Visa Global Acquirer Risk Standards

Visa Supplemental Requirements

1 October 2018

Visa Public

Important Information on Confidentiality and Copyright

Note: This document is a supplement of the *Visa Core Rules and Visa Product and Service Rules.* In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the *Visa Core Rules and Visa Product and Service Rules*, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

Contents

1 About This Guide

The obligation to manage and monitor merchant and third party agent (TPA or agent) relationships has been a long-standing Visa client responsibility. The *Visa Core Rules and Visa Product and Service Rules* (hereafter collectively referred to as the "Visa Rules") place responsibility for merchant and agent oversight and any losses caused by either entity on the acquirer. The Visa Global Acquirer Risk Standards (GARS) were developed to provide acquirers with a set of risk controls to aid in protecting their institutions and the Visa payment system from undue financial harm or reputational damage. **The *Visa Global Acquirer Risk Standards* guide is a 'Visa Supplemental Requirements' document and thus an extension of the Visa Rules.**

1.1 Guide Purpose

The *Visa Global Acquirer Risk Standards* guide is designed to help acquirers:

- Understand their accountabilities and responsibilities to the Visa payment system;
- Manage and control their relationships with merchants and third party agents;
- Ensure day-to-day operations and practices are in compliance with the *Visa Global Acquirer Risk Standards and the Visa Rules*.

This guide should be used in conjunction with the Visa Rules. Please refer to the latest version of the Visa Rules for a full list of requirements.

Authorized Push Payments: Acquirers signing merchants for Authorized Push Payments (APP) must comply with the underwriting standards as outlined in the *Visa Authorized Push Payments Underwriting Standards guide* in lieu of the underwriting standards in this guide. Merchants signing up for traditional pull payments, in addition to push payments, are subject to the underwriting standards outlined in this guide.

Important note: All acquirers must comply with the requirements specified in the *Visa Global Acquirer Risk Standards* guide, except where otherwise restricted by local law. Where there is a conflict between the information provided in this guide and the *Visa Core Rules and Visa Product and Service Rules* ("Visa Rules"), the requirements provided by the Visa Rules take precedence.

1.2 How This Guide Is Organized

The *Visa Global Acquirer Risk Standards* guide is organized as follows:

- **Section 1: About this Guide** explains the rationale for the Visa Global Acquirer Risk Standards.
- **Section 2: Visa Global Acquirer Risk Standards Overview** highlights the acquirer's key risk responsibilities and accountabilities when managing merchant and third party agent relationships.

- **Section 3: Acquirer Policy Framework** outlines the policies an acquirer must have in place to mitigate risks that may impact the Visa payment system.
- **Section 4: Merchant Agreement** focuses on minimum requirements that acquirers must meet when developing and using merchant agreements.
- **Section 5: Merchant Underwriting and Onboarding** defines essential elements to be included in an acquirer's merchant underwriting and onboarding process.
- **Section 6: Reserves and Merchant Funding** describes the acquirer's requirements for holding and controlling merchant reserves and settlement funds.
- **Section 7: Merchant Risk Monitoring** identifies the necessary controls to adequately monitor merchant payment processing activity.
- **Section 8: Managing Third Party Agent Risk** outlines an acquirer's responsibility to provide adequate oversight of its sponsored agents to ensure they follow policies and procedures required to comply with the Visa Rules.
- **Section 9: Use of Payment Facilitators, Staged Digital Wallet Operators (SDWOs) and Marketplaces** describes actions an acquirer must take to mitigate risks presented by payment facilitators, SDWOs and marketplaces.

The Appendices contain important supplemental information. The contents are organized as follows:

- **Appendix A – Acquirer Policy Guidelines** contains recommended minimum policy content to help acquirers ensure their merchants and agents comply with applicable Visa Rules.
- **Appendix B – Disclosure Page** provides a sample copy of the disclosure page that must be included if an agent is a party to an agreement between the acquirer and the merchant.
- **Appendix C – GARS Assessment Questionnaire** provides a checklist to assist the acquirer in maintaining compliance with the minimum risk standards specified by Visa.

A **Glossary** has not been included at the end of this guide, however a comprehensive glossary is available in the *Visa Core Rules and Visa Product and Service Rules*, which can be accessed via Visa Online.

Note: Throughout this guide, an orange checkbox (☑) indicates a requirement and a blue checkbox (☑) indicates a best practice.

2 Visa Global Acquirer Risk Standards Overview

The Visa Global Acquirer Risk Standards protect the Visa payment system and support the safety and soundness of Visa acquirers by clarifying responsibilities for managing merchant and third party agent relationships.

2.1 Acquirer Risk Responsibilities

All acquirers in the Visa payment system must ensure their operations comply with the Visa Rules and the risk standards detailed in this guide.

Key acquirer risk responsibilities identified by Visa include the following:

Area:	Requirements:
Policies	• Implement policies that include the minimum standards established by Visa to mitigate risk to the Visa payment system. • The policies must be approved by the acquirer's Board of Directors or an appropriate senior executive committee. • Policies must be made available to Visa upon request.
Merchant Agreements	• Utilize merchant agreements that meet Visa minimum requirements for disclosure and clearly define both acquirer and merchant obligations. • Ensure merchant agreements in use by the acquirer and third party agents, including subsequent updates, are reviewed and approved prior to their use. • Have a merchant agreement in place with each merchant before transaction services are provided.
Merchant Underwriting	• Control merchant approvals per pre-determined policies and procedures. • Provide Visa acceptance privileges in accordance with the Visa Rules.
Reserves and Funding	• Hold and control all funds related to Visa merchant acceptance, including settlement funds, reserves, suspended settlement, and other funds. • Third party agents are prohibited from direct control over merchant funds and reserves (with the exception of payment facilitators).
Merchant Risk Monitoring	• Maintain adequate risk controls to monitor merchant activity to ensure compliance with the Visa Rules and prevent undue harm to the acquirer and Visa payment system.
Third Party Agent Risk	• Conduct due diligence on all third party agents prior to registration, in accordance with the Visa Third Party Agent Due Diligence Risk Standards. • Perform ongoing monitoring and oversight of third party agents to control the agent relationship and its activities. • Ensure third party agents are aware of the acquirer's policies and requirements to remain in compliance with Visa Rules.

2.2 Control Mechanisms

2.2.1 Compliance and Onsite Reviews

To ensure compliance with the Visa Global Acquirer Risk Standards, acquirers and third party agents may be reviewed as needed on a risk-prioritized basis. Visa may, at its discretion, require that acquirers or agents contract with a Visa-approved firm—or in certain cases with Visa—to perform an onsite review of their operations. Institutions initiating an acquiring program for the first time, or one that does not meet capital requirements, must complete an onsite review within six months of program inception. The purpose of onsite operational reviews is to confirm that acquirers and third party agents maintain sufficient oversight and control over their acquiring operations. The acquirer or agent is responsible for the cost of the review and is accountable for forwarding a copy of the resulting report to Visa. A standardized assessment format, which is included in this guide, has been developed to ensure a consistent framework exists for assessing compliance with the Visa Global Acquirer Risk Standards.

Appendix C contains an onsite review questionnaire that outlines the various items assessed by the Visa-approved reviewer. **Acquirers are encouraged to utilize their own internal audit functions and the questionnaire to routinely self-monitor compliance with the Visa Global Acquirer Risk Standards.**

2.2.2 Remediation Mechanisms

Following the onsite review, a findings report will be developed to identify gaps and corrective actions. The acquirer or agent will respond to the findings with a remediation plan. The reviewer will continue to track the acquirer's or agent's remediation progress and provide periodic updates to Visa. If an acquirer or agent fails to implement an approved remediation plan within the agreed-upon timeframe, Visa may impose Member Risk Reduction Requirements as specified in the Visa Rules.

3 Acquirer Policy Framework

A clearly articulated risk policy framework endorsed by senior management is essential to the operation of a successful acquiring program. A set of well-thought-out written risk policies ensures employees understand management's business objectives and establishes employee expectations and responsibilities, including how exceptions and escalations are to be managed. It is important that employees are educated on the policies that apply to their roles.

3.1 Policy Development

An acquirer must implement written policies to govern the underwriting, monitoring, and control of its merchants and third party agents.

Policy acts as the foundation for a well-managed acquiring program. **Visa mandates that acquirers develop and implement policies that include Visa's minimum policy standards (Appendix A) to mitigate risk exposure to the payment system.** As part of its policy framework, an acquirer must ensure that:

- ☑ Policy exists outlining its acquiring program strategy; including overall risk tolerance (appetite), targeted merchant segments, sales strategy and use of various entities/agents involved and their responsibilities.
- ☑ Policy exists to control underwriting and risk monitoring for its merchants, VisaNet processors and third party agents.
- ☑ A program exists for training employees on the acquirer's policies.
- ☑ Third party agents are provided with, and receive training on, policies applicable to them.

As best practices, an acquirer should ensure:

- ☑ Policies are assigned owners who are responsible for implementation and execution.
- ☑ Policy versions are tracked to ensure only the most recent updates are accessed and distributed.
- ☑ To include key performance indicators and other pertinent reporting standards as part of the institution's acquiring policies designed to keep management informed of important events and risk exceptions.
- ☑ Maintain a central policy depository accessible to policy owners and those governed by policies.
- ☑ Policies are reviewed on an annual basis and updated when necessary.
- ☑ Policies are maintained in electronic format so they can be easily modified to meet an acquirer's changing needs.

3.2 Policy Approval

An acquirer must ensure that all merchant acquiring program and agent management policies are approved by its Board of Directors or an appropriate executive-level committee.

A Board of Directors or executive committee endorsement can assist in increasing awareness and exercising oversight of the risks involved in managing an acquiring program.

3.3 Policy Submission to Visa

An acquirer must provide its written policies to Visa upon request.

The acquirer's policies may be requested and evaluated during a periodic review of the acquirer's operations. Additionally, Visa may request a copy of the acquirer's policies as necessary in conjunction with other compliance efforts. This requirement allows Visa to determine whether an acquirer is adhering to its own policies.

4 Merchant Agreement

A merchant agreement is a legally binding contract establishing mutual obligations of all parties and ensuring merchants operate under the rules and protocols established by Visa and the acquirer; therefore:

- ☑ An acquirer must have a merchant agreement with each of its merchants to accept Visa cards. A payment facilitator must have a merchant agreement with each of its sponsored merchants.
- ☑ An acquirer and a payment facilitator may only accept transactions from a merchant with which it has a valid merchant agreement.

The merchant agreement is an important element of the relationship between the acquirer and the merchant. It should be thorough in providing protection against a merchant's improper use of the payment system, while also establishing obligations that safeguard the merchant. In addition, the merchant agreement must include the minimum provisions stated in the Visa Rules.

4.1 Acquirer Jurisdiction

Acquirers may only execute merchant agreements with payment facilitators, merchants, and sponsored merchants within its licensed acquiring jurisdiction.

An acquirer may only accept transactions from payment facilitators, merchants, and sponsored merchants within the country or countries in which the acquirer is licensed by Visa to operate. Cross-border acquiring, where the payment facilitator, merchant, or sponsored merchant is located outside the acquirer's licensed jurisdiction (and that county's territories and possessions), is not permitted[1].

NA Region: A U.S. acquirer is permitted to accept transactions from a Canadian merchant outlet, and a Canadian acquirer may accept transactions from a U.S. merchant outlet, only for electronic commerce and mail/phone order transactions[2].

4.2 The Role of the Acquirer

The merchant agreement must indicate the acquirer as a principal party to the contract and that merchant acceptance of Visa products is extended by the acquirer.

Granting Visa acceptance to a merchant is the role of the acquirer, not a third party agent. While third party agents play a key role in soliciting and servicing merchants, it is ultimately the acquirer who is responsible for enabling a merchant to access the Visa payment system. Visa recognizes agents perform functions in tandem with, or on behalf of, their sponsoring acquirers. Depending on which functions an agent performs, it is permissible to include the agent as a party to the merchant

[1] Specific exceptions apply; consult the Multinational Merchant Acceptance Program (MMAP) and the Visa Rules for more information.
[2] Consult the Visa Rules for more information.

agreement where applicable. However, adding an agent as a party to the merchant agreement must never promote the agent and its role above the acquirer in the eyes of the merchant.

4.3 Transfer of Merchant Agreements

An acquirer must consent to the assignment or transfer of a merchant agreement to another acquirer.

Acquirers may freely solicit all merchants (subject to any contractual commitment the merchant may have). Individual merchants may also choose to move their relationship from one acquirer to another without obtaining the consent of the acquirer where their current relationship is domiciled. Additionally, agents can freely solicit new merchants for any acquirer that has registered the agent with Visa.

Agents may not transfer or assign multiple merchant relationships (portfolios) from one sponsoring acquirer to another without the express written approval of the acquirer holding the merchant agreement. Ownership of the merchant's Visa transactions rests with the Visa acquirer with whom the merchant has a signed merchant agreement. This ensures that members are aware of, and consent to, an agent's intent to move a group or portfolio of merchants to another acquirer.

4.4 Merchant Agreement Review

An acquirer must implement a policy and procedure for reviewing merchant agreements used by its third party agents.

Acquirers must review and approve all merchant agreements used by their agents, including payment facilitators, to ensure the agreements comply with the minimum content requirements established by Visa. Acquirers that permit an agent to use a merchant agreement that has not been developed by the acquirer must review and approve the document and any subsequent revisions before use to make certain the agreement complies with the acquirer's and Visa's requirements. Additionally, the acquirer should periodically review its agent's merchant agreements, as that can help ensure that the agent does not modify or change any terms contained in the agreement without the acquirer's knowledge and consent.

4.5 Merchant Approvals Prior to Processing

An acquirer must approve a merchant for card acceptance prior to entering any transactions into the Visa payment system for that merchant.

Acquirers must control the approval of all merchants before they allow the merchant to process transactions. Acquirers may use various means to ensure they review and approve all merchants before allowing them to process any Visa transactions:

- ☑ Acquirers may have the merchant application, agreement, and underwriting materials transmitted to its underwriting staff for review and approval prior to activating the merchant.
- ☑ Acquirers may provide their agents with specific criteria that must be met for acquirer approval. This process allows for merchant activation prior to member due diligence review and approval. Acquirers that use this process must ensure they actively monitor their agents and test for compliance with underwriting policies.

Approved merchant agreements must be signed (i.e., executed) by the acquirer by means of a legally acceptable method; agents are not permitted to execute merchant agreements on behalf of the acquirer. The acquirer is required to remain involved with merchant approvals and maintain a system for monitoring policy compliance.

4.6 Merchant Termination

The merchant agreement must include a clause that provides for the immediate termination of a merchant by the acquirer for any activity that may create harm or loss to the goodwill of the Visa payment system.

Acquirers should invoke this clause when a merchant's business practices and exception item activity are such that they create a substantial risk of loss or harm to the Visa payment system. This includes participating in illegal or prohibited activity.

Acquirers should not abdicate their responsibility for terminating a merchant to their agents. In addition to protecting their individual interests, acquirers must make decisions that are in the best interest of the Visa payment system. In turn, agents must make decisions best representing their acquirers and Visa.

4.7 Retention of Merchant Records

An acquirer or a payment facilitator must keep complete, well-documented files containing merchant records, for at least two years after merchant agreement termination.

Merchant records are a central component of maintaining a merchant portfolio. **It is required that an acquirer or payment facilitator maintain files on all its merchants, either in physical or electronic format.**

Merchant records must include the merchant agreement, merchant application, underwriting documentation, and any other records that are pertinent the business relationship with the merchant or sponsored merchant. This must include any information connected to a present or past investigation. **If merchant records are maintained by a payment facilitator or third party agent, the acquirer must be provided with full and unrestricted access to all documentation.** Merchant records must be provided to Visa upon request.

4.8 Information Security Compliance

The merchant agreement must include provisions that ensure merchants and their service providers maintain compliance with applicable PCI DSS and Visa security requirements.

A merchant or sponsored merchant has an obligation to protect transaction information. Acquirers and their agents must educate their merchants on the importance of this contractual obligation and the consequences of failing to adequately protect cardholder and transaction data.

The Payment Card Industry Data Security Standard (PCI DSS) is intended to help protect cardholder data—wherever it is transmitted or resides—ensuring that customers, merchants, and service providers maintain the highest level of information security. It offers a single approach to safeguarding sensitive data for all payment systems.

Merchant agreements must specify that merchants and their service providers with access to cardholder data maintain and demonstrate compliance with the PCI DSS requirements and all subsequent requirement updates.

4.9 Merchants Utilizing Service Providers

The merchant agreement must include a clause that requires the merchant to notify the acquirer of its use of any service provider that will have access to cardholder data.

When merchants utilize service providers—such as a gateway or point-of-sale system integration—for accessing, storing, transmitting, and processing cardholder data, the acquirer must register the service providers as agents (Merchant Servicers). Therefore, the merchant agreement must stipulate that merchants using, or intending to use, a service provider, must:

- ☑ Validate the service providers are certified as compliant with the PCI DSS or a similarly established data security standard.
- ☑ Provide the acquirer with information on any service providers the merchant uses or intends to use.

Acquirers must register applicable service providers as agents and service providers must be registered with each unique acquirer for whose merchants they provide services. Before registering a service provider, the acquirer must validate that the service provider is certified as compliant with PCI DSS (or similar standard). Acquirers should integrate the collecting of service provider information and agent registration as part of its merchant boarding process. **Proper ongoing education and notification (such as statement messages) must be provided to merchants to ensure they understand their obligation to notify their acquirer when they intend to use a service provider**. Acquirers must ensure their merchants only use service providers that are properly registered with Visa.

NA Region only: For point-of-sale application and terminal installation and integration, Visa acquirers must ensure Level 4 merchants use only PCI-certified Qualified Integrator and Reseller (QIR) professionals on the PCI SSC's QIR companies listing available at: www.pcisecuritystandards.org.

Note that single-use terminals without Internet connectivity are considered low risk and may be excluded from these requirements.

4.10 Acquirer Disclosure

An acquirer must ensure each merchant agreement or application includes a disclosure page or disclosure section that identifies the acquirer and its responsibilities when an agent is a party to the agreement.

Tri-party agreements are permitted in the Visa system; however, they may not minimize the importance of the acquirer's relationship with the merchant. If an agent is party to the agreement, the acquirer's responsibilities must be clearly specified.

If an agent is a party to an agreement between the acquirer and the merchant, a disclosure page or disclosure section (see Appendix B) on the merchant application is required to ensure the merchant is aware of the role played by the acquirer. The disclosure page must be signed by the merchant at the time it is solicited by the agent. A copy must be made of the disclosure page or disclosure section on the merchant application, and immediately provided to the merchant. Disclosure page samples have been included in Appendix B for reference.

Payment facilitator merchant agreements used for contracting sponsored merchants are not subject to this requirement.

4.11 Merchant Settlement Responsibility

The merchant agreement must state the acquirer is responsible for providing settlement funds directly to the merchant.

The security and handling of merchant funds is a fundamental acquirer responsibility. This function cannot be delegated to a third party agent or other non-member entity, with the exception of a payment facilitator. Merchants must clearly understand that acquirers have direct responsibility for settlement. They must also be advised that agents are not permitted to directly access or hold merchant funds, whether from settlement or reserves.

This requirement does not prohibit a VisaNet processor or clearing processor from creating a bank transfer file and route funds from Visa, through the acquirer and to the merchant's settlement account.

In the case where a VisaNet processor is also operating as a third party agent, Visa does not grant the processor the right to hold or access a merchant's funds. **If funds cannot be provided directly to the merchant, they must be forwarded to the acquirer.**

4.12 Merchant Agreement Content – Merchant Obligations

An acquirer's merchant agreement must be developed from a risk perspective to ensure the merchant operates under the rules and regulations established by Visa and the acquirer.

The merchant agreement must include the following merchant obligations and requirements:

- ☑ **Laws or Regulations** – Obligations under the merchant agreement must be performed in compliance with applicable laws or regulations.
- ☑ **Compliance with the Visa Rules** – The merchant must comply with the applicable sections of the Visa Rules, including sections regarding use of the Visa-owned marks, Visa acceptance, risk management, transaction processing, and any Visa products, programs, or services in which the merchant is required to, or chooses to, participate.
- ☑ **Employees** – The merchant is responsible for its employees' actions while in its employ.
- ☑ **PCI DSS Compliance** – The merchant must be in compliance with the PCI DSS and have the ability to demonstrate this.
- ☑ **Forensic Investigations** – The merchant, if undergoing a forensic investigation, must fully cooperate with the investigation until completed.

4.13 Merchant Agreement Content – Merchant Prohibitions

An acquirer must specify merchant prohibitions in the merchant agreement as stated in the Visa Rules.

The merchant agreement must specify that a merchant is prohibited from the following:

- ☑ **Previously disputed charges** – Submitting a transaction that was previously disputed and subsequently returned to the merchant. However, the merchant may pursue payment from the customer outside the Visa system.
- ☑ **Illegal transactions** – Submitting any transaction into the payment system that is illegal or that the merchant knows or should have known was illegal. **Transactions must be legal in both the cardholder's and merchant's jurisdiction.**
- ☑ **Fraudulent or unauthorized transaction** – Submitting a transaction into the payment system that the merchant knows or should have known to be either fraudulent or not authorized by the cardholder.
- ☑ **Written cardholder information** – A merchant may not:
  - Require a cardholder to complete a postcard or similar device that includes any of the following in plain view when mailed: the cardholder's account number, card expiration date, signature, or any other card account data.

- Request a Card Verification Value 2 (CVV2) from the cardholder for a card-present environment transaction[3]. EU region: Request the Card Verification Value 2 (CVV2) data on any paper order form.
- Store Card Verification Value 2 (CVV2) information subsequent to authorization.

☑ **Surcharges** – Adding surcharges to transactions, unless explicitly done so in accordance with applicable law, regulations, and Visa Rules specific to the acquirer's region.

- U.S. or U.S. Territory: Surcharges on Visa Credit Card transactions are permitted when carried out in accordance with the Visa Rules.

  Note: Surcharges must not be confused with convenience fees, fees charged on an alternative payment channel outside the merchant's customary payment channel[4].

☑ **Minimum/maximum[5] transaction amount** – U.S. or U.S. Territory: Establishing a minimum or maximum transaction amount as a condition for honoring a Visa Card, except for a transaction conducted with a Visa Credit Card issued in the U.S. or a U.S. Territory.

☑ **Disbursement of funds** – Disbursing funds in the form of cash to a Visa cardholder unless:

- The merchant is participating in Visa Cash-Back Services, a financial institution providing a manual cash disbursement, a hotel or cruise line, as specified in the Visa Rules.
- 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 of fee charged by the merchant.
- South Africa: This does not apply in the CEMEA Region to members in South Africa.

☑ **Travelers cheques** – Disbursing funds in the form of travelers cheques, if the sole purpose is to allow the cardholder to make a cash purchase of goods and services from the merchant.

☑ **Transaction laundering (factoring)** – Accepting a transaction that does not result from an act between the cardholder and the merchant or the cardholder and the sponsored merchant. Payment facilitators may deposit a transaction between the cardholder and a sponsored merchant of the payment facilitator but must not deposit a transaction on behalf of another payment facilitator.

[3] Does not apply in the U.S. to magnetic stripe-read fallback transactions if an agreement is in place between the acquirer and the issuer.
[4] For more information on Convenience Fees, consult the Visa Rules.
[5] U.S. merchants with specific MCCs are permitted to establish maximum transaction amounts with certain restrictions; consult the Visa Rules.

- ☑ **Debt repayment** – Accepting Visa cardholder payments for:
  - Collecting or refinancing existing debt that has been deemed uncollectible by the merchant providing the associated goods or services[6].
  - Previous card charges.
  - A transaction that represents the collection of a dishonored check.
  - United States and EU Region only: Debt repayment is only permitted when performed in compliance with the Visa Rules
- ☑ **Account numbers** – Request or use an account number for any purpose other than as payment for its goods or services.
- ☑ **Adding tax** – 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.

4.14 Additional Merchant Agreement Content

A merchant agreement must specify the contractual requirements as stated in the Visa Rules.

Each merchant agreement must specify:

- ☑ **Transaction terms** – State the terms required to satisfy payment directly to the merchant. This includes, but is not limited to, the name of the financial institution to which the acquirer or sponsored members must deposit funds for payment of Visa transactions.
- ☑ **Right to terminate** – Include the right of Visa to limit or terminate the acquirer's agreement with the merchant or the payment facilitator's agreement with the sponsored merchant.
- ☑ **Differentiation of fees** – Clearly distinguish fees associated with Visa transactions separately from fees associated with other card transactions.
- ☑ **Acquirer disclosure** – Clearly state the acquirer's name and location in a font size consistent with the rest of the merchant agreement printing, and in a manner that makes the acquirer's name readily discernible by the merchant.
- ☑ **Merchant authorization** – Where applicable, obtain the merchant's authorization to research its background including, but not limited to, credit background checks, banking relationships, and financial history.

[6] Consult the Visa U.S. Debt Repayment Program and Visa Rules for additional obligations and eligibility for U.S. merchants engaged in debt repayment transactions.

- ☑ **Provide information to Visa** – Ensure that it has all necessary and appropriate rights under applicable laws or regulations, privacy policies, or agreements to provide merchant information to Visa.
- ☑ **Using competitors**[7] – The acquirer must not prohibit a merchant from using terminal processing services offered by competitors to deliver Visa transactions captured at the point-of-transaction directly to VisaNet for clearing and settlement.
- ☑ **Additional provisions** – A merchant agreement must contain all of these additional provisions:
  - Transaction deposit restrictions, as specified in the Visa Rules
  - Transaction processing prohibitions, as specified in the Visa Rules
  - Prohibit the disclosure of account or Visa transaction information, as specified in the Visa Rules
- ☑ **Use of Third Party Processors** – United States only: A merchant agreement must permit a merchant to designate a third party processor that does not have a direct agreement with the merchant's acquirer as its agent for the direct delivery of transactions to VisaNet for clearing and settlement. The merchant must:
  - Advise the acquirer that it will use a third party processor
  - Agree that the acquirer must reimburse the merchant only for the Visa transactions delivered by that third party processor to VisaNet
  - Assume responsibility for any failure by its third party processor to comply with the Visa Rules

An acquirer may include other provisions in its merchant agreement, provided that the provisions are consistent with the Visa Rules and applicable law.

[7] Only applicable in the United States.

5 Merchant Underwriting and Onboarding

The merchant underwriting process is an important step in managing merchant risk. Whether merchants are solicited directly by the acquirer or through third party agents (such as ISOs and payment facilitators), all merchants must essentially be assessed for risk exposure. **The acquirer is always and solely responsible for the merchants it provides with card acceptance privileges**. If the acquirer allows third party agents to underwrite and board merchants, it is the acquirer that still is ultimately responsible **and it must have a control environment in place to ensure merchant underwriting is carried out in accordance with the policies and procedures set by the bank**.

5.1 Merchant Application

All merchants must be signed up for card acceptance services by means of a merchant application, either paper or electronic.

A well-constructed merchant application is essential to obtaining relevant information about all aspects of a merchant's business. Together with the merchant agreement, the merchant application is a key component of the underwriting package.

5.2 Disclosure of Acquirer Contact Information

The name and contact information of the acquirer must be present on the merchant application and be clear and conspicuous.

Acquirers must ensure their financial institution's name, contact address, phone number, and email address are prominently displayed on the merchant application in a font size that makes this information conspicuous to the reader. **Acquirers are accountable and liable for the actions of their agents.** It is therefore essential that prospective merchants have ready access to the acquirer. Merchants must be able to contact the acquirer at any reasonable time, for any reason.

Acquirers may allow an agent to place its own contact name, phone number, and its logo on the application. This information must not be more prominent than the acquirer contact information and should not discourage the merchant from contacting the acquirer to report service deficiencies. If the agent's logo is present on the merchant application, the acquirer's logo must also be present. For additional acquirer disclosure requirements, see Appendix B.

5.3 Collecting Merchant Information

An acquirer or its agent must request relevant information on the merchant's business background, business model and operations, merchant location(s), and principals who are running the business.

In order to underwrite, validate and authenticate a merchant for card acceptance privileges, pertinent public and non-publicly available merchant information, subject to applicable local data collection laws, must be collected so that a prudent credit decision can be made.

Visa has separated the collection of merchant information into elements that are "required" and elements to be collected as a "best practice."

IMPORTANT: Visa reserves the right to make the collection of "best practice" information elements a requirement for an acquirer, should an acquirer demonstrate lapses in underwriting or risk operations.

5.3.1 Information Elements – Required

Collecting the following information elements from prospective merchants **is required:**

- ☑ **T/A (trading as) or DBA (doing business as) name** – If different from the legal business name, compare the merchant's "doing-business-as" name to its legal name. Some merchants may conduct their daily business activities under one name and apply for legal registration under a different name. If the names are different, it is important to understand the relationships in order to ensure they are valid.

  Note: The merchant name assignment used as the descriptor (on cardholder statements) must be the name used by the merchant to identify itself to its customers to avoid cardholder confusion.

- ☑ **Legal name of business** – Obtain the legal business name as it is filed with government authorities. For a sole proprietor, the information must include the sole proprietor's first and last names.

- ☑ **Registration number** – Collect the merchant business registration number or tax identification number. United States only: This number must be either a Federal Employer Identification Number (FEIN) or Social Security Number (SSN).

- ☑ **Address and telephone number** – Collect the merchant outlet address (including street address, city, state/province and ZIP/postal code) and telephone number (telephone number is not required for sponsored merchants – except Canada).

- ☑ **Legal form of business** – United States only: Merchant's legal business status (for example: corporation, partnership, sole proprietor, nonprofit).

- ☑ **Principal information** – Ask the merchant for the name, address, government identification number, email address, and telephone number of each principal involved in the business. Where applicable under law, collect information on the nationality and residency of the principals.

- ☑ **Ownership information** – Obtain the percentage of ownership held by each principal representing at least material ownership.
- ☑ **Credit background check** – Determine creditworthiness and whether or not merchant or its principals have open or previously filed bankruptcies, or have been registered as having any other credit difficulties now or in the past. If so, find out when. This may provide a good indication of the financial stability of the merchant.

NA Region only:

- ☑ **Merchant MCC** – The merchant's primary and any secondary Merchant Category Code.
- ☑ **Previous termination** – Determine if the merchant has been terminated by an acquirer, the termination date and reason for termination. This may be fulfilled by performing a Terminated Merchant File query.

Please consult the Visa Rules for additional requirements applicable to specific Visa regions.

5.3.2 Information Elements – Best Practice

Acquirers are highly encouraged to collect the following information elements **as a best practice:**

- ☑ **Business license or registration** – Obtain a business license or registration certificate. When appropriate, perform a search with the appropriate business bureaus to verify that the merchant owns or operates a legitimate business. Where possible, validate that the applicant is indeed the principal business owner.
- ☑ **Prior Visa Risk Program identification** – Determine whether the merchant has been previously identified by Visa Risk Program(s). If yes, find out the specific program that identified the merchant and when the identification took place. This provides a good indication of the level of merchant underwriting risk.
- ☑ **Prior processing relationships** – Determine whether the merchant and/or any other principals involved have prior payment processing relationships with acquiring banks. If the merchant was previously terminated by another acquirer, note the reason for termination on the merchant application. Where available and permitted under law, check the merchant and related principals against a terminated merchant file (see Section 5.5 for more details).
- ☑ **Billing terms** – Ask the merchant for its billing terms, if not immediate. For example, does the merchant allow its customers to pay for purchases in monthly installments? Longer service terms (such as annual memberships) carry contingent liability and pose a higher risk to the acquirer.
- ☑ **Return, refund and cancellation policies** – Ask the merchant for details of its return, refund and cancellation policy procedures to ensure the merchant is properly handling returns, refunds and cancellations. The merchant must disclose these policies to the cardholder. It is prudent for the acquirer to obtain a copy of the merchant's standard sales contract (e.g., Terms and Conditions) with the cardholder.

- ☑ **Guarantees and ongoing services** – If the merchant offers guarantees, extended warranties, or other ongoing services, it is prudent to review copies of contracts applicable to such services and determine whether such services are provided by a third party.
- ☑ **Inventory** – Does the merchant's inventory reflect the sales volume disclosed by the merchant? Determine whether the merchant owns or finances its inventory.
- ☑ **Contracts** – Determine whether the merchant has any significant contractual relationships, such as with a manufacturer's agent or exclusive supplier, that may impact the merchant's ability to meet its financial or operational obligations if such a contract is canceled.
- ☑ **Fulfillment** – Does the merchant contract with a fulfillment company to receive orders, package, and ship products to retailers or consumers? If so, verify that such a contract is in place and perform a reference check of the fulfillment company.
- ☑ **Type of environment/location** – Determine the type of business environment of the merchant, such as storefront, office, home-based, mobile, or online. Is the merchant environment or location suitable for the type of merchant? Is the merchant location in a geographic area that has demonstrated excessive levels of fraudulent activity? Underwriters can use search engines to cross-reference businesses to street locations and online maps/street views to obtain a visual on merchant locations.
- ☑ **Time at location** – Ask the merchant how long the business has operated at the present location.
- ☑ **Merchant history** – Establish how long the merchant has been in business. In the event the current principal(s) has/have not owned the business since inception, find out how long the current principal(s) has/have owned the business. New businesses frequently fail within the first few years of operation. If the business is a "start-up," obtain a business plan for merchants requesting higher-tiered processing volume.
- ☑ **Material events** – Examine the merchant's history for any events related to regulator intervention, past and present litigation activity, or data breaches.
- ☑ **Other businesses** – When the merchant is requesting higher processing volumes, ask the merchant to supply information for any other businesses it, or the principals, currently owns or operates, has owned in the past, or in which it is involved as a director.

5.4 Merchant Qualification Standards

The acquirer, payment facilitator, SDWO or marketplace must determine whether a merchant meets minimum qualification standards as part of its underwriting process.

Before entering into a merchant agreement, an acquirer, payment facilitator, SDWO or marketplace must ensure that the prospective merchant or sponsored merchant meets the following Visa qualification standards at a minimum:

- ☑ **Illegal activity** – The merchant will not submit any transactions that are illegal into the Visa payment system. A transaction must be legal in both the cardholder's jurisdiction and the merchant outlet's jurisdiction.
- ☑ **Financial responsibility** – The merchant is financially responsible and there is no significant derogatory information about any of the merchant's principals. The acquirer may obtain this information through the following:
  - Credit reports
  - Personal and business financial statements
  - Income tax returns
  - Other information lawfully available to the acquirer
- ☑ **No harm to the payment system** – The merchant is not engaged in any activity that could cause harm to the Visa system or the Visa brand.
- ☑ **Merchant outlet location** – The merchant outlet location must not be misrepresented.

5.5 Query a Terminated Merchant File

Acquirers must query a Terminated Merchant File where available, or an equivalent terminated merchant database, before onboarding a prospective merchant or sponsored merchant.

If a member receives a response indicating a "possible match" against a merchant listed on a Terminated Merchant File, the member must:

- ☑ Verify the merchant identified in the response is the same merchant for whom the inquiry was generated.
- ☑ Contact the listing member directly to determine why the merchant was added to the file.
- ☑ Make its acceptance decision based on further investigation, and use Terminated Merchant File data only as an informational tool in the decision-making process.

5.6 Special Considerations for Card-Absent Merchants

An acquirer must collect and verify additional application information for card-absent merchants.

Merchants processing in a card-absent environment, including MO/TO and recurring billing merchants, must undergo additional due diligence. Acquirers must clearly understand the business model of card-absent merchants and pay extra attention to how cardholders authorize the merchant to charge them. To establish a legitimate business model, the acquirer should ask card-absent merchants for all website URLs and/or mobile device applications used.

Card-absent merchants requesting higher-tiered processing volume should be asked for business plans, samples of merchandise when appropriate, return policy, and copies of all relevant marketing materials, including catalogs, brochures, telemarketing scripts, and advertisements. Additionally, the acquirer must identify the service provider(s) the merchant uses to process, transmit, or store cardholder data and whether the service provider is compliant with the PCI DSS.

5.7 Separate Internet Merchant Application

Acquirers must use a separate merchant application when signing up a brick-and-mortar merchant for ecommerce services.

When signing up a merchant that conducts business face-to-face as well as through an ecommerce channel, acquirers must use separate merchant applications for each business type. This practice can help facilitate the enhanced due diligence related to ecommerce merchants. It also allows for proper verification of the merchant business name and site content, and helps ensure that appropriate merchant descriptors are displayed on cardholder statements.

Processing face-to-face transactions and ecommerce transactions separately provides an easier way to track and report ecommerce processing volume. Additionally, it will be easier to track a merchant's transactions by respective acceptance mode.

5.8 Additional Internet Merchant Application Information

Acquirers must collect and verify additional application data for internet merchants.

Mitigate potential risk exposure by taking a few extra steps during the application process to obtain additional information from ecommerce merchants. Required data must include:

- ☑ **URLs** – A listing of URLs used by the merchant to promote its business, sell products, and accept payments.
- ☑ **Website/domain ownership** – Verify that the merchant is the registered owner of these domains and websites.

Also recommended as a best practice is the collection of the following information:

- ☑ **Customer service** – Obtain information that describes the merchant's customer service experience, primarily how customers contact the merchant and the type of support that is offered (live person, automated, online support, etc.). Ensure customer service information is clearly displayed. It is helpful to call the merchant's customer service number and find out whether the merchant is legitimate, sells the goods and services represented in the merchant application, and is responsive to inquiries. An email message can also be sent to verify the merchant's email address is legitimate and actually monitored by the merchant. It is important to know the quality and timeliness of the merchant's customer service, as high performance levels will decrease the likelihood of disputes.
- ☑ **Outbound links** – Review descriptions of any links on the merchant's website to other sites with which they may or may not be affiliated. If the external links do not make sense or represent restricted or prohibited merchant types, it should raise a red flag.
- ☑ **Affiliate marketing** – If the merchant uses affiliates as part of its marketing efforts, have the merchant provide a report listing the names and activity of those affiliates.
- ☑ **Terms and conditions** – If goods or services are sold via the Internet, ensure that the merchant's terms and conditions are posted online and find out how and when a cardholder agrees to them. Also review any privacy policy the merchant has posted online.
- ☑ **Mobile device applications** – If goods or services are sold via mobile device applications, ensure such transactions are regarded as internet sales and reviewed according to this section.

5.9 Free Trial Period Merchants

Acquirers must have specific procedures in place in order to underwrite an ecommerce merchant offering free trial periods.

When underwriting an ecommerce merchant that uses free trial periods for a particular product or service, after which the terms or cost of a product and service changes and customers are thereafter charged on a recurring basis, an acquirer must develop standard practices to:

- ☑ Ensure merchants and sponsored merchants clearly disclose the terms and conditions of the free trial promotion, including:
  - Clear disclosure the cardholder will be charged unless the cardholder expressly cancels the before the trial period expires
  - The date or time period after which any charges will commence
  - Clear and simple steps to be taken by the cardholder to cancel the transaction prior to the end of the trial period
  - Clear instructions and policy for returning products and obtaining refunds
  - General cancellation policy
- ☑ Review merchants using trial periods during underwriting, and periodically thereafter, to ensure no deceptive or misleading sales and marketing practices are used.

- ☑ Periodically monitor free-trial merchant dispute rates (disputes and credit vouchers/returns) and complaint board activity as a way to measure the merchant's customer service efforts.
- ☑ Ensure cardholders are notified via email shortly before the trial period ends, in order inform them that their card will imminently be charged unless they take action to cancel the trial.

Merchants using free or discounted trial periods should be managed using a risk-based approach that applies incremental risk management controls and oversight to entities representing heightened risk. Acquirers that fail to properly supervise merchants and agents that abuse free trial periods may be included in Visa's chargeback and fraud monitoring programs and subject to the imposition of Member Risk Reduction Measures.

5.10 Merchant Website Disclosure

A website operated by a merchant, sponsored merchant, payment facilitator, high-brand risk merchant, high-brand risk sponsored merchant, or high-brand risk payment facilitator must contain specific disclosure details.

These include:

- ☑ Visa brand mark in full color to indicate Visa card acceptance, as specified in the Visa Product Brand Standards
- ☑ Legal restrictions (if known)
- ☑ Complete description of the goods or services offered
- ☑ Return/refund policy
- ☑ Customer service contact, including email address or telephone number
- ☑ Address of the merchant's permanent establishment, including the merchant outlet country during the checkout process
- ☑ Transaction currency (e.g., U.S. dollars, Canadian dollars)
- ☑ Export restrictions (if known)
- ☑ Delivery policy
- ☑ Consumer data privacy policy
- ☑ Security capabilities and policy for transmission of payment card details
- ☑ Terms and conditions of a promotion, if restricted

5.11 Control the use of Force Post Transactions

Acquirers and third party agents must control the use of force post transactions.

Effective 26 January 2019: To mitigate potential risk caused through fraudulent use of force post transactions[8] (a.k.a. force sale, force capture, or offline transactions), an acquirer must do all of the following if it has a merchant or sponsored merchant enabled with force post functionality:

- ☑ Conduct an enhanced due diligence review of the merchant or sponsored merchant, as specified in Section A.3 "Higher-risk merchant underwriting (enhanced due diligence)."
- ☑ Validate and document that the merchant or sponsored merchant has a legitimate business case to submit force transactions into interchange.
- ☑ Ensure risk controls are implemented to restrict the merchant or sponsored merchant's ability to submit fraudulent transactions into interchange.

Acquirers that fail to comply with this requirement resulting in the material, artificial manipulation of the clearing position for either a merchant or Visa Card account[9] may be subject to non-compliance assessments, as specified in Section 1.12.3.10, "Willful Violations of the Visa Rules."

Acquirers may be subject to all costs associated with reversing the position(s) created by force post activity.

Section 5.11 does not apply to below-floor limit transactions.

5.12 Use of Automated Underwriting and Onboarding (a.k.a. Auto-Boarding)

Acquirers and third party agents that utilize a form of automated underwriting in their onboarding (e.g., use of rule-based logic and/or machine learning) must do so in compliance with the Visa Rules, Visa Global Acquirer Risk Standards and applicable regulatory requirements.

Entities that use a form of automated underwriting in their onboarding of new merchants are encouraged to follow these **best practices:**

- ☑ **Use a hybrid of automated and traditional underwriting:** Develop and use policy to take an approach where specific merchants are selected for auto-boarding on a risk-prioritized basis, primarily by using predetermined parameters, such as:
  - Low monthly payment volume
  - Low average sales draft amount
  - Low risk Merchant Category Codes (MCCs)
  - Acceptance Method (card-present, card-absent, card-on-file, etc.)
  - No or very limited contingent liability
  - Card acceptance history (if available)

[8] Force post functionality enables a merchant to submit clearing messages with a manually entered authorization code.
[9] Force post fraud involves clearing messages processed with either a fictitious or missing authorization code.

- Financial performance and/or creditworthiness
- IP address validation, device fingerprinting, velocity checks (number of applications), negative database checks (including the Terminated Merchant File as required)

Merchants that do not meet these parameters or with complex business models and/or acceptance practices are traditionally underwritten.

☑ Monitor auto-boarded merchants for performance outside of the aforementioned parameters. Review such merchants by means of traditional underwriting.

☑ Maintain oversight (e.g., use of shadow underwriting and quality assurance goals) to detect potential flaws or increased risk exposure due to auto-boarding.

☑ Perform and document periodic audits (using the Self-Assessment Questionnaire in Appendix D) to ensure auto-boarding is carried out in compliance with acquirer policies, the Global Acquirer Risk Standards, Visa Rules and applicable regulatory requirements.

☑ In case of a significant risk event involving an auto-boarded merchant, review if potential deficiencies or flaws in auto-boarding could have been a contributing factor, or if improvements to the auto-boarding process may prevent similar future events.

6 Reserves and Merchant Funding

Acquirers should maintain merchant reserves that are outside of the merchant and agent's control to reduce financial exposure when appropriate. In the event a merchant closes down its business, the reserve amounts should be sufficient to offset future disputes or other liabilities. **However, acquirers should not rely on merchant reserves as a sole substitute for proper underwriting and risk monitoring**. In addition, merchant reserves do not mitigate harm to the system or damage to the acquirer's reputation, the Visa brand, and cardholder expectations.

6.1 Acquirer Reserve Responsibility

Reserves collected to guarantee a merchant's Visa payment system obligations must be held and controlled by the acquirer.

Acquirers must hold and control reserves that are accumulated and derived from merchant settlement funds or used to guarantee a merchant's payment system obligations to the acquirer. Agents are not permitted to collect, access, or control merchant reserves.

6.2 Reserve Controls

All merchant reserves maintained for the purpose of securing Visa payment system obligations must be held in a manner such that the funds can be readily identified with the merchant for whom they are held.

Acquirers must have controls in place to ensure their agents or merchants cannot access reserve funds.

- ☑ Reserves must be held in a unique deposit account in the merchant's name or in a general account via ledger entries.
- ☑ Merchant reserves are reconciled at least on a monthly basis to ensure:
  - All funds that have been added or removed from the reserves can be accounted for and explained.
  - The funds collected or disbursed can be mapped back to their source (settlement or offset of collection item).

6.3 Payments to Merchants

An acquirer must process the payment of funds to its merchants in a proper and timely manner.

Regardless of any contractual limits of liability between a member and its agents, Visa holds the member responsible for controlling all aspects of merchant funding process.

- ☑ Agents are not permitted to access or control merchant funds.
- ☑ Acquirers must provide settlement funds directly to the merchant, or payment facilitator on behalf of sponsored merchants, or Staged Digital Wallet Operators, promptly after transaction receipt deposit.
- ☑ Funding to merchants must be the same as the transaction totals, less any disputes, credit transaction receipts, or other agreed fees and discounts.
- ☑ The acquirer must not waive, release, abrogate, or otherwise assign to a non-member/agent its obligation to guarantee and ensure payment for all transactions in which the merchant honored a valid Visa Card properly presented for payment.

An acquirer must have controls in place related to establishing and changing merchant bank accounts where settlement funds are deposited, including controls to:

- ☑ Prevent a new bank account number from being established by an unauthorized party to divert merchant funds.
- ☑ Confirm or review all bank account changes, including changes completed by authorized third parties.

6.4 Suspending Settlement Funds

Suspended settlement funds may not be controlled or accessed by agents. Acquirers giving their agents the ability to suspend settlement funds must have controls in place to ensure compliance.

Acquirers may allow agents to monitor their merchants and conduct investigations of any suspected violation activity. Based on the result of those investigations, it may be necessary to delay settlement to a merchant or divert settlement funds to a reserve account. In these instances, an agent may request that a member delay settlement or collect other funds from the merchant, but the agent may not actually receive and possess any merchant funds.

Agents may be granted the authority to make decisions on withholding or delaying a merchant's settlement funds. This authority must not be interpreted by either party to mean funds may be controlled or accessed by the agent. Acquirers that provide agents with this level of system access must have policies and procedures in place to ensure agent compliance.

Following an investigation or the closure of the merchant, the member remains responsible for providing funds due to the merchant.

7 Merchant Risk Monitoring

To protect profitability and reduce losses, acquirers must be able to identify and investigate activity exposing the bank to increased risk at the earliest possible moment. Daily monitoring of merchant and sponsored merchant authorization and settlement activity can help an acquirer recognize any unusual or sudden change in normal merchant activity levels and prompt mitigating action.

7.1 Merchant Activity Monitoring Standards

An acquirer must monitor its merchants in accordance with the merchant activity monitoring standards, at a minimum.

Acquirer monitoring standards for merchants were developed as a baseline for a minimum level of oversight of merchant performance.

☑ At a minimum, acquirers must monitor the following:

- Sudden or unusual changes in transaction velocity; such as spikes in authorization attempts, sales volume, sales draft amounts, or changes in predetermined card-present vs. card-absent sales ratios
- High occurrences of transactions with rounded sales draft amounts, transactions from the same card in a short timeframe (including split-ticket sales), transactions outside the service area of the merchant (for card-present merchants) and cross border sales
- Unusual credit voucher activity (rounded amounts, credits vouchers without offsetting sales)
- Dispute and fraud advice (TC40) activity that approaches or exceeds Visa's established monitoring program thresholds[10]
- Force transaction activity, including unauthorized transactions or transactions with unusual (e.g. identical, missing or potentially fictitious) authorization codes
- New and inactive merchant transaction activity (such as dormant or low-processing merchants that have a sudden velocity spikes)
- Negative or net-zero balance batch deposits
- Merchants which the acquirer has reason to believe are engaged in transaction laundering
- Situations where there are a significant number of low-value transactions compared to the merchant's average transaction value
- Average elapsed time between the authorization and settlement for a transaction
- Other items listed under "Risk Monitoring" in Appendix A of this guide.

[10] It is important that acquirers take action well before a merchant is identified in the Visa chargeback and fraud monitoring programs. Visa provides early warning identifications for its chargeback and fraud monitoring programs and acquirers are expected to action these identifications.

Acquirers may allow their agents to perform daily merchant monitoring for exception reporting. **However, this practice does not absolve the acquirer from its oversight responsibility.** Should an acquirer allow agents to perform merchant monitoring, the acquirer must:

- ☑ Have access to, and review the agent's exception reporting activity (see Section 8).
- ☑ Periodically validate that the agent's risk monitoring complies with the acquirer's monitoring policies and procedures.

7.2 Exception Reporting

Acquirers must use exception reporting to monitor deviations in merchant activity that could indicate suspicious activity.

As part of the acquirer's merchant risk-monitoring activities, acquirers must implement reporting where deviations of merchant monitoring parameters exceed a predetermined threshold. Exception reports are subsequently reviewed and a determination is made whether further investigation is required. Acquirers may opt to suspend settlement of merchant funding if warranted in order to prevent losses while the investigation is in progress. As part of the investigation, an acquirer may ask the merchant to present sales drafts, sales agreements with the cardholder, and other documentation to validate the merchant's recent transaction activity.

7.3 Acquirer Investigation Follow-Up

The acquirer must investigate a merchant outlet within seven[11] calendar days of appearing on an exception report.

If the investigation reveals merchant involvement in illegal activity, fraud, or any other brand-damaging activities listed under the "Brand Protection" section in Visa Rules, the acquirer must:

- ☑ Take appropriate legal action to minimize losses.
- ☑ Cooperate with Visa, issuers and law enforcement agencies.
- ☑ Hold any and all available settlement funds, if possible. Acquirer should validate that their merchant agreement allows the acquirer to hold funds in this scenario.
- ☑ Attempt to make the merchant responsible for the transaction.
- ☑ Initiate criminal and civil proceedings against the merchant, if applicable

[11] In the Europe Region, one business day

As a best practice:

☑ Investigate if the violation occurred due to a lapse of, or deficiency in, policy or procedures and take the necessary corrective action.

7.4 Suspect Violation Report

The acquirer must provide Visa with a "suspect violation report" if it discovers any merchant, sponsored merchant, or agent violations.

If a merchant, sponsored merchant, or agent is identified by the acquirer as processing illegal or prohibited transactions, it must provide Visa with a suspect violation report and send it to acquirerrisk@visa.com. Visa may waive or suspend penalties to accommodate unique or extenuating circumstances or if violations of the Visa Rules are identified and rectified before receipt of formal notification from Visa that a violation has occurred.

7.5 Monitoring of Ecommerce Merchants

The acquirer must have measures in place to periodically review websites of ecommerce merchants on a risk-prioritized basis to ensure compliance with the Visa Rules.

Acquirers must implement measures to periodically review or scan ecommerce-enabled websites of its merchants and sponsored merchants on a risk-prioritized basis. This is to ensure that merchants do not process illegal or prohibited transactions, as specified in the Visa Rules. Criteria for review may include Merchant Category Code (MCC), cross-border activity, merchants on the acquirer's watch list, and other risk-based parameters. Reviews must include:

☑ A scan for products or services violating the Visa Rules or laws in the seller's and/or buyer's jurisdiction.

☑ A review for hyperlinks steering cardholders to other websites that violate the Visa Rules or law.

☑ US Region: At least once each year, an acquirer must examine its ecommerce merchant's website and conduct an enhanced due diligence review, if any of the following applies:

- The merchant or sponsored merchant is required to be classified with a high-brand risk MCC
- The merchant is identified by either the Visa Chargeback Monitoring Program or the Visa Fraud Monitoring Program.
- The acquirer becomes aware the merchant is selling products or services that were not documented in the merchant agreement or disclosed in the merchant's business description

The acquirer conducts a periodic review of the merchant as required by its internal procedures. As a best practice, the acquirer should include:

- ☑ A scan to determine whether the products or services offered are inconsistent with the merchant's transaction activity.
- ☑ Changes in the type of products offered that effectively alter the merchant's MCC.
- ☑ Changes in the method by which products or services are offered, potentially increasing risk exposure or propensity for disputes (e.g., the merchant changed to continuity or membership sales).

Acquirers may outsource the monitoring of merchant websites to third party security companies; however, the acquirer remains responsible for the activity of its merchants. When using third parties, the acquirer must establish controls to ensure such outsourcing is compliant with the Visa Rules.

7.6 Merchant Data Review and Retention

An acquirer must meet the minimum Visa merchant review and data-retention requirements.

As part of its merchant risk-monitoring procedures, an acquirer must:

- ☑ At minimum, retain all of the following data on a daily basis:
  - Gross sales volume
  - Average transaction amount
  - Transaction count
  - Count and amount of disputes and fraud advices (TC40)
  - Count and amount of purchase returns (credit vouchers)
  - Count and amount of authorization reversals
- ☑ Compare a merchant's actual sales volume against the approved sales volume.
- ☑ Compare actual sales draft amounts against the approved average sales draft amounts.
- ☑ Use moving averages to create normal monthly activity for the merchant's processing.
- ☑ Compare the merchant's actual processing activity to the normal monthly activity parameters established for that merchant.

7.7 Monitoring High-Brand Risk Merchants

The acquirer must meet Visa high-brand risk merchant registration, data-retention, and review requirements.

The Global Brand Protection Program was developed to guard against illegal or prohibited transactions from entering the Visa payment system. Merchants posing a high risk to the acquirer and Visa brands must be closely monitored. The MCCs that fall under the Global Brand Protection Program are periodically updated; thus refer to the latest *Global Brand Protection Program Guide for Acquirers*. When an acquirer processes transactions for high-brand risk merchants, it must perform the following:

- ☑ The acquirer must be registered with Visa as a high-risk acquirer. Any applicable agents soliciting high-brand risk merchants must be registered.[12]

  Note: Payment facilitators are restricted from sponsoring certain high-brand risk MCCs; consult the Global Brand Protection Program for details.

- ☑ Where required, high-brand risk merchants must be registered with Visa before transactions are submitted.

- ☑ Use transaction data to establish daily activity for each high-brand risk merchant category

- ☑ Meet Visa high-brand risk merchant data-retention and review requirements, including the following:
  - Meet all monitoring requirements in Section 7.1.
  - Collect the data over a period of at least one month, beginning after each merchant's initial deposit.
  - Use the data to determine the merchant's normal daily activity parameters for each high-brand risk merchant category.
  - Compare current daily processing activity to the normal daily activity parameters at least daily.
  - At least monthly, adjust the merchant's normal daily activity parameters, using the previous month's activity.

- ☑ Identify and address unusual high-brand risk merchant activity if a merchant significantly exceeds normal daily activity for:
  - Number of daily transaction receipt deposits
  - Gross amount of daily deposits
  - Average transaction amount
  - Number of daily disputes or fraud advices (TC40)

[12] To register as a high-risk acquirer or high-brand merchants, certain conditions apply. Consult the Visa Rules for regional requirements.

7.8 Providing Investigation Assistance

An acquirer must, to the best of its ability, assist other acquirers or issuers with fraudulent activity investigations.

Acquirers have a collective obligation to protect the payment system. Therefore, an acquirer must assist other Visa Clients in an investigation of fraudulent activity with a Visa Card by performing tasks including, but not limited to, the following:

- ☑ Interviewing merchants, sponsored merchants, cardholders, suspects, witnesses, and law enforcement personnel.
- ☑ Obtaining handwriting samples, photographs, fingerprints, and any other similar physical evidence.
- ☑ Recovering lost, stolen, or counterfeit cards.
- ☑ Providing information to proper authorities for the possible arrest of suspects, at another Visa Client's request.
- ☑ Performing any other reasonable investigative assistance.

7.9 Information Requests

An acquirer must provide information relating to any request for information presented by Visa, its designees, or any regulatory agency, as required under the Franchise Risk Management compliance programs.

The required information must be provided in writing as soon as possible, but no later than seven business days following receipt of the request for information.

An acquirer may receive a request for any type of information, including, but not limited to, the following:

- Organizational structure
- Employee information
- Sales-related data
- Financial information
- Data Security information

7.10 Submitting Merchant Transactions

A merchant or sponsored merchant must only submit transactions that directly result from cardholder transactions with the merchant or sponsored merchant.

A merchant or sponsored merchant is prohibited from submitting a transaction representing sales of goods or services generated by another merchant or sponsored merchant (transaction laundering).

A merchant or payment facilitator must **not** deposit a transaction until one of the following occurs:

- ☑ The transaction is completed.
- ☑ The merchandise or services are shipped or provided. This does not apply if the cardholder has paid a partial or full prepayment.
- ☑ Cardholder consent is obtained for a recurring transaction.

7.11 Adding Merchants to a Terminated Merchant File

Acquirers must add merchants terminated for just cause to the Terminated Merchant File or participate in the Visa Merchant Trace System (VMTS) or Visa Merchant Alert System (VMAS), where available and permitted under local applicable law.

7.11.1 Terminated Merchant File – U.S. Region

An acquirer must add a terminated merchant, sponsored merchant, or payment facilitator to the Terminated Merchant File as soon as possible, but no later than close of business on the day following the date the merchant is notified of the intent to terminate the agreement for one or more of the following reasons:

- Merchant was convicted of credit or debit card fraud.
- Merchant submitted excessive counterfeit transactions.
- Merchant submitted excessive transactions unauthorized by cardholders.
- Merchant submitted transactions representing sales of goods or services generated by another merchant (transaction laundering).
- Acquirer received an excessive number of disputes or fraud advices (TC40) due to merchant's business practices or procedures.
- Visa or MasterCard identified the merchant as suspected of fraudulent activity, or Visa disqualified the merchant from participating in the Visa program.
- Acquirer determined that serious merchant violations of the merchant agreement may result in increased loss exposure.

The acquirer must add a merchant to the Terminated Merchant File within 24 hours of determining that:

- Merchant was terminated for reasons other than those listed in the Visa Rules; and
- Within 90 calendar days of the termination date, the acquirer determines that the merchant should have qualified for the listing.

7.11.2 Visa Merchant Trace System – AP Region

An acquirer in Australia, Cambodia, Hong Kong, India, Indonesia, Macau, Malaysia, New Zealand, Philippines, Sri Lanka, Thailand, Singapore, Vietnam, or Mainland China must enter terminated merchant or sponsored merchant details into the Visa Merchant Trace System (VMTS), or equivalent terminated merchant database, within one business day after terminating a merchant agreement for a reason specified in the Visa Merchant Trace System.

7.11.3 Visa Merchant Alert Service – EU Region

An acquirer must ensure that a terminated merchant, sponsored merchant, payment facilitator, or marketplace[1] is added to the Visa Merchant Alert Service (VMAS), or equivalent terminated merchant database where available.

8 Managing Third Party Agent Risk

Acquirers are making use of third party agents for a range of services, including merchant solicitation, transaction processing, and customer support. However, acquirers must ensure their use of agents does not increase the risk exposure to the Visa payment system. From an acquirer 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.

8.1 Acquirer Use of Agents

An acquirer that uses any third party agent must comply with all requirements, as stipulated by Visa Rules.

This includes the following requirements:

- ☑ **Before registering an agent, the acquirer must be able to fulfill applicable Tier 1 capital requirements as stipulated in the Visa Rules**. Tier 1 capital requirements depend on the type of agent[13] and the acquirer's region.
- ☑ **The acquirer must complete the requirements outlined in the *Third Party Agent Due Diligence Risk Standards.*** Due diligence and ongoing oversight are imperative components of an acquirer's agent program. The minimum due diligence required before initiating an agent relationship is outlined in the *Third Party Agent Due Diligence Risk Standards* (Visa Supplemental Requirements), and an acquirer must attest to having completed these requirements when registering the agent.
- ☑ **An appropriate senior officer of the acquirer must review all documentation and approve the agent.** Approval to sponsor an agent must be based on proper due diligence and the affirmation of sound business practices that will not compromise either the acquirer or Visa, and may not be based solely on any purported limitation of the acquirer's financial liability or indemnification in any agreement with the agent.
- ☑ **An acquirer must register its agents with Visa prior to the performance of any contracted services or transaction activity**. An agent soliciting merchants under its own business name must be registered with Visa by the sponsoring acquirer before it solicits any merchants on behalf of the acquirer, including using the acquirer's merchant agreement and submitting a merchant application to the bank. As part of the registration process, the agent must be informed that:
  - Registration as a third party agent in the Visa Client Information System (VCIS) must not be represented as an endorsement of its services by Visa.
  - Registration of an agent is specific to each acquirer and requires a separate registration process for each agent-acquirer business relationship.

[13] Tier 1 capital requirements apply to registering payment facilitators, high-brand risk ISOs, and high-brand risk payment facilitators.

- A separate registration is required for each agent classification role the agent fulfills; e.g., if the agent acts as an ISO and a payment facilitator, separate registrations for each classification are required.

Additionally, before registering a third party agent, an acquirer must perform an on-site inspection of the agent's business location as part of the due diligence requirement, primarily to:

- Validate that the agent is a bona-fide business establishment.
- Review solicitation, sales, and training materials.
- Inspect operational controls.
- Review adherence to security standards regarding unauthorized disclosure of, or access to, Visa and other payment-network transaction information.

Visa may conduct an on-site inspection of any third party agent to validate its compliance with the applicable security requirements.

☑ **Maintain a file on the agent that includes all applicable documentation.** To maintain proper oversight over all agents, acquirers must keep pertinent documents (such as agent contracts, financial statements and due diligence materials) on file. Agent files must be retained for a minimum of two years following termination of the relationship or as long as specified by law in the acquirer's jurisdiction.

8.2 Third Party Agent Contract Requirements

An acquirer must execute a written contract with each third party agent before any services are performed.

Any third party agent that performs merchant solicitation or stores, processes, or transmits cardholder or transaction data on behalf of the acquirer must enter into a contract with the acquirer. Only a registered third party agent that has a direct written contract with an acquirer may perform services on behalf of the acquirer. The contract, to the extent permitted by applicable laws or regulations, must comply with all of the following:

☑ Include minimum standards established by Visa and the acquirer, including, but not limited to:

- Policies
- Procedures
- Service levels
- Performance standards

☑ Include stipulations that:

- Permits Visa to conduct financial and procedural audits and general reviews at any time.
- Requires the third party agent to make merchant information available to Visa and regulatory agencies.

- Contains a notice of termination clause.
- Permits Visa to determine the necessity of and impose risk conditions on the third party agent.

☑ Require that the third party agent comply with applicable laws or regulations, the Visa Rules, and acquirer policies and procedures.

☑ Be executed by a senior officer of the acquirer.

☑ Contain at least the substance of the provisions specified in the "Third Party Agents" section of the Visa Rules.

☑ Require that the third party agent comply with the Payment Card Industry Data Security Standard (PCI DSS) or other applicable data security standard.

☑ Include a provision that allows an acquirer or its merchant to terminate a contract if the third party agent participates in any of the activities described in "Prohibition of Third Party Agents from Providing Services" or the acquirer or its merchant becomes insolvent.

☑ Include a provision allowing the acquirer to terminate the contract if the third party agent:

- Participates in fraudulent activity.
- Engages in activity that causes the acquirer to repeatedly violate the Visa Rules.
- Operates in an unsound, unsafe manner.
- Participates in any other activities that may result in undue economic hardship or damage to the goodwill of the Visa payment system, if the third party agent fails to take corrective action.

8.3 Acquirer Responsibilities When Using Agents

An acquirer that uses any agent retains the overall responsibility for establishing and maintaining proper risk controls and procedures.

Acquirers may rely on agents to perform credit underwriting and risk-monitoring activities. In such a scenario, the acquirer remains responsible for having a proper control environment in place, and may not take itself out of the process. Whatever the indemnity arrangements may be between the acquirer and the agent, the acquirer must ensure the Visa Rules and its own policies are complied with by the agent and its merchants and sponsored merchants. **The acquirer's responsibility for establishing a proper agent control environment must include at a minimum:**

☑ **Control of the underwriting and onboarding of merchants.** An acquirer must ensure that agents permitted to underwrite and/or onboard merchants perform the underwriting and onboarding as specified by the Visa Global Acquirer Risk Standards and the acquirer. This is carried out by means of establishing and enforcing clear underwriting policy and criteria. In addition:

- Controls must be used by the acquirer to validate that agents comply with the Global Acquirer Risk Standards and the acquirer's underwriting policies and criteria. Acquirers must

use shadow underwriting procedures as a component of such controls, where all agent-approved merchant application packages—or a sampling of agent-approved merchant applications selected on a risk-prioritized basis—are reviewed by the acquirer.

- Acquirers must have business rules in place that require acquirer concurrence on merchant approvals above predetermined risk thresholds.
- If an agent maintains its own underwriting and onboarding policies, it must be aligned and not in conflict with the acquirer's own policies. The acquirer must periodically review its agents' policies and procedures to ensure they do not conflict with its own.

☑ **Review the agent's pricing models including merchant discount rates, applicable surcharges, and other fees charged for processing Visa transactions.** Acquirers must ensure that pricing schemes used by agents are fair and clearly communicated in writing to the merchant and have the merchant's written acceptance. Transparency is a key component of merchant pricing, and an acquirer is responsible to ensuring its agents are not using deceptive or egregious pricing schemes. To ensure this, acquirers must:

- Review and approve solicitation materials, merchant applications, and agreements used by agents for transparency and clarity.
- Run periodic reports to review an agent's use of discount rates, surcharges, and other fees charged for processing Visa transactions.

☑ **Control the ongoing risk monitoring of merchants.** If an acquirer has agents perform risk-monitoring functions on its merchant portfolio, the acquirer must ensure that the monitoring is carried out as specified by the Global Acquirer Risk Standards and the acquirer's policies. While acquirers are permitted to have an agent perform merchant risk-monitoring functions, the acquirer cannot abdicate its risk-monitoring responsibilities to an agent. The acquirer is ultimately responsible for its merchants' activities and thus must:

- Have controls in place to validate that risk-monitoring functions by its agents comply with the Global Acquirer Risk Standards and the acquirer's policies.
- Establish daily and monthly risk-reporting standards for its agents (where agents report to the acquirer) and use this reporting to generate and review exceptions.

☑ **Providing agents with data-entry capabilities.** An acquirer that provides an agent with data-entry capabilities to the acquirer's system(s) must be able to review all new merchant records and merchant record modifications before they become effective in the acquirer's system(s). Acquirers must monitor Merchant Category Code (MCC) and merchant DDA assignments and modifications.

☑ **Access to agent systems.** Where permitted by law, acquirers must have access to their agents' merchant management/data systems for viewing merchant information held by the agent—this includes payment facilitators.

8.4 Agent and Merchant Training and Education

An acquirer must provide its agents and merchants with training and/or education materials to ensure the agents and merchants understand and comply with their policies.

Agents must understand their sponsoring acquirers' policies and procedures as well as relevant Visa Rules so that they do not violate any expected performance standards. Therefore, acquirers must:

- ☑ Clearly communicate policies, procedures, and requirements to all of their merchants and agents to make sure that they do not violate any expected performance standards.
- ☑ Obtain the agent's commitment to comply with member policies and procedures, as well as relevant Visa Rules.
- ☑ Provide policies and procedures to the agent that include, but are not limited to the following:
  - The Visa Rules
  - Proper merchant solicitation practices
  - Use of member-branded materials
  - Merchant underwriting criteria, including prohibited and restricted merchant types and Merchant Category Codes (MCCs)
  - An Agent Code of Conduct
  - Payment Card Industry Data Security Standard (PCI DSS) and other data security requirements for the protection of cardholder information and transaction data
  - Industry-related laws and regulations (e.g., Code of Conduct for the Credit and Debit Card Industry in Canada)

8.5 Agent Code of Conduct

As a best practice, acquirers should have a written Code of Conduct for their third party agents.

To protect the integrity of the payment system, acquirers using agents should develop and enforce an Agent Code of Conduct. The Agent Code of Conduct would have to be:

- ☑ Used as an addendum to the acquirer's agent agreement (these may be phased in as new contracts are signed or existing agent contracts are renewed).
- ☑ Accepted and signed by the agent's principal owner or corporate officer responsible for compliance.
- ☑ Used by the acquirer when training agents.
- ☑ Utilized by agents when training their employees.

Agents would have to attest they will do the following:

- ☑ **Safety and soundness**: Operate in a responsible manner that protects the Visa payment system, sponsoring financial institutions, and other participants from undue harm or reputational damage.
- ☑ **Compliance**: Comply with Visa Rules and applicable laws and avoid circumvention of risk controls meant to safeguard the payment system and its participants.
- ☑ **General conduct**: Reasonably perform the roles and responsibilities designated by their sponsoring financial intuitions and provide an adequate level of service to the merchants they support.
- ☑ **Transparency**: Ensure any merchant marketing materials (including rates, fees, and terms) are approved by the sponsoring financial institution, compliant with applicable laws, and transparently disclosed to prospective merchants.
- ☑ **Data Security:** Comply with the Payment Card Industry Data Security Standard and other data security requirements for the protection of cardholder information and transaction data.

8.6 Quarterly Agent Reporting

Acquirers must keep quarterly activity reports on each of their agents and submit these reports to Visa upon request.

Quarterly agent reports must include the following information on each agent's merchant portfolio at a minimum:

- Total number of merchants on file at the end of the quarter
- Number of new merchants signed and closed during the quarter
- Total sales volume processed during the quarter
- Total dollar amount of disputes and fraud advices (TC40)
- Total dispute count

Upon request by Visa, an acquirer must submit the quarterly report and any additional information requested regarding the activities and services of each third party agent doing business on its behalf. This report must be signed by a senior officer and sent back to Visa within 30 calendar days of its request. Failure to submit a report in a timely manner or to provide accurate information may result in an on-site risk review or other risk controls to be placed on the acquirer.

8.7 Agent Monitoring

An acquirer must monitor the activity of each of its agents at least on a monthly basis.

Agent performance must be monitored to ensure compliance with the Visa Rules and the acquirer's policies and procedures. As part of monitoring agents, the acquirer must at a minimum perform a review of the following:

- ☑ **The requirements as outlined in the *Third Party Agent Due Diligence Risk Standards*.** The *Third Party Agent Due Diligence Risk Standards* (Visa Supplemental Requirements) delineates key requirements in administering oversight over agents.
- ☑ **The agent's underwriting practices.** The acquirer must generate reporting that identifies merchants approved and on-boarded by the agent along with each merchant's listing MCC, approved volume, and merchant DBA. Based on the approved-merchants report, the acquirer must review a set of underwriting packages to validate compliance with the acquirer's underwriting policies and procedures.
- ☑ **The agent's merchant portfolio performance.** As part of this, the acquirer should periodically review the agent's overall portfolio performance metrics—specifically for high volume merchants. Parameters to include are sales volume, dispute count and amount, fraud advices (TC40) count and amount, and credit voucher amount.
- ☑ **The agent's risk-monitoring activities.** This should include a review of merchant losses and merchants that habitually process outside set transaction parameters.
- ☑ **High-brand risk agent activity.** Agents approved to solicit high-brand risk merchants are required to report to the acquirer:
  - Acquisition of new high-brand risk merchants and sponsored merchants
  - Monthly transaction activity for all high-brand risk sponsored merchants

8.8 Annual Agent Reviews

Acquirers must perform an annual review on each of their agents.

In addition to monthly agent monitoring, acquirers must perform an in-depth review of all third party agents on an annual basis. At a minimum, annual agent reviews must include:

- ☑ **Financial statements.** A review of the agent's most recent financial statements to determine the agent's financial condition.
- ☑ **Ownership changes.** Documentation of any ownership changes and performance of due diligence on the new ownership when applicable.
- ☑ **Use of acquirer policies and procedures.** An examination of the implementation and use of acquirer policies and procedures. The acquirer must also look at agent's internal policies and procedures and how they align with the acquirer's own policies and procedures.

- ☑ **PCI DSS Compliance.** If the agent stores, transmits, or processes cardholder data, the most recent report on compliance validating the agent's compliance with the PCI DSS.
- ☑ **Solicitation Materials.** A review of the agent's merchant solicitation materials and media.
- ☑ **Review of merchant complaints.** A review of the agent's complaint log, any written complaints received by merchants, and a review of online complaint boards to ensure the agent is following high service standards.

When completed, agent reviews must be well documented and kept on file with the acquirer.

8.9 Agent Audits

An acquirer, Visa, or their designees may conduct an agent financial and procedural audit and/or review at any time.

Agents must allow their sponsoring acquirer, Visa, or their designees to conduct an audit at any time. If the acquirer, Visa, 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 the receipt of the request. An acquirer, Visa, its designees, or any regulatory agency may request information of any type, including, but not limited to:

- Organizational structure
- Employee information
- Sales-related data
- Financial information
- Data Security information
- Compliance with the relevant sections of this GARS guide

8.10 Solicitation Material Review

An acquirer must implement policy and procedures for reviewing merchant solicitation materials used by its agents.

Acquirers must have a policy and procedures in place to review their agent's solicitation materials to safeguard their reputation and that of the Visa payment system. **The policy must include a provision that prohibits the agent from positioning itself to merchants in a role superior to the acquirer or from use of any misleading statements.**

An acquirer must ensure that a third party agent complies with all of the following:

- ☑ Uses only solicitation materials—such as advertisements, stationery, business cards, sales brochures, and website promotional content—approved by the acquirer.

- ☑ Uses only solicitation materials that prominently identify the registering acquirer. This should minimally be as follows: "AGENT NAME is a registered agent for ACQUIRER, City, State/Province, Country."
- ☑ The Visa Product and Service Rules: Use of Marks.
- ☑ Does not present itself to prospective merchants under any other trade name or "doing business as" (DBA) except the one registered with Visa in the Visa Client Information System (VCIS). If the agent solicits merchants under different names, each name must be separately registered.
- ☑ If rates or pricing is quoted in solicitation materials, it is done in a clear and transparent manner and is in no way deceptive or misleading in nature.
- ☑ The agent does not present itself as, or appears to be, a principal acquirer of Visa.

As a best practice, acquirers may provide training materials and guidelines to their agents on what standards are considered acceptable for use in developing solicitation materials. However, the use of training materials does not constitute compliance with this requirement and does not absolve the member of the responsibility to review agent solicitation materials. Acquirers must include a review of agent solicitation materials during their periodic assessment of the agent's operations and financial condition.

8.11 Use of High-Brand Risk Agents

An acquirer must register agents soliciting high-brand risk merchants or high-brand risk sponsored merchants as high-risk agents with Visa.

If an acquirer contracts with an Independent Sales Organization (ISO) or a payment facilitator to solicit high-brand risk merchants or high-brand risk sponsored merchants, it must register that agent with Visa as a High-Risk Independent Sales Organization (HRISO) or High-Brand Risk Payment Facilitator (HRPF), whether or not the ISO has already registered with Visa as an agent. Acquirers contracting with high-brand risk agents are subject to minimum Tier 1 capital requirements as stipulated in the Visa Rules.

An acquirer must not process any card-absent, high-brand risk transactions until the high-brand risk agent registration has been approved by Visa.

9 Use of Payment Facilitators, Staged Digital Wallet Operators (SDWOs) and Marketplaces

Payment facilitators, SDWO and Marketplaces fill specific roles in the acquiring value chain. However, there are unique risks connected with sponsoring such entities that must be recognized and addressed. Acquirers that sponsor a payment facilitator, marketplace or SDWO must comply with all third party agent requirements in the Visa Rules, the *Third Party Agent Due Diligence Risk Standards,* and this guide. In addition to the general agent requirements, there are specific risk standards that acquirers must implement and maintain when contracting with a payment facilitator, marketplace or SDWO.

9.1 Acquirer Responsibilities

Acquirers contracting with a payment facilitator, SDWO, or marketplace, must perform an agent due diligence review and ensure its registration is confirmed by Visa.

Payment facilitators are minimally subject to the same agent due diligence and oversight requirements as for all third party agents (See Section 8). **When registering payment facilitators, acquirers must ensure that both the name the payment facilitator uses to identify itself and the attestation of due diligence review are confirmed by Visa before submitting transactions on the payment facilitator's behalf.**

If the payment facilitator is soliciting high-brand risk sponsored merchants, it must be registered as a high-risk Internet payment facilitator even if that payment facilitator has previously been registered with Visa.

In addition:

- ☑ An acquirer must assign the correct location of a payment facilitator, SDWO or marketplace as the country of the payment facilitator, SDWO or marketplace's principal place of business. See Visa Rules for additional requirements.
- ☑ An acquirer must ensure that a terminated sponsored merchant, terminated payment facilitator or terminated marketplace is added to the Visa Merchant Alert System (VMAS), Visa Merchant Trace System, or, where available, an equivalent terminated merchant database.

9.2 Payment Facilitator or SDWO Agreement Content

Acquirers must use separate agent contracts for a payment facilitator or SDWO, containing additional language as stipulated by the Visa Rules.

When contracting with a payment facilitator or a SDWO, the acquirer must use a contract that includes the following content:

- ☑ A requirement that the payment facilitator and its sponsored merchants, or the SDWO comply with the Visa Rules.
- ☑ A requirement that the payment facilitator enter into a contract with each sponsored merchant. This contract must:
  - Adhere to all of the applicable requirements as the acquirer's merchant agreement (see Section 4).
  - Be approved by the acquirer before use and each time the contract is revised.
  - Be provided to the acquirer or Visa upon request.
- ☑ A requirement that each SDWO has an acceptance contract with the retailer and conducts appropriate due diligence.
- ☑ The acquirer's right to immediately terminate a sponsored merchant, payment facilitator, SDWO, or a retailer signed by an SDWO for good cause or fraudulent or other activity or upon Visa request.
- ☑ Statements specifying that the payment facilitator or SDWO:
  - Is liable for all acts, omissions, cardholder disputes, and other cardholder customer service-related issues caused by the payment facilitator's sponsored merchants or the retailer signed by a SDWO.
  - Is responsible and financially liable for each transaction processed on behalf of the sponsored merchant, or for any disputed transaction or credit.
  - Must not transfer or attempt to transfer its financial liability by asking or requiring cardholders to waive their dispute rights.
  - Must not permit a sponsored merchant to transfer or attempt to transfer its financial liability by asking or requiring cardholders to waive their dispute rights.
  - Must not deposit transactions on behalf of another payment facilitator or SDWO.
  - Must not contract with a sponsored merchant, or a retailer in the case of an SDWO, whose contract was terminated at the direction of Visa or a government agency.
  - Must not deposit transactions from sponsored merchant, or retailers signed by an SDWO outside the Acquirer's jurisdiction.
  - Must provide the names of principals and their country of domicile for each of its sponsored merchants, or retailers signed by an SDWO, and transaction reports to its acquirer and to Visa upon request.

- Must ensure that its sponsored merchants comply with the Payment Card Industry Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS).

☑ High-brand risk sponsored merchant agreements must be signed by a senior officer of the high-risk internet payment facilitator.

An acquirer contracting with a payment facilitator or SDWO must implement policy, business processes, and controls that ensure the payment facilitator complies with the agent contract items listed in this section.

9.3 Sponsored Merchants

A sponsored merchant is to be treated as a merchant of the payment facilitator's acquirer.

An acquirer that contracts with a payment facilitator is liable for all acts, omissions, and adverse conditions caused by the payment facilitator and its sponsored merchants; this includes settlement to the payment facilitator or sponsored merchant or related legal costs. The acts of and omissions caused by a sponsored merchant will be treated as those of the payment facilitator and those caused by a payment facilitator or a sponsored merchant as those of the acquirer. Therefore, an acquirer must treat oversight over sponsored merchants in the same manner they do for direct merchants. In addition, an acquirer must comply with the following:

☑ Enter into a direct merchant agreement with sponsored merchants exceeding the annual transaction volume as stipulated in the Visa Rules[14] [15].

☑ Prohibit payment facilitators or high-risk internet payment facilitators from providing services to the following merchant types[15] [16]:

- Internet pharmacies
- Internet pharmacy referral sites
- Outbound telemarketers

☑ Ensure that a payment facilitator does not contract another payment facilitator as a sponsored merchant.

☑ Prohibit the payment facilitator from contracting with a sponsored merchant that is outside the country in which the payment facilitator and its acquirer are located.

☑ Ensure that sponsored merchants of the payment facilitator, and retailers in the case of an SDWO, follow all merchant-related rules.

[14] The payment facilitator may continue to provide payment services (including settlement) to the merchant.
[15] This does not apply to acquirers in Brazil.
[16] This does not apply to acquirers in the EU Region.

- ☑ **Effective 13 April 2019:** Obtain from Visa a unique payment facilitator identifier[17] that must be assigned by the acquirer to each payment facilitator to use in transaction processing.
- ☑ **Effective 13 April 2019:** Assign a unique sponsored merchant identifier[17], as determined by the payment facilitator, to every sponsored merchant.
- ☑ **Effective 13 April 2019:** Ensure that every transaction contains the payment facilitator identifier[17] and the sponsored merchant identifier.
- ☑ Ensure that its payment facilitators provide customer service directly or through their sponsored merchants.
- ☑ Upon Visa request, submit to Visa activity reporting on its payment facilitator's sponsored merchants that includes all of the following for each sponsored merchant:
  - Sponsored merchant name as it appears in the merchant name field
  - Sponsored merchant DBA name
  - Payment facilitator name
  - Monthly transaction count and amount
  - Monthly dispute and fraud advice (TC40) count and amount

Please refer to the Visa Rules for additional region-specific requirements.

9.4 High-Brand Risk Information

An acquirer must ensure that a high-risk internet payment facilitator (HRIPF) is identified in transaction records if cardholders are directed to the HRIPF website for payment.[17]

If a cardholder accesses the website of a high-brand risk sponsored merchant and is then directed to the website or a web page of the high-risk internet payment facilitator for payment, the name of the high-risk internet payment facilitator must appear in the authorization request and clearing record in conjunction with the name of the high-brand risk sponsored merchant.

[17] This does not apply to acquirers in the EU Region.

Appendix A – Acquirer Risk Management Policies

An acquirer must implement an underwriting, monitoring, and control policy framework addressing merchant and third party agent risk. These policies must be approved by the acquirer's Board of Directors or an appropriate executive committee.

The acquirer's risk management policies should cover management and operational functions performed by the acquirer and applicable third party agents. The following content elements help serve as a framework for acquirer risk policies designed to attain compliance with the Visa Rules.

A.1 Merchant Criteria

An acquirer must implement a policy defining designations representing merchant types that pose an unacceptable level of risk and will not be signed. Examples:

☑ **Prohibited Merchants:**

- Merchants posing a high brand (or reputational) risk.
- Questionable products or services that may be prone to consumer disputes and higher levels of disputes.
- Merchants using deceptive marketing or unreasonable guarantees to sell their products/services.

As a best practice, an acquirer should also maintain the following designation for merchant categories or types posing a higher risk that may be accepted under specific conditions, requiring enhanced due diligence. Examples:

☑ **Restricted Merchants:**

- MCCs that involve delayed or future delivery of merchandise or service.
- Merchants deploying free trials that subsequently enroll consumers into a membership program (continuity).
- Merchants selling highly regulated products or services.

The acquirer, with Board or appropriate executive committee approval, will determine which merchant categories or types fall under these designations and develop procedures for enhanced due diligence and conditional approvals where applicable.

A.2 Merchant Application Documentation

Policy outlining the requirements for merchants applying for merchant services should cover the following:

- ☑ Minimum documentation requirements for all new merchant applicants. This should outline a set of documents all merchants must submit, and also documentation requirements for specific situations (e.g., utility merchants, public companies, restricted merchants, etc.).
- ☑ Minimum documentation requirements for an existing merchant adding a new location.
- ☑ Disclosure of all third parties the merchant has involved in the payment process that may have access to transaction data.
- ☑ Change-in-ownership application requirements.
- ☑ Use of addendums for mail order/telephone order (MO/TO) and ecommerce merchants.
- ☑ Signing and execution of each merchant agreement (on paper or electronically) by the acquirer when merchants are approved.
- ☑ Proper storage and retention of merchant documentation.

A.3 Merchant Underwriting and Onboarding

The acquirer must maintain a policy delineating the underwriting process, credit criteria, and how to underwrite merchants with specific circumstances. The policy should address:

- ☑ Standard merchant underwriting criteria:
  - Minimum acceptable criteria for merchant approval
  - Review of requirements before an existing merchant is allowed to add a new location
  - Conditions that require a merchant to be re-underwritten (change in ownership, change in average sales volume/transaction amount, change in products/services offered, etc.)
  - Quantifying a new merchant's financial risk exposure (e.g., sales volume, dispute history, delivery method, contingent liability)
  - Examination of potential regulatory, brand and compliance risk exposure
  - Sanction screening as required
  - Conditions or restrictions that require an application to be declined
  - Minimum levels of ownership required on the merchant application
  - Minimum credit bureau score required for approval
  - Allowable criteria regarding major and minor derogatory credit history
  - Personal guarantees from merchant principals or corporate officers

- Decline procedures and merchant notification requirements

☑ Application data verification:

- Validation of merchant application information
- Conducting telephone screenings if applicable
- Confirming the accuracy of the MCC assignment

☑ Larger business underwriting:

- Minimum acceptable criteria for approval
- Setting commercial lending-based merchant approval criteria for larger companies
- Reviewing business bureau reports for larger merchants
- Evaluating financial reports for publicly traded companies

☑ Higher-risk merchant underwriting (enhanced due diligence):

- Specifying the merchant types subject to enhanced due diligence
- Defining more stringent approval criteria for higher-risk merchants
- Performing higher-risk merchant credit investigation
- Obtaining and reviewing product or service marketing material
- Validation of merchant DDA information (voided checks/bank letters)
- Conducting a detailed review of product or service
- Conducting Better Business Bureau or consumer complaint board reference checks
- Conducting fulfillment house reference checks (if applicable)
- Performing additional positive verification checks to validate merchant address and ownership
- Registration of high brand risk merchants (if and where applicable), and compliance with the Global Brand Protection Program, Visa Chargeback Monitoring Program, and Visa Fraud Monitoring Program

☑ Risk mitigation and controls:

- Use of predetermined merchant sales volume, transaction amount and card-present vs. card-absent transaction parameters for risk monitoring purposes
- Use of daily vs. month-end debiting of discount and fees for higher-risk merchants
- Requiring merchant reserves or other collateral when applicable
- Use of deposit delays
- Establishing more restrictive activity-monitoring parameters for higher-risk merchants

- Ensure use of fraud-prevention controls where applicable (e.g., AVS, CVV2, Visa 3-D Secure, velocity checks, negative/positive database, etc.)
- Suspending settlement for suspicious or questionable transaction activity

☑ Use of Visa Merchant Trace System (VMTS), where available and permitted under local applicable law, or Terminated Merchant File (U.S. Region), or Visa Merchant Alert System (EU Region) or other common terminated merchant database, if VMTS, VMAS or TMF is not available.

- Submitting merchant and principal information into the Visa Merchant Trace System (VMTS), where available and permitted under local applicable law, or Terminated Merchant File (U.S. Region), or Visa Merchant Alert System (EU Region) or other common terminated merchant database, if VMTS, VMAS or the TMF is not available
- Investigating merchants with possible matches
- Investigating merchants with high levels of inquiry from other acquirers
- Suspending merchants that appear on retroactive reports until validity can be determined

☑ Merchant site inspections:

- Use of site inspections of primary business locations when warranted
- Ensuring site-inspection report content is adequate to assess risk and business stability
- Differentiating traditional "store-front" from MO/TO and ecommerce merchants
- Performing inspections, reference checks, and due diligence of fulfillment houses

☑ Website inspections:

- Website content and merchant information standards
- Name displayed on website matching merchant description
- Merchant location within the acquirer's licensed jurisdiction
- Privacy policy
- Products offered for sale
- Links to other sites
- Minimum website requirements for payment purposes
- Transaction data security and encryption practices
- Back order, return, and refund policies
- Terms and Conditions

☑ Ecommerce merchant requirements:

- Complying with all the provisions of the Visa Rules pertaining to ecommerce transactions
- Use of PCI DSS (or other comparable regional data security standard) compliant/certified transaction service providers (e.g., gateway, shopping cart, etc.) per the Visa Rules
- Merchant compliance/certification with PCI DSS (or other comparable regional data security standard) if cardholder data is stored by merchant

☑ Control of force post transactions.

A.4 Approval Policy

The acquirer must maintain a policy on the merchant approval process, exception handling, and signing limits for underwriters.

☑ Approval authority:

- Designating merchant volume approval limits by position and title
- Setting approval limits for certain MCCs and business classifications by position and title
- Establishing and enforcing proper transaction processing requirements
- Tracking of application approval rates, decline reasons, and overrides
- Concurrence limits for third party agents
- Write-off limits for a single loss occurrence above which an approval from a bank officer is required

☑ Override policy:

- Defining formal decline decision override approval authorities
- Establishing new information that, when obtained, may warrant approval or additional risk-control measures to be implemented
- Avoid conflicts of interest, where underwriting decisions can be negatively influenced by elements outside the underwriting and risk organization

A.5 Risk Monitoring

The following provides an outline for an acquirer's risk-monitoring policies. Risk monitoring should encompass an acquirer's activities to identify, track, and mitigate merchant risk.

☑ Establish portfolio-level KPIs for continuous tracking and mitigation of loss exposure to dispute (chargeback) settlement risk, taking into account fluctuations in portfolio sales volume and contingent liability. KPIs must be in line with the acquirer's risk appetite/tolerance.

☑ Establishing merchant selection criteria for periodic reviews:

- Periodic re-underwriting of merchants on a risk-prioritized basis (e.g. merchants with a high-sales volume or MCCs with a predisposition for contingent liability).
- Defining the review timing based on risk-weighted criteria

- Targeting inactive merchants for review
- Conducting risk-prioritized periodic reviews for ecommerce merchants

☑ Establishing periodic review content including:

- Updating merchant file documentation
- Obtaining and evaluating financial reports as appropriate
- Assessing merchants using consumer credit bureau scores
- Using merchant secret shopper programs for higher-risk merchants
- Periodic website reviews (more frequent for higher-risk merchants) for changes in products, delivery methods, or return policies
- Confirming consistency with original application addendums
- Assessing compliance with data security requirements
- Review Visa Chargeback Monitoring Program and Visa Fraud Monitoring Program early warning reports

☑ Actions necessary to mitigate risk:

- Conducting a detailed review if warranted by initial screenings
- Taking actions to mitigate risk exposure discovered by the periodic review
- Follow-up and remediation plans as warranted

☑ Exception activity reporting that includes:

- Activity as outlined in Section 7.1 of this guide
- Force sale/force posts/force capture transactions
- Overall dispute ratios to ensure that monthly Visa thresholds will not be exceeded
- Unusual activity available for review before funding is provided to merchants

☑ Exception activity time frames to ensure:

- Exception activity reports are reviewed on a daily basis
- Highest priority alerts are reviewed first
- Merchant monitoring parameters, thresholds and tolerances are periodically evaluated and adjusted

☑ Establishing policies for investigating suspect activity:

- Exception condition criteria requiring investigation and/or reporting to management
- Suspect violation report filing procedures
- Escalation procedures between agents and acquirer
- Review of merchants with high dispute rates for deceptive or misleading sales/marketing practices or insufficient cardholder interaction/communication

- ☑ Establishing pre-defined suspect activity intervention:
  - Suspension of merchant funding policy and release authority
  - Suspension of merchant processing policy and reactivation authority
  - Merchant notification and timing procedures
- ☑ Terminating merchant relationships:
  - Establishing pre-defined intervention authorities to control losses
  - Holding reserves and deposits from terminated merchants to mitigate dispute risk exposure
  - Establishing criteria and timing for adding merchants to the Visa Merchant Trace System (VMTS), where available and permitted under local applicable law, or Terminated Merchant File (U.S. region), or Visa Merchant Alert System (EU Region) or other common terminated merchant database, if VMTS is not available

A.6 Managing Third Party Agents

From the initial due diligence process through ongoing oversight and termination, acquirers must have a clear policy in place for managing the third party agents they sponsor.

- ☑ Initial due diligence review that must take into consideration:
  - Principals and background information
  - Financial performance review
  - Sanction screening
  - Merchant portfolio risk performance and assessment
  - On-site operations review
  - Approval and signing process for new agents
  - Review of existing solicitation materials, websites, and marketing practices
  - Identify third party agents with access to cardholder and/or transaction data and ensure that they are PCI DSS compliant
  - The Third Party Agent Due Diligence Risk Standards
- ☑ Registration
  - Ensure all third party agents have been registered with Visa
  - Where applicable, ensure that agents used by merchants (e.g. Merchant Servicers) are registered with Visa

- ☑ Usage policies for agents with sales responsibilities
  - Establishing merchant signing and underwriting criteria for third party agents
  - Agent solicitation materials and marketing practices
  - Establishing merchant monitoring standards for third party agents
  - Agent reserves (opposed to merchant reserves) held by the acquirer
  - Acquirer holds and controls reserves and merchant settlement funds
  - Controls over ACH processes
  - Ongoing compliance with the PCI DSS
  - Monitor for use of unauthorized agents or sub-agents
- ☑ Ongoing Due Diligence
  - Due diligence review frequency (annual reviews at a minimum)
  - Minimum review requirements
  - Onsite review procedures
  - Compliance with acquirer's policies on underwriting and onboarding
  - Compliance with acquirer's policies on risk monitoring
  - Practices to review merchants with high dispute rates or suspicious activity
  - Agent financial statement reviews
  - Operational statistics and performance review
- ☑ Review of merchant solicitation materials
  - Requirements for all merchant solicitation materials (including websites)
  - Compliant use of Visa-owned marks
  - Proper disclosure of acquirer
  - Pricing that is transparent and not misleading

Appendix B – Disclosure Page

Appendix B provides two examples of the disclosure page that must be included in the agreement if an Agent is a party to an agreement between an acquirer and a merchant.

B.1 Rules for Disclosure Page

A disclosure page clearly communicates to the merchant the name of the financial institution with whom they have a merchant agreement. The following are specific rules for the disclosure page.

BANK DISCLOSURE

Member Bank (Acquirer) Information: ABC Bank, 12345 ABC Drive, City, State, ZIP, Phone (800) 555-1234

Important Bank Responsibilities:

- A Visa member is the only entity approved to extend acceptance of Visa products directly to a merchant.
- A Visa member must be a principal party to the merchant agreement.
- The Visa member is responsible for, and must provide settlement funds to, the merchant.
- The Visa member is responsible for all funds held in reserve that are derived from settlement.
- The Visa member is responsible for educating merchants on pertinent Visa Rules with which merchants must comply.

Important Merchant Responsibilities:

- Ensure compliance with cardholder data security and storage requirements.
- Maintain fraud and disputes below thresholds.
- Review and understand the terms of the merchant agreement.
- Comply with Visa Rules.

The responsibilities listed above do not supersede terms of the merchant agreement and are provided to ensure

Example of a Bank disclosure page as standalone document:

BANK DISCLOSURE

Member Bank (Acquirer) Information:

Acquirer Name: _____

Acquirer Address: _____

Acquirer Phone: _____

Important Member Bank (Acquirer) Responsibilities

- A Visa member is the only entity approved to extend acceptance of Visa products directly to a merchant.
- A Visa member must be a principal party to the merchant agreement.
- The Visa member is responsible for, and must provide settlement funds to, the merchant.
- The Visa member is responsible for all funds held in reserve that are derived from settlement.
- The Visa member is responsible for educating merchants on pertinent Visa Rules with which merchants must comply.

Merchant Information:

Merchant Name: _____

Merchant Address: _____

Merchant Phone: _____

Important Merchant Responsibilities:

- Ensure compliance with cardholder data security and storage requirements.
- Maintain fraud and disputes below thresholds.
- Review and understand the terms of the merchant agreement.
- Comply with Visa Rules.

The responsibilities listed above do not supersede terms of the merchant agreement and are provided to ensure the merchant understands important obligations of each party and that the Visa Member, ABC Bank, is the ultimate authority should the merchant have any problems.

Merchant Signature: _____ Date: _____

Print Name: _____ Title: _____

Appendix C – GARS Assessment Questionnaire

The GARS Assessment Questionnaire provides acquirers with a comprehensive checklist that can be used to assist in maintaining compliance with the minimum risk standards specified by Visa. This Assessment Questionnaire is also used in the event of a Visa-mandated third party review. For periodic check-ups of your acquirer risk control environment, use the Self-Assessment Questionnaire in Appendix D.

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
1: ACQUIRER POLICY FRAMEWORK					
1.1	**The acquirer has implemented written policies to govern the underwriting, risk monitoring, and control of its merchants, VisaNet processors and third party agents.**	3.1			
1.2	**The acquirer is able to provide a copy of its acquiring program strategy.**	3.1			
1.3	**A program exists that trains employees on the acquirer's policies.**	3.1			
1.4	**Third party agents are provided with, and receive training on, policies applicable to them.**	3.1			
1.5	**The acquirer provided a copy of a Board resolution or an appropriate executive committee approval of current policy.**	3.2			
1.6	**The acquirer is able to provide a copy of its policy governing:**				
1.6.A	Merchant Criteria – In compliance with Section A.1	A.1			
1.6.B	Merchant Application Documentation – In compliance with Section A.2	A.2			
1.6.C	Merchant Underwriting – In compliance with Section A.3	A.3			
1.6.D	Approval Policy – In compliance with Section A.4	A.4			
1.6.E	Risk Monitoring – In compliance with Section A.5	A.5			
1.6.F	Managing Third Party Agents – In compliance with Section A.6	A.6			
2: MERCHANT AGREEMENT					
2.1	**The acquirer has a merchant agreement in place with each of its merchants.**	4			
2.2	**Payment facilitators sponsored by the acquirer have a merchant agreement in place with their sponsored merchants.**	4			
2.3	**The acquirer only solicits and contracts with merchants, sponsored merchants, and payment facilitators, within its licensed acquiring jurisdiction.**	4.1			
2.4	**The acquirer's merchant agreement(s) indicate the acquirer as a principal party to the contract(s) and outline that merchant acceptance of Visa products is extended by the acquirer.**	4.2			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
2.5	**The acquirer reviews and approves all merchant agreements used by its agents, including payment facilitators, prior to use.**	4.4			
2.6	**The acquirer periodically reviews the merchant agreement(s) used by its agents.**	4.4			
2.7	**Merchants are approved for card acceptance prior to the acquirer's entering transactions into the Visa payment system for that merchant.**	4.5			
2.8	**Merchant agreements from approved merchants are signed (i.e., executed) by the acquirer by means of a legally acceptable method.**	4.5			
2.9	**The acquirer's agents do not execute merchant agreements on behalf of the acquirer.**	4.5			
2.10	**The merchant agreement(s) used by the acquirer include a clause that provides for the immediate termination of a merchant by the acquirer for any activity that may create harm or loss to the goodwill of the Visa payment system.**	4.6			
2.11	**The acquirer keeps complete, well-documented files containing merchant records for at least two years after merchant agreement termination.**	4.7			
2.12	**If merchant records are maintained by a payment facilitator or third party agent, the acquirer has full and unrestricted access to all documentation.**	4.7			
2.13	**The merchant agreement used by the acquirer includes provisions that ensure merchants and their service providers maintain compliance with applicable PCI DSS and Visa security requirements.**	4.8			
2.14	**The merchant agreement includes a clause that requires the merchant to notify the acquirer of its use of any service provider that will have access to cardholder data.**	4.9			
2.15	**The merchant agreement used by the acquirer stipulates that merchants using, or intending to use, a service provider, must:**	4.9			
2.15.A	Validate the service providers are certified as compliant with the PCI DSS or a similarly established data security standard.	4.9			
2.15.B	Provide the acquirer with information on any service providers the merchant uses or intends to use.	4.9			
2.16	**The acquirer provides ongoing education and notification (such as statement messages) to merchants to ensure they understand their obligation to notify their acquirer when they intend to use a service provider.**	4.9			
2.17	**The acquirer requires all newly boarded merchants to use only PCI-certified Qualified Integrator and Reseller (QIR) professionals from companies that are included on the PCI SSC's QIR Companies.**	4.9			
2.18	**An acquirer has a disclosure page or disclosure section included in each merchant agreement/application that identifies the acquirer and its responsibilities when an agent is a party to the agreement.**	4.10			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
2.19	**If an agent is a party to an agreement between the acquirer and the merchant, a disclosure page or disclosure section (see Appendix B) on the merchant application is required to ensure the merchant is aware of the role played by the acquirer.**	4.10			
2.20	**The acquirer's merchant agreement includes a statement that the acquirer is responsible for providing settlement funds directly to the merchant.**	4.11			
2.21	**The merchant agreement used by the acquirer is developed from a risk perspective to include the merchant obligations outlined in the Visa Rules and Section 4.12.**	4.12			
2.22	**The acquirer specifies merchant prohibitions in the merchant agreement as stated in the Visa Rules and Section 4.13.**	4.13			
2.23	**The acquirer's merchant agreement must specify the contractual requirements as stated in the Visa Rules and Section 4.14.**	4.14			
3: MERCHANT UNDERWRITING AND ONBOARDING					
3.1	**The acquirer has a control environment in place to ensure merchant underwriting is carried out in accordance with the policies and procedures set by the bank.**	5			
3.2	**All merchants are signed up for card acceptance services by means of a merchant application, either paper or electronic.**	5.1			
3.3	**The name and contact information of the acquirer is present on the merchant application and is clear and conspicuous.**	5.2			
3.4	**If the acquirer allows an agent to place its own contact name, phone number, and its logo on the application, this information is not more prominent than the acquirer contact information.**	5.2			
3.5	**If an agent's logo is present on a merchant application, the acquirer's logo is also present.**	5.2			
3.6	**The acquirer or its agent requests relevant information on the merchant's business background, business model and operations, merchant location(s), and principals who are running the business.**	5.3			
3.7	**In order to underwrite a merchant for card acceptance privileges, the acquirer collects the required information elements.**	5.3			
3.8	**The acquirer determines whether a merchant meets minimum qualification standards as part of its underwriting process, specifically:**	5.4			
3.8.A	The merchant will not submit any transactions that are illegal into the Visa payment system.	5.4			
3.8.B	The merchant is financially responsible and there is no significant derogatory information about any of the merchant's principals.	5.4			
3.8.C	The merchant is not engaged in any activity that could cause harm to the Visa system or the Visa brand.	5.4			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
3.8.D	The merchant does not misrepresent their merchant outlet location	5.4			
3.9	**The acquirer queries a Terminated Merchant File where available, or an equivalent terminated merchant database, before onboarding a prospective merchant or sponsored merchant.**	5.5			
3.10	**The acquirer collects and verifies additional application information for card-absent merchants.**	5.6			
3.11	**The acquirer uses separate merchant applications when signing up brick-and-mortar merchants for ecommerce services.**	5.7			
3.12	**The acquirer collects and verifies additional application data for internet merchants. This includes:**	5.8			
3.12.A	A listing of URLs used by the merchant to promote its business, sell products, and accept payments	5.8			
3.12.B	Verification that the merchant is the registered owner of these domains and websites	5.8			
3.13	**The acquirer has specific procedures in place in order to underwrite an ecommerce merchant offering free trial periods, which include:**	5.9			
3.13.A	The review of merchants using trial periods during underwriting, and periodically thereafter, to ensure no deceptive or misleading sales and marketing practices are used	5.9			
3.13.B	Periodically monitoring free-trial merchant dispute rates (disputes and credit vouchers/returns) and complaint board activity as a way to measure the merchant's customer service efforts	5.9			
3.13.C	Ensuring cardholders are notified via email shortly before the trial period ends, in order inform them that their card will imminently be charged unless they take action to cancel the trial	5.9			
3.14	**The acquirer ensures that websites operated by a merchant, sponsored merchant, payment facilitator, high-brand risk merchant, high-brand risk sponsored merchant, or high-brand risk payment facilitator must contain specific disclosure details as stipulated in Section 5.10.**	5.10			
3.15	**The acquirer controls the use of force transactions.**	5.11			
4: RESERVES AND MERCHANT FUNDING					
4.1	**Reserves collected to guarantee a merchant's Visa payment system obligations are held and controlled by the acquirer.**	6.1			
4.2	**All merchant reserves maintained for the purpose of securing Visa payment system obligations are held in a manner such that the funds can be readily identified with the merchant for whom they are held.**	6.2			
4.3	**Reserves are held in a unique deposit account in the merchant's name or in a general account via ledger entries.**	6.2			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
4.4	**Merchant reserves are reconciled at least on a monthly basis to ensure:**	6.2			
4.4.A	All funds that have been added or removed from the reserves can be accounted for and explained.	6.2			
4.4.B	The funds collected or disbursed can be mapped back to their source (settlement or offset of collection item).	6.2			
4.5	**The acquirer manages the payment of funds to its merchants in the following manner:**	6.3			
4.5.A	Agents are not permitted to access or control merchant funds.	6.3			
4.5.B	The acquirer provides settlement funds directly to the merchant, or payment facilitator on behalf of sponsored merchants, or SDWOs promptly after transaction receipt deposit.	6.3			
4.5.C	Merchant funds payments are the same as the transaction totals, less any disputes, credit transaction receipts, or other agreed fees and discounts.	6.3			
4.5.D	The acquirer does not waive, release, abrogate, or otherwise assign to a non-member/agent its obligation to guarantee and ensure payment for all transactions in which the merchant honored a valid Visa Card properly presented for payment.	6.3			
4.6	**The acquirer has controls in place related to establishing and changing merchant bank accounts where settlement funds are deposited, including controls to:**	6.3			
4.6.A	Prevent a new bank account number from being established by an unauthorized party to divert merchant funds.	6.3			
4.6.B	Confirm or review all bank account changes, including changes completed by authorized third parties.	6.3			
4.7	**Suspended settlement funds are not directly controlled or accessed by agents. If the acquirer gives its agents the ability to suspend settlement funds, it must have controls in place to ensure compliance.**	6.4			
5: MERCHANT RISK MONITORING					
5.1	**An acquirer monitors its merchants in accordance with the merchant activity monitoring standards—at a minimum the acquirer monitors for:**	7.1			
5.1.A	Sudden or unusual changes in transaction velocity; such as spikes in authorization attempts, sales volume, sales draft amounts, or changes in predetermined card-present vs. card-absent sales ratios	7.1			
5.1.B	Unusual credit voucher activity (rounded amounts, credits without offsetting sales)	7.1			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
5.1.C	Disputes that approach or exceed Visa's established monitoring program thresholds	7.1			
5.1.D	New and inactive merchant transaction activity (such as dormant or low-processing merchants that have a sudden spike in activity)	7.1			
5.1.E	Negative or net zero balance batch deposits	7.1			
5.1.F	Situations where there are a significant number of low-value transactions compared to the merchant's average transaction value	7.1			
5.1.G	Average elapsed time between the authorization and settlement for a transaction	7.1			
5.2	**If the acquirer allows agents to perform merchant monitoring, the acquirer:**	7.1			
5.2.A	Has access to, and reviews the agent's exception reporting activity (see Section 8).	7.1			
5.2.B	Periodically validates that the agent's risk monitoring complies with the acquirer's monitoring policies and procedures.	7.1			
5.3	**The acquirer uses exception reporting to monitor deviations in merchant activity that could indicate suspicious activity.**	7.2			
5.4	**The acquirer investigates a merchant outlet within seven calendar days of appearing on an exception report.**	7.3			
5.5	**The acquirer provides Visa with a "suspect violation report" if it discovers any merchant, sponsored merchant, or agent violations.**	7.4			
5.6	**The acquirer has measures in place to periodically review websites of ecommerce merchants on a risk-prioritized basis to ensure compliance with the Visa Rules. This includes:**	7.5			
5.6.A	A scan for products or services violating the Visa Rules or laws in the seller's or buyer's jurisdiction	7.5			
5.6.B	A review for hyperlinks steering cardholders to other websites that violate the Visa Rules or law	7.5			
5.6.C	US Region: At least once each year the acquirer examines ecommerce merchant websites and conducts enhanced due diligence reviews if any merchant is: i. assigned a high-brand risk MCC; ii. identified in VCMP/VFMP; iii. selling products/services not documented in the merchant agreement or disclosed in the merchant application; iv. or, if the acquirer is required to do so in accordance with internal procedures.	7.5			
5.7	**When using third parties for website reviews, the acquirer has controls to ensure such outsourcing is compliant with the Visa Rules.**	7.5			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
5.8	**The acquirer retains and reviews the following merchant-level data on a daily basis:**	7.6			
5.8.A	Gross sales volume	7.6			
5.8.B	Average transaction amount	7.6			
5.8.C	Transaction count	7.6			
5.8.D	Count and amount of disputes or fraud advices (TC40)	7.6			
5.8.E	Count and amount of returns (credit vouchers)	7.6			
5.9	**The acquirer compares the actual sales volume against the approved transaction volumes.**	7.6			
5.10	**The acquirer compares actual transaction amounts against the approved average transaction amounts.**	7.6			
5.11	**The acquirer uses moving averages to create normal monthly activity for the merchant's processing.**	7.6			
5.12	**The acquirer compares the merchant's actual processing activity to the normal monthly activity parameters established for that merchant.**	7.6			
5.13	**If the acquirer processes transactions for high-brand risk merchants, it performs the following:**	7.7			
5.13.A	The acquirer is registered with Visa as a high-risk acquirer.	7.7			
5.13.B	Agents soliciting high-brand risk merchants are registered as high-brand risk agents/payment facilitators.	7.7			
5.13.C	High-brand risk merchants are registered with Visa before transactions are submitted (check regional requirements).	7.7			
5.13.D	Transaction data is used to establish daily activity for each high-brand risk merchant category.	7.7			
5.14	**The acquirer meets Visa high-brand risk merchant data-retention and review requirements, including the following:**	7.7			
5.14.A	Meeting all data collection requirements in Section 7.1	7.7			
5.14.B	Collecting the data over a period of at least one month, beginning after each merchant's initial deposit	7.7			
5.14.C	Using the data to determine the merchant's normal daily activity parameters for each high-brand risk merchant category	7.7			
5.14.D	Comparing current daily processing activity to the normal daily activity parameters at least daily	7.7			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
5.14.E	At least monthly, adjusting the merchant's normal daily activity parameters, using the previous month's activity	7.7			
5.15	**The acquirer identifies and addresses unusual high-brand risk merchant activity if a merchant significantly exceeds normal daily activity for:**	7.7			
5.15.A	Number of daily transaction receipt deposits	7.7			
5.15.B	Gross amount of daily deposits	7.7			
5.15.C	Average transaction amount	7.7			
5.15.D	Number of daily disputes or fraud advices (TC40)	7.7			
5.16	**The acquirer, to the best of its ability, assists other acquirers with fraudulent activity investigations.**	7.8			
5.17	**The acquirer ensures merchants or sponsored merchants only submit transactions that directly result from cardholder transactions with the merchant.**	7.10			
5.18	**Acquirers must add merchants terminated for just cause to the Terminated Merchant File or participate in the Visa Merchant Trace System (VMTS) or the Visa Merchant Alert System (VMAS)where available and permitted under local applicable law.**	7.11			
6: MANAGING THIRD PARTY AGENT RISK – Applicable to sponsors of TPAs					
6.1	**The acquirer fulfills applicable Tier 1 capital requirements for sponsoring certain third party agents as stipulated in the Visa Rules.**	8.1			
6.2	**Requirements outlined in the *Third Party Agent Due Diligence Risk Standards* have been completed for each sponsored agent.**	8.1			
6.3	**A senior officer of the acquirer reviews all documentation and approves the agents.**	8.1			
6.4	**Agents are registered with Visa prior to the performance of any contracted services or transaction activity and agents are informed that:**	8.1			
6.4.A	Registration as a third party agent in the Visa Client Information System (VCIS) must not be represented as an endorsement of its services by Visa.	8.1			
6.4.B	Registration of an agent is specific to each acquirer and requires a separate registration process for each agent-acquirer business relationship.	8.1			
6.5	**A separate registration is required for each agent classification role the agent fulfills; e.g., if the agent acts as an ISO and a payment facilitator, separate registrations for each classification are required.**	8.1			
6.6	**Before registering third party agents, the acquirer performs on-site inspections of the agent's business location as part of the due diligence requirement, including:**	8.1			
6.6.A	Validation that the agent is a bona-fide business establishment	8.1			

Operational Questionnaire and Compliance Statement				Compliant		
Requirements			**Section**	**Yes**	**No**	**N/A**
6.6.B	Review of merchant solicitation, sales, and training materials		8.1			
6.6.C	Inspection of operational controls		8.1			
6.6.D	Review of adherence to security standards regarding unauthorized disclosure of, or access to, Visa and other payment-network transaction information		8.1			
6.7	**The acquirer maintains a file on each agent that includes all applicable documentation.**		8.1			
6.8	**The acquirer has executed a written contract with each third party agent before any services were performed.**		8.2			
6.9	**Agent contracts, to the extent permitted by applicable laws or regulations, comply with all of the following:**		8.2			
6.9.A	Includes minimum standards established by Visa and the acquirer, including, but not limited to:		8.2			
	i.	Policies	8.2			
	ii.	Procedures	8.2			
	iii.	Service levels	8.2			
	iv.	Performance standards	8.2			
6.9.B	Permits Visa to conduct financial and procedural audits and general reviews at any time.		8.2			
6.9.C	Requires the third party agent to make merchant information available to Visa and regulatory agencies.		8.2			
6.9.D	Contains a notice of termination clause.		8.2			
6.9.E	Permits Visa to determine the necessity of and impose risk conditions on the third party agent.		8.2			
6.9.F	Requires that the third party agent comply with applicable laws or regulations, the Visa Rules, and acquirer policies and procedures.		8.2			
6.9.G	Is executed by a senior officer of the acquirer.		8.2			
6.9.H	Contains at least the substance of the provisions specified in the "Third Party Agents" section of the Visa Rules.		8.2			
6.9.I	Requires that the third party agent comply with the Payment Card Industry Data Security Standard (PCI DSS) or other applicable data security standard.		8.2			

Operational Questionnaire and Compliance Statement				Compliant		
Requirements			**Section**	**Yes**	**No**	**N/A**
6.9.J	Includes a provision that allows an acquirer or its merchant to terminate a contract if the third party agent participates in any of the activities described in "Prohibition of Third Party Agents from Providing Services" or the acquirer or its merchant becomes insolvent.		8.2			
6.9.K	Includes a provision allowing the acquirer to terminate the contract if the third party agent:		8.2			
	i.	Participates in fraudulent activity.	8.2			
	ii.	Engages in activity that causes the acquirer to repeatedly violate the Visa Rules.	8.2			
	iii.	Operates in an unsound, unsafe manner.	8.2			
	iv.	Participates in any other activities that may result in undue economic hardship or damage to the goodwill of the Visa payment system, if the third party agent fails to take corrective action.	8.2			
6.10	**The acquirer has an agent control environment in place for the underwriting and onboarding of merchants by its agents, including:**		8.3			
6.10.A	Controls to validate that agents comply with the Global Acquirer Risk Standards and the acquirer's underwriting policies and criteria (i.e., shadow underwriting procedures)		8.3			
6.10.B	Business rules that require acquirer concurrence on merchant approvals above predetermined risk thresholds		8.3			
6.10.C	Periodic review of agent policies and procedures to ensure they do not conflict with the bank's own		8.3			
6.10.D	The review of agent pricing models including merchant discount rates, applicable surcharges, and other fees charged for processing Visa transactions		8.3			
6.10.E	Review and approval of solicitation materials, merchant applications, and agreements used by agents for transparency and clarity		8.3			
6.10.F	Running periodic reports to review agent use of discount rates, surcharges, and other fees charged for processing Visa transactions		8.3			
6.11	**The acquirer has an agent control environment in place for the risk monitoring of merchants by its agents, including:**		8.3			
6.11.A	Controls in place to validate that agent risk-monitoring functions comply with the Global Acquirer Risk Standards and the acquirer's own policies		8.3			
6.11.B	Daily and monthly risk-reporting standards for its agents (where agents report to the acquirer) and use this reporting to generate and review exceptions		8.3			
6.12	**If the acquirer provides any agents with data-entry capabilities to the acquirer's system(s):**		8.3			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
6.12.A	It is able to review all new merchant records and merchant record modifications before they become effective in the acquirer's system(s)	8.3			
6.12.B	It monitors Merchant Category Code (MCC) and merchant DDA assignments and modifications	8.3			
6.13	**The acquirer has access to its agents' merchant management/data systems for viewing merchant information held by the agent—this includes payment facilitators (where permitted by law),**	8.3			
6.14	**The acquirer provides its agents and merchants with applicable training and/or education materials,**	8.4			
6.15	**The acquirer obtains agent commitment to comply with member policies and procedures, as well as relevant Visa Rules,**	8.4			
6.16	**The acquirer communicates applicable policies, procedures, and requirements to its agents, including:**	8.4			
6.16.A	The Visa Rules	8.4			
6.16.B	Proper merchant solicitation practices	8.4			
6.16.C	Use of member-branded materials	8.4			
6.16.D	Merchant underwriting criteria, including prohibited and restricted merchant types and Merchant Category Codes (MCCs)	8.4			
6.16.E	An Agent Code of Conduct	8.4			
6.16.F	Payment Card Industry Data Security Standard (PCI DSS) and other data security requirements for the protection of cardholder information and transaction data	8.4			
6.16.G	Industry-related laws and regulations (e.g., Code of Conduct for the Credit and Debit Card Industry in Canada)	8.4			
6.17	**AS A BEST PRACTICE (not a requirement): The acquirer has a written Code of Conduct for third party agents, which is:**	8.5			
6.17.A	Used as an addendum to the acquirer's agent agreement	8.5			
6.17.B	Accepted and signed by agent principal owner(s) or corporate officer responsible for compliance	8.5			
6.17.C	Used by the acquirer when training agents	8.5			
6.17.D	Utilized by agents when training their employees	8.5			
6.18	**AS A BEST PRACTICE (not a requirement): The Code of Conduct requires that agents attest they will do the following:**	8.5			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
6.18.A	Operate in a responsible manner that protects the Visa payment system, sponsoring financial institutions, and other participants from undue harm or reputational damage.	8.5			
6.18.B	Comply with Visa Rules and applicable laws and avoid circumvention of risk controls meant to safeguard the payment system and its participants.	8.5			
6.18.C	Reasonably perform the roles and responsibilities designated by their sponsoring financial intuitions and provide an adequate level of service to the merchants they support.	8.5			
6.18.D	Ensure any merchant marketing materials (including rates, fees, and terms) are approved by the sponsoring financial institution, compliant with applicable laws, and transparently disclosed to prospective merchants.	8.5			
6.18.E	Comply with the Payment Card Industry Data Security Standard and other data security requirements for the protection of cardholder information and transaction data.	8.5			
6.19	**The acquirer keeps quarterly activity reports on each of its agents and submits these reports to Visa upon request,**	8.6			
6.20	**The quarterly agent reports include the following information on each agent's merchant portfolio at a minimum:**	8.6			
6.20.A	Total number of merchants on file at the end of the quarter	8.6			
6.20.B	Number of new merchants signed and closed during the quarter	8.6			
6.20.C	Total sales volume processed during the quarter	8.6			
6.20.D	Total dollar amount of disputes or fraud advices (TC40)	8.6			
6.20.E	Total dispute count	8.6			
6.21	**The acquirer monitors the activity of each of its agents at least on a monthly basis and at a minimum performs a review of the following:**	8.7			
6.21.A	The requirements as outlined in the *Third Party Agent Due Diligence Risk Standards*	8.7			
6.21.B	Agent underwriting practices	8.7			
6.21.C	The agent's merchant portfolio performance	8.7			
6.21.D	Agent risk-monitoring activities	8.7			
6.21.E	Agents approved to solicit high-brand risk merchants report to the acquirer:	8.7			
	i. Acquisition of new high-brand risk merchants and sponsored merchants	8.7			
	ii. Monthly transaction activity for all high-brand risk sponsored merchants	8.7			

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
6.22	**The acquirer performs an annual review on each of its agents, which includes:**	8.8			
6.22.A	Financial statements	8.8			
6.22.B	Ownership changes	8.8			
6.22.C	Use of acquirer policies and procedures	8.8			
6.22.D	PCI DSS Compliance	8.8			
6.22.E	Solicitation Materials	8.8			
6.22.F	Review of merchant complaints	8.8			
6.23	**Agent reviews are well documented and kept on file with the acquirer.**	8.8			
6.24	**The acquirer has policy and procedures for reviewing merchant solicitation materials used by its agents.**	8.10			
6.25	**The acquirer's policy includes a provision that prohibits the use of misleading statements in all solicitation materials or places the importance of the agent above that of the acquirer.**	8.10			
6.26	**The acquirer ensures that its agents comply with the following:**	8.10			
6.26.A	Only use solicitation materials that are approved by the acquirer.	8.10			
6.26.B	Solicitation materials prominently identify the acquirer.	8.10			
6.26.C	The *Visa Product and Service Rules: Use of Marks.*	8.10			
6.26.D	Agents do not present themselves to prospective merchants under any other trade name or "doing business as" (DBA) except the one registered with Visa.	8.10			
6.26.E	If rates or pricing is quoted in solicitation materials, it is done in a clear and transparent manner and is in no way deceptive or misleading in nature.	8.10			
6.26.F	Agents do not present themselves as principal acquirers of Visa.	8.10			
6.27	**If the acquirer sponsors agents soliciting high-brand risk merchants or high-brand risk sponsored merchants, such agents must be registered as high-risk agents with Visa where applicable.**	8.11			
7: USE OF PAYMENT FACILITATORS, SDWOs AND MARKETPLACES – Applicable to sponsors of such agents					
7.1	**The acquirer performed an agent due diligence review on its payment facilitators, SDWOs and marketplaces.**	9.1			
7.2	**The acquirer ensures that the name a payment facilitator uses to identify itself has been confirmed by Visa before submitting transactions on the payment facilitator's behalf.**	9.1			

Operational Questionnaire and Compliance Statement				Compliant		
Requirements			**Section**	**Yes**	**No**	**N/A**
7.3	**The acquirer assigns the correct location of a payment facilitator, SDWO or marketplace as the country of the payment facilitator, SDWO or marketplace's principal place of business.**		9.1			
7.4	**The acquirer adds terminated sponsored merchants, payment facilitators or marketplaces to the terminated merchant file or equivalent where available.**		9.1			
7.5	**The acquirer uses separate agent contracts for payment facilitators or SDWOs, containing the following additional content:**		9.2			
7.5.A	A requirement that the payment facilitator, its sponsored merchants or the SDWO comply with the Visa Rules.		9.2			
7.5.B	A requirement that each SDWO has an acceptance contract with the retailer and conducts appropriate due diligence.		9.2			
7.5.C	A requirement that the payment facilitator enter into a contract with each sponsored merchant and that such contracts:		9.2			
	i.	Adhere to all of the applicable requirements as the acquirer's merchant agreement (see Section 4).	9.2			
	ii.	Are approved by the acquirer before use and each time the contract is revised.	9.2			
7.5.D	The acquirer's right to immediately terminate a sponsored merchant, payment facilitator, SDWO, or a retailer signed by an SDWO for good cause or fraudulent or other activity or upon Visa request.		9.2			
7.5.E	Statements specifying that the payment facilitator or SDWO:		9.2			
	i.	Is liable for all acts, omissions, cardholder disputes, and other cardholder customer-service-related issues caused by the payment facilitator's sponsored merchants or the retailer contracted with the SDWO.	9.2			
	ii.	Is responsible and financially liable for each transaction processed on behalf of the sponsored merchant, or for any disputed transaction or credit.	9.2			
	iii.	Must not transfer or attempt to transfer its financial liability by asking or requiring cardholders to waive their dispute rights.	9.2			
	iv.	Must not permit a sponsored merchant to transfer or attempt to transfer its financial liability by asking or requiring cardholders to waive their dispute rights.	9.2			
	v.	Must not deposit transactions on behalf of another payment facilitator or SDWO.	9.2			

Operational Questionnaire and Compliance Statement				Compliant		
Requirements			**Section**	**Yes**	**No**	**N/A**
	vi.	Must not contract with a sponsored merchant, or a retailer in the case of an SDWO, whose contract was terminated at the direction of Visa or a government agency.	9.2			
	vii.	Must not deposit transactions from sponsored merchant, or retailer signed by an SDWO, outside the Acquirer's jurisdiction.	9.2			
	viii.	Must provide the names of principals and their country of domicile for each of its sponsored merchants, or retailers signed by an SDWO, and transaction reports to its acquirer and to Visa upon request.	9.2			
	ix.	Must ensure that its sponsored merchants comply with the Payment Card Industry Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS).	9.2			
7.5.F	High-brand risk sponsored merchant agreements are signed by a senior officer of the high-risk internet payment facilitator.		9.2			
7.6	**The acquirer has implemented policy, business processes, and controls that ensure the payment facilitator complies with the agent contract items listed in Section 9.2.**		9.2			
7.7	**Sponsored merchants are treated as a merchant of the payment facilitator's acquirer.**		9.3			
7.8	**The acquirer enters into direct merchant agreements with sponsored merchants exceeding the annual transaction volume as stipulated in the Visa Rules.**		9.3			
7.9	**Payment facilitators or high-risk internet payment facilitator are prohibited from, and do not provide services to the following merchant types:**		9.3			
7.9.A	Internet pharmacies		9.3			
7.9.B	Internet pharmacy referral sites		9.3			
7.9.C	Outbound telemarketers		9.3			
7.10	**The acquirer ensures that a payment facilitator does not contract with another payment facilitator as a sponsored merchant.**		9.3			
7.11	**Prohibit the merchant facilitator from contracting with a sponsored merchant that is outside the acquirer's jurisdiction.**					
7.12	**The acquirer ensuresthat sponsored merchants of the payment facilitator, and retailers in the case of an SDWO, follow all merchant-related rules.**		9.3			
	The acquirer obtains from Visa a unique payment facilitator identifier that must be assigned by the acquirer to each payment facilitator to use in transaction processing.					

Operational Questionnaire and Compliance Statement			Compliant		
Requirements		**Section**	**Yes**	**No**	**N/A**
	The acquirer assigns a unique sponsored merchant identifier, as determined by the payment facilitator, to every sponsored merchant, and uses the identifier in every transaction.				
7.13	**The acquirer ensures that payment facilitators provide customer service directly or through their sponsored merchants.**	9.3			
7.14	**The acquirer is able to submit to Visa activity reporting on its payment facilitator's sponsored merchants that includes all of the following for each sponsored merchant:**	9.3			
7.14.A	Sponsored merchant name as it appears in the merchant name field	9.3			
7.14.B	Sponsored merchant DBA name	9.3			
7.14.C	Payment facilitator name	9.3			
7.14.D	Monthly transaction count and amount	9.3			
7.14.E	Monthly dispute and fraud advice (TC40) count and amount	9.3			
7.15	**High-risk internet payment facilitators (HRIPFs) are identified in transaction records if cardholders are directed to the HRIPF website for payment.**	9.4			

Appendix D — Self-Assessment Questionnaire

Visa recommends that acquirers conduct periodic check-ups of their acquiring program risk control environment by completing the Self-Assessment Questionnaire below. Once completed, maintain a copy and any accompanying documentation for your records.

Topic and Question		Performance		
		Pass	Fail	N/A
Policy				
1	Does your acquiring program possess formal policies specifically governing the following aspects of your acquiring program (See Appendix A for reference):			
1.a	Overall Acquiring Strategy			
1.b	Merchant Agreements			
1.c	Merchant Application Documentation			
1.d	Merchant Criteria, Underwriting, Approval Limits and Onboarding			
1.e	Merchant Reserves and Funding			
1.f	Merchant Risk Monitoring			
1.g	Third Party Agents (Due diligence, oversight and compliance)			
3	Has the Board of Directors or a designated executive management committee formally approved and adopted such policies?			
4	Are policies periodically reviewed and updated to in response to environmental or operational changes?			
5	Are applicable staff and third party agents trained on the acquirer's risk policies and policy changes?			
Merchant Agreement				
6	Are any merchant agreements in use by your acquiring program, and any sponsored third party agent(s), in compliance with Section 4 of the Global Acquirer Risk Standards?			
7	Does your acquiring program only execute merchant agreements with merchants or sponsored merchants located within your licensed acquiring jurisdiction per the Visa Rules?			
8	Are merchant agreements reviewed and approved by the acquirer before use?			
9	If a third party agent is party to the agreement, is the acquirer name and contact information disclosed in the agreement?			
Underwriting and Onboarding				
10	Are all merchants signed for card acceptance services by means of an application?			
11	Are sufficient underwriting controls in place to validate compliance with the Merchant Qualification Standards (see Section 5.4)?			
12	Are applications for card-not-present (e.g., internet, MO/TO, card-on-file) acceptance given special consideration per Section 5.6?			
13	Are card-present merchants or sponsored merchants applying for ecommerce card acceptance signed up by means of a separate application requesting additional information per Sections 5.7 and 5.8?			

Topic and Question		Performance		
		Pass	Fail	N/A
14	Is a risk-based approach in place to periodically review merchant that pose a higher risk, such as merchant with high payment volume, contingent liability or High Brand Risk merchant (if applicable)?			
15	**Effective 26 January 2019** - Are merchants enabled with force post functionality only on an exception basis and only under specific conditions (see Section 5.12)?			
Use of Auto-Boarding (Best Practices)		**Yes**	**No**	**N/A**
16	Does your acquiring program, including any sponsored third-party agent(s), utilize any form of automated underwriting and onboarding (a.k.a. "auto-boarding" as described in Section 5.12) as part of your Visa acquiring program?			
17	Does your institution maintain a list of third party agents that utilize a form of auto-boarding?			
18	Does your acquiring program, including any applicable sponsored third party agent(s) use a risk-based approach, where only merchants within predetermined parameters (payment volume, average sales draft amount, MCC, acceptance method, contingent liability, etc.) are auto-boarded, and any merchants falling outside of such parameters is traditionally underwritten?			
19	Do your acquiring program perform periodic audits to ensure any form of auto-boarding is in full compliance with the Global Acquirer Risk Standards, Visa Rules, and any applicable regulatory requirements?			
Reserves and Merchant Funding				
20	Are any and all reserves collected to guarantee a merchant's settlement obligations held and controlled by the acquirer?			
21	Are such reserves in held in a manner that funds can be readily identified with a specific merchant and reconciled at least on a monthly basis?			
22	Does your acquiring program restrict sponsored third party agents from access or control of merchant reserves?			
Merchant Risk Monitoring				
23	Are all merchants monitored per the Merchant Activity Monitoring Standards (see Section 7.1)?			
24	Are exception reports generated and actioned based on parameter threshold violations and/or processing anomalies?			
25	Are ecommerce merchant websites periodically reviewed on a risk-prioritized basis to ensure compliance with the Visa Rules?			
26	Is there a process in place to re-underwrite merchants as needed based on changes in their processing patterns or service/product selections?			
27	Are merchants terminated for cause added to a terminated merchant file?			
Third Party Agent Oversight				
30	Does your acquiring program perform due diligence on all prospective agents (per the Third Party Agent Due Diligence Risk Standards) prior to performing any contractual services?			
31	If your acquiring program use and sponsor third party agents to fulfill any aspect of your Visa acquiring program, is each agent registered with Visa?			
32	Is there an established control environment and monitoring in place to ensure third party agents comply with your policies, the Global Acquirer Risk Standards, and the Visa Rules?			

Topic and Question		Performance		
		Pass	Fail	N/A
33	Are third party agent merchant solicitation materials (including websites) reviewed for compliance with the Visa Rules before use?			