a “decline” response, contact the customer and request an alternate payment method for the amount that was not approved.</li> </ul>
	✓	✓	✓		<p><b>Settle only for the cumulative approved authorization amount if an incremental authorization was declined.</b> Good settlement practices will help you minimize chargebacks, processing costs, and potential losses when Issuers decline incremental authorization requests for travel extensions.</p> <ul style="list-style-type: none"> <li>– Submit a settlement transaction for the total approved authorization amount and do not include any amount(s) that received an authorization decline</li> <li>– Obtain alternate payment means for the declined incremental amount(s).</li> </ul>
	✓	✓	✓		<p><b>Submit an authorization reversal if the originally approved authorization amount exceeds the actual cost.</b> In some cases, the actual cost of a service 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 agreement.</p>
		✓	✓	✓	<p><b>Clearly disclose all terms and conditions of the sale.</b> 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:</p> <ul style="list-style-type: none"> <li>– The amount of the fee</li> <li>– How the fee will appear on the cardholder statement (in total or billed separately)</li> <li>– When the fee will be billed</li> <li>– What name will appear on the cardholder statement.</li> </ul> <p>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.</p>

<i>Special Considerations</i>				
Airlines	Car Rental	Cruise Lines	Hotels	Travel Agents
<b>Visa Card Acceptance Cont'd</b>				
				✓
<p><b>Ensure that your agency name and toll-free telephone number or URL address appear on the cardholder statement with your airline partner's name.</b> 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 reach you when they have questions.</p>				
<b>Fraud Prevention</b>				
✓		✓		✓
<p><b>Screen higher-risk bookings.</b> This practice can help you detect and prevent fraud before it happens. Be sure to screen bookings with such characteristics as:</p> <ul style="list-style-type: none"> <li>- Third-party purchase</li> <li>- Date of travel less than six days after ticket purchase</li> <li>- First or business class tickets</li> <li>- E-tickets or tickets not delivered to billing address</li> <li>- Customer not enrolled in frequent-flyer program.</li> </ul>				
✓				
<p><b>Track fraud by ticket source.</b> 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.</p>				
				✓
<p><b>Queue large-value bookings for fraud review.</b> 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.</p>				
				✓
<p><b>Track key fraud characteristics.</b> 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:</p> <ul style="list-style-type: none"> <li>- Passenger names, addresses, and telephone numbers</li> <li>- Cardholder names, addresses, and telephone numbers</li> <li>- E-mail addresses, Internet Protocol (IP) addresses, and Internet Service Providers (ISPs)</li> <li>- Transaction times, amounts, air carriers, classes of service, and travel itineraries.</li> </ul>				

<i>Special Considerations</i>					
Airlines	Car Rental	Cruise Lines	Hotels	Travel Agents	e-Commerce Startup
				✓	<p><b>Recognize your potential sales agent liability.</b> 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:</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- 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.</li> </ul>



## 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*

- **BBBOnline** - An array of resources provided by the Better Business Bureau to assist consumers and businesses interested in e-commerce: <http://www.bbbonline.com/>
- **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/>
- **TrustSG** - information on Singapore’s trust mark initiative, known as the TrustSg Programme: <http://www.trustsg.org.sg>
- **NOIE** - The Australian Government’s National Office for the Information Economy (NOIE) is the lead body for Australian e-Commerce merchants to keep up to date on information economy issues: <http://www.govonline.gov.au/>
- **Visa Home Page** - Starting point to access a wide range of information provided by Visa: <http://www.visa.com>
  - **Visa for businesses** - resources for businesses including products, merchant news, vendor information and useful downloads: <http://www.visa.com/fb>
  - **Visa Account Information Security (AIS)** - General Information about AIS requirements for e-commerce merchants and their service providers: <http://www.visa-asia.com/secured>
- **WebMonkey Electronic Commerce** - Introduction to getting started in e-commerce, including a tutorial on site development and marketing: <http://www.hotwired.com/webmonkey/e-business/>

#### *Web Site Privacy*

- **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/>
- **TrustSG** - information on Singapore’s trust mark initiative, known as the TrustSg Programme: <http://www.trustsg.org.sg>
- **NOIE** - The Australian Government’s National Office for the Information Economy (NOIE) is the lead body for Australian e-Commerce merchants to keep up to date on information economy issues: <http://www.govonline.gov.au>

---

## Fraud Prevention



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 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 simply enters a password to verify his or her identity. The issuer then confirms the cardholder's identity to the merchant.

For more information on Verified by Visa, contact your acquirer or refer to [www.visa-asia.com/verified](http://www.visa-asia.com/verified)

### *Telephone Directory Services and Reverse Directories*

- **Excite Directory** - Includes a World Directory, containing links to telephone and address verification/reference Web sites: <http://www.excite.com/>

---

## Business-to- Business e-Commerce

The Web sites listed below are designed to help e-commerce merchants perform the due diligence that is sometimes necessary in order to conduct business transactions over the Internet.

- **Better Business Bureau Online** - A free service that provides listings of businesses that have registered with BBBOOnline, but the listing is far from comprehensive: <http://www.bbbonline.com/>
- **Excite Directory** - Includes a variety of telephone and address verification/reference Web sites: <http://www.excite.com/>
- **NetCheck** - A free public service Web site that allows customers to submit comments on Internet merchants and search for comments submitted by other customers: <http://www.netcheck.com/>
- **Network Solutions "Who Is?"** - Domain registration authority that confirms whether a domain name exists and provides key contact phone numbers that can be used for verification: <http://www.netsol.com/cgi-bin/whois/whois>
- **Register.com** - Web site to identify whether an Internet domain name is currently assigned, and to identify key contacts for that site: <http://www.register.com/>



## 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.

**Account Information Security (AIS)** – A Visa program that provides e-commerce merchants with standards, procedures, and tools for data protection.

**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.

**AIS** – See *Account Information Security*

**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.

**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 cryptographic check of the information embossed on a card, and assures the merchant, acquirer, and issuer that the card is valid. The CVV2 is housed in the signature panel immediately after the full account number or the last four digits of the account number. CNP merchants should ask the customer for the CVV2 to verify the card's authenticity. For information security purposes, merchants should not store 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 re-presented to the issuer.

\*At time of publishing, the CVV2 service has limited availability in the Asia Pacific region.

**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 *transaction receipt 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*.

**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 cards to cardholders, and with which each cardholder has an agreement to repay the outstanding debt on the card. Also known as a consumer bank.

**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 re-presented, 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** – See *Transaction receipt request*.

**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*.

**Transaction receipt 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 sales draft request or copy request. This is often a first step prior to chargeback and indicates some initial question about the transaction on the cardholder’s part.

**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 then confirms the cardholder’s identity to the merchant.

## Appendix B. Checklist for Success

---

### e-Commerce Start-Up

#### 1 Know the risks and train your staff

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

#### 2 Select the right acquirer and service provider(s)

- Choose an acquirer with robust e-commerce capabilities
- Make sure the acquirer supports Visa's Account Information Security (AIS) requirements
- Understand the terms and conditions of your acquirer contract
- Research the service provider business
- Make sure your service provider can ensure maximum security for account data received
- Partner with a risk-focused service provider.

---

### WebSite Utility

#### 3 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
- Discourage the use of e-mail for transactions
- Make sure your goods or services are accurately described on your Web site
- 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 a description of your billing practices and make it available to customers at the time of the online purchase
- Establish a clear, concise statement of your refund and credit policy
- Provide an e-mail inquiry option
- Develop an e-mail inquiry response policy so customers can easily contact you with questions or concerns
- Develop an e-mail response to customers of any goods or service delivery delays
- Establish e-mail inquiry response standards and monitor staff compliance
- Offer toll-free telephone customer service support and display your phone numbers on your Web site.

---

## Website Utility cont'd

### 4 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
- Implement a "Mod 10" card number check before submitting a transaction for authorization
- 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

### 5 Build internal fraud prevention

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

### 6 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 Verified by Visa
- Work with your acquirer to implement CVV2\*
- Use Visa's CVV2 code to verify the card's authenticity
- For information security purposes, do not store CVV2 data.

\*At time of publishing, the CVV2 service has limited availability in the Asia Pacific region.

---

## Fraud Prevention

### 7 Apply fraud screening

- Implement fraud-screening tools to identify high-risk transactions
- Treat anonymous e-mail addresses as higher risk
- Screen for high-risk shipping addresses
- Treat international transactions as higher risk
- Use third-party tools for fraud-screening to reduce fraud for high-risk transactions
- Perform internal fraud screenings 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 manual fraud screening
- Establish effective procedures for cardholder verification calls.

### 8 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 Visa's Account Information Security (AIS) requirements are in place.

---

## Visa Card Acceptance

### 9 Create a sound process for routing authorizations

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

### 10 Be prepared to handle transactions post-authorizations

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

---

## Account Information Security

### 11 Safeguard cardholder data through AIS compliance

- Work with your acquirer to understand your information security role and what's required of you and your service providers in regard to AIS compliance
- Train employees on the 15 top-level AIS requirements for protecting Visa account information
- Do not store CVV2 data
- Know your liability for data security problems
- If an information security breach occurs, take immediate action to contain and limit exposure.

---

## Chargebacks and Processing Costs

12

### **Avoid unnecessary chargebacks and processing costs**

- Act promptly when customers with valid disputes deserve credits
  - Provide data rich responses to transaction receipt requests
  - Provide timely responses to transaction receipt requests
  - Know your representment rights to avoid unnecessary chargeback losses for your business
  - Track Internet chargebacks separately from non-Internet chargebacks
  - Track chargebacks and representments by reason
  - Include initial amounts and net chargebacks after representment as part of your chargeback monitoring efforts.
-

