Electronic Commerce Risk Management

Merchant Best Practices

April 2000

VISA

Table of Contents

INTRODUCTION

RISK MANAGEMENT BEST PRACTICES

APPENDICES

Introduction

About This Guide

The fastest growing segment of the Asia Pacific retail market, electronic commerce generated USD$2.19 billion in 1998 and is expected to grow well over USD$5.01 billion in 2002, according to IDC statistics. For merchants, this e-commerce growth translates into major opportunities to deepen and expand customer relationships, attract new accounts, and increase revenues in a global, high-ticket market where payment cards are the principal form of payment.

To help merchants tap the e-commerce opportunity, Visa has been working actively to ensure that the Internet provides a secure infrastructure for payment card transactions. A key focus of this effort is to identify "best practices" for e-commerce risk management and to share this information with businesses like yours. As a result, Visa commissioned two studies of e-commerce risk management practices: one that examined current Visa Acquirer practices and one that examined current Visa merchant practices. The findings of the second study are presented in this guide.

GUIDE PURPOSE

This guide is based on the actual experiences of nine leading U.S. Internet merchants that have established e-commerce programs and recently participated in a high-level risk management study by Visa and Risk Management Consulting (RMC), an independent consulting firm. The purpose of the guide is to recommend a set of "best practices" that your business can use to manage e-commerce risk. Some of these practices reflect policies, procedures, and capabilities already in place in the e-commerce programs studied. Some are recommendations from Visa and RMC after working with study participants to identify areas for improvement.

WHO WILL BENEFIT FROM THIS GUIDE

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

- **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 Internet program 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 you have already been conducting commerce over the Internet for some time, this guide can help you identify areas for improvement and explore advanced strategies and tactics for reducing risk exposure and improving profitability as your Internet volume continues to grow.

HOW TO USE THIS GUIDE

Depending on your current e-commerce experience, you can use this guide sequentially as a step-by-step planning tool, or move directly to the topics that are of immediate concern to your business. To facilitate use, the guide is organized as follows:

- **Introduction.** In addition to this guide overview, the "Introduction" includes an executive summary highlighting the risk management "best practices" that Visa and RMC jointly identified for e-commerce after assessing the strengths and weaknesses of the Internet merchants participating in the study. The section also offers background information about the study and how it was conducted.
- **Risk Management Best Practices.** From setting up your e-commerce program, to developing your Web site and sales-order 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.
- **Appendices.** Appendix A lists useful information resources available through the Internet as of August 1999. Appendix B is a glossary of key terms commonly used in the e-commerce market today. Appendix C is a checklist summary of the more than 80 risk management practices discussed in this guide.

FOR MORE INFORMATION

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

Note: The information in this guide is offered to assist you, on an "as is" basis. Nothing in this guide is intended to offer legal advice or to change or affect any of the terms of your agreement with your Visa Acquirer. 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.

Executive Summary

The Internet is rapidly evolving into a major marketing and sales channel that offers your business tremendous opportunities to strengthen customer relationships, attract new business, and increase sales revenues through differentiated value-added services. However, the risks of accepting payment cards over the Internet present challenges for merchants. For this reason, Visa has been leading industry efforts to ensure that the Internet provides a secure infrastructure for payment card transactions. A focus of these efforts is to identify risk management "best practices" for merchants in the Internet marketplace and to share this information with businesses like yours.

BACKGROUND

In the effort to promote Internet security, Visa partnered with an independent consulting firm, to study the operational practices of nine leading Internet merchants and to use the findings of these high-level reviews to derive a set of e-commerce risk management "best practices" that any Internet merchant can adopt. This guide summarizes the conclusions of the study which was conducted from February through June 1999.

RISK MANAGEMENT BEST PRACTICES

This guide offers more than 80 best practices for managing risk in the e-commerce marketplace. These practices reflect policies, procedures and capabilities actually in place among Internet merchants studied and include recommendations from Visa after identifying areas for improvement in these programs. Following are the most important steps that your business can take to manage e-commerce risk:

- **Find the right Visa Acquirer for your e-commerce program.** If you have not yet launched an electronic storefront, be sure to review your options carefully and partner with a Visa Acquirer that can meet your unique Internet needs, provide effective risk management support - particularly in the area of data security - and demonstrate a thorough understanding of Internet fraud risk and liability. For details, see "E-Commerce Start-Up Strategies."
- **Develop Web site content that promotes both security and sales.** When designing your Web site, keep operational needs and risk factors foremost in mind. Key areas to consider are privacy, reliability, and refund policies as well as customer service access. How you handle e-mail and communicate business policies can significantly affect customer decisions to buy or not buy at your Web site. For details, see "Web Site Content."

- **Establish an effective sales order function for e-commerce.** For best results, your sales order function should help you efficiently and securely meet a number of key business needs, such as building customer relationships, highlighting required transaction data fields, verifying payment card and customer data that you receive through the Internet, and processing sales orders. For details, see "Web Site Sales Order Functionality."
- **Develop sound policies for accepting Visa cards through the Internet.** To ensure security, you need a precise understanding, planning, and design of Internet transaction routing processes. Focus on how you will obtain authorizations through the Internet and how you will handle transactions after authorization. For details, see "Visa Card Acceptance Practices."
- **Be prepared to track and analyze Web site activities.** By understanding the traffic patterns and purchasing habits of your Web site visitors, you can not only build a dynamic and profitable electronic storefront, but also protect your business from high-risk transactions. For details, see "Web Site Tracking and Analysis."
- **Know how to prevent and detect Internet fraud.** The profitability of your electronic storefront will depend greatly on the strategies and tools you use to minimize fraud. To avoid losses, for example, you need a sound risk management infrastructure, robust internal fraud avoidance files, intelligent transaction controls, and highly adaptive fraud detection tools. For details about fraud control, see "Fraud Prevention and Detection."
- **Ensure maximum security for cardholder data received through the Internet.** You can earn customer trust and enhance your business image by ensuring data protection for Internet transactions. For maximum security, you need reliable transaction encryption capabilities to protect Internet data transmissions, effective internal security controls to protect stored data, and rigorous review and testing of data security on a regular and ongoing basis. You should post your privacy and security policies so cardholders can read them. For details, see "Data Security."
- **Be prepared to handle chargebacks and recover losses.** By establishing an effective chargeback process in accordance with Visa regulations, you will be well positioned to identify loss control weaknesses and reduce the negative impact of fraud and customer disputes. To minimize losses, you need an adequate chargeback tracking system, procedures in place to avoid unnecessary chargebacks, a thorough understanding of your re-presentment rights, and a strong cardholder collection effort. For details, see "Chargeback Handling and Loss Recovery."

For a checklist summary of the more than the 80 risk management best practices that these key steps include, see "Checklist for Success" in Appendix C of this guide.

Study Overview

In 1999, Visa partnered with an independent consulting firm to learn more about the merchant risks of accepting Visa cards through the Internet. This section describes the study that resulted and the merchants that participated.

OBJECTIVE AND TIMELINES

The purpose of the study was to assess the current operational and risk management practices of individual Internet merchants, identify areas for improvement, and use the findings to derive a general set of "best practices" that any Internet merchant can use to manage e-commerce risk.

From February to June 1999, Visa conducted high-level reviews of nine leading Internet merchants and their online risk management practices.

PARTICIPANT PROFILES

As shown in the following table, the nine study participants represented a broad spectrum of e-commerce merchants. Their Internet experience ranged from a few months to a few years, and their products collectively included both hard goods and digital content with online fulfillment. Sales figures were not disclosed.

Study Participants		
Merchant Category	**Number in Study**	**Internet Only**
Sporting Goods Retailer	1	Yes
Software Resellers	2	Yes
Major Retailers	2	No
Travel Agency	1	Yes
Auction Site and Retailer	1	Yes
Major Airline	1	No
Major Car Rental Company	1	No

SCOPE AND APPROACH

The study had the following key characteristics:

- An on-site risk assessment review for each participating merchant was performed. This review focused only on the operating and risk management practices that the merchant had adopted to accept Visa cards through the Internet.
- The nature and scope of the on-site reviews were purposely limited to provide merchant management with a high-level assessment of its e-commerce risk management practices.
- The study centered around non-proprietary risk management techniques that could be shared anonymously with other Internet merchants.

CONCLUSIONS

After analyzing the operational practices of the nine study participants, Visa identified a set of risk management "best practices" for each functional area of a merchant e-commerce program. In some cases, these practices reflect policies, procedures, and capabilities that have been actually implemented by study participants. In other cases, these practices are suggestions from Visa. The next section of this guide highlights the key conclusions of the study.

Risk Management Best Practices

E-Commerce Start-Up Strategies

If you want to tap the e-commerce opportunity but have not yet established an Internet storefront, there are a number of start-up strategies to consider. You can position your business for long-term success by taking the time now to address issues related to your Acquirer relationship, data security, and fraud and chargeback risk.

ACQUIRER SELECTION

Your Visa Acquirer will play a key role in your Internet success by enabling you to accept Visa cards through the Internet and by processing the sales volume that results. Your Acquirer also can help you increase operational efficiency, lower costs, manage risk, and build profitability. To ensure the success of your electronic storefront:

- **Select 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 to select an Acquirer that offers:
  - Expertise in e-commerce platforms and security measures, particularly transaction data encryption and secure storage of cardholder information
  - Technical solutions or alliances with technology vendors that support your unique Internet business needs
  - Risk management tools to avoid or minimize fraud losses, such as fraud scoring technologies
  - Transaction identification using the Electronic Commerce Indicator (ECI)
- **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:
  - Length of time and conditions under which your deposits may be held
  - Your liability for fraudulent transactions - 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
  - The nature and causes of chargebacks, including:
    - Customer disputes
    - Fraudulent activity
    - Technical factors, such as "expired card" or "no authorization"
  - Time frames for providing additional documentation to your Acquirer in order to fulfill a sales draft request or represent a chargeback.

DATA SECURITY

Data security is of utmost importance on the Internet, where hackers are continually trying to exploit weaknesses and obtain card numbers and other information. You need to consider how you will receive transaction data from Internet customers, and how and where you will maintain this sensitive information. For best results:

- **Use a secure gateway to encrypt transaction data.** To avoid the risk of payment card numbers being stolen and used fraudulently, use the best gateway available to receive customer data through the Internet and transmit it to your Acquirer.
  - For domestic transactions, use industry-accepted encryption algorithms, such as RSA 128-bit standards within a Secure Socket Layer (SSL). Standard SSL encryption keys are 40-bits long and provide very secure transactions. Longer encryption keys, such as 56- and 128-bit keys, make it even more difficult for hackers to decrypt and steal data.

For additional information on data security restrictions, visit the RSA Security Web site at http://www.rsa.com

- **Encrypt and securely store transaction data.** All stored cardholder data should be kept behind firewalls or in an area inaccessible from the Internet. For maximum security, encrypt this sensitive data before you store it. You also should know your liability for data security problems. Many Acquirers today are providing contracts which explicitly hold merchants liable for losses resulting from compromised card data if the merchant lacks adequate data security.

FRAUD AND CHARGEBACK RISK

Before establishing your presence in the Internet marketplace, you should know how your electronic storefront can affect your exposure to fraud and chargeback risk. For best results:

- **Know the risks of selling on the Internet.** Your exposure to Internet fraud will depend greatly on your business policies, operational practices, fraud prevention and detection tools, other risk controls, and the type of merchandise you sell. Your entire organization should have a thorough understanding of the fraud risk associated with any Internet transaction and should be well versed in your unique risk management approach. To minimize risk exposure:

- Let all staff know that Internet transactions are subject to card-not-present chargeback rules and regulations - for example:
  - An approved authorization request indicates that the account is in good standing. **It is not proof that the true cardholder is making the purchase**. Therefore, the merchant is liable for fraudulent card-not-present transactions even if they have been approved by the card Issuer.
  - Issuers have the right to charge back transactions in which the cardholder claims to have not participated for up to 120 days. Fraudulent activity can thus pose a significant risk to the merchant long after the transaction has been processed.
  - As a sales channel, Internet merchant chargebacks have been very similar overall to those for direct marketing - between 0.20% to 0.30% of sales volume. However, some Internet merchants have incurred losses of 10% or more when little or no fraud controls were in place.

- **Take measures to avoid customer disputes.** Dispute resolution can be a time-consuming and costly process that detracts from your business and marketplace reputation. To maintain high customer satisfaction, the best measures are preventative:
  - Ensure that your goods and services are described accurately on your Web site
  - Deliver merchandise on a timely basis and advise cardholder when they can expect it.
  - Notify cardholder of any delays
  - Wait until the merchandise has been shipped before you bill the cardholder
  - Provide full information about the sale when responding to a sales draft inquiry (see "Chargeback Handling and Loss Control" for more information)
  - Display your refund and return policy on your Web site
  - Provide contact information - including e-mail addresses, telephone numbers, and physical address - so customers can reach you directly when they have questions

- **Understand the chargeback process.** Be sure to follow your Acquirer's processing instructions to avoid chargebacks related to authorizations and sales drafts requests:
  - Work with your Acquirer to develop an awareness and understanding of the various reasons for chargebacks, particularly in regards to:
    - Transaction authorization requirements
    - Expired authorization rules for unshipped merchandise
    - Time limits for fulfilling sales draft requests
    - Cardholder disputes
    - Fraudulent use of account numbers
  - Know your rights to resubmit transactions that have been charged back for fraud reasons.

Web Site Content

In addition to showcasing your merchandise and promoting sales, the Web offers an important opportunity to inform customers about your business practices. To minimize risk, your Web site content should clearly state your privacy, reliability, and refund policies and make sure these can be easily accessed from all pertinent screens by the cardholder, and also provide customer service information so that customers know whom to contact when they have questions.

BUSINESS POLICIES

You can strengthen customer relationships by using your Web site not only as a marketing tool to increase revenue, but also as a risk management tool to avoid customer disputes. Best practices include:

- **Establish a comprehensive privacy policy and post it on your Web site.** To allay customer concerns about providing personal data, your privacy policy should clearly define what customer data is collected and tracked, with whom this information is shared, and how customers can opt out.

  Develop a clear, concise statement of this privacy policy and make it available to Web site visitors through links on your homepage

  - What type of information is collected on your Web site
    - Is it the customer's name, email address or other personal data?
    - Is it system information such as browser used or entry and exit page points etc?
  - What is the purpose of you collecting customer data
    - Is it being used to better the service that you can provide to customers?
    - Is it for internal tracking and measurement only?
    - Is it to enhance the personalisation of the site for customers?
    - Is it to collect and sell to third parties?
  - To what extent will you share this data with any third party(ies)
    - Will the information shared be detailed giving the customer's name, email etc?
    - Will the information shared be aggregated, i.e. no individual information?
  - When is the information being collected
    - Browsing and the use of cookies. For more information about cookies visit **http://www.cookiecentral.com**
    - Responding to games, surveys or promotions
    - Email

- A commitment to data security, how is it being held and where
  - Is it the data being held offline; if not is it behind firewalls?
- What steps are taken to ensure customer data quality and access
  - Who has access to this information? Is it anyone in your organisation or a specific person?
- The consequences, if any, of refusal to not provide information. What are the benefits to the consumer for providing data and what are they missing out on if they do not.
  - For example, if a customer does not want to provide their email address or details about their interests, you will be unable to correspond with them or personalize information specific to them
  - If a customer turns off the ability for them to accept cookies, what are the consequences for their shopping experience at your business?
- The accountability measure that you have in place
  - If and how a customer can restrict the use of their personal information and how they can do so
- If you need assistance, TRUSTe, an independent privacy organization, has a "wizard" you can use to create a customized privacy policy at http://www.truste.org/wizard

- **Provide a complete description of goods or services provided.** To minimize any confusion in the product and to limit potential returns you should provide detailed information about what you sell on your Web site.
  - For example, if you are selling electrical goods, make sure you state the voltage requirements, or if selling videos ensure that you state the format for VHS (PAL, NTSC) etc.
  - State sizes, colors and material make up of products being sold. Placing an image of a shirt, for example, on your Web site does not convey to your customers the type of material that it is made from or the sizes that it comes in.
- **Provide corporate information.** Your customers will only want to shop with reputable merchants, so it is in your interest to provide information to them that will allow them to establish your identity.
  - Include the full name of your company. If your trading name is different to the holding company name, provide both.
  - Provide your registration number or license that is provided to you when you have registered your business name and the organisation that provided such to you. This will allow the customer to perform a legitimacy check.

- Provide your geographic location. When selling to international customers it is important for them to know where your head office is as well as any country offices.

- **Register with a privacy organization and post a "seal of approval" on your Web site.** You also can allay customer concerns about providing personal data by displaying a privacy "seal-of-approval" on your Web site homepage. To obtain this seal, you need to apply to a major privacy program, such as TRUSTe or see if one of your government agencies or major consumer groups provides a similar service.

- **Establish and display your refund and credit policy.** This policy should be consistent with your business objectives and the type of merchandise that you sell. For best results, try to find the right balance between excellent customer service and excellent risk management:

  - Develop a clear, concise statement of this refund and credit policy, and make it available to Web site visitors through links on your homepage.
  - Provide a 'click through' acceptance for important elements of the policy - for example, when purchasing tickets to sporting events, customers click on a button to acknowledge that tickets are non-returnable unless the event is postponed or cancelled.
  - Provide information on the length of your refund and return period. For example, if you offer a refund and return facility, how do customers use this service. Also ensure that you state who is responsible for the cost of the return postage.
  - Provide your Web site visitors with any information about the refund process. How long will it take for a customer to get a refund, will it be a refund to their credit card or will it be offered in the form of a gift voucher.

- **Develop a marketing e-mail message policy.** Well-designed and well-timed promotional e-mail messages can help you increase sales and build customer loyalty. Keep in mind, however, that such messages can be detrimental if you send them to customers who do not want them. To protect good customer relationships:

  - Require customer approval before sending e-mail marketing messages
  - Ensure that each message allows the customer to opt out of future messages, or select a reduced frequency of mailings

- **Implement effective marketing e-mail message practices.** To develop the best e-mail marketing tactics for your Internet customers, test your messages with select groups before doing mass mailings. For best results:

- Segment your Internet customer base, and try different frequency and content of e-mail messages with different segments
- For each segment, track Web site visits and sales, and evaluate the impact of your e-mail messages on customer retention and revenue
- Compare the results of your tests with the customer retention and sales of a control group who received no e-mail messages, and use the findings to confirm or modify your e-mail practices

CUSTOMER SERVICE ACCESS

You can promote sales, ensure customer satisfaction, and avoid customer disputes by making it easy for your customers to access your customer service group. Best practices include:

- **Offer toll-free telephone customer service and display the number on your Web site.** Some customers may be reluctant to submit payment card numbers over the Internet. Others may have customer service questions or concerns, and are not comfortable with e-mail correspondence. Though telephone customer service can be costly, it can help preserve sales and customer relationships that might otherwise be lost.
  - Display links on your homepage to a toll-free customer service number that cardholders can use to complete a sale or get a quick response to an inquiry.
  - Display the same number on your sales order page to save transactions when cardholders are reluctant to submit their payment card numbers over the Internet.
  - Adequately staff and schedule customer service staff to respond to telephone inquiries on a timely basis.
  - Provide the customer with information about your standard procedure for handling customer complaints. Is it different to handling all customer service inquiries? Make sure that you provide information on any dispute resolution arrangements if a complaint cannot be successfully resolved with you.
- **Provide customer service e-mail contacts and encourage customers to use them when they have inquiries.** Many Internet users are comfortable with e-mail, and some prefer it instead of the phone. By offering e-mail customer service, you can meet the needs of these convenience-oriented customers. And, by encouraging e-mail inquiries over telephone inquiries, you can lower the call volume and costs of your telephone customer service. For best results:

- Display e-mail "Contact Us" options on your Web site, and make them prominent and easily accessible
- To facilitate internal processing and expedite customer responses, provide different e-mail contacts for product and sales information, customer service, and back order and shipping information

- **Develop an e-mail inquiry response policy.** Timely and robust responses to e-mail inquiries can lead to greater customer satisfaction and increased sales. For best results:
  - 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 ways to assist customers who forget their passwords.** Internet merchants have successfully used different automated and manual approaches to help registered customers who cannot remember their passwords. To ensure service quality and risk control, consider either or a combination of these approaches:
  - Use customer-provided security data instead of the password to verify the registered customer's identity
    - 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 and, if it is correct, send an 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

- **Make effective use of permanent and session Web browser cookies.** Recognizing and acknowledging existing customers can help you increase sales and reduce risk.
  - Use permanent browser cookies to retain cardholder information and enable repeat customers to make purchases at your site without having to re-enter information
  - Use session cookies to let cardholders retain merchandise in shopping carts while linking to other areas of your Web site before check out
  - Require customers to enter their user names and passwords if they visit your Web site from a different computer

- **Use Electronic Commerce Modeling Language (ECML) to develop your order page.** ECML provides a set of uniform data elements to help streamline the process that merchants use to gather electronic data for shipping, billing, and payment. To enhance the online shopping experience for consumers and merchants, for example, Visa and other industry leaders have partnered to develop ECML-based digital wallets for consumers. A digital wallet is a software application or service that lets the consumer store billing, shipping, and payment information in one place, and use this information to automatically complete a merchant's check-out page.

For more information about the benefits of ECML visit the ECML Web page at http://www.ecml.org

- **Establish e-mail response standards and monitor staff compliance.** E-mail response standards will help ensure quality service and create positive customer impressions. By monitoring staff compliance with these standards, you can strengthen customer relationships and increase sales.
  - Establish a standard timeframe for responding to 100 percent of e-mail inquiries - for example, 24 hours
  - Establish 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 compliance with e-mail response standards on a daily basis

Web Site Sales Order Functionality

To encourage purchases and minimize losses, you need to develop a sales order function that addresses the unique characteristics of the Internet. Factors to consider include: how you will establish and manage Internet customer relationships, what transaction data fields customers will be required to complete before making purchases, how you will validate both the card and customer during an Internet transaction, and how you will process orders.

CUSTOMER RELATIONSHIPS

Your electronic storefront gives you the opportunity to establish and build relationships with customers who want the convenience of making purchases any time, day or night, from their computers. To minimize risk while establishing Internet customer relationships:

- **Register Internet customers.** Ask the customer if they would like to register at your site. By registering Internet customers at your Web site, you enable them to return and make additional purchases without having to re-enter their payment information. This approach translates into greater convenience for your customer, and greater sales and customer loyalty for your business. An alternative approach is to embed Web browser "cookies" on the user's computer. When registering Internet customers:
  - Allow them to select their own user names and passwords
  - Advise them to keep these user names and passwords secure to avoid unauthorized use
  - Ensure that adequate automated and manual customer service support is available for customers who forget their user names or passwords
  - Suspend user-name accounts after a certain number of failed log-on attempts - particularly if card account information is stored on your site
- **Identify repeat customers.** Your customer registration process or embedded Web browser "cookies" will enable you to identify repeat customers so they do not have to re-enter their payment information on return visits. These repeat customers may warrant less restrictive fraud screening measures. For best results:
  - Acknowledge and welcome repeat customers
  - Use existing customer profiles to pre-populate sales order screens. However, limit payment card information to the last four digits of the registered card.
  - Determine how to update the customer profile permanently when a repeat customer provides new information during a transaction

REQUIRED TRANSACTION DATA FIELDS

Your customers will provide you with certain information during sales transactions. You need to define the data fields that your customers must complete, and ensure that the resulting information will help you provide quality service and keep risk exposure low. For best results:

- **Establish transaction data fields that can help you identify risk, 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 making purchases. Key risk data fields include:
  - Demographic information, such as telephone numbers, that can be validated using reverse directory look-ups or cross-reference tables to addresses
  - 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.** By highlighting these required fields, you can make it easier for the customer to complete the transaction and avoid problems related to incomplete Web form processing. For best results, use color, shading, or bold fonts to highlight the required data fields and accompany this highlighting with explanatory notes to the cardholder.
- **Edit and validate required data fields in real-time.** You can improve sales, avoid customer frustration and processing delays, and reduce fraud risk exposure by providing 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 cardholder to page back, correct personal information or alter the request while retaining previously entered information.

CARD VALIDATION

To protect your business from potential losses, you need to ensure the validity of the payment card being presented for an Internet purchase. For best results:

- **Ask the customer for both a card type and an account number, and make sure that they match.** Different types of payment cards have different types of account numbers - for example, all Visa cards begin with a "4." To minimize errors and losses:
  - 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.
- **Implement a "Mod 10" card number check before submitting a transaction for authorization.** You can save time and lower costs by catching card entry errors prior to authorization. Use a "Mod 10" check to determine whether an entered card number is valid. This simple precaution can help avoid the expense and delay that results when a cardholder enters a valid card number incorrectly - for example, types a wrong number or transposes digits - and then receives an authorization decline.
  - 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
- **Avoid default card expiration date.** Do not provide a default month and year for the card expiration date that the cardholder is required to enter. The cardholder may erroneously select the default date which will most likely differ from the actual card expiration date. Many Issuers decline the transaction when this error occurs.

- **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 another card for purchase.

CARDHOLDER VALIDATION

In addition to checking the payment card, you need to validate the cardholder presenting the card for purchase. Best practices include:

- **Check the validity of the customer's telephone number, physical address, and e-mail address.** Simple verification steps can help identify data entry errors by customers and often uncover fraudulent transactions. To identify high risk transactions for further review:
  - 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 postal code table to verify that the entered postal code is valid for the entered city and state
  - Test the validity of the e-mail address by sending an order confirmation message
- **Screen for high-risk international addresses.** Product deliveries to certain international locations carry high levels of risk. To minimize losses, identify high risk international addresses and perform additional verification and fraud screening when orders involve these locations.
  - Ask your Acquirer for assistance in identifying high risk countries
  - 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 billing address to equal shipping address, and require that the customer has a legitimate e-mail address.

SALES ORDER PROCESSING

Your sales order process will play a key role in the profitability of your electronic storefront. When processing Internet orders, you need to ensure that the sale will be successfully completed and that it will not lead to unnecessary inquiries for the customer or unnecessary cost and risk exposure for your business. Best practices include:

- **Perform an exact calculation of sales tax and shipping costs at the time of the transaction.** Some merchants estimate these amounts initially and then bill the actual amounts later. This practice often results in a different transaction total on the cardholder statement and can lead to customer inquiries and disputes. To avoid the customer dissatisfaction and related customer service costs, always show the exact sales tax and shipping costs on the Internet sales order.
- **Display an "Order Being Processed" message during wait time.** This type of message assures the customer that the transaction is in process and that the pause in screen activity is not due to computer malfunction. As a result, the message helps avoid consumer confusion, duplicate processing, and unnecessary customer service calls while also encouraging the customer to wait and complete the sale.
  - Send the message immediately after the cardholder requests a purchase
  - If the cardholder stops activity on the site for an unusually long time prior to selecting a purchase, end the shopping session or require re-entry of the customer password before completing a transaction
- **Before completing a purchase, let the customer know whether the merchandise is in stock.** By including inventory information in your sales order process, you can give customers an estimated time of delivery. This practice helps promote customer goodwill and avoid unnecessary inquiries about delivery delays for out-of-stock items. Some merchants display the estimated shipping days next to each item so that customers know the estimated delivery time prior to making a purchase.
  - If an item is delayed for any reason, notify the cardholder, give them the estimated arrival time and the option of canceling the transaction.
- **Provide comprehensive order confirmation details.** To provide excellent customer service and to meet customers expectation provide the following information:
  - Unique transaction number so that your customers can easily identify themselves and their purchase to your customer service representatives
  - Transaction date
  - Purchaser name
  - Transaction amount including all fees and charges associated with the purchase

- Transaction currency especially if the customer is international
- Authorization code (if any)
- Your business name and your online address
- A brief description of the order
- Refund/return policy if it is restricted. For example, if your policy is to allow a refund or return 30 days after delivery, reinforce this to the consumer
- Transaction type for the payment of the goods - debit, credit, cash-on-delivery, cheque etc.
- Customer service contact details

- **Limit storage of payment card numbers.** To minimize the risk of card numbers being stolen and used fraudulently, store only payment card numbers that have been captured as part of a customer profile. For maximum security:

  - Encrypt these card numbers and related cardholder personal information before storing this data on your server or in your back-office system
  - Restrict internal access to stored payment card data
  - Ensure that your system logs and tracks any access to payment card data

- **Develop controls to avoid duplicate orders.** Duplicate sales orders lead not only to higher processing costs, but also customer dissatisfaction. Establish controls to prevent cardholders from inadvertently submitting two orders for one purchase. To avoid duplicate orders:

  - Require customers to make positive clicks on purchase selections rather than hit the "Enter" key
  - Display an "Order Being Processed" message to customers after they have submitted a sales transaction
  - Systematically check for identical orders within short timeframes and out sort these orders for review to ensure that they are not duplicates of one order
  - Send e-mail messages to customers to confirm whether a duplicate order was intentional

- **Develop a Java script to alert customers of expired card data stored on your site.** An expired payment card will most likely be declined by the Issuer during authorization. You can ensure excellent customer service and avoid delays in booking tickets by prompting customers for updates of their account numbers and card expiration dates.

Visa Card Acceptance Practices

Before you accept Visa cards for payment through the Internet, you must ensure that you have a secure and efficient process in place to submit authorization requests through the Internet and appropriately handle transactions that are approved or declined.

AUTHORIZATION

The authorization process protects you from losses due to customers with insufficient funds or fraudulent card use. The process must be well managed since it has a significant impact on risk, customer service, operational expense and approved sales volume. Best practices include:

- **Implement cost-effective authorization routing.** You can control authorization expenses by setting up an authorization routing sequence that uses the lowest cost alternatives first. When an Internet customer requests a purchase:
  - First, perform any internal screening for fraud such as velocity, high risk locations and negative files to decline unacceptable transactions.
  - And if you use a third-party scoring service, obtain a fraud score for transactions that have not yet been declined by you or the Issuer.
- **Perform real-time authorizations.** Some merchants batch transactions and submit them for authorization up to 24 hours after the purchase requests. Such delays can increase customer service costs and result in lost sales, as the cardholder has to be contacted if there is an issue with some of the information provided. To promote customer satisfaction and preserve sales, perform real-time authorizations for all Internet transactions and provide an immediate response - approval or decline - to the cardholder. If the response is a decline, suggest corrective actions that the cardholder can take - for example, use an alternate Visa card for the purchase or contact the card Issuer about the decline.
- **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, 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 requirements. Work with your Acquirer to implement the ECI which is required for all Internet transactions.

POST-AUTHORIZATION

If an Internet transaction is approved by the card Issuer, you can complete the sale and fulfill the order. If the transaction is declined, your procedures should specify how to handle the situation with the customer. Use the

information that you learn to determine whether this type of decline can be avoided in the future. Proceed in a way that best serves the customer and your business. Best practices include:

- **Issue an e-mail order confirmation for approved transactions.** You can minimize customer inquiries and disputes by sending an e-mail order confirmation which reminds the cardholder of the approved purchase and provides details about it. This practice also enables you to check the validity of the cardholder's e-mail address. If the e-mail address it not valid, research the situation to determine whether the order is legitimate.
- **Queue Issuer authorization declines for review.** 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, do not proceed with a sale unless you obtain an authorization approval from the Issuer.
  - 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 and understand trends, track order declines by reason on a daily basis segmented by Issuer declines versus those you decline for suspected fraud or other reasons.
- **Obtain a new authorization if the original expires before shipment.** If you are shipping merchandise to the customer more than seven days after the original authorization, i.e., a backorder, you should obtain a new authorization before proceeding with the shipment. This practice is required by Visa regulations and helps protect you from chargebacks due to no authorization.
- **Reverse authorizations for partial shipments.** This practice lets you receive the best possible interchange rate for your transaction volume. Submit an authorization reversal for the difference between the original amount and the amount of the shipped goods. When doing this, keep in mind that:
  - To qualify for the lowest interchange rate, settled Visa transaction amounts must equal the authorized amounts.
  - Visa permits the merchant or Acquirer to submit one authorization reversal to meet this requirement

Web Site Tracking and Analysis

By tracking and analyzing Web site activity, you can learn more about your Internet visitors and develop marketing offers that best meet their specific needs. You also gain important opportunities to monitor the ongoing performance of your electronic store, and also identify shopping patterns with high levels of risk exposure for your business. Best practices include:

- **Track the sources of Web site visitors.** You can gain valuable marketing and risk management information by tracking the Web addresses that are used to reach your site. Look for associated banner ads, affiliate Web sites, and direct accesses that can help you identify the sources of your travel customers.
- **Collect and analyze Internet customer "click-through" patterns.** These patterns tell you where individuals travel to and from within your Web site and provide useful data that you can use for marketing purposes and fraud risk screening.
  - Warehouse Internet customer click-through pattern data
  - Analyze this data to assess customer preferences and buying patterns
  - Perform retroactive analyses to compare click-through data with known fraudulent sales to determine high-risk shopping patterns
- **Track sales non-conversion, or abandon rates.** Some Web site visitors select items for purchase but leave without completing the transaction. Tracking this type of activity can help you identify Web site navigation issues, impediments to completing sales, and new problems resulting from Web site changes. For best results, correlate click-through patterns with customers that do not check out. This practice can help you identify new marketing strategies - for example, using more dynamic screens that build on the customer's past purchases or current shopping interests to promote sales.
- **Track purchase patterns of registered customers.** This type of data can provide a valuable foundation for targeting e-mail marketing messages and also screening for fraud.
  - Determine individual customer preferences by tracking the purchase activity of registered customers. Deviations from these patterns may be an indication of fraud.
  - Use this information to present shopping alternatives targeted to these customers based on their prior purchases
  - Distinguish between gift purchases and personal purchases in making recommendations
  - Consider offering gift registry and reminder e-mail service

Fraud Prevention and Detection

There are many steps you can take to prevent and detect fraud as you grow your Internet business. To minimize losses associated with fraud, be sure to implement a sound risk management infrastructure, robust internal fraud avoidance files (see page 31), intelligent transaction controls, and highly adaptive fraud detection tools for transaction screening.

RISK MANAGEMENT INFRASTRUCTURE

To protect your business from losses associated with Internet fraud, you need to ensure that you have an effective risk management infrastructure in place. Best practices include:

- **Establish a formal fraud control function.** A specialized fraud control group can provide the focus that your business needs to prevent and detect fraud activity. When establishing this dedicated group:
  - Make fraud prevention and detection strategies the highest priority
  - Establish day-to-day objectives that promote profitability - for example, to reduce fraud as a percentage of sales, and to minimize the impact of this effort on legitimate sales
  - For larger merchants, encourage the fraud control group to work closely with the chargeback group, identify causes of chargeback loss, and use this information to improve fraud prevention techniques
  - Clearly define responsibilities for fraud detection and suspect transaction review
- **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

Internal fraud avoidance files store details of your history with fraudulent transactions, and are cost-effective tools to help you prevent fraud losses. Best practices include:

- **Establish and maintain an internal fraud avoidance file.** By storing details of fraudulent transactions or suspected fraud, you gain a valuable source of information to protect you from future fraud perpetrated by the same person or group. For best results:

- Record all key elements of fraud transactions, such as names, e-mail addresses, shipping addresses, telephone numbers, and payment card numbers
- Establish a process to remove from the file or flag information about legitimate customers whose payment data has been compromised. Criminals may use the personal data of innocent victims to commit the fraud.

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

TRANSACTION CONTROLS

A key way to minimize risk is to establish transaction controls that help you avoid fraudulent transactions and flag questionable activity for further review. Best practices include:

- **Prevent excessive digital content downloads.** Excessive software or digital content downloads may indicate lack of computer savvy, customer abuse, or fraud. In any case, it is a good business practice to establish reasonable controls over such downloads.
  - Define a maximum number of downloads to prevent excessive software or digital content downloads and decrease fraud risk
  - Develop communications to assist customers with technical problems
- **Establish transaction controls and velocity limits.** You can reduce your risk exposure by using basic transaction screening procedures to flag high-risk transactions for review prior to authorization approval.
  - Establish individual cardholder review limits based on the number and dollar amount of transactions that have been approved within a specified number of days, and adjust these limits, as needed, to reflect prior purchase patterns
  - Establish review limits for single transaction amounts
  - Ensure that velocity limits are checked across multiple characteristics, including shipping address, telephone number, and e-mail address
  - Contact customers who exceed review limits to determine whether the transaction activity is legitimate and should be approved, providing that the card Issuer also approves the transaction

- **Modify transaction controls and velocity limits based upon transaction risk.** You can best utilize your resources by varying transaction controls and velocity limits based on your risk experience with selected products, shipping locations, and purchase patterns. Key characteristics to consider include:
  - High risk merchandise, such as downloadable software, digital content, consumer electronics, or gift certificates
  - International versus domestic transactions
  - Express shipping regardless of purchase amount
  - Unusual purchase quantities or rapid repeat sales

TRANSACTION SCREENING

By screening Internet transactions carefully, you can detect and avoid fraud activity before it results in a loss for your business. A number of risk-management tools, services, and practices can help you cost-effectively screen transactions and increase the likelihood that you are dealing with a legitimate customer who is presenting a legitimate Visa card for purchase. Best practices include:

- **Implement fraud screening tools. Such tools help reduce losses by enabling you to detect and prevent fraudulent transactions.** Fraud screening tools can be developed internally or acquired from third parties.
  - Implement fraud screening tools to identify high-risk transactions and suspend processing for those with high-risk attributes, such as transactions that:
    - Match data stored in your internal fraud avoidance 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 with the goals of reducing fraud as a percentage of sales and minimizing 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

- **Treat non-A.P. transactions as higher risk.** For best results:
  - Require greater scrutiny and verification for international transactions. - for example, reduce transaction controls and velocity thresholds for these transactions to increase screening frequency
  - Require billing address to equal shipping address and that the customer has a legitimate e-mail address.
  - Assess risk based on such transaction factors as the type of merchandise, the amount of the transaction, and the country in which the card was issued
  - Contact the Issuer prior to shipping merchandise for a high-risk transaction

- **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 Internet transaction. You may be able to keep costs down by eliminating low-risk transactions from third-party scoring.
  - Analyze your contractual agreements with third-party scoring services and determine the costs of submitting transactions to them
  - Do not obtain fraud scores for transactions declined by the Issuer or by you for suspected fraud or other reasons, as noted earlier.
  - Identify transactions with fraud risk lower than the cost of third-party scoring, considering such factors as:
    - Dollar amount of the sale
    - Cardholder relationship: new or repeat customer
    - Type of merchandise being sold
    - Your Web site click-through patterns
  - Consider eliminating these low-risk transactions from third-party scoring as a way to lower processing expenses without significantly increasing risk

- **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 are having merchandise shipped to the same address as before
  - A shipping address that is the same as the billing address, and a purchase amount that is below the dollar threshold
- **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 order, resolve any discrepancies, and let the cardholder know that you are performing this confirmation to protect him or her from fraud

Data Security

Your Internet customer relationships, business reputation, and profitability will all be shaped by your ability to keep cardholder payment data secure. To minimize risk, you need to implement reliable transaction encryption, internal data security controls, and rigorous review and testing of security systems on an ongoing basis.

DATA TRANSMISSION

Through cryptography, information is automatically encoded, or scrambled, before it is sent through the Internet and then automatically decoded, or unscrambled, after it reaches its destination. This easy-to-use process prevents unauthorized persons from accessing and reading the data while it is in transit. To ensure transaction security:

- **Encrypt cardholder data transmissions.** By encrypting cardholder data sent to your Web server from the cardholder's computer, you can deter "sniffers" from obtaining valid account numbers while transactions are in transit.
  - Establish the capability to support 128-bit Secure Sockets Layer (SSL) encryption, but allow 40- or 56-bit encryption for those customers who do not use 128-bit encryption
  - Encrypt the customer's personal data as well as the card number
  - Make SSL encryption the default for your Web site
  - In the unusual situation when an Internet browser does not support SSL, ask the customer to acknowledge non-secure processing by actively selecting an option on the screen
  - Tell your customers that you are committed to higher security such as SET Secure Transaction (when it is available and appropriate to the market place.
- **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, stressing that:
  - E-mail and faxes are not secure communication methods and should never be used to transmit card numbers or other sensitive information
  - The transaction encryption capabilities of your electronic storefront offer reliable protection from unauthorized access and give cardholders the safest way to make purchases over the Internet

INTERNAL DATA STORAGE AND ACCESS

Cardholder payment data is highly sensitive information that must be handled with utmost care both during and after a transaction. You need to develop secure data storage and handling practices to guard against data theft by staff as well as external parties. Best practices include:

- **Limit internal access to payment card data.** To minimize the risk of internal theft of cardholder account numbers, display only a portion of account numbers internally and use password control to limit the number of users who have access to card data.
  - Provide customer service functions with only the last four digits of the cardholder account number.
  - Give employees who need the entire card number - such as draft retrieval and chargeback staff - access to this information via a password
  - Identify, record, and track each internal access to payment card data
- **Prevent unauthorized access to stored card data.** Card account numbers that you store, however briefly, present substantial risk exposure. Should the card numbers be stolen and used fraudulently, your business may be held liable for the loss. For maximum protection, encrypt all card numbers stored on your server and retain this encrypted data behind firewalls to prevent hacker intrusions.
- **Ensure that your server environment is secure.** Server security is essential to prevent tampering that could disrupt your Web site or result in compromise of cardholder data.
  - Ensure that your server is maintained in a secure site with restricted access
  - If you use a third-party provider, conduct a review to ensure that adequate server security is in place

SECURITY REVIEW AND TESTING

In a dynamic and rapidly evolving marketplace like the Internet, you need to review and test security on an ongoing basis. Best practices include:

- **Continually test Web site security.** A good way to identify weak links in your Web site security is to keep trying - on an ongoing basis - to compromise the site. Some security firms specialize in testing security by attempting to break into merchant Web sites and can offer recommendations to strengthen risk controls.
  - Use ongoing internal or third-party resources to try breaking into your Web site
  - Identify weaknesses in Web site security and correct them
- **Implement an ethical hacker program.** Savvy Internet merchants leverage the resident knowledge and expertise of their own employees to test data security and Web site operations. Employees receive rewards if they can identify security weaknesses by successfully breaking into the system.
- **Conduct annual reviews of systems controls.** Regular systems reviews help ensure that changes in your Web site, your business, or the marketplace have not weakened data security. Many large accounting firms offer this type of review service.
  - Perform annual reviews of systems controls to assess the soundness of data security measures
  - Use the results of these reviews to improve areas of weakness and prevent hacker intrusions
- **Detect and log attempts by hackers to break into your system.** This practice can help you identify individual hackers and prevent future system break-ins.
  - Access attempts, at a minimum, should be logged for all invalid/ unsuccessful attempts.
  - Analyze errors from attempts to hack into your system and write identity characteristics to a log file.
  - Capture the Internet Protocol (IP) and e-mail addresses.
  - Contact individual and IP service provided to investigate break-in attempts.

Chargeback Handling and Loss Recovery

For your business, a chargeback translates into extra processing time and cost, a narrower profit margin for the sale, and possibly a loss of revenue. It is important to carefully track and manage the chargebacks that you receive, take steps to avoid future chargebacks, and know your representment rights. It is also important to develop effective collection techniques to recover losses when the customer is responsible for a transaction that has been charged back.

TRACKING CHARGEBACKS

By carefully monitoring chargebacks, you can analyze trends and determine whether there are corrective actions that you can take to minimize future chargebacks and their costs. A best practice is:

- **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. This practice allows you to identity the cause of any change in either chargeback rate so that you can take corrective action.
  - Track chargebacks and representments by reason
  - Include initial amounts and net chargebacks after representment

AVOIDING CHARGEBACKS

Timely action is often the key to avoiding chargebacks. When handling legitimate credit requests from customers and sales draft requests from your Acquirer, always respond promptly and appropriately. This practice can help keep questionable situations from escalating into unnecessary chargebacks and processing costs for your business. Best practices include:

- **Act promptly when customers with valid disputes deserve credits.** When customers contact you directly to resolve a dispute, be sure to handle the dispute promptly and issue a credit immediately if necessary, to ensure the dispute does not turn into a chargeback.
  - Credit customers on a timely basis to avoid unnecessary customer disputes and their associated chargeback processing costs
  - Send cardholders an e-mail to let them know as soon as possible of the impending credit

- **Provide data rich responses to sales drafts requests.** By supplying details of the sales transaction in question, you may be able to resolve the request and avoid a chargeback.
  - Respond to sales draft inquiries from your Acquirer with full information about the sale, and be sure to include the following required data elements:
    - Account number
    - Card expiration date
    - Cardholder name
    - Transaction date
    - Transaction amount
    - Authorization code
    - Merchant name
    - Merchant online address
    - Merchandise or service description
    - "Ship to" address, if applicable
  - Provide optional data to assist in resolving inquiries and reducing chargebacks, such as:
    - Transaction time
    - Customer e-mail address
    - Customer telephone numbers
    - Billing address
    - Detailed merchandise description
    - Whether merchandise receipt signature was obtained upon delivery
- **Fulfill sales draft requests on a timely basis.** An Issuer may charge a transaction back if a sales draft is not received within 30 days of a request to the Acquirer. By fulfilling sales draft requests promptly, you can avoid such chargebacks and their associated processing expenses.
  - Work with your Acquirer to design and implement a timely, efficient process for fulfilling sales draft requests
  - Investigate facsimile fulfillment by your Acquirer, if this is appropriate for the goods or services you provide

COLLECTION EFFORTS

In some cases, customers are responsible for transactions that have been charged back to your business. For example, the cardholder claimed the transaction was fraudulent but you have confirmation that the merchandise was received by the cardholder. To recover losses such as these:

- **Develop cost-effective collection practices.** You often can recover unwarranted chargeback losses by contacting the customer directly through internal resources or an external collections agency. If a cardholder letter was received as part of the chargeback documentation, try to address the customer's concerns and arrive at a mutually satisfactory solution. For best collection results:
  - Use e-mail collection messages and letters as first steps toward collecting low-dollar amounts
  - Follow-up with phone calls to those who do not respond to your initial correspondence
  - Outsource remaining customers with unpaid balances to a collections agency on a contingent fee basis

Appendices

Appendix A. Internet Resources

The following information resources and customer screening tools are available through the Internet as of August 1999. Whether you are a new or established Internet merchant, you can use these resources to learn more about the e-commerce market, ensure the security of your electronic storefront, and explore the opportunities of business-to-business e-commerce.

HOW TO DEVELOP AN E-COMMERCE BUSINESS

Visa Merchant Resource Center - Developed by Visa to assist you in transforming your online business ideas into reality. Provides comprehensive information on Visa Best Practices, key considerations you need to make when developing your E-Commerce business and vendors and service providers that can help you achieve your goals **http://www.VISAmrc.com**

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/
- **CommerceNet Electronic Resources** - Broad range of information on establishing Internet commerce Web sites and conducting business over the Internet: http://www.commerce.net/resources/
- **Electronic Commerce Guide** - Resource guide, news summary, and discussion forum on electronic commerce: http://ecommerce.Internet.com/
- **Electronic Commerce Modeling Language** - ECML provides a set of uniform data names that streamlines the process by which merchants gather electronic data for shipping, billing and payment: http://www.ECML.org/
- **Shop.Org** - Trade association for e-commerce retailers with over 150 members. Includes information on sponsored conferences, research, and other resources provided by the association: http://www.shop.org/
- **Visa Home Page** - Starting point to access a wide range of information provided by Visa: http://www.visa-asia.com/
  - **Visa for Businesses** - Visa web site oriented toward businesses that accept Visa cards: http://www.visa-asia.com/fb/main.html
  - **Internet Shopping** - Overview of key considerations for merchants interested in selling their goods and service over the Internet: http://www.visa-asia.com/nt/ecomm/main.html

- **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/
- **GII The Standard for Internet Commerce** - codifies the best practices used by merchants in Internet commerce and with a focus on attaining higher levels of customer satisfaction, protection and confidence: http://www.gii.com/standard/index.html
- **Personalization.com**- Provides information, news and chat about 1 to 1 marketing: http://www.personalization.com/
- **APEC Center for Technology Exchange and Training for SME's (ACTETSME)**- Comprehensive site featuring information for SME's : http://www.actetsme.org/

WEB SITE PRIVACY

- **Anonymizer.Com** - An array of Internet privacy information for consumers and businesses: http://www.anonymizer.com/3.0/index.shtml
- **Electronic Privacy Information Center** - Comprehensive resource and reference guide about Internet privacy issues: http://www.epic.org/
- **Truste.Org** - Extensive information on ensuring privacy for Web publishers and users: http://www.truste.org/
- **Online Privacy Alliance** - a diverse group of corporations and associations which have come together to introduce and promote business-wide actions that create an environment of trust and foster the protection of individuals' privacy online: http://www.privacyalliance.org/
- **EPIC.org** - Comprehensive information on privacy issues in the news: http://www.epic.org/

CONSUMER SATISFACTION SITES

- **Better Business Bureau Online** - A free service that provides listings of businesses that have registered with BBBonline, but the listing is far from comprehensive: http://www.bbbonline.org/
- **NetCheck** - A free public service Web site allowing customers to submit comments on Internet merchants and search for comments submitted by other customers: http://www.netcheck.com/
- **Web Watchdog** - A free public service Web site allowing customers to rate and review the overall quality of Internet merchants: http://www.webwatchdog.com/

DOMAIN NAME VERIFICATION/REGISTRATION

- **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.networksolutions.com/cgi-bin/whois/whois/
- **Register.com** - Additional Web site to identify whether an Internet domain name is currently assigned, and to identify key contacts for that site: http://www.register.com/
- **AddMe** - Web site promotion and submission service: http://www.addme.com/
- **Submit-It** - Similar to AddMe, offering free submission of your Web site to seven search engines: http://www.siteowner.com

Appendix B. Glossary

The Internet and e-commerce have generated a number of new terms and acronyms. The payment card 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.

anonymous e-mail address - An Internet contact point assigned to a Web user 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 (SP) 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.

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.

Card-not-present - 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.

chargeback - A processed payment card transaction that is later rejected and returned to the Acquirer by the Issuer for a specific reason, such as a cardholder dispute or fraud. The Acquirer may then return the transaction to the merchant which may have to accept the dollar loss unless the transaction can be successfully represented to the Issuer.

cookie - A special text file created by a Web site service and written onto the computer hard drive of a Web site visitor. The Internet relies upon a computer language called Hypertext Transfer Protocol (HTTP) to let users access Web pages. Since each request for a Web page is independent of all other requests, the Web page server has no memory of what pages it has sent to a user previously or anything about the user's previous visits. Cookies allow the server to retain information about a visitor or a visitor's actions on its Web site and to store this data in its own file on the visitor's computer. There are two types of cookies. "Permanent cookies" retain information about visitors, such as log-in names, addresses, and past preferences. "Sessions cookies" typically let customers fill virtual shopping carts with more than one selection before checking out. Also known as Web browser cookies.

copy request - See sales draft request.

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

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

digital wallet - A software application or service that assists consumers in conducting Internet transactions by enabling them to store billing, shipping, and payment information in one place. The wallet can be used to automatically complete an e-commerce merchant's check-out page.

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.

Electronic Commerce Modeling Language (ECML) - A computer language that provides a set of uniform data elements to help streamline the process by which merchants gather electronic data for shipping, billing and payment. In an effort to enhance the online shopping experience for consumers and merchants, Visa and other industry leaders have been partnering to develop ECML-based digital wallets that make the Internet shopping experience faster and easier for consumers.

ECML - See Electronic Commerce Modeling Language.

encryption - the process of encoding, or scrambling, data so it cannot be read by unauthorized parties as it travels over the Internet.

firewall - A security tool that blocks access to files from the Internet and is used to ensure the safety of sensitive cardholder payment 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.

Issuer - A financial institution that issues Visa payment 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 payment 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 Internet merchants and the global VisaNet transaction processing system owned and managed by Visa. 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 vendor authentication, the safe transmission of payment data, and the authorization and capture of e-commerce transactions.

real-time - The seemingly instantaneous time it takes to process a Web site visitor's request for a purchase or other screen option. In fact, it may take several seconds to process the request, depending on network transmission speeds or the priorities and needs of the Web site service.

representment - A chargeback that is rejected and returned to an Issuer by an Acquirer on the merchant's behalf. A chargeback may be represented, or re-deposited, if the merchant or Acquirer can remedy the problem that led to the chargeback, and do so in accordance with Visa's rules and regulations.

RSA encryption – A public-key cryptosystem for both encryption and authentication, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. Its name comes from their initials.

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

Secure Sockets Layer (SSL) - An established industry standard that encrypts the channel between a Web browser and Web server to ensure the privacy and reliability of data transmitted over this channel. However, SSL does not provide ways to validate the identities or banking accounts of the parties exchanging this data. SSL was developed by Netscape Communications Company prior to the implementation of SET™.

SET Secure Electronic Transaction™ - An emerging industry standard that uses advanced cryptography to ensure the safety, confidentiality and integrity of payment data traveling over the Internet. Also known as SET™, the SET Secure Electronic Transaction™ protocol is the only Internet security system that authenticates buyers and sellers by associating them with financial institutions. SET™ was developed by Visa and MasterCard with the support of many technology companies such as IBM, Microsoft, Netscape, SAIC, GTE, Terisa Systems, VeriSign, and RSA Data Security. The SET™ specification is free to anyone who wishes to develop SET™-compliant software, available via the Visa web site: http://www.visa.com/.

SSL - See Secure Sockets Layer.

Appendix C. Checklist For Success

This section provides a checklist summary of the more than 80 risk management best practices discussed in this guide. You can use this checklist to plan, reevaluate, and periodically check the ongoing performance of your e-commerce program.

E-COMMERCE START-UP STRATEGIES

Acquirer Selection

- ❑ Select a qualified e-commerce Acquirer
- ❑ Understand the terms and conditions of your Acquirer contract

Data Security

- ❑ Use a secure gateway to encrypt transaction data
- ❑ Encrypt and securely store transaction data

Fraud and Chargeback Risk

- ❑ Know the risks of selling on the Internet
- ❑ Take measures to avoid customer disputes
- ❑ Understand the chargeback process

WEB SITE CONTENT

Business Policies

- ❑ Establish a comprehensive privacy policy and post it on your Web site
- ❑ Develop a comprehensive product description template
- ❑ Develop detailed corporate information
- ❑ Register with a privacy organization and post a "seal of approval" on your Web site
- ❑ Establish and display your refund and credit policy
- ❑ Develop a marketing e-mail message policy
- ❑ Implement effective marketing e-mail message practices

Customer Service Access

- ❑ Offer toll-free telephone customer service and display the number on your Web site
- ❑ Provide customer service e-mail contacts and encourage customers to use them when they have inquiries
- ❑ Develop an e-mail inquiry response policy
- ❑ Establish e-mail response standards and monitor staff compliance

WEB SITE SALES ORDER FUNCTIONALITY

Customer Relationships

- ❑ Register Internet customers
- ❑ Identify repeat customers
- ❑ Make effective use of permanent and session Web browser cookies
- ❑ Use Electronic Commerce Modeling Language (ECML) to develop your order page

Required Transaction Data Fields

- ❑ Establish transaction data fields that can help you identify risk, 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

Card Validation

- ❑ Ask the customer for both a card type and an account number, and make sure that they match
- ❑ Implement a "Mod 10" card number check before submitting a transaction for authorization
- ❑ Avoid default card expiration date
- ❑ Display only the last four digits when showing a card number to a repeat customer at your Web site

Cardholder Validation

- ❑ Check the validity of the customer's telephone number, physical address, and e-mail address
- ❑ Screen for high-risk international addresses

Sales Order Processing

- ❑ Perform an exact calculation of sales tax and shipping costs at the time of the transaction
- ❑ Display an "Order Being Processed" message during wait time
- ❑ Before completing a purchase, let the customer know whether the merchandise is in stock
- ❑ Develop a comprehensive order confirmation template
- ❑ Limit storage of payment card numbers
- ❑ Develop controls to avoid duplicate orders

VISA CARD ACCEPTANCE PRACTICES

Authorization

- ❑ Implement cost-effective authorization routing
- ❑ Perform real-time authorizations
- ❑ Use Electronic Commerce Indicator (ECI) for all Internet transactions

Post-Authorization

- ❑ Issue an e-mail order confirmation for approved transactions
- ❑ Queue Issuer authorization declines for review
- ❑ Track order decline rates
- ❑ Obtain a new authorization if the original expires before shipment
- ❑ Reverse authorizations for partial shipments

WEB SITE TRACKING AND ANALYSIS

- ❑ Collect and analyze Internet customer "click-through" patterns
- ❑ Track sales non-conversion rates
- ❑ Track purchase patterns of registered customers

FRAUD PREVENTION AND DETECTION

Risk Management Infrastructure

- ❑ Establish a formal fraud control function
- ❑ Track fraud control performance.

Fraud Avoidance Files

- ❑ Establish and maintain an internal authorization fraud avoidance file
- ❑ Use the fraud avoidance file to screen transactions

Transaction Controls

- ❑ Prevent excessive digital content downloads
- ❑ Establish transaction controls and velocity limits
- ❑ Modify transaction controls and velocity limits based upon transaction risk

Transaction Screening

- ❑ Implement fraud screening tools
- ❑ Treat anonymous e-mail addresses as higher risk
- ❑ Screen for high-risk shipping addresses
- ❑ Treat non-A.P. transactions as higher risk
- ❑ Use third-party fraud screening tools
- ❑ 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

DATA SECURITY

Data Transmission

- ❑ Encrypt cardholder data transmissions
- ❑ Discourage the use of e-mail for transactions

Internal Data Storage and Access

- ❑ Limit internal access to payment card data
- ❑ Prevent unauthorized access to stored card data
- ❑ Ensure that your server environment is secure

Security Review and Testing

- ❑ Continually test Web site security
- ❑ Conduct annual reviews of systems controls

CHARGEBACK HANDLING AND LOSS RECOVERY

Tracking Chargebacks

- ❑ Track Internet chargebacks separately from non-Internet chargebacks

Avoiding Chargebacks

- ❑ Act promptly when customers with valid disputes deserve credits
- ❑ Provide data rich responses to sales drafts requests
- ❑ Fulfill sales draft requests on a timely basis

Collection Efforts

- ❑ Develop cost-effective collection practices