Visa USA Guidelines for Non-Member Agents
# Table of Contents

About This Document ......................................................... 1  

**Chapter 1: Introduction** ...................................................... 3  
What You Should Know About Visa Member/Agent Relationships ...... 4  
Non-Member Agents Defined .................................................. 5  
Visa Member Agent Relationship Management Obligations .......... 7  
Agent Responsibilities ....................................................... 9  

**Chapter 2: Agent Registration** ............................................ 13  
Types of Organizations That Members Must Register .................. 14  
How Agent Registration Works .............................................. 15  
Registration Fees ............................................................ 17  
Due Diligence Monitoring .................................................... 19  
Prohibited Activities and Reasons for Agent Termination .......... 20  

**Chapter 3: Risk Management** ............................................. 21  
Visa Corporate Risk Reduction Procedures ................................. 22  
High-Risk Telemarketing Merchant (HRTM) Monitoring Standards .. 23  

**Chapter 4: Cardholder Information Security** .......................... 25  
Data and CVV2 Storage and Security ...................................... 26  
What is the Visa Cardholder Information Security Program (CISP)? . 27  
In the Event of “Compromise”.................................................. 31  

**Chapter 5: Personal Identification Number (PIN) Security** ........ 33  
The Importance of PIN Security Requirements .......................... 34  
About the Visa PIN Security Program ..................................... 35  
Visa Security Requirements for POS PIN-Entry Devices (PEDs) ...... 37  
Visa PIN Security Resources and Education ............................... 39  

**Chapter 6: Visa Risk Control Programs** ................................. 41  
Risk Identification Service (RIS) ............................................ 42  
Merchant Chargeback Monitoring Program (MCMP) ................... 45  
High-Risk Chargeback Monitoring Program (HRCMP) ................. 47
Many Visa Members rely on Agents to increase their growth and revenue opportunities with minimal cost. This growth has led some financial institutions to shift control and responsibility for various functions to their Agents. Often, this is accompanied by a shift of liability for losses as well. From a Member perspective, a well-controlled Agent relationship can reduce the possibility of bank failure, minimize risk of loss to the payment system, and protect the goodwill of the Visa brand.

The Visa USA Guidelines for Non-Member Agents document addresses the risk management and control issues most pertinent to the Agent organization. This document explains in terms for the Agent the minimum requirements for Visa Members and their Agents. It is intended to help Agents:

- Understand their accountabilities and responsibilities to the Visa payment system.
- Ensure their day-to-day operations and practices are consistent with what will keep their associated Visa Members in compliance with the Visa U.S.A. Inc. Operating Regulations.

The Visa USA Guidelines for Non-Member Agents document presents a partial summary of the Visa U.S.A. Inc. By-Laws and Operating Regulations that all Members must comply with to participate in the Visa payment system. It has been created to help explain to Agents those standards which apply to Agent entities and to communicate each Member’s obligation in monitoring Agent compliance at all times. Agents with questions regarding precise contours of the Visa U.S.A. Inc. By-Laws and Operating Regulations, or those with a need for further information about Agent obligations should work directly with their sponsoring Visa Member.

The Visa U.S.A. Inc. By-Laws and Operating Regulations are periodically amended and subject to change. Members and Agents should continue to have an ongoing dialog to ensure that the agent always has the most up-to-date information.
What’s Covered  The Visa USA Guidelines for Non-Member Agents document has been divided into nine chapters, each with a different main focus. You can work through this document in its entirety, or move directly to any of the topics listed here.

✔ **Chapter 1: Introduction** clarifies the Visa Member and non-member Agent relationship and the Agent’s responsibilities to the Member and Visa payment system.

✔ **Chapter 2: Agent Registration** focuses on the Visa U.S.A. Inc. Operating Regulations that cover Agent registration and attestation requirements and fees. It walks through registration process and supporting documentation and discusses the consequences of Member non-compliance.

✔ **Chapter 3: Visa Risk Management** looks at the requirements and recommended standards developed by Visa to help Members and Agents minimize risk.

✔ **Chapter 4: Cardholder Information Security** offers background information about the Visa Cardholder Information Security Program (CISP) for Members and their Agents.

✔ **Chapter 5: Personal Identification Number (PIN) Security** covers the Visa PIN Security Program requirements intended for use by all acquiring Members, their merchants, and Agents.

✔ **Chapter 6: Visa Risk Control Programs** looks at the risk control services developed by Visa to help reduce risk and associated fraud losses.

✔ **Chapter 7: Merchant Agreements** contains the mandatory and optional Merchant Agreement provisions defined by Visa.

✔ **Chapter 8: Visa Rules and Requirements for Card Acceptance** covers Visa card acceptance procedures for merchants.

✔ **Chapter 9: Merchant Fraud and Prevention** provides merchant requirements for checking Visa card security features and the cardholder’s signature, as well as what to do if a fraudulent card or transaction is suspected. Information on Code 10 call actions is also included.

A **Glossary** has also been provided to define commonly used key terms throughout this document.
Since the 1970’s, Visa Members have used Agents to perform various sales and service functions. Agents that perform services for merchants, or act on behalf of a Member in connection with Visa payment services fall into six categories: Independent Sales Organization (ISO), Encryption and Support Organization (ESO), Merchant Servicer, Third-Party Servicer (TPS), High-Risk Internet Payment Service Provider (HRIPSP), and Processor. This chapter helps clarify the roles of Members and their non-member Agents.

**WHAT’S COVERED**

- What You Should Know About Visa Member/Agent Relationships
- Non-Member Agents Defined
- Visa Member Agent Relationship Management Obligations
- Agent Responsibilities
What You Should Know About Visa Member/Agent Relationships

Visa Members that make use of Agents for such functions as account solicitation, transaction processing, and customer support are required to monitor closely these groups and their bankcard-related activities to minimize fraud exposure and protect cardholder information. To build and maintain proper Agent control, Visa Members must:

- Ensure that all Agents are registered with Visa as outlined in the Visa U.S.A. Inc. Operating Regulations, and that they are compliant with the Visa Cardholder Information Security Program (CISP) and Visa PIN Security Requirements (as applicable).
- Comply with established Visa Enhanced ISO/Service Provider Risk Standards during the Agent registration process and throughout the life of the relationship, (if applicable).
- Require a written contract between the Member and the Agent (except with Merchant Servicers). The contract should define Member program responsibilities, requirements, and standards.
- Develop policies and procedures that ensure appropriate controls are in place to adequately monitor the Agent relationship and protect the payment system.
- Conduct periodic reviews of Agent activities and perform on-site inspections of Agent business locations.
Non-Member Agents Defined

The following chart identifies the six categories of non-member Agents and defines the payment services provided by each group.

<table>
<thead>
<tr>
<th>VISA DEFINES THIS ENTITY:</th>
<th>AS AN:</th>
</tr>
</thead>
</table>
| Independent Sales Organization (ISO) | Organization or individual that is not a Member and whose bank card-related business relationship with a Member involves any of the following:  
- Merchant solicitation, sales, or service  
- Merchant transaction processing solicitation  
- Cardholder solicitation or card application processing services  
- Deployment of and/or services for qualified ATMs and Point-of-Sale (POS) systems |
| Merchant Servicer | Organization that is not a Member of Visa, but has a direct relationship with a merchant instead of a Member. The Agent has access to cardholder data and performs services such as gateway, fraud scrubbing, loyalty programs, etc. |
| Third-Party Servicer (TPS) | Organization that is not a Member of Visa and is not directly connected to VisaNet, but provides the following services to the Member:  
- Response processing for Visa program solicitations  
- Transaction processing, including gateways  
- Data capture  
- Other administrative functions, such as chargeback processing, risk/security reporting, and customer service |
| Encryption and Support Organization (ESO) | Organization that is not a Member, but whose bank card-related business relationship with a Member includes:  
- Merchant solicitation, sales, or service  
- Terminal or Personal Identification Number (PIN) pad encryption, key loading, or injecting  
- Merchant help desk support which includes re-programming of terminal software  
- Cryptographic key loading into ATMs and cash dispensers |
### VISA DEFINES

<table>
<thead>
<tr>
<th>THIS ENTITY: High-Risk Internet Payment Service Provider (HRIPSP)</th>
<th>AS AN: Internet Payment Service Provider (IPSP) that:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Enters into a contract with an Acquirer to provide payment services to Sponsored Merchants, <strong>and</strong></td>
</tr>
<tr>
<td></td>
<td>• Includes one or more Sponsored Merchants classified with Merchant Category Code 5967 (Direct Marketing–Inbound Teleservice merchants) in its Sponsored Merchant portfolio.</td>
</tr>
</tbody>
</table>

HRIPSPs are identified and monitored as merchants in the Visa payment system. However, for purposes of clarity they have been included in the Agent portion of this guide. Members must register HRIPSPs with Visa by utilizing the same process established for ISOs.

| Processor | Organization that is acting as the Agent of a Member to provide authorization, clearing, or settlement services for merchants and Members. |
Visa Member Agent Relationship Management Obligations

Agent Monitoring
A Member’s obligation to monitor the practices of its Agent(s) is a long-standing requirement. Visa places the responsibility for losses and damages arising from Agent activity squarely on the Member. The Visa U.S.A. Inc. Operation Regulations impose specific monitoring standards and prescribe fees for non-compliance.

Agent Contracts
Members must execute a written contract with each Agent (except for Merchant Servicers). This agreement, to the extent permitted by applicable law, is executed by an authorized officer of the Member and must insure that the Agent is compliant with the Visa U.S.A. Inc. Operating Regulations, Interlink Network, Inc. and Plus System, Inc. Operating Regulations, and the Visa Cardholder Information Security Program (CISP). The Member is responsible for informing the Agent of the governing requirements.

Processor Contract Provisions
A contract between a Member and Processor must contain provisions that ensure:

- All Agents and Merchant Servicers with access to the Member’s Bank Identification Numbers (BINs) are registered by the Member with Visa.
- The Processor notify the Member in writing and receive written approval from the Member prior to allowing an Agent or Merchant Servicer access to a Member’s BINs or cardholder information.
- The Processor notify (at least quarterly) the Member and Visa of any Agents or Merchant Servicers with access to the Member’s BINs.

Merchant Servicer Attestation
Members that do not have a contract with a Merchant Servicer must complete Exhibit VV-2 and ensure that it is signed by an authorized officer of the Member bank. The revised VV-2 includes the attestation that Members use in place of an agreement with the Merchant.

Reporting Quarterly
On a quarterly basis, each Member will receive a listing of all its registered Agents from Visa. Members must complete the information requested on that form and return it to Visa USA within 30 days of receipt. Visa USA will assess a fee if a Member fails to provide a quarterly report within the required timeframe.

Members that use an Agent as a Processor must submit a quarterly report to Visa USA, that includes the following minimum information:

- Identification of the services provided by the Agent
- Products and programs supported
- BINs under which the Member’s activity is processed
Audits and Reviews

The Member, Visa USA, or their designees may conduct financial and procedural audits and/or reviews at any time. Audits and/or reviews will be conducted at the Member’s expense.

Member Use of Agents

Members must:

- Control approval and review of merchants, approval of cardholder applications, and establishment of merchant fees for Visa transactions.
- Maintain a file on the Agent including all applicable documentation, and retain this file for a minimum of two years following discontinuance of the Agent relationship.
- Ensure that the Member and Agent activities will comply with all of the Visa U.S.A. Inc. Operating Regulations.
- Register each Agent and designate the activities that the Agent is authorized to perform on the Member's behalf.
- Ensure that the Agent has access to and uses the information contained in the current Visa Interchange Directory, if the Member uses the Agent for processing of any of the following:
  - Chargebacks
  - Arbitration
  - Compliance
  - Authorizations
  - Referrals
  - Fraud reporting
  - Settlement
- Ensure that Agents make available cardholder, merchant, and/or Sponsored Merchant records as soon as possible, but not later than seven business days from the receipt of a request from a Member or Visa USA, their designees, or any regulatory agency.

Members must advise the Agent that:

- Such organization or individual must not represent registration in the Agent Reference File as endorsement of its services by Visa USA.
- Registration of an Agent is specific to each Member, and requires a separate registration process for each Agent MEMBER business relationship.

Member and Agent Site Inspections

To ensure compliance with the Visa U.S.A. Inc. Operating Regulations, Visa may inspect the premises of a Member or its Agents at any time and assess a reasonable fee for such an inspection.
Agent Responsibilities

Agents who are engaged by Members to provide sales and/or services on their behalf must adhere to specific standards and requirements as specified below.

Agent Education

To ensure their Agents understand Visa payment system obligations, as well as relevant Visa U.S.A. Inc. Operating Regulations. Members are required to:

• Clearly communicate policies, procedures, and operational requirements.
• Obtain the Agent’s commitment to comply with Member policies and procedures, as well as the substance of relevant Visa U.S.A. Inc. Operating Regulations.

Providing Information

If the Member, Visa USA, its designees, or any regulatory agency requests cardholder or merchant information, the Agent must provide the information in writing as soon as possible, but no later than seven business days from receipt of a request. An Agent can receive a request for any type of information, including the following:

• Organizational structure
• Employee information
• Sales-related data
• Financial Information
• Security Information

Marketing Materials

Agents must use only solicitation materials, (e.g., advertisements, sales brochures, and web site promotional content) that have been approved by the Member and meet these basic guidelines:

• The material must prominently identify the Member by name and city next to the Visa-owned marks. The material must not identify the Agent, unless the Agent is prominently identified as an Agent or representative of the Member.
• The Agent must clearly disclose on its solicitation material that:
  – Any subsequent cardholder or Merchant Agreement is between the Member and the individual cardholder or merchant.
  – The Member is the Issuer of the Visa card, not the Agent (in cardholder solicitation material situations).
• The Agent must not use any Visa-owned mark on any marketing material, including business cards and letterhead or stationery.
Data Security

The Visa Cardholder Information Security Program (CISP) helps ensure that all merchants and Agents with access to Visa cardholder data have met a set of minimum requirements for protecting sensitive information. These requirements are designed to safeguard Visa cardholder account information and protect Members from the risk of increased losses associated with compromised cardholder data.

All Agents with access to cardholder data must be CISP compliant at the time they are submitted to Visa for registration. CISP requirements and a list of all known compliant entities can be obtained at www.visa.com/cisp.

**Merchants must notify their Acquirer of any Merchant Servicer that will have access to cardholder data.** The Acquirer is required to notify Visa if its Merchant is using a Merchant Servicer and the Merchant Servicer meets Visa's CISP standards. An Acquirer that discloses transaction information or allows its merchant to provide the information to a Merchant Servicer that is not CISP compliant may be liable for fees.

Personal Identification Number (PIN) Security

Members registering PLUS or Interlink Agents must provide Visa with an adequate PIN security self-audit and conduct an on-site review of the Agent’s PIN security controls before registration may proceed.

Unregistered Sub-Agents Prohibited

Members are required to properly register their Agents with Visa before transaction activity or solicitation may begin. Agents that contract services to other Agents that are not properly registered with Visa may cause the Member to violate Visa regulations and become liable for fees.

Representation

An Agent must not present itself as, or appear to be, a Member of Visa.

Agent Disclosure of Cardholder Data

Agents must **not** disclose cardholder account numbers, personal information, or other Visa transaction information to third-parties, other than:

- For the sole purpose of completing the transaction,
- As required by local law, or
- With the permission of the Issuer, Acquirer, or Visa, as specified in the Visa U.S.A. Inc. Operating Regulations.

**An Agent does not own Visa transaction information.** In the event of an Agent failure, including bankruptcy, insolvency, or other suspension of business operations, an Agent must not sell, transfer, or disclose any materials that contain cardholder account numbers, personal information, or other Visa transaction information to third parties. The Agent must return this information or provide acceptable proof of destruction of this information to its Visa Member.
To prevent compromise and protect the integrity of the payment system, Agents that transmit, store, or process cardholder data must:

- Keep all material containing account numbers—whether on paper or electronically—in a secure area accessible only to selected personnel.
- Render all data unreadable prior to discarding.
- Not retain full-track, magnetic-stripe and/or Card Verification Value 2 (CVV2) data. Once an authorization is processed, magnetic-stripe and/or CVV2 data should no longer exist.

Visa Bank Identification Number (BIN) information provided by an Acquirer to a merchant or an Agent is proprietary, confidential, and it belongs to Visa USA. A merchant or Agent must not disclose Visa BIN information to any third party without prior written permission from Visa USA.

Merchants or Agents that receive BIN information from their Acquirers must not use it for any reason other than to identify Visa Debit Category products at the point of sale, unless authorized by Visa USA.

Merchants that provide BIN information to a Merchant Servicer must ensure the above BIN information requirements are clearly stated in their contract with the Merchant Servicers.

Given the confidential and proprietary nature of Visa processing systems, Agents with access to the V.I.P. System or BASE II, or related documentation are prohibited from:

- Providing access to or disclosing these systems and documentation to any third-party, and
- Using these systems and documentation for any purpose not authorized in the Visa U.S.A. Inc. Operating Regulations.
Chapter 2  
Agent Registration

Visa Members must register certain Agents in accordance with the Visa U.S.A. Inc. Operating Regulations. This chapter identifies the types of Agents that must be registered and discusses the registration process. It also outlines ongoing Member and Agent responsibilities once both parties have entered into a working relationship.

**WHAT'S COVERED**
- Types of Organizations That Members Must Register
- How Agent Registration Works
- Registration Fees
- Due Diligence Monitoring
- Prohibited Activities and Reasons for Agent Termination
Types of Organizations That Members Must Register

A Visa Member must register an Agent that provides any of the following services listed below.

### Acquirer Services/Activities
- Solicits merchants
- Provides a gateway for transactions from merchant locations to Processors
- Transmits, captures or stores Visa cardholder information
- Has access to Member Bank Identification Numbers (BINs)
- Provides Merchant 3D Secured/Verified by Visa services
- Provides back office support, e.g. customer service and exception processing
- Supports loyalty programs
- Deploys and/or services qualified ATMs and Point-of-Sale (POS) systems
- Loads or injects encryption keys into terminals or POS Personal Identification Number (PIN) pads
- Loads cryptographic keys into ATMs and cash dispensers
- Provides merchant help desk support which includes re-programming of terminal software
- Processes transaction authorizations

### Issuer Services/Activities
- Solicits cardholders
- Provides response support for solicitation of cardholders
- Provides prepaid solicitation and marketing services
- Provides back-office support (e.g. customer service and exception processing)
- Supports loyalty programs
- Provides Verified by Visa Access Control and Enrollment Services
- Processes transactions
- Provides Healthcare Spending Account programs
How Agent Registration Works

Visa Members must complete the following Agent registration steps and in doing so, supply the appropriate registration materials to Visa:

1. **Contact Franchise Management to query the Agent Reference File.** Requests can be sent by e-mail to Agentregistration@visa.com or fax (650) 432-1862 and must contain the following information: Agent name, Agent city & state, and full name of principals.

2. **Complete background investigations to verify the financial responsibility of the Agents and their principals to ensure that no significant derogatory information exists.** Conduct on-site inspections of business locations to verify inventory, and if applicable review all Agent solicitation or sales material.

3. **Complete the required registration form and supporting documentation to confirm the Member’s compliance with Visa’s standards.** Members must submit a registration form, which can be accessed via Visa Online or through Visa Franchise Management. A Senior Officer from the Member must sign the registration materials.

4. **Verify Visa Cardholder Information Security Program (CISP) compliance status.**

5. **Conduct due diligence to ensure compliance with the Enhanced ISO/Service Provider Risk Standards.**

Below is a list of the documentation that Visa requires in order to register each Agent type:

<table>
<thead>
<tr>
<th>AGENT CATEGORY</th>
<th>REQUIRED DOCUMENTS</th>
</tr>
</thead>
</table>
| Visa ISO & TPS | • Exhibit VV, which can be accessed via Visa Online or through Visa Franchise Management  
• Documentation confirming compliance with the Enhanced ISO/Service Provider Risk Standards |
| Visa HRIPSP    | • Exhibit VV, which can be accessed via Visa Online or through Visa Franchise Management  
• Documentation confirming compliance with the Enhanced ISO/Service Provider Risk Standards  
• A comprehensive list of all High-Risk Sponsored merchants in an electronic format specified by Visa USA |
| Merchant Servicer | • Exhibit VV-2, which can be accessed via Visa Online or through Visa Franchise Management  
• Documentation confirming compliance with the CISP |
| Interlink ISO  | • Exhibit E, located in the Interlink Network Inc. Bylaws and Operating Regulations  
• Documentation confirming compliance with the Enhanced ISO/Service Provider Risk Standards |
| Plus ISO       | • Exhibit 2, located in the Plus System, Inc. Operating Regulations  
• Documentation confirming compliance with the Enhanced ISO/Service Provider Risk Standards |
## Agent Category Required Documents

<table>
<thead>
<tr>
<th>Agent Category</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Interlink ESO  | • Exhibit F, located in the *Interlink Network Inc. By-laws and Operating Regulations*  
                 • Documentation confirming compliance with the Enhanced ISO/Service Provider Risk Standards |
| Plus ESO       | • Plus non-member Registration Program Application Packet  
                 • Documentation confirming compliance with the *Enhanced ISO/Service Provider Risk Standards* |
| Processor      | • Exhibit WW and Exhibit K, which can be accessed via Visa Online or through Visa Franchise Management |
Registration Fees

The following fees are assessed to Members for their registered ISOs, ESOs, and *HRIPSPs and Processors. The same registration fee structure applies to TPSs and Merchant Servicers, however, these entities are billed directly.

<table>
<thead>
<tr>
<th>INITIAL</th>
<th>ANNUAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5,000</td>
<td>$2,500</td>
</tr>
</tbody>
</table>

A Visa Member is responsible for fees not paid by the TPS or Merchant Servicer within 30 days. If a TPS or Merchant Servicer does not pay within the allotted timeframe, the fees will be collected from the Member through Visa USA's Integrated Billing.

Any Member that fails to comply with Visa U.S.A. Inc. Operating Regulations regarding use of Agents will be assessed substantial fees. Whether the Member chooses to assess any fees to the Agent is a matter of contract between the Member and the Agent and is not governed by Visa. Agents should consult their Member if they have questions about what fees may be applicable to them.

For repeated violations in a 60-month rolling period, Visa may assess additional fees at management's discretion. Fees are cumulative.

Visa also assesses an additional fee for each 30-calendar-day period, or a portion thereof, during which the Member fails to:

- Register the Independent Sales Organization, Third-Party Servicer, or Merchant Servicers.
- Notify Visa of a change.

If a Member repeatedly fails to comply with registration or notification requirements in a 60-month rolling period, Visa may assess the Member further fees. Such fees may be assessed at Visa management's discretion and are cumulative.

Fees may also be assessed to an Acquirer for a Merchant Servicer’s failure to comply with registration requirements for merchant services.

* Members are also assessed a registration fee for each HRIPSP Sponsored Merchant.
Fees for HRIPSP Registration Non-Compliance

A Member that fails to comply with registration program requirements for HRIPSPs, is assessed a fee as follows:

- $25,000 per month per high-risk Sponsored Merchant or HRIPSP.
- After three violations in a calendar year:
  - $100,000 for each 30-day calendar period of non-compliance, and/or
  - Prohibition against signing high-risk Sponsored Merchants.

See Chapter 6: Visa Risk Control Programs for further details.
Due Diligence Monitoring

After the initial registration period, Visa requires its Members to proactively monitor and manage their Agents. In doing so, all Members:

- Must perform an Agent review at least once annually to confirm ongoing compliance with the Enhanced ISO/Service Provider Risk Standards, PIN Security Requirements Self-Audit, (if applicable) and/or Cardholder Information Security Program (CISP).

- May be required, upon request from Visa USA, to provide documentation to confirm compliance with any of Visa’s programs.

- Must have operational policies and procedures in place to ensure Agent compliance.

- Must have a policy and procedure in place to identify all Agents or Processors that facilitate, store and/or use transaction data at the request of the Member or its merchants. If an Agent is unregistered, Members may be subject to unregistered Agent fees and must register the Agent immediately.

A Visa Member may conduct more frequent reviews of Agents, as appropriate.
## Prohibited Activities and Reasons for Agent Termination

Agents have a duty to operate in a professional manner to protect the integrity of the Visa payment system. Agents that act to circumvent Visa regulations or take actions that harm the Visa brand may be removed from the system.

<table>
<thead>
<tr>
<th>Prohibited Activity</th>
<th>Visa may permanently prohibit an Agent and its principals from providing services with respect to Visa products based on any of the following grounds:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Fraudulent activity</td>
</tr>
<tr>
<td></td>
<td>• Activity that causes the Member to repeatedly violate the Visa U.S.A. Inc. Operating Regulations</td>
</tr>
<tr>
<td></td>
<td>• Operating in an unsound or unsafe manner</td>
</tr>
<tr>
<td></td>
<td>• Any other activities that may result in undue economic hardship or damage to the goodwill of the Visa system, if the Agent fails to take corrective action where an opportunity to take corrective action is appropriate.</td>
</tr>
</tbody>
</table>

| Agent Termination   | If a Member becomes insolvent, the contract between the Member and Agent will be terminated.                                  |
While Agents may provide sales and operational support, Members retain overall responsibility for establishing risk controls, policies, and procedures. This chapter reviews how Members protect their relationships with their Agents through careful communication and internal controls.

### WHAT’S COVERED
- Visa Corporate Risk Reduction Procedures
- High-Risk Telemarketing Merchant (HRTM) Monitoring Standards
Visa Corporate Risk Reduction Procedures

In order to protect the Visa payment system, a Visa Member or its Agent may be required to implement Visa Corporate Risk Reduction procedures and measures, which may include, but are not limited to:

- Blocking cardholder transaction authorizations or prohibiting Acquirers from obtaining authorization on transactions on behalf of certain merchants.
- Prohibiting or limiting:
  - Issuing new or reissued cards.
  - Signing or re-signing of merchants or Sponsored Merchants.
  - Using any Independent Sales Organizations (ISOs).
- Terminating some or all merchants or Sponsored Merchants that conduct card-not-present transactions or deliver goods and services after the transaction date.
- Terminating some or all merchants or Sponsored Merchants that generate chargebacks substantially in excess of the system average.
- Pledging collateral to secure a Member’s or Agent’s obligations and reimbursement to Visa USA for any expenses incurred in assuring the compliance of those obligations.
- Implementing procedures or practices deemed necessary by Visa to maintain the integrity of Visa transactions.
- Redirecting settlement funds to avoid potential losses. This can include, but is not limited to any of the following:
  - Rerouting settlement funds around the bank that normally holds the Member or Agent funds
  - Holding funds to ensure the correct application of cardholder funds
  - Holding funds for the payment of merchants or Sponsored Merchants
  - Holding funds for the future payment of chargebacks
  - Withholding funds for the purpose of obtaining collateral or meeting other Membership obligations
- Terminating or limiting a Member’s right to sponsor participant-type Members.
- Requiring a Member to change one or more of its designated Agents.
High-Risk Telemarketing Merchant (HRTM) Monitoring Standards

Before accepting transactions from a High-Risk Telemarketing Merchant (HRTM), an Acquirer must submit to Visa USA a completed Visa U.S.A. High Risk Merchant Registration and Certification (Exhibit U). An HRTM may not begin transaction processing until the Member conducts an adequate due diligence. Members are also responsible for monitoring their registered HRTMs as defined in the Visa U.S.A. Inc. Operating Regulations.

A Member must monitor all normal and unusual daily activity as outlined below.

NORMA L DAILY ACTIVITY REPORTING

- Retain the following daily data
  - Gross sales volume,
  - Average transaction amount,
  - Number of transactions,
  - Average elapsed time between the merchant date of the merchant receipt and the central processing date (CPD) (counting each as one day), and
  - Number of chargebacks.

- Collect data for a period of at least 15 calendar days, beginning after each merchant’s initial deposit.

- Use the data to determine the merchant’s normal daily activity for each High-Risk Telemarketing Merchant (HRTM) category.

- Begin daily monitoring of the merchant’s deposit activity processed on the 15th calendar day from the first deposit.

- Compare current related data to the normal daily activity parameters at least daily.

- Review and adjust the merchant’s normal daily activity at least weekly, using the previous week’s activity.

UNUSUAL ACTIVITY REPORTING

Generate unusual activity reports on a daily basis and report any unusual activity to Visa within two business days, if either of the situations below occurs:

- Current weekly gross sales volume equals or exceeds $5,000, and any of the following exceeds 150 percent of the normal daily activity:
  - Number of daily transaction receipt deposits
  - Gross amount of daily deposits
  - Average transaction amount
  - Number of daily Chargebacks

- Average elapsed time between the transaction date and the Acquirer’s processing date for a transaction (counting each as one day) exceeds 15 calendar days.

HRTMs include the following merchant types:

- Direct Marketing Travel Related Services (MCC #5962)
- Inbound Telemarketing (MCC #5966)
- Outbound Telemarketing (MCC #5967)—Includes video text and audio-text merchants.

An HRTM that generates excessive chargeback rates may be entered in Visa’s high-risk chargeback program if they exceed acceptable chargeback ratios.
It is up to Visa to determine if the Acquirer has met the High-Risk Telemarketing Merchant Monitoring Standards defined in the Visa U.S.A. Inc. Operating Regulations. At Visa’s request, the Acquirer must demonstrate compliance by providing copies of actual reports or records used to monitor merchant deposits and any other data requested.

### Merchant Investigation

The Acquirer must investigate any HRTM appearing on an unusual activity report within one business day of generating the report. If an investigation reveals that a merchant is involved in illegal or fraudulent activity, the Acquirer must:

- Take appropriate legal action to minimize losses.
- Cooperate fully with Visa in any investigation, and release all information relative to the merchant upon request.
- Cooperate with Issuers and law enforcement agencies.
- Attempt to make the merchant responsible for the transaction.
- Hold funds, if possible.
- Contact law enforcement, if appropriate.

### Revocation of Merchant Privileges

Visa may impose conditions on, or permanently prohibit, a merchant or its principals from participating in a Visa Program for any reasons it deems appropriate to protect the Visa payment system, such as:

- Fraudulent activity
- Presenting transaction receipts that do not result from an act between the cardholder and the merchant (laundering)
- Entering into a Merchant Agreement under a new name with the intent to circumvent the Visa Risk Programs
- Activity that causes the Acquirer to repeatedly violate the Visa U.S.A. Inc. Operating Regulations
- Any other activity that may result in undue economic hardship or damage to the goodwill of the Visa system
The Visa USA Cardholder Information Security Program (CISP) helps minimize the threats and risks to which account and transaction information is exposed. The program provides a comprehensive set of requirements that must be implemented by Visa Members, their merchants, and non-member Agents. These requirements represent the minimum standards acceptable for participation in the Visa payment infrastructure. All non-member entities that have access to cardholder data must comply with CISP requirements at the time they are submitted to Visa for registration. This chapter introduces CISP and also covers data storage requirements.

WHAT’S COVERED
✓ Data and CVV2 Storage and Security
✓ What is the Visa Cardholder Information Security Program (CISP)?
✓ In the Event of “Compromise”
Data and CVV2 Storage and Security

Today, an internal or external compromise of any system where full-track, magnetic-stripe and/or Card Verification Value 2 (CVV2) data has been retained can result in the perpetration of counterfeit fraud, fraudulent use of account data, and identity theft.

To prevent compromise and protect the integrity of the payment system, **Members, merchants, and Agent organizations that transmit, store, or process cardholder data must:**

- Keep all material containing account numbers—whether on paper or electronically—in a secure area accessible only to selected personnel.
- Render all data unreadable prior to discarding.
- Not retain full-track, magnetic-stripe and/or CVV2 data. Once an authorization is processed, magnetic-stripe and/or CVV2 data should no longer exist.
What is the Visa Cardholder Information Security Program (CISP)?

**Visa Member Responsibilities**

Members, merchants, and service providers—regardless of size—or in the case of service providers, whether they support issuing or acquiring activity—must comply with the CISP requirements. **Under CISP, Visa Members must:**

- Designate an individual or group of individuals to play an active role in fully implementing and enforcing CISP.
- Adequately inform merchants and service providers of their CISP-compliance role and responsibilities and the penalties of non-compliance.
- Ensure that merchants and service providers contractually require all associated third parties with access to cardholder data to adhere to CISP security requirements.
- Provide tools and training opportunities to ensure merchants and service providers understand the CISP requirements, as well as specific data security measures and procedures.
- Validate that their merchants and all supporting service providers comply with the program.

**CISP Compliance**

Members are responsible for ensuring that all merchants who store, process, or transmit Visa cardholder data must **comply** with the CISP requirements specified in the Operating Regulations. This includes mail/telephone order, e-commerce, and card-present merchants (e.g., retailers, lodging, restaurants). As merchants in all acceptance channels are increasingly victimized by compromises, their compliance is critical to ensure the protection of Visa cardholder data.

**CISP Compliance Validation**

Separate and distinct from the mandate to comply with CISP requirements is the **validation** of compliance. It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring appropriate levels of cardholder information security are maintained. Visa has prioritized validation of CISP compliance based on the volume of transactions, the potential risk, and exposure introduced into the Visa System by merchants and service providers.
**Merchant Levels of CISP Compliance Validation**

Visa merchant levels of CISP compliance criteria and validation actions are listed below.

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>SELECTION CRITERIA</th>
<th>VALIDATION ACTION</th>
<th>VALIDATED BY</th>
</tr>
</thead>
</table>
| 1     | Any merchant processing over 6,000,000 Visa transactions per year, or identified by any other payment card brand as Level 1. | • Annual On-Site Security Audit  
• Quarterly Network Scan | • Independent Security Assessor or Internal Audit if signed by Officer of the company  
• Qualified Independent Scan Vendor |
| 2     | Any e-commerce merchant processing 150,000 to 6,000,000 Visa transactions per year. | • Annual Self-Assessment Questionnaire  
• Quarterly Network Scan | • Merchant  
• Qualified Independent Scan Vendor |
| 3     | Any e-commerce merchant processing 20,000 to 150,000 Visa transactions per year. | • Annual Self-Assessment Questionnaire  
• Quarterly Network Scan | • Merchant  
• Qualified Independent Scan Vendor |
| 4     | Any e-commerce merchant processing less than 20,000 Visa transactions per year, and all other merchants processing up to 6,000,000 Visa transactions per year. | • Recommended Annual Self-Assessment Questionnaire  
• Recommended Annual Network Scan | • Merchant  
• Qualified Independent Scan Vendor |
### Service Provider Levels of CISP Compliance Validation

CISP compliance criteria validation actions for service providers are defined below.

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>SELECTION CRITERIA</th>
<th>VALIDATION ACTION</th>
<th>VALIDATED BY</th>
</tr>
</thead>
</table>
| 1     | All VisaNet processors (Member and nonmember) and all payment gateways. | • Annual On-site Security Audit | • Qualified Independent Security Assessor  
• Qualified Independent Scan Vendor  
• Quarterly Network Scan |
| 2     | Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually. | • Annual On-site Security Audit | • Qualified Independent Security Assessor  
• Qualified Independent Scan Vendor  
• Quarterly Network Scan |
| 3     | Any service provider that is not in Level 1 and stores, processes, or transmits less than 1,000,000 Visa accounts/transactions annually. | • Annual Self-Assessment Questionnaire | • Service Provider  
• Qualified Independent Scan Vendor  
• Quarterly Network Scan |

### Why Comply?

Consumer trust in the security of sensitive information is more critical than ever. To build the confidence of mutual customers, all Visa constituents need to be vigilant in their efforts to maintain data security. CISP requirements help Visa Members, merchants, and service providers meet the obligations to the Visa payment system.
If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the acquiring Member
- Impose restrictions on the merchant or its Agent, or
- Permanently prohibit the merchant or its Agent from participating in Visa programs

Members that fail to comply with CISP standards may be assessed fees and may be restricted from participating in Visa programs.

**CISP Enforcement and Fees for Non-Compliance**

**For Further Information**

CISP compliance requirements and validation tools can be found at www.visa.com/cisp.
**In the Event of “Compromise”**

**Member Responsibilities**

In the event of a security breach, the Visa U.S.A. Inc. *Operating Regulations* require Members, their merchants, and service providers to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. A Member must, upon completion of the investigation, demonstrate its ability—or that of its merchants or service providers—to prevent future loss or theft of transaction information consistent with Visa’s CISP requirements. Visa USA, or an independent third party acceptable to Visa, must verify the ability by conducting a subsequent security review.

If Visa USA determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating the loss of this information, Visa USA may require immediate corrective action.

If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Assess a fee to the Member financial institution,
- Impose restrictions on the merchant or service provider, or
- Permanently prohibit the merchant or service provider from participating in Visa programs.

To assist Members and their merchants or service providers in the event of compromise, Visa offers a complete set of step-by-step guidelines. Visa may also require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records, including copies of forensic analysis. For details, visit www.visa.com/cisp.

**Recognizing what constitutes a security incident is crucial to minimizing the impact an incident might have on your organization. In general, incidents may be defined as deliberate electronic attacks on the communications or information processing systems. Whether initiated by a disgruntled employee, a malicious competitor or a misguided hacker, deliberate attacks often cause damage and disruption equal to or greater than any natural disaster.**
Visa’s efforts to protect Personal Identification Numbers (PINs) have extended well beyond the development of standards and regulations. Since the mid-1990s, Visa has maintained a worldwide comprehensive PIN Security Compliance program. In this chapter, you’ll find a high-level explanation of the Visa PIN Security Program requirements for all acquiring institutions and Agents responsible for PIN transaction processing.

WHAT’S COVERED

✔ The Importance of PIN Security Requirements
✔ About the Visa PIN Security Program
✔ Visa Security Requirements for POS PIN-Entry Devices (PEDs)
✔ Visa PIN Security Resources and Education
The Importance of PIN Security Requirements

By submitting a transaction through Interchange, an Acquirer warrants that required safeguards are in place to protect the Issuer’s PIN. Should there be a breach of this warranty, the Acquirer must indemnify and hold harmless the Issuer for all claims and liabilities.

Visa places tremendous importance on PIN security. Its PIN Security Program has been implemented to effectively manage the PIN security risks unique to the US Region and maintain the highest levels of protection for Interchange PINs at Point-of-Sale (POS) and ATM PIN-entry Devices (PEDs).

The program includes publication of documents such as the Payment Card Industry (PCI) PIN Security Requirements and the Payment Card Industry (PCI) POS PED Security Requirements manuals. These documents require annual compliance reporting for designated program participants involved in the acceptance or processing of Interchange PINs. Visa USA also performs on-site PIN Security Field Reviews to validate compliance.

To enhance Member compliance efforts, Visa provides educational workshops for entities that require knowledge of cryptographic methods and more detailed information of Visa’s PIN Security Requirements.

Visa U.S.A. Inc. Operating Regulations, Plus System Inc. Operating Regulations and Interlink Network Inc. Operating Regulations require Members and their Agents to be in full compliance with the PCI PIN Security Requirements. Visa USA will enforce these requirements through its rule enforcement procedures. These procedures include PIN Security Field reviews, the annual submission of self-audits for designated program participants. Where necessary, fees, conditions, collateral and limitations on Agent sponsorship may be enforced. If these procedures do not address a PIN security problem at a particular Member or their Agent adequately, Visa USA may terminate that institution’s membership in the Visa system.

PIN Security is a matter of collective security, rather than an area for competition. Visa encourages Members, Agents, and other networks to freely share security information that can help further protect cardholder PINs.
### Program Overview

The Visa PIN Security Program is designed to ensure that institutions and their sponsored Agents that acquire, process, or perform cryptographic key management and support functions for POS and ATM PEDs, have received a yearly risk-based assessment. On an annual basis, Visa validates program participants.

### Program Elements

<table>
<thead>
<tr>
<th><strong>Program Participants</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Each year, certain entities are identified for an on-site PIN Security field review. The selection of entities as program participants is based on established risk-based criteria.</td>
</tr>
</tbody>
</table>

**Annual Self-Attestation**

Annually, program participants will be notified by Visa to submit the Visa PIN Security Self-Audit Compliance Statement and the Visa PIN Security Self-Audit Processing Environment forms. The Self-Audit Exception Form must be completed for each exception. Other supporting documentation may be requested.

Each participant in the transaction processing chain that manages cardholder PINs and encryption keys must be in compliance with the PCI PIN Security Requirements manual. Principal, sponsoring and Processor Members, and any other entity sponsoring Agents or third parties, are responsible for verifying that their group, as a whole, is in full compliance. It is the responsibility of the designated auditing staff of each group to explore the possible security implications of each unique implementation.

Any time a participant makes substantive security changes, Visa may require re-validation of the participant’s compliance with the PCI PIN Security Requirements.

**Security Self-Audit for New Agents**

The Visa PIN Security Requirements Self-Audit, the Self-Audit Compliance Statement and applicable Self-Audit Exception Form(s) and the Self-Audit Processing Environment forms must be completed with all other registration forms for Plus and Interlink Agent registrations prior to commencing any acquiring or processing of Interchange PINs.

The PIN program manager will review all PIN Security self-audits for new Agent registrations and provide feedback to the sponsoring Member and Visa staff as appropriate to ensure accurate information is being provided.
A Self-Audit Exception Form must be completed for any requirements that are not in full compliance. The audit exception form identifies why the participant is not in compliance and what actions are being taken to bring the participant into full compliance. When compliance is not possible, Visa contacts the Member to review and resolve any exceptions.

**Auditor Verification**

The Visa PIN Security Requirements Self-Audit is to be completed and certified by an internal or independent auditor annually as evidenced on the Self-Audit Compliance Statement. The auditor must have sufficient skill and experience to determine compliance for each area being reviewed. Visa may request validation of the skill level of the auditor.

**Officer Attestation**

In addition to verification by a qualified auditor, Visa requires an attestation of compliance by an Officer of the participant. Visa will notify each participant of the appropriate organizational level for this attestation.

**Field Review**

Visa, at its discretion, may perform an onsite inspection to verify the participant’s compliance with the submitted security self-audit. All auditor work papers from the self-audit may be requested and should be retained for a minimum of three years.

**Non-Compliance Fees**

An Acquirer is subject to fees as specified in the Visa U.S.A. Inc. Operating Regulations for the failure to submit the Self-Audit or the Self-Audit Compliance Statement. An Acquirer who fails to respond to a non-compliance notification following an on-site inspection is subject to fees, sanctions, conditions or having its membership/registration suspended as specified in the Visa U.S.A. Inc. Operating Regulations until the response has been received and acknowledged by Corporate Risk Management.

**In all cases a Member is responsible and subject to fees or other sanctions for the actions or inactions of its Agents.**
Visa Security Requirements for POS PIN-Entry Devices (PEDs)

**Visa PIN Security Requirements** also require that all Members and their Agents deploy only POS PIN-entry devices (PEDs) that have passed an evaluation performed by a PCI-recognized independent laboratory. This evaluation is used to determine that the device is compliant with the *PCI POS PED Security Requirements* manual, that it has been approved by the PCI office, and is listed at www.visa.com/pin as an approved device.

Currently, Visa’s enhanced PIN Security Requirements apply to any PEDs used in a POS device for authorization—either online PIN verification by the Issuer or offline PIN verification by the card’s chip.

**Visa’s POS PED Testing Requirements are as follows:**

**POS PED Testing**
- **Effective January 1, 2004**, all newly deployed POS PED models (i.e., newly purchased devices from the original equipment manufacturer, not previously acquired devices being installed for the first time) must be evaluated by a PCI-recognized laboratory and been approved by the PCI office.
- **Effective July 1, 2010**, all POS PED models must be evaluated by a PCI-recognized laboratory and approved by the PCI office.

**POS TDES Device Deployment**
- **Effective January 1, 2004**, all newly deployed POS PEDs must be PCI compliant (i.e., newly purchased devices from the original equipment manufacturer; not previously acquired devices being installed for the first time) must support Triple Data Encryption Standard (TDES).

(Note: POS PEDs submitted for PCI evaluation are also evaluated for TDES support).

**ATM and EPP PED Model Testing Deferral**

At the current time, Visa has deferred the requirement that all newly deployed ATM, EPP, and cash dispensing PED models (i.e., newly purchased devices from the original equipment manufacturer, not previously acquired devices being installed for the first time) be evaluated through a Visa-recognized laboratory and approved by Visa. In 2005, new *PCI ATM PED Security Requirements* will be released along with a lab evaluation mandated for newly purchased ATMs. Until Visa extends lab evaluation requirements to ATMs and cash dispensers, purchasers of new ATMs and cash dispensers should obtain a written attestation from the device manufacturer that certifies that the device(s) being purchased are TRSM- and TDES-capable as delivered, with no additional hardware, software, or firmware needed to execute the TDES.
| ATM TDES Device Deployment | Effective January 1, 2003, all newly deployed ATMs (including replacement devices/upgrades) must support the TDES. Additionally, vendors are required to manufacture upgrades for existing ATMs and cash dispensers that have Triple Data Encryption Algorithm (TDEA) Encrypting PIN pads (EPPs). |
Visa PIN Security Resources and Education

Online Tools
For the most recent listing of PCI approved PIN-entry devices and other testing, as well as additional PIN Security Program information, visit www.visa.com/pin. The PCI PIN Security Requirements and PCI POS PED Security Requirements manuals are also available in a downloadable format at this site.

This site also provides the most recent listing of PCI-approved POS PIN-entry devices and other testing and program information.

Education Requirements
To ensure that Members and Agents properly safeguard PIN data, Visa requires that all Plus sponsoring Members and their Plus Independent Sales Organizations (ISOs), Encryption and Support Organizations (ESOs), and Third-Party Servicers (TPSs), that operate or deploy or process transactions for non-financial institution branded ATMs, attend either a Visa Key Management Workshop or a Visa PIN Security Auditor’s Workshop every three years. These PIN Security education requirements can help improve Member and Agent cryptographic skills and ensure that Visa interchange PINs are properly safeguarded. All Plus Agents registered on or before February 29, 2004, are required to attend either a Visa Key Management Workshop or a Visa PIN Security Auditor’s Workshop by April 30, 2007. All Plus Agents registered after March 1, 2004, have three years from the date of their Plus registration to complete this requirement. Members that sponsor Plus Agents should ensure that the Agent satisfies the training requirements by the applicable date or earlier if possible.

Key Management Workshop
Visa’s one-day Key Management Workshop provides up-to-date information on the management of cryptographic keys used in ATMs, PIN pads, cash dispensers, and hardware security modules. The workshop is for staff involved in the management or operation of devices that accept cardholder PINs and for personnel who need practical knowledge about the elements of data encryption standard (DES) cryptography and the management of secret DES encryption keys. The Key Management Workshop offers the latest information on the best practices for data encryption standard (Single-DES and Triple-DES) cryptographic key management. Plus Acquirers and their sponsored third-party Agents should send personnel involved with the management, deployment or operation of devices that accept cardholder personal identification numbers (PINs), and/or who require practical knowledge about the elements of DES cryptography and approved key management methodologies.
**PIN Security Auditor’s Workshop**

The three-day PIN Security Auditor’s Workshop includes topics covered at the one-day Key Management Workshop. It also addresses current and future threats and provides an in-depth review of the Payment Card Industry (PCI) PIN Security Requirements. This workshop features a case study that is carried out by teams throughout the course. The case reinforces the topics covered in the presentations by enabling participants to put the information to immediate practical use. Discussions among the teams members add further value to this interactive session.

*Note: Completion of either workshop entitles participants to obtain continuing professional education (CPE) credit. For more information about the above PIN Security education requirements for registered Plus Agents, contact your Visa Member.*
Visa has risk programs in place to reduce exception item activity and to protect the integrity of the Visa payment system. This chapter provides an overview of the Visa USA services and programs developed specifically for Acquirers.

**WHAT'S COVERED**
- Risk Identification Service (RIS)
- Merchant Chargeback Monitoring Program (MCMP)
- High-Risk Chargeback Monitoring Program (HRCMP)
- Global Merchant Chargeback Monitoring Program (GMCMP)
- High-Risk Internet Payment Service Provider Registration Program
- Online Gambling Audit Program
- Other Corporate Risk Reduction Control Programs
- Acquirer Risk Program
Risk Identification Service (RIS)

The Risk Identification Service (RIS) assists Acquirers in their ongoing risk-control efforts by identifying merchants that generate a disproportionally high percentage of fraud activity. RIS evaluates transactions processed through VisaNet and reports various fraud and risk activities to Members. Visa notifies an Acquirer when its merchants exceed the Visa-specified fraud and risk parameters. Using RIS data, Acquirers can pinpoint merchant locations where risk-related activity has occurred, investigate causes, and take appropriate corrective action. By carefully monitoring merchant activity and imposing timely and effective corrective measures, Members can reduce their exposure to merchant fraud and subsequent financial losses.

How RIS Works

The RIS gathers and analyzes the following types of merchant transaction data to determine whether risk-related activity is occurring at merchant locations:

- Unusual deposit activity as compared to established Visa parameters
- Issuer-reported fraud activity transactions from the Visa Fraud Master File
- Consumer-dispute chargebacks, fraud-related chargebacks, and requests for copies
- Manual-entry fraud transactions
- Other types of risk-related data

Each type of risk-related activity found at a merchant location is compared against established Visa parameters for that activity type. If the activity level exceeds the parameters, RIS identifies the merchant and a report is sent to the Acquirer.

RIS Reports

The following RIS reports are produced for Acquirers from data accumulated in the merchant screening process. Acquirers must review these reports on a regular basis to detect and resolve any unusual or suspicious change in merchant activity.

<table>
<thead>
<tr>
<th>REPORT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant Identification</td>
<td>Generated for each type of risk-related activity RIS monitors. There are four levels of suspect or fraud activity risk severity — Advises (the least severe), Notifications, Alerts, and Warnings (the most severe, requiring corrective action). Excessive warnings trigger fee liabilities (See next page).</td>
</tr>
<tr>
<td>Summary</td>
<td>Provides an overview of risk-related activity occurring at merchant locations, merchant market comparisons, and identifications that occurred during the month for each Bank Identification Number (BIN).</td>
</tr>
<tr>
<td>Chargeback Exception</td>
<td>Notifies Acquirers and Issuers of their chargeback liabilities and rights.</td>
</tr>
<tr>
<td>(Code 93)</td>
<td></td>
</tr>
</tbody>
</table>
RIS Fees for Excessive Warnings

Current Visa U.S.A. Inc. Operating Regulations allow Visa to assess fees to Acquirers for “high-risk merchants” identified by the RIS. The fees are assessed on the Member and may be substantial. Whether a Member can assess any fee on an Agent or merchant is a matter determined by the Merchant Agreement, to which Visa is not a party. The Member should be consulted about any questions of Agent or merchant fee liability. The program structure is as follows:

<table>
<thead>
<tr>
<th>STATUS</th>
<th>IDs</th>
<th>ACQUIRER RESPONSIBILITY</th>
<th>VISA PROGRAM ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Notification</td>
<td>1st ID</td>
<td>• Analyze merchant activity.</td>
<td>Fee to Member &amp; forfeit of workout period for non-receipt/incomplete required documentation</td>
</tr>
</tbody>
</table>
|                      | 2nd ID | WO Month 1  
• Submit a Corporate Risk Questionnaire to Visa within 10 days of date of the WO Month 1 Notification.  
• Initiate actions to reduce fraud.  |                                                                                                          |
|                      | 3rd ID | WO Month 2  
• Submit a Fraud-Reduction Plan to Visa within 10 days of the date of the WO Month 2 Notification.  
• Provide Visa with a copy of merchant notification regarding their inclusion in RIS program.  
• Continue to implement fraud-reduction initiatives.  |                                                                                                          |
|                      | 4th ID | WO Month 3  
• Continue working with merchant to ensure plan is fully implemented and is effectively reducing fraud.  
• Provide written status to Visa on the merchant’s progress.  |                                                                                                          |
| Enforcement Period   | 5th ID | • Continue working with merchant to ensure plan is fully implemented and is effectively reducing fraud.  
• Set-up conference call with Visa and merchant.  
• Provide written status to Visa on the merchant’s progress.  | Fee to Member                                                                                              |
| Month 1              |     |                                                                                                                                  |                                                                                                          |
| Enforcement Period   | 6th ID | • Continue working with merchant to ensure plan is fully implemented and is effectively reducing fraud.  
• Provide Visa with a copy of merchant notification that excessive fraud may lead to disqualification.  
• Provide written status to Visa on the merchant’s progress.  | Fee to Member                                                                                              |
| Month 2              |     |                                                                                                                                  |                                                                                                          |
| Enforcement Period   | 7th ID | • Continue working with merchant to ensure plan is fully implemented and is effectively reducing fraud.  
• Provide Visa with Member Sr. Management’s acknowledgement of the problem and decision to continue processing for the merchant.  
• Provide written status to Visa on the merchant’s progress.  | Fee to Member                                                                                              |
| Month 3              |     |                                                                                                                                  |                                                                                                          |
| Enforcement Period   | 8th ID | • Conduct a complete review of merchant’s processing history.  
• Determine why fraud has not reduced below thresholds.  
• Provide written 60-day strategy to Visa for managing the merchant’s performance.  | Fee to Member                                                                                              |
| Month 4              |     |                                                                                                                                  |                                                                                                          |
| Enforcement Period   | 9th ID | • Consider developing an exit strategy.  
• Provide second notification to merchant of potential for disqualification.  
• Provide written 30-day strategy to Visa for managing the merchant’s performance.  | Fee to Member                                                                                              |
| Month 5              |     |                                                                                                                                  |                                                                                                          |
| Enforcement Period   | 10th ID | • If received from Visa, communicate any pending disqualification action to merchant.  
• Provide final written recap to Visa of merchant’s performance, fraud reduction-initiatives and Acquirer actions.  | Fee to Member revocation of merchant                                                                       |
### Other Fees and Penalties

<table>
<thead>
<tr>
<th>IF VISA USA DETERMINES THAT:</th>
<th>THEN VISA USA MAY:</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Acquirer or its merchant changed, modified, or altered merchant data in any way to avoid RIS detection</td>
<td>Assess a substantial fee to the Acquirer for each occurrence identified.</td>
</tr>
<tr>
<td>Transactions from a single merchant are entered into Interchange under multiple names</td>
<td>• Consolidate the merchant activity from all names into one.</td>
</tr>
<tr>
<td></td>
<td>• Track and report the consolidated merchant activity under current RIS parameters.</td>
</tr>
<tr>
<td></td>
<td>• Track the fraud activity-to-sales ratio on a month-to-month basis.</td>
</tr>
<tr>
<td></td>
<td>• Designate and monitor the merchant as a high-risk merchant.</td>
</tr>
<tr>
<td></td>
<td>• Subject the Acquirer of the merchant to the RIS chargeback as specified in the Risk Identification Service User’s Manual and assess fees, if applicable.</td>
</tr>
</tbody>
</table>
Merchant Chargeback Monitoring Program (MCMP)

The Merchant Chargeback Monitoring Program (MCMP):

- Monitors the chargeback activity of all merchants and Acquirers monthly, and notifies Acquirers when excessive chargeback activity occurs.
- Helps reduce the impact of chargebacks in the payment system and prevents those merchants with excessive chargeback levels and/or business practices from creating undue harm to the goodwill of the Visa brand.
- Helps to reimburse Issuers for some of the expense related to chargebacks.

To qualify for the MCMP, the merchant must have experienced all of the following activities during the same month:

- 100 Interchange Transactions
- 100 Chargebacks
- A 1.00 percent or greater ratio of overall Chargeback-to-Interchange volume

If a merchant meets or exceeds the above-listed chargeback thresholds, the Acquirer is notified and assessed fees as charted on the next page.

Ongoing monitoring of merchant chargeback-to-sales ratios can help Acquirers spot excessive chargeback activity, proactively minimize high-risk behavior, and with proper intervention—prevent the merchant from entering the MCMP. However, if an Acquirer receives notification from Visa of excessive chargeback activity, appropriate steps should be taken immediately to bring chargeback rates back down to acceptable levels. This may mean reviewing card acceptance procedures with the merchants, or developing a detailed and comprehensive chargeback reduction plan according to Visa requirements.

If the Acquirer fails to resolve the problem and excessive chargeback activity is not reduced within an appropriate period of time, fees may be assessed. The fees are assessed by Visa on the Member and may be substantial. Whether a Member can assess any fee on an Agent or merchant is a matter determined by the Merchant Agreement, to which Visa is not a party. The Member should be consulted about any questions of Agent or merchant fee liability. Ultimately, the merchant may also lose Visa payment acceptance privileges. MCMP fees, thresholds and requests are defined in the Visa U.S.A. Inc. Operating Regulations.
<table>
<thead>
<tr>
<th>EVENT</th>
<th>VISA PROGRAM ACTIONS</th>
</tr>
</thead>
</table>
| 1. Merchant outlet meets or exceeds the chargeback activity thresholds. | • Initial Notification – month 0  
• No fee |
| 2. Merchant outlet continues to meet or exceed the chargeback activity thresholds for the month following initial notification. | • Notification – month 1  
• Fee to Member for failure to return completed documentation within ten calendar days of the notification letter date  
• Additional fee to Member per day until completed documentation is received |
| 3. Merchant outlet continues to meet or exceed the chargeback activity thresholds for the second month. | • Notification – month 2  
• Fee to Member for failure to respond with an acceptable chargeback reduction plan within ten calendar days of the notification letter date  
• Additional fee to Member per day until acceptable chargeback reduction plan is received |
| 4. Merchant outlet continues to meet or exceed the chargeback activity thresholds for months 3, 4, and 5. | • Fee to Member per chargeback for every month the merchant continues to meet or exceed the chargeback thresholds |
| 5. Merchant outlet continues to meet or exceed the chargeback activity thresholds for months 6 and 7. | • Fee to Member per chargeback for every month the merchant continues to meet or exceed the chargeback thresholds |
| 6. Merchant outlet continues to meet or exceed the chargeback activity thresholds for months 8 and 9. | • Review fee to Member  
• Fee to Member per chargeback for every month the merchant continues to meet or exceed the chargeback thresholds |
| 7. Merchant outlet continues to meet or exceed the chargeback activity thresholds beyond month 9. | • Fee to Member per chargeback for every month the merchant continues to meet or exceed the chargeback thresholds  
• Merchant and its principals eligible for disqualification proceedings |
High-Risk Chargeback Monitoring Program (HRCMP)

The High-Risk Chargeback Monitoring Program (HRCMP) is designed to reduce the number of chargebacks generated by high-risk merchants. The program applies to merchant businesses in the following Merchant Category Code (MCC) groups:

- **5962**—Direct Marketing—Travel-Related Arrangement Services
- **5966**—Direct Marketing—Outbound Telephone Merchants
- **5967**—Direct Marketing—Inbound Telephone Merchants
- **7995**—Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks

To underscore the importance of addressing excessive chargeback activity, the program assesses fees to Acquirers whose merchants exceed program ratios. The objectives of the HRCMP are to:

- Ensure that Acquirers thoroughly understand high-risk merchant business models before setting up an account.
- Encourage Acquirers to ensure that their high-risk merchants use sound business practices that do not generate excessive chargeback activities.
- Motivate Acquirers to focus their approval criteria on sound business practices and financial responsibility, rather than on the merchant’s ability to provide reserve deposits.
- Reimburse Issuers for some of the expense incurred in handling excessive numbers of cardholder disputes.
- Promote consumer confidence in the Visa brand.
- Ensure proper controls and chargeback reduction initiatives are in place when the merchant is signed.

**How the Program Works**

To qualify for the HRCMP, the merchant in the MCC groups identified above must have experienced all of the following activities during the same month:

- 100 Interchange Transactions
- 100 Chargebacks
- A 1.00 percent or greater ratio of overall Chargeback-to-Interchange volume
Under the HRCMP, there is no warning period and the fees to the Member begin immediately when the merchant has excessive chargebacks. Visa USA assesses HRCMP fees to the Acquirer, from the date of notification. The fees are assessed by Visa on the Member and may be substantial. Whether a Member can assess any fee on an Agent or merchant is a matter determined by the Merchant Agreement, to which Visa is not a party. The Member should be consulted about any questions of Agent or merchant fee liability.

### Event Table

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Required Action</th>
</tr>
</thead>
</table>
| 1. During months 1–3, the merchant meets or exceeds the chargeback activity thresholds | • Review fee to Member – month 1  
• Fee to Member per chargeback – months 1–3 |
| 2. During months 4–6, the merchant meets or exceeds the applicable chargeback ratios specified in (1) above | • Fee to Member per chargeback – months 4–6  
• Review fee to Member – month 5 |
| 3. After 6 months in which the merchant has met or exceeded the chargeback thresholds | • Visa may disqualify the merchant from participation in Visa Program. |
| 4. Acquirer does not:  
  • Identify HRTM with the correct MCC  
  • Register a HRTM | • Additional fee to Member per merchant per month  
• Additional fee to Member after three violations in calendar year and/or prohibition against signing HRTM¹ |
| 5. Acquirer knowingly signs a disqualified merchant or any of the disqualified merchant’s principals | • Fee to Member per month until the Acquirer terminates the Merchant Agreement |

¹ Visa USA also may impose conditions on Acquirers for violations of the Visa U.S.A. Inc. Operating Regulations, up to and including termination of the Acquirer program.
Global Merchant Chargeback Monitoring Program (GMCMP)

The Global Chargeback Monitoring Program (GMCMP) is operated by Visa International and administered by each region. The program augments the U.S. Merchant Chargeback Monitoring Program (MCMP) in effect today and is intended to:

• Encourage merchants to reduce their incidence of chargebacks by using sound best practices.
• Help to reimburse Members for some of the expenses incurred in managing cardholder disputes.
• Promote consumer confidence in using Visa cards for all their purchasing needs.

GMCMP Remedial Action and Penalties

The GMCMP applies when a merchant has a two percent international chargeback-to-International sales ratio. In order to qualify for the program, merchants must have 200 or more International Interchange transactions and 200 or more International “first” chargebacks. Under GMCMP, there is no warning period and fees to Members begin immediately at $100 per chargeback. The fees are assessed by Visa on the Member and may be substantial. Whether a Member can assess any fee on an Agent or merchant is a matter determined by the Merchant Agreement, to which Visa is not a party. The Member should be consulted about any questions of Agent or merchant fee liability.

<table>
<thead>
<tr>
<th>STATUS</th>
<th>ACQUIRER RESPONSIBILITY</th>
<th>VISA PROGRAM ACTIONS</th>
</tr>
</thead>
</table>
| Month 1 | • Submit the following to Visa within 10 days of date on Notification letter:  
- Questionnaire,  
- Acceptable Chargeback reduction plan,  
- Copy of Merchant Application, and  
- Copy of Merchant Agreement. | • Fee to Member per chargeback |
| Month 2 | • Work with the merchant to ensure the plan is effectively implemented.  
• Submit update to Visa on progress to date and implementation of chargeback reduction initiatives. | • Fee to Member per chargeback |
| Month 3 | • Continue working with merchant to ensure plan is fully implemented and is effectively reducing chargebacks.  
• Provide written status to Visa on Acquirer’s progress to reduce merchant’s chargebacks. | • Fee to Member per chargeback |
| Month 4 | • Continue working with merchant to ensure plan is fully implemented and is effectively reducing chargebacks.  
• Provide written status to Visa on Acquirer’s progress to reduce merchant’s chargebacks.  
• Provide Visa with a copy of Acquirer’s notification to the merchant that excessive chargebacks may lead to disqualification. | • Fee to Member per chargeback  
• If requested by Visa, Member and merchant to attend a meeting at Visa for a discussion on remediation plan |

[continued]
<table>
<thead>
<tr>
<th>STATUS</th>
<th>ACQUIRER RESPONSIBILITY</th>
<th>VISA PROGRAM ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Month 5</td>
<td>• Consider developing an exit strategy.</td>
<td>• Fee to Member per chargeback</td>
</tr>
<tr>
<td></td>
<td>• Provide Visa copy of second notification to merchant of potential for disqualification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provide written status to Visa on the merchant's progress to reduce chargebacks.</td>
<td></td>
</tr>
<tr>
<td>Month 6</td>
<td>• If received from Visa, communicate any pending disqualification action to Merchant.</td>
<td>• Fee to Member per chargeback</td>
</tr>
<tr>
<td></td>
<td>• Provide final written recap to Visa of merchant’s performance, chargeback reduction initiatives and Acquirer actions.</td>
<td>• Revocation of merchant</td>
</tr>
</tbody>
</table>
High-Risk Internet Payment Service Provider Registration Program

The High-Risk Internet Payment Service Provider Registration Program applies to Acquirer relationships with any Internet Payment Service Provider (IPSP) that accepts Visa transactions on behalf of a Sponsored Merchant classified with MCC 5967. The program requirements apply to existing High-Risk Internet Payment Service Providers (HRISPs) and newly acquired HRISPs. As part of the program, an Acquirer is required to register a HRISP and each high-risk Sponsored Merchant with Visa prior to entering transactions into Interchange.

How the Program Works

Under the High-Risk Internet Payment Service Provider Registration Program:

- An Acquirer must:
  - Maintain a minimum Tier 1 capital requirement of $100 million as a prerequisite for registration of an HRISP.
  - Register all HRISPs and each high-risk Sponsored Merchant with Visa.
  - Provide to Visa monthly reports on high-risk Sponsored Merchant activity.
  - During the underwriting process, ensure the HRISP web site does not contain illegal or prohibited activity.

- The HRISP merchant name field must comply with a specific naming convention specified in the Visa U.S.A. Inc. Operating Regulations. Sponsored Merchant web site payment pages must contain specific disclosure statements.

Additionally, Acquirers registering HRISPs are required to comply with general Visa U.S.A. Inc. Operating Regulations that govern IPSPs. However, IPSPs that do not sign Sponsored Merchants defined by MCC 5967 are not required to comply with the more stringent HRISP program requirements.
A Member that fails to comply with registration program requirements for HRIPSPs, is assessed a fee as follows:

- Fees to Members per month per high-risk Sponsored Merchant or HRIPSP.
- After three violations in a calendar year:
  - Additional fees to Members for each 30-day calendar period of non-compliance, and/or
  - Prohibition against signing high-risk Sponsored Merchants

The fees are assessed by Visa on the Member and may be substantial. Whether a Member can assess any fee on an Agent or merchant is a matter determined by the Merchant Agreement, to which Visa is not a party. The Member should be consulted about any questions of Agent or merchant fee liability.
Online Gambling Audit Program

How the Online Gambling Audit Program Works

The Online Gambling Audit Program strengthens Visa and Member efforts to effectively manage the risks associated with transactions that may be related to online gambling or to the purchase of chips or credits that may be used for gambling. Acquirers must ensure that merchant engaged in transactions are identified with the correct data elements in the authorization messages. Acquirers whose merchants are in violation will be assessed fees and other actions as specified in the table below.

The program identifies a merchant involved in these transactions as non-compliant if its authorization requests do not contain the following:

- MCC 7995 (Field 18)
- POS Condition Code 59 (Field 25)

Program Enforcement

To help ensure compliance with the Online Gambling Audit Program, the following non-compliance fees and actions have been implemented.

Online Gambling Audit Program Fees

<table>
<thead>
<tr>
<th>MERCHANT VIOLATION</th>
<th>VISA PROGRAM ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncorrected violation for up to three months in a rolling 12-month period</td>
<td>Fees to Member for each merchant URL identified*</td>
</tr>
<tr>
<td>Uncorrected violation for four or more months in a rolling 12-month period</td>
<td>Merchant considered for global revocation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACQUIRER VIOLATION</th>
<th>FEES AND ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more non-compliant merchants identified for four or more months in a rolling 12-month period</td>
<td>Acquirer may be prohibited from signing new online gambling merchants for at least one year</td>
</tr>
</tbody>
</table>

*All fees will be assessed to the Acquirer of the violating merchant engaged in transactions that may relate to online gambling or the purchase of chips or credits that may be used to engage in online gambling. Whether any fees may be assessed by the Member or any Agent or merchant is a matter determined by the Merchant Agreement, to which Visa is not a party. Members should be consulted about any questions of Agent or merchant fee liability.
Other Corporate Risk Reduction Control Programs

**Electronic Commerce Merchant Monitoring Program**

The **Electronic Commerce Merchant Monitoring Program** safeguards the Visa payment system and the brand from illegal child pornography transactions. Members identified by the program are required to terminate the offending merchants and face possible Visa actions that may include the revocation of their Visa Membership. The program works with law enforcement to facilitate their efforts to identify and prosecute child pornographers.

The Visa Electronic Commerce Merchant Monitoring Program:

- Protects the Visa brand and the Visa payment system from the harm caused by child pornography transactions.
- Identifies child pornography merchants and terminates their Visa acceptance privileges.
- Ensures that Members take appropriate action to prevent illegal transactions from entering the Visa payment system.
- Supports law enforcement efforts to identify and prosecute child pornographers.

**High-Risk Telemarketing Reviews**

The **High-Risk Telemarketing Review** process ensures that Members that register merchants in the High-Risk Telemarketing Merchants (HRTMs) are in good standing with all Corporate Risk Management Programs and are eligible to sign such merchants. It also identifies Acquirers that fail to register HRTMs participants and includes financial assessments. The review procedures prevent HRTM businesses that have lost their Visa acceptance privileges from re-entering the system. They also prevent illegal activity and cross-border acquiring.

HRTMs include the following merchant types:

- Direct Marketing with Travel Related Services (MCC #5962)
- Inbound Telemarketing (MCC #5966)
- Outbound Telemarketing (MCC #5967)—Includes video text and audiotext merchants.

**Electronic Commerce Indicator (ECI)**

Visa’s **Electronic Commerce Indicator (ECI)** program enforces the accurate and complete use of the ECI in Internet transactions. The program identifies merchants where the incorrect ECI is being utilized. It also helps Acquirers ensure prompt resolution. Fees can be assessed if Acquirers fail to respond in a timely manner. The program applies a fee structure as necessary for Acquirers with non-compliant merchants. Without an ECI, Internet transactions cannot be identified.
Acquirer Risk Program

The Acquirer’s Risk Responsibilities

All Acquirers in the payment system must ensure their operations adhere with Visa U.S.A. Inc. Operating Regulations and the minimum standards detailed in this Guide. Key Acquirer risk responsibilities identified by Visa include the following:

<table>
<thead>
<tr>
<th>IN THIS AREA</th>
<th>MEMBERS MUST:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Have policies that include at least the minimum standards established by Visa to mitigate risk to the payment system. The policies must be approved by the Member’s Board of Directors or an appropriate senior oversight committee and be made available to Visa upon request.</td>
</tr>
</tbody>
</table>
| Merchant Agreements | • Have Merchant Agreements that meet Visa minimum requirements for disclosure and clearly define both Member and Merchant obligations.  
• Control Merchant approval.  
• Ensure any Third-Party Merchant Agreements are reviewed and approved prior to their use. |
| Funding      | Control all funds related to Visa Merchant acceptance, including settlement, reserves, holdbacks and other funds; non-Members are prohibited from direct control over such funds. |
| Monitoring Agents and Merchants | Have adequate controls to monitor Agent and Merchant activity to ensure compliance with Visa requirements and prevent harm to the payment system. |
| Education    | • Provide Agents with the necessary education and training as required in the Visa U.S.A. Inc. Operating Regulations.  
• Ensure Agents are aware of the Member’s policies and guidelines and remain in compliance. |

Compliance and On-site Reviews

Visa has developed an Acquirer review process to ensure compliance with the Acquirer Risk Program requirements. Acquirers may be reviewed annually or as needed on a risk-prioritized basis. At Visa’s discretion, Acquirers will be required to contract with an approved vendor to have a review of their operations performed and a copy of their report of compliance forwarded to Visa. Each review will utilize various techniques to ensure an Acquirer’s compliance with the key responsibilities and other key operational requirements.
**Remediation Mechanisms**

Visa Corporate Risk will work with Members whose independent report of their operations indicates non-compliance with the Acquirer Risk Program requirements. Members must provide an acceptable plan to address the deficiencies identified. Visa’s response is determined by the severity of the deficiency issues identified and the Member’s ability and willingness to rapidly address them. This response could include specific corrective actions, fees in various amounts, and ultimately, if a Member fails to implement an approved plan, suspension of the Member’s Visa program and/or termination of their membership privileges.

**Quarterly Reporting for Agents**

Visa’s current requirements for reporting on Agent performance was revised to include specific information on each Agent. Members must maintain a file on each Agent and review their performance on a quarterly basis. The report must be signed by a senior officer and be made available to Visa upon request.
Upon acceptance of a new merchant account, an Acquirer and merchant must sign an agreement specifying the terms and conditions under which Visa transactions will be processed. This agreement is the legal contract between the Acquirer and the merchant that specifies pricing, procedures, and rules of the acquiring service provided. Once a Merchant Agreement has been signed, the business must be set up with the appropriate equipment for card acceptance, as well as the proper information in the authorization and clearing records.

In this chapter, you’ll find the Visa requirements and recommendations for developing Merchant Agreements. It also offers a few practical suggestions for new merchant start-up.

WHAT’S COVERED

- Looking at the Merchant Agreement from a Risk Perspective
- Merchant Agreement Provisions
- Recommended Agreement Provisions
- Tri-Party Agreements
Looking at the Merchant Agreement from a Risk Perspective

An Acquirer’s Merchant Agreement should be designed from a risk perspective to:

- Reduce the institution’s exposure to fraud and business failure losses to the greatest extent allowable by law.
- Ensure the agreement makes clear the circumstances under which the Acquirer has the right of termination. These can include changes in ownership or any activity that (in the Acquirer’s opinion) might indicate increased risk of credit/fraud loss.
- Confirm any right of the Acquirer to hold funds.
- Guarantee the safe and sound operation of merchant activities.
- Include provisions that add protection against fraud and credit losses beyond the minimum requirements stated in the Visa U.S.A. Inc. Operating Regulations.
- Outline all regulatory issues.
- Require the merchant to comply with applicable Visa U.S.A. Inc. Operating Regulations.

The Merchant Agreement must indicate that the Member is a principal party to the contract and that the merchant acceptance of Visa products is extended by the Member. Visa payment system acceptance is the role of the Member, not the Agent. Members are responsible for all merchant relationships that access the payment system through their licensed Bank Identification Numbers (BINs). Visa recognizes that Agents often perform other functions for merchants they solicit on behalf of a Member. However, in allowing the Agent to perform these services, the Agent must never be promoted above the Member in the eyes of the merchant.
Merchant Agreement Provisions

A Merchant Agreement must include the substance of the following provisions. It is important to note the list of provisions presented here may be comprehensive in scope, but is not all inclusive.

<table>
<thead>
<tr>
<th>AREA:</th>
<th>PROVISIONS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>• Merchants must not disclose cardholder account information to third-parties, except when needed to complete a transaction or when required by law.</td>
</tr>
<tr>
<td></td>
<td>• All merchants, merchant servicers and third-party service organizations that transmit, store, or process cardholder data for the merchant must be compliant with the Cardholder Information Security Program (CISP).</td>
</tr>
<tr>
<td></td>
<td>• Merchants must store all material containing account numbers—whether on paper or electronically—in a secure area accessible only to selected personnel.</td>
</tr>
<tr>
<td></td>
<td>• The merchants’ disposal procedures must also ensure security; materials containing account information must be made unreadable before they are discarded.</td>
</tr>
<tr>
<td></td>
<td>• Merchants must not retain or store Card Verification Value 2 (CVV2) data subsequent to the authorization of a transaction.</td>
</tr>
<tr>
<td></td>
<td>• Merchants (and their merchant servicers, and third-party service organizations) must not retain full-track magnetic-stripe data subsequent to authorization.</td>
</tr>
<tr>
<td></td>
<td>• Merchant contracts with any Merchant Servicer must contain CISP requirements.</td>
</tr>
<tr>
<td></td>
<td>• Merchants must require Merchant Servicers to demonstrate CISP compliance.</td>
</tr>
<tr>
<td>Transaction Deposits</td>
<td>• A merchant must deposit only transaction receipts that directly result from cardholder transactions with that merchant. An Internet Payment Service Provider (IPSP), however, may deposit transaction receipts on behalf of a Sponsored Merchant.</td>
</tr>
<tr>
<td></td>
<td>• A merchant or IPSP must not deposit a transaction receipt until it:</td>
</tr>
<tr>
<td></td>
<td>• Completes the transaction,</td>
</tr>
<tr>
<td></td>
<td>• Ships or provides goods,</td>
</tr>
<tr>
<td></td>
<td>• Performs the purchased service, or</td>
</tr>
<tr>
<td></td>
<td>• Obtains the cardholder’s consent for a recurring transaction.</td>
</tr>
<tr>
<td>Anti-Laundering</td>
<td>A Merchant must not deposit a transaction receipt that does not result from an act between the cardholder and the merchant or the cardholder and its Sponsored Merchant.</td>
</tr>
<tr>
<td>Split Sales Transaction Receipts</td>
<td>Split sales transaction receipts are not allowed. Specifically, merchants may not use two or more sales transaction receipts for a single transaction to avoid or circumvent authorization limits, or monitoring programs.</td>
</tr>
<tr>
<td>AREA:</td>
<td>PROVISIONS:</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Minimum or Maximum</td>
<td>Merchants are not allowed to set minimum or maximum transaction amounts as a condition of honoring Visa cards.</td>
</tr>
<tr>
<td>Surcharges</td>
<td>Merchants may not impose surcharges on transactions.</td>
</tr>
<tr>
<td>Visa Marks</td>
<td>The Visa logo or mark may only be used on a merchant’s promotion-al materials to indicate that Visa cards are accepted as payment for the business goods and services. The logo and mark may not be used, either directly or indirectly, to imply that Visa endorses a merchant’s goods or services; nor may a merchant refer to Visa when stating eligibility requirements for purchasing its products, services, or memberships.</td>
</tr>
<tr>
<td>Credit Vouchers</td>
<td>Credit vouchers may not be submitted for noncredit transactions.</td>
</tr>
<tr>
<td></td>
<td>A merchant must not:</td>
</tr>
<tr>
<td></td>
<td>• Accept a payment from a card holder for the purpose of depositing funds to the cardholder’s account.</td>
</tr>
<tr>
<td></td>
<td>• Process a credit transaction receipt without having completed a previous retail transaction with the same cardholder.</td>
</tr>
<tr>
<td>Cash Disbursements</td>
<td>• Disbursements made by merchants who sell travelers cheques or foreign currency are limited to the value of cheques, Visa TravelMoney, or currency sold in a single transaction, plus any applicable commissions.</td>
</tr>
<tr>
<td></td>
<td>• Under no circumstances may a Visa transaction represent collection of a dishonored check.</td>
</tr>
<tr>
<td>Scrip</td>
<td>Merchants may not accept Visa cards for the purchase of scrip.</td>
</tr>
<tr>
<td>Authorization Requirements</td>
<td>Merchants must obtain authorization for transaction amounts above the specified floor limits required by Visa U.S.A.</td>
</tr>
<tr>
<td>Uncertain Cardholder Identification</td>
<td>• If cardholder identification or the card’s validity is uncertain, the merchant must contact its Acquirer for instructions. If the Acquirer asks the merchant to recover the card, the merchant must comply according to established procedures.</td>
</tr>
<tr>
<td></td>
<td>• Merchants are prohibited against requiring additional ID as part of card acceptance.</td>
</tr>
<tr>
<td>Termination of Agreement</td>
<td>The Acquirer reserves the right to terminate the Merchant Agreement for causing harm to the payment system.</td>
</tr>
</tbody>
</table>
**Recommended Agreement Provisions**

While not required by the Visa U.S.A. Inc. *Operating Regulations*, the following provisions can help Acquirers reduce their exposure to fraud and credit risk losses. In all cases, local law should be observed.

<table>
<thead>
<tr>
<th>AREA:</th>
<th>PROVISIONS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to Hold Funds</td>
<td>Payment of funds to the merchant is provisional. The Acquirer has the right to freeze or hold deposits whenever fraudulent activity is suspected.</td>
</tr>
<tr>
<td>Change in Ownership</td>
<td>Merchants must notify the Acquirer of any changes in ownership, such as limited partnership agreements, or any other changes in business practices or sales method—including expected changes in average draft or deposit amount. Specifically, a merchant must notify the Acquirer (and agree in writing) before adding and performing mail order, telephone order, or Internet sales activity and/or making changes to the products or services being sold.</td>
</tr>
<tr>
<td>Secured Interest</td>
<td>The merchant must grant the Acquirer a secured interest in all its assets. This means the Acquirer will be recognized as a legal creditor in case the merchant declares bankruptcy.</td>
</tr>
<tr>
<td>Use of Personal Accounts</td>
<td>Merchants may not use their own merchant accounts for personal Visa card transactions. For example, merchants cannot use their personal Visa cards to withdraw cash.</td>
</tr>
</tbody>
</table>
Tri-Party Agreements

The acquiring Member must be a principal to all Merchant Agreements. Even though tri-party contracts are currently permitted in the Visa system, a Member may not delegate its Visa obligations to a non-member. Whenever a Member engages in a tri-party agreement with an Agent and merchant, a Disclosure Page must be used to clarify and reinforce the Member’s role in the merchant relationship. **Failure to use the Disclosure Page as required will be deemed a serious violation of the Acquirer Risk Program and could be sufficient cause for the imposition of fees or risk reduction conditions.**

<table>
<thead>
<tr>
<th>Tri-Party Agreement Content Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>All tri-party agreements must include a Disclosure Page which contains statements on important Member and Merchant responsibilities. The Disclosure Page is a separate, stand-alone document that contains the following:</td>
</tr>
<tr>
<td>• The Visa Member is a principal party to the Agreement, and is the only entity authorized to offer or extend Visa products or services to the merchant.</td>
</tr>
<tr>
<td>• The Visa Member (Acquirer) is responsible for:</td>
</tr>
<tr>
<td>- Merchant education regarding pertinent <em>Visa U.S.A. Inc. Operating Regulations</em> with which merchants must comply.</td>
</tr>
<tr>
<td>- Settlement funds (and providing these funds to the merchant).</td>
</tr>
<tr>
<td>- All funds held back or in reserve that are derived from settlement.</td>
</tr>
<tr>
<td>• The Visa merchant is responsible for:</td>
</tr>
<tr>
<td>- Ensuring compliance with the cardholder data security and storage requirements.</td>
</tr>
<tr>
<td>- Reviewing and understanding the terms of the Merchant Agreement.</td>
</tr>
<tr>
<td>- Complying with those <em>Visa U.S.A. Inc. Operating Regulations</em> as described in the Merchant agreement.</td>
</tr>
</tbody>
</table>

The Disclosure Page must also contain a contact address and phone number for the Member, along with an explanation that the Member is primarily responsible for the merchant relationship and may be contacted at any time and for any reason. In addition, the Disclosure Page must include the following items, which must be completed:

- Merchant’s printed name
- Position of the individual signing the document
- Business address/Phone number
- Agent name/Salesperson’s name

Acquiring Members must ensure the merchant understands that the Acquirer has complete responsibility for the merchant relationship and is available to assist when needed.
The Disclosure Page must be dated and signed by the Principal owner or senior authorized officer of the merchant at the time of solicitation to indicate they have received and reviewed the document. A copy of the executed Disclosure Page must be provided to the merchant at the time that it is signed, and must be maintained by the Member in the merchant’s file as a part of the required due diligence. The merchant is also required to retain a copy of the Disclosure Page.
To increase profitability and reduce fraud losses, Acquirers and/or their Agents must ensure that proper card acceptance procedures are being followed by all merchants in their daily business. Collectively, these procedures, outlined in the *Visa U.S.A. Inc. Operating Regulations*, serve as a critical tool for loss reduction at the point of sale.

**WHAT’S COVERED**

- Prohibited Merchant Activities
- Point-of-Sale Requirements
- Merchant Web Site Requirements
- Internet Payment Service Provider (IPSP) Requirements
- New Merchant Start-up and Preparation
Prohibited Merchant Activities

The list of prohibited activities presented here is not all inclusive.

**Point-of-Sale Transactions**

- A merchant must **not**:
  - Accept cardholder payments for previous Visa card, Electron card or Visa Electron card charges incurred at the Merchant location.
  - Establish a minimum or maximum transaction amount as a condition for honoring a Visa card, Electron card or Visa Electron card.
  - Require a cardholder to complete a postcard or similar device that includes the cardholder’s account number, card expiration date, signature, or any other card account data in plain view when mailed.
  - Add any surcharge to transactions.
  - Add any tax to transactions, unless applicable law expressly requires that a merchant be permitted to impose a tax. Any tax amount, if allowed, must be included in the transaction amount and not collected separately.
  - Request or use an account number of any purpose other than as payment for its goods or services.

**Interchange**

A merchant must **not** enter into Interchange:

- Any transaction receipt for a transaction that was previously charged back to the Acquirer and subsequently returned to the merchant, irrespective of cardholder approval. The merchant may pursue payment from the customer outside the Visa payment system.

**Funds Disbursement**

A merchant must **not**:

- Disburse funds in the form of travelers cheques, in order to allow the cardholder to make a cash purchase of goods or services from the merchant.
- Disburse funds in the form of cash, unless the merchant is dispensing funds in the form of travelers cheques, Visa TravelMoney cards, or foreign currency. (In this case, the transaction amount is limited to the values of the travelers cheques, Visa TravelMoney card, or foreign currency, plus any commission or fee charged by the merchant).
### Card Acceptance

A merchant must **not** accept:

- A Visa card, Electron card, or Visa Electron card to purchase scrip.
- An Electron card or Visa Electron card for a manual cash disbursement (except in situations involving travelers cheques or foreign currency).
- A Visa TravelMoney card for a manual cash disbursement.
- A card to collect or refinance existing debt that has been deemed uncollectible by the merchant providing the associated goods or services.

### Merchant Disclosure of Information

- Merchants must **not** disclose a cardholder account number, personal information, or other Visa transaction information to third parties, other than:
  - For the sole purpose of completing the transaction,
  - As required by law, or
  - With the permission of the Acquirer or Visa, as specified in the Visa U.S.A. Inc. Operating Regulations.

- In the event of a merchant failure, including bankruptcy, insolvency, or any other suspension of business operations, the merchant must not sell, transfer, or disclose materials that contain cardholder account numbers, personal information, or other Visa transaction information to third-parties. The merchant is required to return this information or provide acceptable proof of destruction of this information to its Acquirer.
Point-of-Sale Requirements

Convenience Fees
A merchant that applies a “convenience fee” must ensure that the fee is a bona fide charge for the use of an alternate payment channel outside of the merchant’s customary channel (e.g. conference fees, utility fees, etc.). The convenience fee must be a flat or fixed amount, regardless of the value of the payment due, and be included as part of the total transaction amount and be:

- **Added only to a non face-to-face transaction.** Mail/Telephone Order (MO/TO) and Internet merchants whose payment channels are exclusively non face-to-face may not impose a convenience fee.
- **Disclosed prior to the completion of the transaction.** The fees must be disclosed as a charge for the alternative payment channel convenience. The cardholder must also be given the opportunity to cancel.
- **Applicable to all forms of payment accepted in the alternative payment channel.**

A convenience fee may only be charged by the merchant that actually provides goods or services to the cardholder. A convenience fee may not be charged by any third party.

A convenience fee may not be added to a recurring transaction.

Discounts
Merchants may offer a discount as a way to get cardholders to use a preferred means of payment. **The discount, however, must be:**

- Clearly disclosed as a discount from the standard price.
- Non-discriminating between a cardholder who pays with a Visa card and someone who pays with a “comparable card” (i.e., any other branded payment card that requires a signature and authorization.)

A merchant may use a cash discount as an inducement for the cardholder to use a means of payment other than a Visa card.

Honor All Cards
Most merchants choose to accept all categories of Visa debit and credit cards. However, U.S. merchants may accept:

- All Visa cards.
- Visa credit and business cards only.
- Visa consumer debit and prepaid cards only.

These acceptance options apply only to cards issued in the United States. Merchants accepting any category of Visa cards must honor all foreign-issued Visa cards presented for payment.
Credit Refunds

If a customer requests a refund for returned merchandise purchased with a Visa card, the merchant must prepare a Visa credit voucher to credit the cardholder's account. To prevent fraudulent transactions, merchants should not:

- Give cash refunds for merchandise purchased with a Visa card.
- Credit refunds to any Visa card other than the card used for the original transaction.

A merchant must not:

- Accept a payment from a cardholder for the purpose of depositing funds to the cardholder’s account.
- Process a credit transaction receipt without having completed a previous retail transaction with the same cardholder.

*Note: Visa does not require a merchant to refund a transaction if its establishment’s merchandise return and exchange policies are clearly disclosed to customers and written on sales receipts as “No Return,” “In-store Credit Only,” or “Exchange Only.”*

A merchant may provide a cash refund or in-store credit if the original transaction was conducted with a pre-paid card that has been discarded.

Deposits

A merchant must deposit only transaction receipts that directly result from cardholder transactions with that merchant. An Internet Payment Service Provider (IPSP), however, may deposit transaction receipts on behalf of a Sponsored Merchant.

A merchant or IPSP must not deposit a transaction receipt until it:

- Completes the transaction,
- Ships or provides the goods,
- Performs the purchased service, or
- Obtains the cardholder consent for a recurring transaction.

*Note: There are some exceptions to the above rule (e.g. delayed deliveries, prepayment of services, etc.). For further information about these exceptions, contact your Acquirer.*

Multiple Transaction Receipts and Partial Payments

A merchant must include the total amount of goods and services purchased at the same time on a single transaction receipt. Split sales transaction receipts are not allowed. Specifically, merchants may not use two or more sales transaction receipts for a single transaction to avoid or circumvent authorization limits or monitoring programs.
Merchant Web Site Requirements

All Internet merchants must meet minimum site content requirements for Visa card payments. These requirements help ensure a satisfactory shopping experience for consumers, as well as minimize cardholder copy requests, disputes, and chargebacks.

- **Web site content must include:**
  - **Complete description of goods or services.**
  - **Customer service contact information, including e-mail address or telephone number.** To improve customer communications, merchants must display a customer service contact telephone number or e-mail address. If a Merchant delivers goods or services internationally, both local and internationally accessible telephone numbers must be included.
  - **Return, refund, and cancellation policy.** This policy must be clearly posted to inform cardholders of their rights and responsibilities (e.g., if the merchant has a limited or no refund policy, this must be clearly disclosed to cardholder on the merchant’s web site before the purchase decision is made to prevent misunderstandings and disputes).
  - **Delivery policy.** Not all merchants are able to support the delivery of goods worldwide and may instead restrict sales to within their own country or to a limited number of countries, based on delivery experience or import and export regulations. Because merchants may sustain a loss when shipped goods fail to arrive, they are entitled to establish their own policies regarding the delivery of goods. However, when a merchant does have restrictions or other special conditions in place, those special conditions must be clearly stated on its web site.
  - **Transaction currency or currencies.** Since the Internet merchant’s customer base is worldwide, it is important that the cardholder be made aware of the transaction currency before proceeding with a purchase. The currency should be clearly stated, including the country name when the name of the unit of currency is not unique.
- **Merchant outlet’s permanent establishment.** The address of the merchant outlet’s permanent establishment (including the merchant outlet country) must be displayed:
  - On the same screen view as the checkout screen used to present the total purchase amount, or
  - Within the sequence of Web pages the cardholder accesses during the checkout process.
- **Export restrictions (if known).**
- **Consumer data privacy policy.**
- **Security method for transmission of payment data.**

- **Additional items that ideally should be included on a merchant’s web site include:**
  - An Internet transaction receipt completed for an Internet transaction that includes the merchant name most recognizable to the cardholder, such as:
    - Merchant “doing business as” name (DBA)
    - Merchant “universal resource locator” (URL)
    - Merchant name used in the VisaNet Clearing Record
  - Identifiers that easily match the web site to the “doing business as” name.
  - Statements that address when credit cards are charged. Merchants should wait until the merchandise has been shipped or service completed before billing the cardholder.
  - Commitments to process orders promptly and send an e-mail confirmation and order summary within one business day of the initial order. Provide up-to-date stock information if item is back-ordered.
  - Commitment to respond to all customer service e-mails and phone calls within two business days.
  - A statement explaining the security controls in place to protect customers.
  - A statement encouraging cardholders to retain a copy of the transaction record.
Internet Payment Service Provider (IPSP) Requirements

Internet Payment Service Provider (IPSPs) that provide Sponsored Merchant acquisition, authorization, payment processing, or monitoring functions must perform such functions according to the Visa U.S.A. Inc. Operating Regulations.

Sponsored Merchant Restrictions

IPSPs are not allowed to provide payment services to the following merchant types:

- Buyers clubs/Membership clubs
- Credit counseling or credit repair services
- Credit protection/Identity theft protection
- Direct marketing—subscription merchants
- Infomercial merchants
- Multi-level marketing businesses
- Outbound telemarketers
- Prepaid phone cards
- Prepaid phone services
- Rebate-based businesses
- “Up-Sell” merchants

These merchant types are classified with Merchant Category Codes (MCCs): 4814, 5962, 5966, 5968, and 5969, and are ineligible for Sponsored Merchant status. A Member, however, may sign a Merchant Agreement directly with these entities. Agents should periodically review this list with their Visa Member as it may be revised.

IPSP Reporting of Sponsored Merchants

An IPSP must provide comprehensive lists (including names of principals and their country of domicile) for all of its Sponsored Merchants and transaction level detail reports to its acquiring Member and upon request to Visa.
CHAPTER EIGHT: VISA RULES FOR MERCHANT CARD ACCEPTANCE

Visa USA Guidelines for Non-Member Agents

© 2004 Visa U.S.A. Inc.

• **IPSP Name.** If the customer accesses an IPSP web site directly (e.g., Toymall.com), the IPSP name may appear alone on the cardholder transaction receipt (e.g., confirmation e-mail or invoice). In this example, the consumer is intentionally shopping at Toymall and expects to be billed by Toymall. The IPSP name must remain obvious to the cardholder during the goods/services selection, and order and payment processes.

Visa will require the Sponsored Merchant’s name to also appear in the clearing record if the IPSP (or some or all of its Sponsored Merchants) generate excessive customer disputes (e.g., qualifies for the Global Merchant Chargeback Monitoring Program or generates excessive copy requests or other indicators as determined by Visa).

• **IPSP Name/Sponsored Merchant Name.** If the customer logs onto a Sponsored Merchant’s website and is then hyperlinked to the IPSP site for payment, the IPSP name may only appear in conjunction with the Sponsored Merchant’s name on the transaction receipt and in the clearing record.

---

**Transaction Processing**

The location of the Sponsored Merchant determines where a transaction takes place, not the country of the IPSP. The merchant country code included in the authorization and clearing records must contain the country code for the Sponsored Merchant.

The Sponsored Merchant must be in the same country as the Acquirer through which the transaction is processed.

**Customer Service**

The IPSP may provide customer service and after-sales support either directly or via its Sponsored Merchants. In either case, the IPSP must take full responsibility for any disputes, credits, or customer service-related issues. An IPSP must not attempt to transfer its financial liability by asking or requiring a cardholder to waive his or her dispute rights.

**Web Site Requirements**

• **Display of Visa Marks.** IPSPs and their Sponsored Merchant web sites must display the Visa marks in accordance with the *Visa U.S.A. Inc. Operating Regulations.*

• **Customer Service Access.** If the customer accesses the IPSP web site directly when placing an order, the customer must be able to access customer service through the IPSP.
New Merchant Start-Up and Preparation

The setting up of a new card-present merchant account should be viewed as a key opportunity to establish clear underwriting practices and standards. To ensure terminal and transaction data security, as well as reduce overall fraud exposure:

- Make sure all POS devices are fully Card Verification Value (CVV) capable and meet Visa U.S.A. Inc. Operating Regulations for suppression of account information on transaction receipts.

- Wherever possible and/or if required, ensure terminals:
  - Read/transmit full magnetic-stripe Track 1 or 2 data; but not display the full track data (i.e., CVV) at any point.
  - Prompt the user to enter the last four digits of the embossed account number (“read and compare”). This is an effective deterrent to counterfeiting.
  - Ensure that software packages and systems do not contain data retention scenarios.

- Educate merchant on card security features, card acceptance, key-entered transaction, Code 10 call, and card recovery procedures.

- Equip merchants with reference materials to aid with card acceptance and fraud prevention.

- Review Visa Cardholder Information Security Program (CISP) requirements with the merchant.
  - Instruct merchants to restrict access to transaction data and limit payment system software to authorized personnel.
  - Instruct merchants to make sure magnetic-stripe data is not retained.
  - Discuss data security issues and the CISP requirements with merchants. Make sure arrangements have been made for verification of CISP compliance.
  - Document that the merchant has received the CISP information, understands the issues, and accepts liability.

- Ensure that merchants do not retain full-track, magnetic-stripe and/or CVV2 data. Once the authorization is processed, magnetic-stripe and/or CVV2 data should no longer exist. Merchants with cardholder registration needs (i.e., car rental, travel agency, etc.) should key, not swipe, account information at the time of registration.

- Conduct terminal/authorization testing prior to your merchant launch.

- Ensure data quality, including merchant name, location, and Merchant Category Code (MCC).

- Review merchant business model to make sure that the merchant’s selling methods are not associated with high chargeback rates (e.g., upselling, free-trial offers, negative renewal options, etc.).

- Ensure Agents that manage merchant relationships are properly trained and knowledgeable regarding Visa U.S.A. Inc. Operating Regulations and risk programs.
When setting up new card-not-present merchants:

- **Establish a clear merchant description for cardholder statements.** Ensure merchant name, telephone number, or URL address appears on the cardholder statement. This will help to help facilitate easier merchant name recognition.

- **Maintain data integrity by ensuring that transactions include merchant name, location, and MCC.**

- **Review the Visa Cardholder Information Security Program (CISP) requirements with the merchant.**
  - Discuss data security issues and the program requirements. Make arrangements for verification of CISP-compliance.
  - Document that the merchant has received the CISP information, understands the issues, and accepts liability.

- **Educate the merchant about the risk exposure and liability associated with accepting Visa cards in the card-not-present environment.**

- **Discuss internal fraud-screening solutions that can be used to identify and block high-risk transactions.** This can include transactions that:
  - Match data stored in your internal negative files.
  - Exceed velocity limits and controls.
  - Generate an AVS mismatch.
  - Match high-risk profiles.

- **Ensure necessary fraud-detection tools are in place prior to merchant activation.** Offer Address Verification Service (AVS) and Card Verification Value 2 (CVV2) support. Also inform all card-not-present merchants that they may qualify transactions at a lower interchange rate by sending AVS.

- **Ensure that merchants do not retain full-track, magnetic-stripe and/or CVV2 data.** Once the authorization is processed, magnetic-stripe and/or CVV2 data should no longer exist. Merchants with cardholder registration needs (i.e., car rental, travel agency, etc.) should key, not swipe, account information at the time of registration.

- **Advise the merchants of available third-party, fraud-screening services.**

- **Clarify and support dynamic currency conversion/multi-currency support activities.**

- **If the merchant is processing recurring transactions, make sure the merchant is well trained in the use of recurring payment indicators.**

- **Review merchant business model to make sure that the merchant’s selling methods are not associated with high chargeback rates (e.g., upselling, free-trial offers, negative renewal options, etc.).**
• **To prevent unwanted chargebacks:**
  - Review the merchant’s terms and conditions to ensure they are not deceptive or misleading.
  - Counsel merchants about the inherent risks of using negative renewal options.
  - Educate the merchant about maintaining adequate customer service staffing to manage customer inquiries and complaints. Good customer service prevents unwanted chargebacks.

**For Internet Merchants:**

• **Ensure that the Merchant Category Code (MCC) reflects the merchant’s principal line of business, rather than placing all Internet merchants into a designated e-Commerce MCC.**
  - Use the MCC to reveal the type of business being transacted and the Electronic Commerce Indicator (ECI) to indicate that a transaction was conducted on the Internet. In order to qualify for certain types of chargeback protection against fraudulent transactions, the merchant must indicate an ECI value of 5 or 6, along with the Cardholder Authentication Verification Value (CAVV) for Verified by Visa transactions. ECI values 7 and 8 do not offer Internet merchant chargeback protection.
  - Do not place Internet merchants in the high-risk telemarketing MCCs unless they meet the definition for high-risk telemarketing merchants as defined in the Visa U.S.A. Inc. Operating Regulations.

• **Notify the Internet merchant of the availability of Verified by Visa.** If an Internet merchant elects to participate in Verified by Visa, ensure that the merchant understands all service requirements as specified in the Visa U.S.A. Inc. Operating Regulations. The Merchant Agreement must include the substance of these requirements.
All Acquirers and/or their non-member Agents must provide merchants and their employees with appropriate card acceptance and fraud-prevention education. This chapter is intended to help you in this effort.

**WHAT'S COVERED**

- Helping Merchants Prevent Fraud
- Transaction Procedures and Fraud Control for Card-Present Merchants
- What to Look For On All Visa Cards
- How Do You Handle an Unsigned Card?
- Making a Code 10 Call
- Fraud Control Tools for the Card-Not-Present Merchant Environment
Helping Merchants Prevent Fraud

Merchants are important partners in minimizing fraud risk. As such, merchant training and ongoing education efforts are vital to ensure that merchant employees understand and continue to follow appropriate card acceptance and data security procedures for all transactions. With this in mind, Members and their Agents should:

• Provide card acceptance, fraud prevention and data security training before new merchant account is opened.
• Ensure that merchants conduct periodic training refresher courses for all sales staff. Fraud awareness sessions should be especially encouraged prior to any seasonal highs in a merchant’s business, when sales volumes and fraud risks are likely to increase.

As part of merchant training and on-the-job support, merchant employees should be provided with quick reference aids and other materials covering key steps and decisions.
Transaction Procedures and Fraud Control for Card-Present Merchants

Whenever a Visa card is present at the time of a transaction, merchants are required to take all reasonable steps to ensure that the card, cardholder, and transaction are legitimate. **Basic card acceptance and fraud control for card-present transactions include the following merchant actions:**

1. Check the Visa card security features to make sure the card is valid and has not been visibly altered in any way.
2. Obtain an authorization and take appropriate action.

<table>
<thead>
<tr>
<th>RESPONSE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Ask the customer to sign the sales receipt.</td>
</tr>
<tr>
<td>Declined</td>
<td>Return the card to customer and ask for another Visa card.</td>
</tr>
<tr>
<td>Call or Call Center</td>
<td>Call your voice authorization center for instructions.</td>
</tr>
<tr>
<td>Pick Up</td>
<td>Keep the card if you can do so peacefully.</td>
</tr>
<tr>
<td>No Match</td>
<td>Swipe the card and re-key the last four digits. If “no match” response appears again, keep the card if you can do so peacefully. Request a Code 10 authorization.</td>
</tr>
</tbody>
</table>

3. Compare card information (i.e., account number or cardholder name) to the POS terminal or sales transaction receipt.
4. Check the cardholder’s signature on the imprinted sales transaction receipt against the signature on the card.
5. Be on the lookout for suspicious behaviors.
6. If you receive an authorization approval, but still suspect fraud, make a Code 10 call.

**Many of these actions are explained in more detail on the following pages.**
What to Look For On All Visa Cards

Front of Card

Compare the printed and embossed numbers. A four-digit number is printed below the first four digits of the embossed account number on all valid cards. These numbers should be identical, and both should begin with a “4.” If the numbers are not identical or the printed number is missing, the card is not valid and should not be accepted.

Place card under an ultraviolet light to see ultraviolet dove. It will be visible on the face of the card.

Check the embossed account number for evenness and clarity. Look closely at the embossed account number for any signs that the card has been flattened and re-embossed. On valid cards, the numbers will be crisp and even; on altered cards, they may have fuzzy edges, or you may be able to see “ghost images” of the original numbers. The last grouping of numbers is embossed into the hologram. Pay special attention to that area, where ghost images are easiest to spot.

Look at the dove design hologram. It should appear three-dimensional, and the dove should seem to “fly” when the card is tilted back and forth. If the dove looks flat or doesn’t move, the card may be counterfeit.

Check the Visa acceptance mark. It should have micro-printing around the border. The fine print is barely readable without magnification.

Look at the “flying V.” The “flying V” is a stylized, embossed V located to the right of the “Good Thru” date on all valid cards. If this character is missing or is not a flying V, the card should not be accepted.

Check the “Good Thru” or “Expires End” date. Make sure the date of the transaction is no later than the date on the card. If the transaction date is after the Good Thru date, the card has expired. In such instances, an authorization request can be called in to your authorization center, or you can ask the customer for a Visa card that is currently valid.
**On the Back of the Card**

Look at the signature panel. An altered signature panel is one of the most common signs of a fraudulent card, and the easiest to spot. On valid cards, the panel contains a pattern of the repeated word “Visa” printed at an angle in blue-and-gold lettering on a white background. Possible indicators that a card has been altered include:

- Signs of scratching or erasure, and the word “Void.”
- White tape or white-out.
- Ghost images or other evidence that a criminal has written over or tampered with the original signature.

The account number and a three-digit code, the **Card Verification Value 2 (CVV2)**, may also be indent printed on the signature panel in reverse italics.
How Do You Handle an Unsigned Card?

Some cardholders believe that it is safer to carry an unsigned card, or instead write “See ID” in place of a signature. Nothing can be further from the truth. **Merchants should be trained to follow these procedures for unsigned Visa cards.**

**If the Signature Panel Is Left Blank...**

- Check the cardholder’s ID. Ask the cardholder for some form of official government identification, such as a driver’s license or passport before you complete the transaction.
- Ask the customer to sign the card. The card should be signed within your full view, and the signature checked against the customer’s signature on the ID. A refusal to sign means the card is still invalid and cannot be accepted. Ask the customer for another signed Visa card.
- Compare the signature on the card to the signature on the ID.

**If You Have a “See ID” In Place of Signature...**

- Politely explain that “See ID” is not a valid substitute for a signature.
- Ask the cardholder to sign the card (over the “See ID”) in your presence.
- Some cardholders write “See ID” or “Ask for ID” in the signature panel because they think that this is a deterrent against fraud or forgery. In reality, criminals don’t take the time to practice signatures; they use cards as quickly as possible after theft and prior to the accounts’ being blocked. The criminals are actually counting on the merchant to process the transaction without checking the back of the card.
Making a Code 10 Call

If a merchant receives an electronic authorization, but still suspect fraud, the merchant should:

✔ Keep the card in hand to respond quickly to questions.
✔ Call its voice authorization center.

*The call will first be received by the Acquirer who may need to ask for some merchant and/or transaction details. The merchant will then be transferred to the card Issuer and immediately connected to a special operator. A series of yes/no questions will be asked to determine whether the merchant is suspicious of the card or cardholder.*

✔ When connected to the special operator, the merchant should answer all questions calmly in a normal tone of voice, and follow all operator instructions.

✔ If the operator asks the merchant to retain the card, the merchant should comply with this request only if it is safe to do so.

**If the merchant receives a “pick-up” response or is instructed to recover the card during a Code 10 call, the merchant should:**

✔ Comply only if it is safe to do so.
✔ Tell the cardholder they have been instructed to keep the card and that he or she may call the Issuer for more information.
✔ Remain calm and courteous. If the cardholder becomes threatening, return the card immediately.

**After a card has been recovered; the merchant should:**

✔ Notify their bank that they have recovered a card and ask for further instructions.
✔ Cut the card horizontally, being careful not to damage the dove hologram, the embossed account number, or magnetic stripe.
✔ Send the card pieces directly to their bank.
Fraud Control Tools for
The Card-Not-Present Merchant Environment

Unlike merchants who operate in the physical world, card-not-present merchants do not have face-to-face contact, a card in hand, or an actual signature. To the greatest extent possible, they need to use fraud-prevention controls and tools to validate the cardholder’s identity. Here is a brief look at the Visa tools that can be used by mail order/telephone order (MO/TO) and Internet merchants to verify the legitimacy of the Visa cardholder and card.

**Asking for the Card Expiration Date** When possible, card-not-present merchants should ask customers for the card expiration, or Good Thru, date. Including the date in your authorization request helps to verify that the card and transaction are legitimate. A MO/TO or Internet order containing an invalid or missing expiration date can be an indicator that the person on the other end does not have the actual card in hand.

**Asking for CVV2** CVV2 is an important security feature for merchants who accept Visa cards as payment over the telephone and/or online. Located on the back of all Visa cards, the CVV2 consists of the last three digits printed on the signature panel.

In the card-not-present sales environment, CVV2 is an excellent tool for verifying that the customer has a legitimate Visa card in hand at the time of the order.

**Using AVS** AVS is an effective risk management tool for card-not-present merchants. It increases authorization effectiveness by allowing an Issuer to verify the billing address of a customer presenting a Visa card for payment. The merchant submits the address with the transaction authorization request and receives a result code indicating whether the address given by the cardholder matches—exactly, partially, or not at all—with the address in the Issuer’s file. A partial or no-match response may indicate fraud risk.
**Using Verified by Visa**

Verified by Visa is an online system designed to make Internet purchase transactions safer by authenticating a cardholder’s identity at the time of purchase. Verified by Visa enables Issuers to validate the identity of their registered Visa cardholders during online payment transactions. The service software installed at the merchant’s site activates the cardholder interface during the authentication process.

**How Verified by Visa Works**

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

2. A Verified by Visa window appears. The cardholder is prompted to enter the password he or she created when registering for the service.

3. The Issuer validates the cardholder’s identity and sends a response to the merchant to proceed with the payment authorization. The consumer is returned to the merchant purchase confirmation screen.

The key requirements necessary for Verified by Visa authentications are summarized below:

**Issuers** participating in Verified by Visa support the ability to authenticate cardholders during online purchases using an Access Control Server (ACS). An Issuer may operate an ACS itself or contract with an ACS Processor. The Issuer ACS processes authentication transactions received from participating merchants.

**Cardholders** must have access to a PC with browser and Internet connectivity. Cardholders enter identity information or a Verified by Visa password during online purchases to confirm their identity as authorized users.

**Acquirers and merchant/gateway Processors** assist merchants in meeting VisaNet transaction processing standards for the inclusion of authentication-related data in authorization and settlement transactions.

**Merchants** offering Verified by Visa to their customers incorporate a software module called a Merchant Plug-in (MPI), as part of their commerce server application.
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquirer</strong></td>
</tr>
<tr>
<td><strong>Address Verification Service (AVS)</strong></td>
</tr>
<tr>
<td><strong>Agent</strong></td>
</tr>
<tr>
<td><strong>Agent Registration Program</strong></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td><strong>Authorization</strong></td>
</tr>
<tr>
<td><strong>Authorization Center</strong></td>
</tr>
<tr>
<td><strong>Bankcard</strong></td>
</tr>
<tr>
<td><strong>Bank Identification Number (BIN)</strong></td>
</tr>
<tr>
<td><strong>BASE I</strong></td>
</tr>
</tbody>
</table>
**BASE II**
BASE II provides global electronic processing of clearing and settlement transactions. Operating six days a week, the system collects and distributes financial and non-financial information and reports between members. It also calculates fees, charges, and settlement totals and produces reports to help reconciliation.

**Card-Not-Present**
A sales environment where transactions occur without a valid Visa card being present at the merchant location. Card-not-present is used to refer to mail order/telephone order merchants and sales environments, as well as transactions over the Internet.

**Card-Present**
A sales environment where a transaction can be completed only if both a valid Visa card and cardholder are present at the merchant location and the sale is processed by an individual representing the merchant or Acquirer. Card-present transactions include face-to-face retail sales and cash disbursements.

**Card Security Features**
Alphanumeric, pictorial, and other design and functional elements on Visa cards. The exact physical dimensions and placement of these features are specified by the Visa U.S.A. Inc. Operating Regulations and are difficult to copy exactly. Card security features are checked by merchants at the Point-of-Sale to ensure the card is valid.

**Card Verification Value (CVV)**
A unique three-digit “check number” encoded on the magnetic-stripe of all cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe-encoded account information and is verified online at the same time a transaction is authorized.

**Card Verification Value 2 (CVV2)**
A unique three digit “check number” indent printed on the signature panel of all cards. The number is calculated by applying an algorithm, and is used by mail order/telephone order and Internet merchants to verify the user.

**Cardholder**
The person or entity to whom a card is issued.

**Chargeback**
A formal process that allows an Issuer to charge the amount of sale back to the Acquirer, because the Acquirer or merchant has not complied with requirements for a Visa transaction.

**Code 10**
The term used by merchants or Acquirers when they call an authorization center to let the center know they are suspicious of a card, cardholder, or transaction. Code 10 calls are generally switched directly to Issuers for special handling.

**Compromise**
In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).
**Cryptographic key**  A parameter used in conjunction with a cryptographic algorithm that determines:

- The transformation of plaintext data into ciphertext data,
- The transformation of ciphertext data into plaintext data,
- A digital signature computed from data,
- The verification of a digital signature computed from data,
- An authentication code computed from data, or
- An exchange agreement of a shared secret.

**Data Encryption Algorithm (DEA)**  A published encryption algorithm used to protect critical information by enciphering data based upon a variable secret key. The Data Encryption Algorithm is defined in ANSI X3.92: “Data Encryption Algorithm” for encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly.

**DES**  Data Encryption Standard. The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm. (See Data Encryption Algorithm.)

**Draft**  See “Sales Transaction Receipt.”

**Embossed Number**  The 16-digit account number that appears in raised print on the front of most Visa cards. The embossed number is one of the card security features that should be checked by merchants to ensure that a card-present transaction is valid.

**Exception File**  Visa’s worldwide data base of account numbers of lost/stolen or other cards Issuers have listed for pickup, referral, or other special handling. The account numbers for all transactions routed to Visa’s stand-in processing system are checked against the Exception File.

**Expired Card**  A card on which the expiration date embossed and/or encoded by the Issuer has passed.

**Face-to-Face Transactions**  Transactions in which both the cardholder and the card are present at the point of sale.

**Floor Limit**  A dollar amount established for a single transaction over which authorization must be obtained by the merchant from its authorizing Member. In the United States, floor limits are only used by paper-based merchants (i.e., those without electronic terminals that automatically authorize all transactions).

**High-Risk Internet Payment Service Proficed (HRIPSP)**  An Internet Payment Service Provider that:

- Enters into a contract with an Acquirer to provide payment services to Sponsored Merchants and
- Includes one or more Sponsored Merchants required to be classified with Merchant Category Code 5967 (Direct Marketing—Inbound Teleservice Merchant) in its Sponsored Merchant portfolio.
| **Independent Sales Organization (ISO)** | An organization that is not a Member and whose bankcard-related business relationship with a Member involves any of the following:  
- Merchant solicitation, sales, or services  
- Merchant transaction processing solicitation  
- Cardholder solicitation or card application processing services |
<p>| <strong>Interchange</strong> | The exchange of clearing records between Members. |
| <strong>Internet Payment Service Provider (IPSP)</strong> | An online entity that contracts with an Acquirer to provide payment services to Sponsored Merchants. |
| <strong>Issuer</strong> | A financial institution that issues Visa cards. |
| <strong>Key encrypting (encipherment or exchange) key</strong> | A cryptographic key that is used for the encryption or decryption of other keys. |
| <strong>Key loading</strong> | Process by which a key is manually or electronically transferred into a secure cryptographic device. |
| <strong>Key loading device</strong> | A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module. |
| <strong>Key management</strong> | The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving. |
| <strong>Magnetic Stripe (Mag Stripe)</strong> | A strip of magnetic tape on the back of all bankcards. The stripe is encoded with identifying account information as specified in the Visa U.S.A. Inc. Operating Regulations. On a valid card, the account information on the magnetic-stripe matches similar embossed or printed information on the front of the card. |
| <strong>Mail Order/Telephone Order Merchant (MO/TO)</strong> | Businesses where the primary or a major source of income comes from merchandise or services sold by mail or telephone. |
| <strong>Member</strong> | An organization which is a Member of Visa and which issues cards and/or signs merchants. |
| <strong>Merchant</strong> | A principal or entity entering into a card acceptance agreement with a Visa Member financial institution. |
| <strong>Merchant Agreement</strong> | A contract between a Merchant and an Acquirer containing their respective rights, duties, and obligations for participation in the Acquirer’s Visa or Visa Electron Program. |
| <strong>Merchant Bank</strong> | See “Acquirer.” |</p>
<table>
<thead>
<tr>
<th><strong>Merchant Category Code (MCC)</strong></th>
<th>A code assigned by an Acquirer to a merchant to identify the merchant’s principal trade, profession, or line of business.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Identification Number (PIN)</strong></td>
<td>An alphabetic and/or numeric code which may be used as a means of cardholder identification.</td>
</tr>
<tr>
<td><strong>PIN Entry Device (PED)</strong></td>
<td>A keypad, laid out in a prescribed format, combined with electronic components housed in a tamper resistant or tamper evident shell that can capture and encrypt cardholder PINs.</td>
</tr>
<tr>
<td><strong>Point-of-Sale (POS)</strong></td>
<td>The location at which the sale/transaction takes place.</td>
</tr>
<tr>
<td><strong>Recurring Transaction</strong></td>
<td>A transaction for which written permission has been granted by a cardholder to a merchant to periodically charge the cardholder’s account for recurring goods or services. Examples include periodic membership fees (such as for a health club), magazine subscription renewals, and insurance premiums.</td>
</tr>
<tr>
<td><strong>Referral Messages</strong></td>
<td>A “call” or “call center” response to a merchant’s or Member’s request for an authorization. A referral message indicates that the Issuer needs more information about the transaction or cardholder before an approval can be issued.</td>
</tr>
<tr>
<td><strong>Sales Transaction Receipt</strong></td>
<td>A paper or electronic record of a sale, rental or service which the merchant presents to the bank for processing. The cardholder’s card account can then be debited and the merchant account may be credited. (also referred to as draft or sales draft).</td>
</tr>
<tr>
<td><strong>Settlement</strong></td>
<td>The reporting and transfer of settlement amounts owed by one Member to another, or to Visa, as a result of clearing.</td>
</tr>
<tr>
<td><strong>Sponsored Merchant</strong></td>
<td>An electronic commerce merchant that contracts with an Internet Payment Service Provider (IPSP). The IPSP performs some or all of the Sponsored Merchant’s payment-related operations on its behalf. The Sponsored Merchant must meet all card acceptance requirements in the Visa U.S.A. Inc. Operating Regulations, with the single exception that it may have a contract with an IPSP, rather than an Acquirer.</td>
</tr>
<tr>
<td><strong>Stand-In Processing (STIP)</strong></td>
<td>Visa’s on-line authorization processing system that responds to merchants’ requests for transaction authorization when Issuers are unable to respond or when they have chosen to let Visa process certain transactions.</td>
</tr>
</tbody>
</table>
| **Third-Party Service Provider (TPSP)** | An organization that:  
  • Is not a Member of Visa USA  
  • Is not directly connected to VisaNet  
  • Provides response processing for Visa Members related to program solicitations, transaction processing, data capture, and/or other administrative functions, such as chargeback processing, risk/security reporting, and customer service. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction</strong></td>
<td>The act between the cardholder and merchant or cardholder and financial institution which results in the sale of goods, services, or a cash disbursement involving a Visa card.</td>
</tr>
<tr>
<td><strong>Triple Data Encryption Algorithm (TDEA)</strong></td>
<td>The algorithm specified in ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.</td>
</tr>
<tr>
<td><strong>Triple Data Encryption Standard (TDES)</strong></td>
<td>See Triple Data Encryption Algorithm.</td>
</tr>
<tr>
<td><strong>Triple-length key</strong></td>
<td>A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.</td>
</tr>
<tr>
<td><strong>TRSM</strong></td>
<td>Tamper-Resistant Security Module. The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.</td>
</tr>
<tr>
<td><strong>Verified by Visa (VbV)</strong></td>
<td>A service that validates a cardholder’s ownership of an account in real time during an online Visa card transaction. When the cardholder clicks “buy” at the checkout of a participating merchant, the merchant server recognizes the registered Visa card and the “Verified by Visa” screen automatically appears on the cardholder’s desktop. The cardholder enters a password to verify his or her identity and the Visa card. The Issuer then confirms the cardholder’s identity.</td>
</tr>
<tr>
<td><strong>Visa Cardholder Information Security Program (CISP)</strong></td>
<td>A Visa U.S.A. Inc. program that provides Acquirers, merchants, and their Agents with requirements for handling, storing, and protecting Visa account and transaction data.</td>
</tr>
<tr>
<td><strong>VisaNet</strong></td>
<td>The data processing systems, networks and operations which are used to support and deliver authorization services, exception file services, clearing and settlement services and any other services.</td>
</tr>
<tr>
<td><strong>Voice Authorization Center</strong></td>
<td>An authorization center operated either by Issuers or by Processors on behalf of Issuers.</td>
</tr>
<tr>
<td></td>
<td>It is used to respond to requests for authorizations for purchases from merchants who do not have terminals, or whose terminals are not functioning properly, or for transactions for which special assistance is required.</td>
</tr>
</tbody>
</table>