

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

Background

Electronic commerce is the business of buying and selling products, information, or services in an Internet based environment. Unlike traditional face-to-face transactions, ecommerce shoppers and merchants communicate through a public computer network, enabling business to conclude to customers worldwide.

For Merchants who have decided to progress beyond the traditional “brick and mortar” storefront, there are many opportunities to enhance customer relationships, attract new customers and increase sales revenue.

Like with all opportunities, this business should be addressed for the level of risk associated with it with stronger need for strategic actions to help effectively control fraud and better safeguard cardholder account information.

Unlike merchants who operate in the physical world, we do not have fact to face contact, a card-in-hand, or an actual signature. The Security Standards have been designed with a view to help our merchants to understand and effectively minimize risk associated with the e commerce business.

Typical Risk Associated With E-commerce

Area	Risk Possibilities
Fraud	Customer uses a stolen card or account number to fraudulently purchase goods / services online. Family member uses bankcard to order goods/services online, but has not been authorized to do so. Customer falsely claims that he or she did not receive a shipment. Hackers find their way into e-commerce merchant's payment processing system and misuse account information.
Account Information Theft (Cyber Theft)	Hacker captures customer account data during transmission to / from merchant Hackers gain access to service provider's unprotected payment processing system and steal cardholder account data.
Account Information Theft (Physical Site)	Unauthorized individuals access and steal cardholder data stored at merchant or service provider site and fraudulently uses or sells it for unauthorized use or identify theft purposes. Employees of merchant / service provider steal cardholder data and fraudulently use the same or sell the same for unauthorized use or identify theft purpose Compromise of cardholder data from unshredded / unpurged stationery / files from merchant / service provider location.
Customer Disputes and Chargeback	Good and services are not as described on the website Customer is billed before goods/ services are shipped or delivered. Confusion and disagreement between customer and merchant over return and refund Customer is billed twice for the same order and / or billed for an incorrect amount Customer does not recognize the merchant name on the statement. Goods or services are billed without customer approval

Guidelines to Manage E Commerce Risk Effectively

- **Be Aware of the Risks associated with your business and Train the Team**

It is imperative that merchant to clearly understand the risk of doing business online to effectively deal with Internet fraud and/or security breaches and to avoid costs related to the same. Your entire staff dealing with the E-commerce operations should have a through working knowledge of the fraud and chargeback risk associated with any Internet transaction. They should also be well versed in your unique risk management approach.

Consider these best practices when getting your business off the ground

Being better involved about the different kinds of risk involved, will help you fine-tune your business policies, operational practices, fraud prevention tools and security controls.

Understand the chargeback process. Follow your Fund Acquirer's processing instructions to avoid chargeback related to authorizations and sales drafts request. Beware of various reasons for chargeback, particularly in regard to – Transaction authorization requirements

- Expired authorization rules for unshipped goods
- Time limits for fulfilling sales drafts request
- Cardholder disputes
- Fraudulent use of account numbers

Know your rights to resubmit transactions that have charged back for fraud reasons.

Use verified by Visa & Secure Code to substantially reduce chargeback risk exposure

You should yourself follow minimum in house risk control measures and train your employees in e-business risk management. You can implement all of the control you need to deter fraud, minimize customer disputes, and protect your site from hacker intrusions, but they don't mean much without proper employee training. To be truly effective your entire staff should:

- Have thorough understanding of the fraud risk and security issues involved in an Internet transaction.
- Know the chargeback rules and regulations for Internet transactions.
- Be well versed in your risk management policies and Procedures.

- **Develop Essential Web Site Content**

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

1. Need to have a clear and Concise statement of the Privacy policy.
2. Displays information about the site' security practices and controls
3. Customer service / help desk contact numbers
- 4.. Customer Registration process and guidelines
5. Product / service description. (to include product specifics, guarantee / warranty, safety / health warnings etc.)
6. Price / cost (whether inclusive / exclusive of taxes / octroi, delivery charges etc.). Discounts, offers if any - validity or expiry date.
7. Delivery mode and time taken for delivery Areas not serviceable to be clearly listed.
8. Cancellation / Refund policy
9. Terms and Conditions

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

Develop a clear concise statement of your privacy policy and make it available to the web site visitors through links on your homepages. Your privacy must include

- Which customer data is collected and tracked
- With whom this customer information is shared, and
- How customer can opt out
- Register with a privacy origination and post a “Seal of Approval” on your web site

Create a page that educates customer about your site's information security practices and controls

Explain how card payment information is protected:

- During transmission,
- While on your server, and
- At your physical work site.

Discourage the use of e-mail for transactions. Due to misguided concerns about Internet security some customers may send their card number to you by email, which is a non-secure way to do business. To protect your customers and foster their loyalty, highlight security practice on your web site and in reply e-mail. Stress that:

- E-mail is not a secure communication method and should never be used to transmit card number or other sensitive information

The transaction encryption capabilities of your web site offer reliable protection from unauthorized access and give cardholders safest way to make purchases over Internet.

• **Focus on Risk reduction**

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

- **Passwords and Cookies** – Make effective use of permanent Web browse cookies to recognize and acknowledge existing customers. User browser cookies to maintain active user sessions, but once a session expires, request that the user log in again, regardless of the computer being used.
- Establish ways to assist customers who forget their passwords. To help stop fraudsters in their tracks, consider either one or both of the approaches described below.
- Establish transaction data fields that can help you detect risky situation and require the customer to complete them. Include certain transaction data fields that can play an important role in helping you assess the fraud risk of a transaction. To minimize losses, define data fields that will help you recognize high-risk transactions and require customer to complete these fields before purchasing goods or services. Key risk fields include the following
 - Demographic information, such as telephone number, that can be validated using reverse directory look-ups.
 - Email address, particularly when it involves as “anonymous” services
 - 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 cardholders billing information

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Highlight the data fields that the customer must complete. Use color, shading, bold fronts or asterisks to highlight the required data fields and accompanies this with explanatory notes to the cardholder. Edit and validate required data fields in real-time to reduce risk exposure.
- Develop controls to avoid duplicate transactions. Duplicate orders can lead not only to higher processing costs, but also customer dissatisfaction. Establish controls to prevent cardholders from inadvertently submitting a transaction twice
- Card information Validation: Request for an additional card number check before submitting a transaction for authorization.
- Check the validity of the customers telephone number, physical address, and email address. Simple verification steps can help alert you to data-entry errors by customer and often uncover fraudulent attempts
- Use a telephone area code and prefix tables to ensure that the entered area code and telephone prefix are valid for the entered city and state. Identify mismatches and allow cardholder to re-enter if desired-the information initially entered may be valid due to recent additions or changes in telephone area codes
- Use a zip code table to verify that the entered zip code is valid for the entered city & state. Allow cardholders to override alerts since the information may actually be valid due to delayed updates or erroneous data.
- Test the validity of the email address by sending an order confirmation.

• **Build Internal Fraud Prevention Techniques / Methods**

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

- Risk Management Infrastructure
 - A dedicated fraud control individual or group can provide the direction that your business needs to deter fraud.
 - Establish a formal fraud control function.
 - Clarify 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.
- Internal Negative File
 - Establish and maintain an internal negative file. Make use of the details of your own history with fraudulent transactions or suspected fraud. By storing these details, you gain a valuable source of information to protect you from future fraud perpetrated by the same person or group.
 - Record all key elements of fraudulent transactions, such as names, e-mail addresses shipping addresses customer identification numbers, telephone numbers and card numbers used. For information security purpose all merchants are prohibited from storing card verification value (CVV2) data.
 - Establish a process to remove from the file information about legitimate customers whose payments data has been compromised. Criminals may use the personal data of innocent victims to commit the fraud.
 - Use the internal negative file to screen transactions. If transactions data matches negative file data, decline the transactions or- if warranted –out sort the transactions for internal review and follow up with the appropriate action.
- Transaction controls
 - Establish transactions control and velocity limits. You can significantly reduce risk exposure by using internal transactions controls to identify high risk transactions. These controls help determine when an individual cardholder or transaction should be flagged for specific review.
 - Set review limits based on the number and dollar amount of transaction approved within a specified period of time. Adjust these limits to fit average customer purchasing patterns.
 - Ensure that velocity limits are checked across multiple characteristics, including shipping address, telephone number and email address

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Adjust velocity limits as customers build history with your business. The limits should be set tighter for new customers and looser for those customers who have a solid purchasing & payment track record.
- Modify transactions controls & velocity limits based upon transaction risk. Vary transactions controls and velocity limits to reflect your risk experience with selected products, shipping locations & customer purchasing patterns

- **Apply Fraud Screening**

Today there are wide varieties of frauds screening services and practices available to help you assess the risk of a transaction & increase the likelihood that you are dealing with a legitimate customer with valid card. Fraud screening tools can be developed internally or acquiring third parties. Best practices in this area include the following:

Screening for High-Risk Transactions

- Implement fraud screening to identify high-risk transactions. Suspend processing for transactions with high risk attributes.
- Develop effective and timely manual review procedures to investigate high risk transactions
- Treat international IP addresses as higher risk. Merchants have found that international IP addresses have a substantially higher fraud rate than domestic addresses
- Carry out due diligence to match shipping addresses with billing address as may pose higher risk
- Screen for higher risk shipping addresses. You can reduce fraud by comparing 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.
- Tighten transactions controls & velocity thresholds for these transactions to increase screening frequency
- Treat with high suspicion billing addresses and shipping addresses that are not the same
- Customers who use anonymous e-mail address
- Confirm cardholder information prior to shipping transactions
- Contact the issuer to confirm cardholder information prior to shipping goods for a high risk transactions

- **Secure Code / Verified by Visa Implementation**

Verified by visa / secure code enables issuers to validate the identify of their activated visa/master cardholders during online payment transactions

Ensure transactions Qualification: Ensure the Acquirer or processor is providing the authentication results and ECI in the authorization message to obtain fraud chargeback protection

Perform Transactions Fraud Screening: Verified by Visa / Secure Code has proven to be an effective fraud prevention tool, but can't eliminate online fraud solely on this town, particularly for attempted authentication for which no authentication occurs. In addition, fraud may occur on fully authenticated transactions in account takeover situation or fraudulent cardholder claims.

Additional Operational Considerations: If using Verified by Visa / Secure Code, add the logo on your home, security information, add checkout pages to promote reliable and secure on-line shopping

To learn more about the service visit

<http://www.mastercardmerchant.com/securecode/index.html>

AND

<http://www.visa.com/verifiedmerchants>

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Avoid unnecessary Chargeback and processing cost and monitor Chargeback

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

To minimize losses, you need an adequate chargeback and effective tracking system, procedure in place to avoid unnecessary chargeback & a thorough understanding of your representation rights. Follow these best practices: Act promptly when customers with valid disputes deserve credits

- When cardholders contact you directly to resolve a dispute, issue the credit on a timely basis to avoid unnecessary disputes and their associated chargeback processing cost.
- Send cardholder an e-mail message to let them know immediately of the impending credit.

Provide data rich responses to sales draft (documentation) request. Respond to sales draft inquires 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 online address
- General description of goods or services
- "Ship to" address, if applicable
- Address Verification response Code, if applicable

Optionally provide additional data to help resolve inquiries and reduce chargeback such as:

- Transaction time
- Customer e-mail address
- Customer telephone number
- Detailed description of goods or services
- Whether a receipt signature was obtained upon delivery of goods of services

Document customer phone calls, keep copies of emails, delivery signatures, and web logs for period of 24 months from the date of shipment.

As with copy requests, monitoring chargeback rates can help merchant pinpoint problem areas in their business and improve prevention efforts. However while copy request volume is often a good indicator of potential chargeback, actual chargeback rates and monitoring strategies vary by merchant type. General best practices for chargeback monitoring include:

- Track chargeback and representation by reason code. Each reason code is associated with unique risk issue and requires specific remedy and reduction strategies
- Include initial chargeback amount and net chargeback after representation
- If your business combines MO/TO and internet sales, these chargeback should be monitored separately

- **Use Collection efforts to recovery losses**

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

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- User e-mail collection message and letters as first steps towards collecting low-amount transactions
- You often can recover unwarranted chargeback losses by contacting the customer directly through internal resources or external collection agency.
- Follow –up with phone calls to those does not respond to your initial correspondence.
- Outsource remaining customers with unpaid balances to a collection agency on a contingent fee basis.

Focus on Data Security

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

- Conduct daily monitoring of authorizations and transactions
- Monitor your batches
- Change the password of your payment gateway's system regularly
- Make sure user id and password are different and having some in-build complexity
- Ensure the requirements of Cardholder Information Security Program (CISP) are in place

Merchant Data Security Standards

Build and maintain a Secure Network

Firewalls are computer devices that control computer traffic allowed into a Company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the internet, whether for ecommerce, employees' Internet-based access via desktop browsers, or employees' e-mail, access.

Often, seemingly insignificant paths to and from the Internet can unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Install and maintain a firewall configuration to protect data

Establish firewall configuration standards. Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. Prohibit direct public access between external networks and any system component that stores cardholder information (for example, databases).

Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Always change vendor-supplied defaults before you install a system on the network (for example, passwords, Simple Network Management Protocol [SNMP] community strings and elimination of unnecessary accounts).

Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices.

Implement only one primary function per server (for example, Web servers, database servers, and DNS should be implemented on separate servers).

Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)

Configure system security parameters to prevent misuse.

Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (for example, unnecessary Web servers)

Encrypt all non-console administrative access. Use technologies such as SSH, VPN or SSL/ Transport Layer Security (TLS) for Web-based management and other non-console administrative access.

Protect Cardholder Data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration on the defense in depth principle.

Protect Stored Data

Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purpose, as documented in the data retention policy.

Do not store sensitive authentication data subsequent to authorization (not even if encrypted):

Do not store the full contents of any track from the magnetic strip (on the back of a chip, etc). Do not store the card-validation code (CVC) (Three-digit or four-digit value printed on the front or back of a payment card (for example CVV2, and CVC2 data) Do not store the PIN Verification Value (PVV)

Mask account numbers when displayed (the first six and last four digits are the maximum numbers of digits to be displayed).

Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- One-way hashes (hashed indexes) such as SHA-1
- Truncation
- Index tokens and PADs, with the PADs being securely stored
- Strong cryptography, such as Trips-DES (Data Encryption Standard) 128-bit or AES 256-bit with association key management processes and procedures

The minimum account information that is to be rendered unreadable is Payment card account number.

Protect encryption keys against both disclosure and misuse.

Restrict access to keys to the fewest number of custodians necessary

Store keys securely in the fewest possible locations and forms.

Fully documents and implement all key management processes and procedures, including:

- Generation of strong keys.
- Secure key distribution.
- Secure key storage.
- Periodic key changes.
- Destruction of old keys.

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key to reconstruct the whole key).
- Prevention of unauthorized substitution of keys.
- Replacement of known or suspected compromised keys.
- Revocation of old or invalid keys (mainly for RSA keys).
- Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.

Encrypt transmission of cardholder data and sensitive information across public networks

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/ or divert data while in transit.

Use strong cryptography and encryption techniques (at least 128 bit) such as SSL, Point-to-Point Tunneling Protocol (PPTP), and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks.

Never send cardholder information via unencrypted e-mail.

Maintain a Vulnerability Management Program

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all e-mail systems and desktops to protect systems from malicious software.

Use and regularly update anti-virus software

Deploy anti-virus mechanisms on all systems commonly affected by viruses (for example PC's and servers). Ensure that all anti-virus mechanisms are current, actively running and capable of generating audit logs.

Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to system. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

Ensure that all system components and software have the latest vendor supplied security patches.

Install relevant security patches within one month of release.

Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.

Develop software applications based on industry best practices and include information security throughout the software development life cycle. Include the following:

- Testing of all security patches and system and software configuration changes before deployment.
- Separate development/test and production environments.
- Separation of duties between development/test and production environments.
- Production data (real credit card numbers) are not used for testing or development.
- Removal of test data and accounts before production systems become active.
- Removal of custom application accounts, usernames and passwords before applications become active or are released to customers.
- Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.

Follow change control procedures for all system and software configuration changes. The procedures should include:

- Documentation of impact
- Management sign-off by appropriate parties
- Testing that verifies operational functionality
- Back-out procedures.

Develop Web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. **See www.owasp.org, “The Ten Most Critical Web Application Security Project guidelines vulnerabilities.”** Covers prevention of common coding vulnerabilities in software development processes, to include:

- Unvalidated Input
- Broken access control (for example, malicious use of user IDs)
- Broken authentication/session management (use of account credentials and session cookies)
- Cross site scripting (XSS) attacks.
- Buffer overflows
- Injection flaws (for example, SQL injection)
- Improper error handling
- Insecure storage
- Denial of service
- Insecure configuration management

Implement Storing Access Control Measures

This ensures critical data can be accessed in an authorized manner.

Restrict access to data by business need-to-know

- Limit access to computing resources and cardholder information to only those individuals whose job requires such access.
- Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.
- Assign a unique ID to each person with computer access
- This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.
- Identify all users with unique username before allowing them to access system components or cardholder data.
- Employ at least one of the methods below, in addition to unique identification, to authenticate all users:
 - Password
 - Token devices (for example, SecureID®, certificates, or public key)
 - Biometrics
- Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) with tokens or VPN with individual certificates.
- Encrypt all passwords during transmission and storage, on all system components.

Ensure proper user authentication and password management for non-consumer users and administrators, on all system components:

- Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects
- Verify user identity before performing password resets.
- Set first-time passwords to a unique value per user and change immediately after first use.
- Immediately revoke accesses of terminated users.
- Remove inactive user accounts at least every 90 days.
- Enable accounts used by vendors for remote maintenance only during the time needed.
- Distribute password procedures and policies to all users who have access to cardholder information.
- Do not use group, shared, or generic accounts/passwords
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
- Authenticate all access to any database containing cardholder information. This includes access by applications, administrators and all other users.

Restrict physical access to cardholder data

Any physical access to data or system that cardholder Data allows the opportunity to access devices or data and remove systems or hardcopies and should be appropriately restricted.

Use appropriate facility entry controls to limit and monitor physical access to systems that stores, process, or transmit cardholder data.

- Use cameras to monitor sensitive areas. Audit this data and correlate with others entries. Stores for at least three months, unless otherwise restricted by law.
- Restrict physical access to publicly accessible network jacks.
- Restrict physical access to wireless access points, gateways, and handheld devices.
- Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholders' information is accessible.

“Employee” refers to full time and part time employees, temporary employees/personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

Make sure all visitors are:

- Authorized before entering areas where cardholder data is processed or maintained.
- Given a physical token (for example, badge, or access device) that expires and that identifies them as non-employees.
- Asked to surrender the physical token before leaving the facility or at the date of expiration.

Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless restricted by law.

Store media back ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

Physically secure all paper and electronic media (For e.g. computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports and faxes) that contain cardholder information.

Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information:

- Label the media so it can be identified as confidential.
- Send the media via secured courier or a delivery mechanism that can be accurately tracked.
- Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals)
- Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information:
- Properly inventory all media and make sure it is securely stored.
- Destroy media containing cardholder information when it is no longer needed for business or legal reasons:
- Cross-cut shred, incinerate, or pulp hardcopy materials.
- Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Regularly Monitor and Test Networks

Logging mechanisms and the ability to track user activity are critical. The presence of logs in all environments allows through tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Track and monitor all access to network resources and cardholder data. Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.

Implement automated audit trails to reconstruct the following events, for all system components:

- All individual user accesses to cardholder data.
- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.

Record at least the following audit trail entries for each event, for all system components:

- User identification
- Type of event
- Data and time
- Success or failure identification
- Origination of event
- Identity or name of affected data, system components or resource.

Synchronize all critical system clocks and times.

Secure audit trails so they cannot be altered, including the following:

- Limit viewing of audit trails to those with a job-related need.
- Protect audit trail files to those with job-related need.
- Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Copy logs for wireless network onto a log server on the internal LAN.
- Use file integrity monitoring/change detection software (such as Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being should not cause an alert)
- Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like Intrusion Detection System (IDS) and Authentication, Authorization, and Accounting (AAA) servers (for example, RADIUS)
- Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.
- An audit history usually covers a period of at least one year, with a minimum of 3 months available online.
- Regularly test security system and processes

Vulnerabilities are continually being discovered by hackers/ researchers and introduced by new software. Systems, processes and custom software should be tested frequently to ensure security is maintained over time and through changes.

Test security controls, limitations, network connections and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is delayed, use a wireless analyzer periodically to identify all wireless devices in use.

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (for example, new system components installations, changes in network topology, firewall rule modifications, product upgrades.)

Note that external vulnerability scans must be performed by a scan vendor qualified by the payment card industry.

Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or medication (for example, operating system upgrade, sub-network added to environment, Web server added to environment).

Use network intrusion detection system, host-based intrusion detection system, and/or intrusion prevention system to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up to date.

Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files, and perform critical file comparisons at least daily (or more frequently if the process can be automated).

Critical files are not necessarily those containing cardholder data. For files integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications must be evaluated and defined by the merchant or service provider.

Maintain an information security policy

A strong security policy sets the security tone for the whole company and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

Maintain a policy that addresses information security policy that:

- Addresses all requirements in this specification.
- Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.
- Includes a review at least once a year and updates when the environment changes.

Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

Develop usage policies for critical employee-facing technologies, such as modems and wireless, to define proper use of these technologies for all employees and contractors. Ensure these usage policies require.

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Explicit management approval.
- Authentication for use of the technology
- A list of all such devices and personnel with access.
- Labeling of devices with owner, contact information and purpose.
- Acceptable uses of the technology.
- Acceptable network location for these technologies.
- A list of company approved products.
- Automatic disconnects of modem sessions after a specific period of inactivity.
- Activation of modems for vendors only when needed by vendors with immediate deactivation after use.
- When accessing cardholder data remotely via modem, disable storage of cardholder data onto local hard drives floppy disks or other external media. Also disable cut and paste and print functions during remote access.

Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.

Assign to an individual or team the following information security management responsibilities:

- Establish, document and distribute security policies and procedures
- Monitor and analyze security alerts and information and distribute to appropriate personnel.
- Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Administer user accounts including additions, deletions and modifications.
- Monitor and control all access to data.

Make all employees aware of the importance of cardholder information security:

- Educate employees (for example, through posters, letters, memos, meetings, and promotions)
- Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

Screen potential employees to minimize the risk of attacks from internal sources. For those employees who only have access to one card number at a time to facilitate a transaction, such as store cashiers, this requirement is a recommendation only.

Contractually require all third parties with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address:

Acknowledgement that the 3rd party is responsible for security of cardholder data in their possession. "Ownership by each Payment Card brand, Acquirer, and Merchants of cardholder data and acknowledgement that such data can ONLY be used for others uses specially required by law.

- Business continuity in the event of major disruption, disaster or failure.
- Audit provisions that ensure that Payment Card Industry representative or a Payment Card Industry Security Standards for protecting cardholder data.
- Termination provision that ensure that 3rd will continue to treat cardholder data as confidential.

Implement an incident response plan. Be prepared to respond immediately to a system breach.

- Create an incident response plan to be used in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing Acquirers and credit card associations).
- Test the plan at least annually.

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

- Designate specific personnel to be available on a 24/7 basis to respond to alerts.
- Provide appropriate training to staff with security breach response responsibilities.
- Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
- Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

Please note that this particular training material is not exhaustive in the sense that it covers all the pros & cons for E-commerce risk related information. Any E-commerce merchant must continuously update himself/herself regarding risk involved in E-commerce business based on recent trends and technological updates and make suitable arrangement to rule- out the possible threats in the business.

E-COMMERCE MERCHANT – RISK EDUCATION & TRAINING MANUAL

Acknowledgment

I hereby acknowledge the receipt of E-commerce Merchant – Risk Education / training Manual from E-Billing Solutions Pvt. Ltd., and have understood the same and will take necessary security and fraud prevention measure at my end with regards to e-commerce business facilitated through E-Billing Solutions Pvt. Ltd. In event of non-adherence of same, would be liable for all losses.

And also agree to maintain the transaction-related information like –

- Documentation of customer phone calls
- Copies of email
- Delivery signature (proof of delivery), and
- Web logs For a period of 24 months from the date of shipment or service rendered

Authorized Signatory/signatories

Company Seal

Name :

Designation :

Merchant Code :

Merchant Name :

Internet URL :

Business Address :

Site Physical address: