# Visa Prepaid Issuer Risk Program Standards Guide

## Visa Supplemental Requirements

24 April 2015

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

# Introduction to the Visa Prepaid Issuer Risk Program Standards Guide

The *Visa Prepaid Issuer Risk Program Standards Guide* has been developed to:

- Identify prepaid issuer accountabilities and responsibilities to the Visa payment system when implementing and managing prepaid card programs.
- Provide instructions on how to reduce the risk exposure generated by the use of third party agents.
- Ensure prepaid program operations and practices are in compliance with the *Visa Prepaid Issuer Risk Program Standards* and the Visa Rules.

The questionnaires located in the back of the guide are used to assess compliance with the various *Visa Prepaid Issuer Risk Program* requirements.

**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.

## Guide Organization

Designed for ease of use, this guide is divided into four main sections, each covering a specific aspect of prepaid program risk:

**Policy Requirements** – Policy is the cornerstone of any effort to mitigate the risks involved with managing a card program. As such, this section focuses on the need to implement policies and procedures that govern an issuer's prepaid card program.

**Agent Oversight** – Many prepaid issuers rely on third party agents to manage various aspects of their prepaid program. It is therefore important for issuers to maintain control over their agents and understand they're accountable for the agents' activities.

**Security Procedures** – There are various risks associated with the issuing, fulfillment, and processing of Visa prepaid cards, such as the potential for theft and fraud. Therefore, prepaid issuers must maintain a proper control environment in order to protect card inventory and any applicable data systems.

**Funding Accountability** – Proper handling of funds is an essential aspect of managing a prepaid program. Issuers must closely monitor the manner in which they hold and control prepaid funds and reserves in order to safeguard the integrity of the program.

## Audience for the *Visa Prepaid Issuer Risk Standards Guide*

This guide is intended for issuers of prepaid Visa cards and their third party agents who manage various aspects of their prepaid programs.

### Contact Information

For questions relating to this guide or Visa Prepaid Issuer Risk Standards, contact Visa Global Brand Protection, **brandprotection@visa.com.**

# 1 Background

Prepaid cards continue to grow as a form of payment right alongside traditional debit and credit cards. They present a significant opportunity for Visa issuers and their agents to extend their reach and achieve incremental growth through new distribution channels. Prepaid cards also provide merchants and cardholders with unique benefits as opposed to using cash or checks. The guaranteed availability of funds on approved transactions and the speed of settlement are both features that make prepaid cards a preferred choice over checks for merchants. Additionally, cardholders enjoy the protection prepaid cards offer as opposed to carrying cash as they carry the same Zero Liability[1] protection as Visa credit and debit cards.

As with any other card product, the issuing of prepaid cards involves operating principles issuers must adhere to in order to mitigate risk. As opposed to addressing day-to-day risk management functions for which alternate publications exist, the *Visa Prepaid Issuer Risk Program Standards Guide* specifically addresses core risk-mitigation components all issuers must implement in order to manage a prepaid program.

One such component deals specifically with the use of third party agents. While agents are often key contributors to the growth and development of prepaid products and services, their involvement results in issuers assuming additional layers of risk. To mitigate such risk, issuers must ensure appropriate oversight and control processes are implemented for all third party agents that support their Visa prepaid programs. With this in mind, the *Visa Prepaid Issuer Risk Program Standards Guide* provides prepaid issuers with the basis for building and managing a program in full compliance with the *Visa Core Rules and Visa Product and Service Rules*, collectively hereafter referred to as the "Visa Rules."

[1] The Visa Zero Liability Program is not available in all regions and does not apply to all card products. See Visa Core Rules and Visa Product and Service Rules for details.

# 2 Program Overview

## 2.1 Program Responsibility

While it's not uncommon for an issuer to outsource its prepaid programs to third party agents, the ultimate program responsibility always rests with the issuer. An issuer should never abdicate the responsibility for its prepaid programs to a third party agent. This responsibility remains with the issuer and the individuals managing the prepaid programs, which may include:

**Financial Institution Executives** – whose role is to develop and implement an issuer's policies and procedures.

**Prepaid Issuer Operations Managers** – who are responsible for the overall prepaid issuing operations and the oversight and management of third party agents.

**Underwriters/Credit and Risk Managers** – who manage day-to-day operations and ensure that program guidelines are adhered to.

**Compliance and Anti-Money Laundering (AML) Officers** – who ensure that program due diligence is carried out and AML requirements are adhered to.

**Security Managers and Loss Prevention Officers** – who are responsible for safeguarding the issuer's computer systems and data networks.

**Internal Auditors** – who conduct periodic internal audits to ensure their institution's prepaid programs are managed in a manner that keeps the issuer safe and compliant with laws and Visa Rules.

## 2.2 Control Mechanisms

The *Visa Prepaid Issuer Risk Program* is a compliance program mandated and enforced by the Visa Rules. Two control mechanisms are available to verify issuer compliance with the guide and the Visa Rules:

- **Prepaid Self-Assessment Questionnaire** – Visa issuers must complete the *Prepaid Issuer Self-Assessment Questionnaire* (SAQ) upon entry into the prepaid program and on an annual basis thereafter. The SAQ must be kept on file with the prepaid issuer and Visa may request that the issuer submit a copy of this document when applicable. Visa may opt to follow up with an on-site review based on examination of the SAQ. A copy of the SAQ can be found in Appendix C.
- **Operational on-site risk reviews of issuers and agents** – Visa will select prepaid issuers and agents for on-site reviews on a risk-prioritized basis, or as needed to address operational deficiencies. These on-site reviews are an integral and valuable component of the *Visa Prepaid Issuing Risk Program* compliance process. When selected, issuers and agents are required to contract with a Visa-approved vendor to conduct the on-site review. Visa will provide a list of approved vendors when an issuer or agent is selected for a review. Operational on-site reviews are detailed in Section 7 of this guide, *Operational On-site Reviews*.

These control mechanisms assess the prepaid issuer's compliance with the *Visa Prepaid Issuer Risk Standards*. **Non-compliance can lead to a lack of adequate prepaid program oversight and may affect the safety and soundness of the financial institution.** Where egregious cases of non-compliance are found, Visa may impose non-compliance assessments and corporate risk reduction measures to ensure no further damage is sustained to the prepaid issuer and/or the Visa payment system.

In addition to the requirements and best practices highlighted in the *Visa Prepaid Issuer Risk Program Standards Guide*, prepaid issuers must also comply with requirements, controls, and standards outlined by their management and regulators.

**This guide is not a substitute for such requirements and does not constitute all of the risk standards that issuers and agents should follow.**

As the Visa Prepaid Issuer Risk Program Standards evolve, further enhancements may be made. Prepaid issuers are encouraged to diligently monitor their operations and implement additional controls as necessary to mitigate any loss exposure and protect the payment system in general.

## 2.3 Related Publications

For additional information about managing prepaid programs, including program requirements and guidelines, please refer to the following publications[2]:

***Visa International Prepaid Program Guidelines***
This publication provides program information and product guidelines for issuers, their third party agents, acquirers, and processors that support prepaid card programs.

***Visa Prepaid Products Risk Management Guide***
This guide is intended to help issuers improve their prepaid portfolio profitability by preventing and reducing losses in key risk areas.

***Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors***
An essential Visa manual intended for issuers and their third party vendors who perform data preparation, encryption support, fulfillment, and warehouse distribution of Visa products.

***Third Party Agent Due Diligence Risk Standards***
All Visa clients that use third party agents to perform sales and/or operational service functions must comply with these risk standards, in addition to those outlined within this guide and the Visa Rules. Appendix A of this guide summarizes pertinent information from the Risk Standards; however, issuers are required to periodically review the Third Party Agent Due Diligence Risk Standards in whole to account for any changes that may not be reflected within this guide.

***Visa Global Instant Card Personalization Issuance Security Standards***
This publication outlines a set of Global Instant Card Personalization Issuance (ICPI) Security Standards developed by Visa to alleviate the concern of removing the card personalization process from a highly restricted environment of controlled accountability to a more open and distributed posture.

[2] Please refer to publication versions applicable to your specific region. All publications can be accessed at Visa Online (VOL).

# 3 Risk Policies

## 3.1 Policy Requirements

### 3.1.1 Maintaining a Policy Framework

A prepaid issuer must maintain a policy framework that identifies and mitigates risks associated with the management of a prepaid program. Additionally, the policy framework must be aligned with the issuer's overall operational strategies, and all policies must be formally approved by the financial institution's Board of Directors or a designated executive management committee. **A clearly stated policy framework is essential to maintaining an efficient and sound prepaid card program** and helps ensure the issuer and agents understand the strategic objectives, risk tolerances, and compliance requirements of the program.

In addition to having a policy framework in place, the issuer and agent employees must be educated on the guidelines that apply to their job functions and know what is expected of them. Once approved, policies must be implemented by training applicable staff on those policies, including how to properly handle policy exceptions.

### 3.1.2 Policy Ownership

Many third party agents specialize in managing an issuer's entire prepaid program. Hence, such agents often have their own policies and procedures that govern the management of the issuer's prepaid programs. **However, prepaid issuers must author, adopt, and follow their own underwriting, monitoring, and control policies and cannot simply copy or use their agent's policy in lieu of maintaining their own.**

### 3.1.3 Minimum Policy Requirements

There is a minimum set of risk-based policies that every prepaid issuer must possess in order to operate a prepaid card program. At a minimum, a prepaid issuer's policies must address the following:

| | |
|---|---|
| **Program Strategy** | Outlines the issuer's prepaid program strategy, which includes the targeted market(s), the various entities involved, and their responsibilities. The operational workflow of the prepaid program should also be included. |
| **Agent Diligence and Monitoring** | Establishes the minimal and initial third party agent due diligence and registration processes. Additionally, these policies also outline the requirements for the ongoing agent oversight and reporting requirements. |
| **Funding and Reserve Requirements** | Highlights the proper processes that will ensure prepaid program funds are held and controlled by the prepaid issuer. |
| **Data Security** | Clarifies the roles and responsibilities of the various entities involved in the issuer's prepaid programs to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS) is maintained. |
| **Regulatory and Legal Compliance** | Provides the basis by which issuers can ensure compliance with the numerous laws and regulations that apply to the issuing of prepaid cards. |
| **Education and Training** | Summarizes the processes necessary to ensure prepaid issuers provide their third party agents with the necessary education and training to support their Visa prepaid programs. |

## 3.2 Agent Policies

### 3.2.1 Agent Policy Requisites

Issuer must develop policies and procedures to ensure proper management and oversight of third party agents. Issuers must take the following requisites into consideration when developing their policies and procedures:

- ☑ Policies and procedures governing third party agents must be in place before the issuer enters into a contract with any third party agent.
- ☑ These policies must provide an oversight and control mechanism to ensure agent-operated prepaid programs are in compliance with the Visa Rules (e.g., perform due diligence, implement reporting standards, review soliciting materials, use applicable controls, etc.).

☑ Issuer policies must be formally approved and adopted by the prepaid issuer's Board of Directors or a designated executive management committee.

### 3.2.2 Accountability and Control

While outsourcing the management of prepaid programs (either partially or as a whole) is a strategy widely used by prepaid issuers, it is essential that issuers never lose sight of their responsibility and accountability for their prepaid programs.

To ensure prepaid issuers maintain complete accountability and control over all facets of their prepaid program(s), **a prepaid issuer must implement policies defining how the issuer controls its agents; specifically addressing the following areas of agent management and oversight:**

☑ Initial due diligence

☑ Agent agreements/contracts

☑ Agent application requirements

☑ Agent registration

☑ Change in ownership requirements

☑ Ongoing due diligence

☑ Reporting standards for agents

☑ Communication and training

☑ Holding of funds

☑ Agent termination

For additional information on the requirements that must be implemented when third party agents are used, refer to the "Use of Third Party Agents" section of this guide.

# 3.3 Anti-Money Laundering Program

## 3.3.1 AML/ATF Program Requirements

Financial institutions are mandated to abide by laws and regulations designed to detect and prevent money laundering and the financing of terrorism. **Issuers must implement a written prepaid card Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) program and/or incorporate prepaid card issuance into their existing written AML/ATF program.** AML/ATF program requirements must at a minimum include:

- ☑ Written AML/ATF policies, procedures, and controls over the issuer's prepaid program.
- ☑ Appointment of a designated "AML Officer" (or equivalent) responsible for the implementation and management of the AML/ATF program.
- ☑ Screening of government trade-sanction watch-lists in accordance with applicable laws and regulations.
- ☑ Ongoing training of employees on the AML/ATF program.
- ☑ Ongoing independent testing of the AML/ATF program.

In the event a prepaid issuer outsources any portion of its AML/ATF program to a third party, the issuer remains fully responsible for compliance with the aforementioned requirements. **Prepaid issuers that outsource AML/ATF functions to a third party must periodically review the third parties' activities in order to maintain an effective AML/ATF program.**

## 3.3.2 Cardholder Due Diligence

In adherence to Visa requirements, financial institutions issuing reloadable cards or prepaid cards that allow for cash access are required to maintain a written Customer Identification Program (CIP) that complies with all applicable regulatory requirements, including procedures for elements such as customer verification, recordkeeping, and retention requirements. At a minimum, financial institutions must obtain the following identifying information from each cardholder:[3]

- ☑ Name
- ☑ Physical Address

[3] Please consult with your legal counsel regarding privacy, data storage, and data security regulations relevant in your region.

- ☑ Date of Birth
- ☑ Government Identification Number

The Customer Identification Program must include procedures for monitoring systems and reporting; specifically:

- ☑ **Procedures for determining whether the cardholder appears on any government sanctions lists before issuing cards, and periodically thereafter.** Positive identifications of consumers (after scrubbing for false positives) should be managed per applicable government regulations.
- ☑ As a best practice, issuers should cross-reference consumer names, addresses, and other related information against their own databases to ensure consumers don't have access to an unreasonable number of reloadable prepaid cards, which may be an indication of suspicious activity.

### 3.3.3 Risk Controls and Monitoring Processes

**Issuers must maintain internal controls and monitoring processes to identify and prevent inappropriate card use that poses potential AML/ATF risk.** To help mitigate money laundering and terrorist financing risk, **issuers must implement internal controls and procedures including, but not limited to, the following:**

**Card issuance:**

- ☑ Controls to prevent issuance of prepaid cards in countries/regions outside the issuer's licensed jurisdiction, except when permitted by the Visa Rules.
- ☑ Controls to prevent the unintended bulk sale of cards or use of unintended distribution channels.
- ☑ Controls to limit the number of cards issued to each cardholder.
- ☑ Procedures for customer identification and due diligence reviews at account opening (for reloadable cards or prepaid cards that allow for cash access).

**Screening cardholder information and blocking transactions:**

- ☑ Procedures to screen cardholder information obtained through the CIP against government sanctions lists prior to account opening, during transaction processing, and periodically thereafter.
- ☑ Controls to block cash disbursements and quasi-cash transactions for non-reloadable cards when no cardholder information is on file.
- ☑ Controls to identify and block transactions occurring in countries designated as state sponsors of terrorism by the issuer's local government.

**Ongoing monitoring:**

- ☑ Controls for velocity and transaction limits on account loads, withdrawals, and ATM cash and POS transactions (daily, weekly, monthly, and annually).
- ☑ Procedures to monitor for high-volume account funding transactions followed by cash withdrawals (either distributed over several locations or at one single site).
- ☑ Card-usage pattern and program comparison controls—e.g., determine whether card usage is consistent with the specific card program and review card-to-card transfers within card programs.

### 3.3.4 AML/ATF and Third Party Agents

Issuers using third party agents must ensure that each of their agents have sufficient AML/ATF controls in place to meet all relevant legal requirements; therefore the issuer must:

- ☑ Conduct adequate due diligence to ensure agents abide by the issuer's AML/ATF policy, or have policies in place that the issuer has reviewed and approved.
- ☑ Communicate and train agents on their AML/ATF expectations and requirements on an ongoing basis.
- ☑ Monitor each agent's transaction activity directly rather than relying solely on agents providing monitoring data to the issuer. Periodically test transaction activity to ensure card usage is commensurate with the type of prepaid programs.
- ☑ Require agents to allow issuers access to Customer Identification Program records.
- ☑ Adopt a restricted-issuance policy that agents must use, which includes a list of prohibited industries based on an internal risk assessment.

In addition to these requirements, the following are AML/ATF best practices for issuers with third party agents:

- ☑ Collect certifications from agents to ensure AML/ATF training was provided to appropriate employees.
- ☑ Periodically evaluate and test each agent's AML/ATF program.

### 3.3.5 AML/ATF Program Training

Issuers must include employee training as a primary component of its AML/ATF program and provide AML/ATF-related training for new employees and applicable staff members, annually at a minimum. Training materials must include:

- ☑ Updates to AML/ATF laws and regulations (when applicable)
- ☑ Sanctions compliance
- ☑ Customer Identification Program procedures
- ☑ Monitoring and detection of unusual activity
- ☑ Suspicious activity reporting requirements and procedures
- ☑ AML/ATF oversight of third party agents

### 3.3.6 Suspicious Activity

Issuers must have documented policy and procedures in place for investigating unusual or suspicious activity in accordance with all applicable regulations. Such policies and procedures must include:

- ☑ Descriptions of what may constitute suspicious activity and the development of exception condition criteria.
- ☑ Processes on how to identify, investigate, track, and report suspicious activity.

As a best practice, a prepaid card issuer should:

- ☑ Closely collaborate with third party agents to exchange information on suspicious activity report filings.

# 4 Use of Third Party Agents

## 4.1 Initial Due Diligence

### 4.1.1 Performing Initial Due Diligence

**As part of underwriting a new third party agent, prepaid issuers must ensure compliance with the *Third Party Agent Due Diligence Risk Standards* (addressed in Appendix A).** These standards must be administered before and during the registration process as well as throughout the life of the agent contract.

It is recommended that the issuer develop a comprehensive agent application form that can be used to collect all pertinent information from prospective agents. This can be accompanied by a list of all items required from the agent as part of the initial due diligence process (based on the *Third Party Agent Due Diligence Risk Standards* and the content in this section). Once completed and submitted to the issuer, the application packet can be used as part of the agent underwriting process. All information collected as part of the initial due diligence process should be placed in a dedicated file for each third party agent. The agent file should be augmented over time with ongoing due diligence documentation.

**As part of the initial due diligence of a third party agent, prepaid issuers must conduct the following actions** (as legally permitted):

☑ Verify agent application information and documentation for accuracy.

☑ Obtain legal and business information for each third party agent, including, but not limited to:

- "Doing business as" (DBA) name.
- Third party agent legal name.
- Third party agent location information, including full physical address—not post office or mail center boxes.
- Government-issued company identification numbers, such as tax identification numbers, and the source or issuing authority of the government identification numbers.
- Company legal status (e.g., corporation, partnership, sole proprietorship, or other) and location of legal filing.
- First and last names of company principals. If the agent is a sole proprietor, also collect middle initial and tax identification number.

☑ Conduct a background check of the third party agent and its principal(s) to identify potential negative business practices that could impact the business relationship, and determine whether there has been a PCI DSS violation/breach or any other compliance issue in the past. This background check should include:

- References from various external third party entities, such as:
  - Government agencies and regulators
  - Suppliers and vendors
  - Trade associations and chambers of commerce
  - Creditors and banking relationships
- AML/ATF review on the principal(s) as required by local law
- Research of prior public business filings—e.g., bankruptcies and past civil litigations
- Commercial or mercantile credit report
- Detailed review of agent's website and screening of customer service phone number(s)
- Internet complaint boards and consumer advocacy sites/forums

☑ Conduct a physical site inspection of the agent's business to validate the suitability for the type of business the agent will engage in—e.g., follow guidelines within the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*—where applicable.

☑ Conduct a thorough review of the agent's financial condition and historical performance—e.g., examine financial statements, operational metrics, and key performance indicators.

☑ Obtain and review product or service marketing materials and any other advertising collateral in order to ensure they are compliant with the Visa Rules.

☑ If applicable, ensure a security assessment has been completed and findings have been remediated, in order to protect the integrity of cardholder information in accordance with the PCI DSS. (Obtain a PCI DSS Report on Compliance or equivalent.)

☑ Ensure all applicable registrations or licenses required are in place for the third party agent to conduct business.

☑ Complete an adequate financial review of the agent's principals if they accept any financial liability (e.g., personal guarantee).

The following best practices are recommended:

☑ Prepaid issuers with an internal audit department or contracting with external auditors should engage these resources to review the new agent and ensure that all appropriate risk controls are

in place prior to the prepaid program launch, including all provisions related to the use of third party agents in Appendix B, "Prepaid Issuer On-site Operational Review Questionnaire."

☑ If the third party agent has one or more principals with a 10% or higher ownership stake in the company, the issuer should perform enhanced due diligence on such principals by collecting additional personal information.

### 4.1.2 Agent Risk Analysis

Upon receipt of the initial due diligence documentation, prepaid issuers must **conduct quantitative and qualitative risk analyses to properly evaluate the risk exposure the new agent poses** and to **underwrite the agent for the specific role they will fulfill**. If the agent is deemed a suitable partner for the issuer based on this analysis, the issuer may proceed with agent registration.

The issuer must establish conditions that are cause for re-underwriting third party agents, including ownership changes, legal business status, role of the agent, or deterioration of the agent's financial condition.

## 4.2 Agent Registration

Visa prepaid issuers that use third party agents for the fulfillment or management of any facets of their prepaid program(s) must**:**

☑ Have a direct written contract in place with each agent prior to agent registration, **as only registered agents may perform services on behalf of the issuer.** Information on third party agent contract requirements is described later in this section.

☑ **Perform a thorough due diligence review of the agent** as previously described prior to registering the agent.

☑ **Register their agents with Visa prior to the performance of any contracted services or transaction activity,**

For additional information on the registration process, issuers must refer to the Visa Membership Management (VMM) application which includes an "attestation of completion of due diligence" as outlined in the *Third Party Agent Due Diligence Risk Standards* (see Appendix A). VMM is a component of Visa Online (VOL) and may be accessed at: https://www.visaonline.com[4]

In addition to completing the third party agent registration process, prepaid issuers must:

[4] User registration is required.

- ☑ Pay registration fees for each registered agent, both initially and annually, where applicable.
- ☑ Submit a *Prepaid Program Information Form* (PIF) to Visa in order to obtain approval for each new prepaid program prior to card issuance.

For questions regarding the agent registration process or for assistance with the Visa Membership Management (VMM) application, please contact the Visa Third Party Agent group at:

**CAN, LAC and US** – agentregistration@visa.com
**AP and CEMEA** – agents@visa.com

Questions regarding the PIF submission process can be directed to:

**CAN, LAC and US** – PrepaidPrograms@visa.com
**AP and CEMEA** – Prepaid-PIF@visa.com

When registering a third party agent, the prepaid issuer must make the agent aware of the following two principles:

- ☑ Registration as a third party agent does not act as an endorsement of the agent's services by Visa.
- ☑ Registration of an agent is specific to each Visa prepaid issuer; separate agent registrations are required for each agent/issuer business relationship.

## 4.3 Third Party Agent Types

There are various types of third party agents, noted below, that a prepaid issuer may utilize. Agents may be classified as one or more of these agent types and must be registered for each unique agent type they represent.

**ISO Cardholder (ISO-C)** – Directly solicits prepaid cards to cardholders.

**ISO Prepaid (ISO-PP)** – Solicits other entities (e.g., merchants, large corporate clients, government entities, etc.) for the deployment and management of prepaid card programs. Many prepaid issuers outsource sales and marketing functions to ISOs and often have relationships with separate ISOs for each prepaid program.

**Third Party Servicers (TPS)** – Provide transaction functions (acceptance device connectivity, authorizations, clearing, and settlement) as well as back-office related activities (customer service, chargebacks/RFC processing, and reporting). Many Third Party Servicers are also able to manage fraud control and risk management functions. Third Party Servicers are required to be certified as PCI DSS compliant as they store, process, and/or transmit prepaid card information. A Third Party Servicer is also able to take on various ISO functions in addition to payment processing activities.

**Fulfilment Entities** – Are generally responsible for the packaging, storing, and shipping of non-personalized Visa products (e.g., warehouses, wholesalers, and logistics companies). There are two types of Fulfillment Entities that a prepaid issuer can contract with for the support of their prepaid programs: **Visa Approved Vendors** or **Distribution Channel Vendors (DCVs)**.

- **Visa Approved Vendors** – Are enrolled in the Visa Approved Vendor Program (AVP), which allows them to work with any Visa issuer without the issuer having to directly register the agent. For a global list of Approved Visa Vendors, visit the following Visa website: http://www.visa.com/splisting/
- **Distribution Channel Vendors (DCVs)** – Are also responsible for the packaging, storing, and shipping of non-personalized Visa products (e.g., warehouses, wholesalers, and logistics companies). However, **a DCV is not enrolled in the Visa Approved Vendor Program and thus each prepaid issuer utilizing their services must register them accordingly.**

For any questions whether a specific entity—contracted or subcontracted with a prepaid card issuer—falls under an aforementioned agent type and requires to be registered with Visa, please email:

**CAN, LAC and US** – agentregistration@visa.com
**AP and CEMEA** – agents@visa.com

Questions about the Visa Approved Vendor Program may be emailed to:
**CAN, LAC and US** – AVPamericas@visa.com;
**AP and CEMEA** – VendorCompliance@visa.comSection Footnote Style Examples (Heading 2)

## 4.4 Ongoing Due Diligence

### 4.4.1 Monitoring Third Party Agents

Prepaid issuers are fully accountable for the risks (financial, regulatory, reputational, and other) associated with their use of third party agents. Therefore, prepaid issuers are required to perform ongoing due diligence of all their third party agents. As part of this continuous oversight, issuers must conduct the following actions on an annual basis:

☑ Identify each third party agent and designate its role and activities it is authorized to perform on the issuer's behalf.

☑ Monitor ongoing compliance with the applicable agent oversight provisions in Appendix B, "Prepaid Issuer On-site Operational Review."

☑ Ensure that third party agents have access to a current version of the *Visa Interchange Directory* if the prepaid issuer uses the third party agent for processing of any of the following:

- Chargebacks
- Arbitrations
- Compliance
- Authorizations
- Referrals
- Fraud reporting
- Settlement

☑ Perform a financial analysis of each third party agent to evaluate continued solvency and the ability to support and maintain business operations; this must include periodic reviews of the agent's:

- Commercial or mercantile credit report,
- Updated financial statements,
- Recent income tax returns, and
- Other financial information lawfully available to the issuer.

☑ If applicable, obtain a valid PCI DSS Report on Compliance.

☑ Conduct ongoing reviews of product or service marketing materials, collateral, point-of-sale promotional materials, and any other advertising collateral in order to ensure they are compliant with the Visa Rules.

The following best practice is recommended:

☑ Third party agents with multiple roles (specifically ISO-PP and TPS) pose a higher concentration of risk. Therefore, such agents should be clearly identified and more closely monitored by the prepaid issuer.

### 4.4.2 File Retention

Prepaid issuers must maintain due diligence files on their third party agents, which should contain all initial due diligence documentation as well as all records pertaining to ongoing agent oversight. The issuer should maintain a unique file for each individual third party agent, and such agent files are to be retained for as long as applicable laws and regulations mandate, but no less than two years after the termination of the agent relationship.

## 4.5 Reporting Standards

When using third party agents, **a prepaid issuer must implement reporting standards for its agents** to track each agent's performance. These reporting standards are required to minimally include the following:

- ☑ Identification of key performance metrics that are to be reported (consult Section 6, "Funding Accountability: Monitoring).
- ☑ The manner in which reports are delivered to the issuer.
- ☑ How the issuer will access reporting systems used by the agent (where allowable and in compliance with laws and regulations).
- ☑ The frequency in which various reports are to be presented.
- ☑ The assignment of reporting responsibilities to specific employees in the third party agent's organization.

Agents must be made contractually responsible for compliance with the prepaid issuer's reporting standards. Any neglect by the agent to comply with the issuer's reporting standards may negatively jeopardize both the issuer and Visa.

**As part of the reporting standards, issuers are responsible for collecting summary-level reporting for each of their agents, quarterly at a minimum, and making this available to Visa upon request.**

## 4.6 Agent Risk Controls

**In conjunction with pre-defined reporting standards, issuers must ensure their agents have risk controls in place to rapidly detect a deviation in key performance metrics, indicating a potential threat.**

Issuers must work with their agents to develop and implement risk controls, which must remain in place throughout the duration of a prepaid card program. Issuers must ensure that their agents' risk control processes include:

- ☑ The use of key performance metrics as defined by the issuer's reporting standards.
- ☑ The assignment of specific thresholds for key performance metrics based on the issuer's risk tolerance.
- ☑ Generation of exception reports when thresholds are violated.

- ☑ Investigation of exception reports within a set timeframe in order to establish a cause for the threshold violation.
- ☑ A process outlining when and why specific exception reports are escalated to executive management for special handling.
- ☑ Remediation of what caused the threshold violation, mitigating any risk exposure.

Additionally, to ensure transparency, the prepaid issuer must have its agent:

- ☑ Provide the prepaid issuer with direct access to its systems (where legally permitted) to periodically monitor key performance metrics instead of relying on the agent's own monitoring.
- ☑ Provide the prepaid issuer with direct access to exception reports so the issuer can verify exceptions as having been investigated and resolved.

The proper use of agent risk controls, together with the issuer's direct inspection of the process, significantly contributes to a safe and sound prepaid program.

In scenarios where third party agents have direct relationships and agreements with VisaNet processors, **issuers must ensure third party agents acknowledge that the ultimate responsibility and accountability for Visa prepaid card programs lies with the prepaid issuer.**

## 4.7 Third Party Agent Contract Requirements

When entering into a relationship with a third party agent, prepaid issuers are to execute a contract **prior to the commencement of the agent's services. The issuer's third party agent contract must include the following elements:**

- ☑ Clear assignment of each party's roles and responsibilities.
- ☑ Regulatory and legal compliance requirements for the agent.
- ☑ Issuer approval of all prepaid program marketing, signage, and solicitation materials before they are used by the agent.
- ☑ The issuer name—and city if Visa-owned marks are used—must be easily identifiable on marketing materials.
- ☑ The agent's agreement to abide by the prepaid issuer's policies, Visa Rules, the Visa Prepaid Issuer Risk Program Standards, and applicable Visa supplemental requirements and guidelines.
- ☑ Clearly stated control requirements, timing, and responsibilities for funding, settlement, and reserves.

- ☑ The agent's responsibility for compliance with the issuer's reporting standards.
- ☑ The rights of the issuer or Visa to monitor, investigate, review, audit, and inspect the premises, records, performance metrics, or procedures of the third party agent as legally permitted.

The issuer must ensure that its contract with each third party agent contains the following clauses:

- ☑ **Agent acknowledgement of its obligation to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS) and/or Payment Application Data Security Standard (PA-DSS) as applicable.** Agents have an obligation to protect cardholder data, and issuers must educate their agents on the importance of this contractual obligation.
- ☑ **Provide for the immediate termination of an agent by the prepaid issuer for any circumstances that create harm or loss to the goodwill of the Visa payment system**. Prepaid issuers should invoke this clause when a prepaid agent's practices and exception item activity, including illegal activity, create a substantial risk of loss and/or harm to the payment system.
- ☑ **Clarify specific terms and conditions related to card shipping and storage.** If any of the prepaid cards are being distributed from a remote location under the direction of an agent, the agent contract must include card inventory management controls.

A prepaid issuer must ensure that its contract with each agent:

- ☑ **Prohibits card sales or issuance outside the licensed jurisdiction of the issuer unless in accordance with the *Visa Core Rules and Visa Product and Service Rules* or Visa Supplemental Requirements.**
- ☑ **Requires secure destruction of cardholder data after it is no longer needed.**
- ☑ **Executes a confidentiality/non-disclosure agreement with the third party agent.** This can be part of a broader agent agreement or as a standalone or addendum to the contract. The confidentiality/non-disclosure agreement must specifically ensure that:
  - Materials labeled as "Visa Confidential" are not distributed to outside the parties without written authorization from Visa.
  - Third party agents must comply with all applicable privacy laws, regulations, and PCI DSS in regards to any non-public (personal) information received by the third party agent under the program.

Each agent contract must be signed by the issuer and must remain on file at the issuer's place of business. After termination of the agent relationship, agent contracts are to be kept on file with the issuer no less than two years after termination/expiration or as long as the legal requirements of the issuer's jurisdiction mandate.

## 4.8 Agent Training

**Prepaid issuers must provide their agents with ongoing training to ensure agents are well versed on issuer and Visa policies, procedures, and regulations**. Issuers have an obligation to the Visa payment system to provide their agents with sufficient information to ensure they're able to comply with the Visa Rules.

To ensure compliance, the prepaid issuer should:

- ☑ Provide training after executing a contract with the third party agent and ongoing at least on an annual basis.
- ☑ Be actively engaged with their agents by providing necessary communications in order to support Visa prepaid programs.

# 5 Security Procedures

## 5.1 Issuing and Fulfillment

### 5.1.1 Card and PIN Fulfillment and Activation

As newly issued prepaid cards are delivered to customers, cards are at risk of being intercepted and used fraudulently. Not-received items (NRI) fraud risk can be reduced by using secure card-distribution and card-activation controls. Because prepaid cards may involve the use of third-party distribution warehouses to store cards, manage inventory, and ship cards for sale or distribution, issuers must ensure security controls are implemented.

In addition to the risks associated with physical card plastics, issuers must be aware of the risks associated with Prepaid Card Virtual Accounts. These are prepaid card programs where a physical card is not issued, but a Prepaid Card Virtual Account number is communicated to the account holder for ecommerce purchases. Visa Prepaid Card Virtual Account numbers can be communicated through use of a reference card or by other means and must be done in a secure manner.

The following requirements will help mitigate risks associated with prepaid card fulfillment, card activation, and PIN fulfillment:

**Card Fulfillment:**

- ☑ **Use secure card delivery methods as described in the *Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors.***
- ☑ **Send cards to an individual's verified address and not to a "ship to" address,** with the exception of gift cards as outlined below. Ensure correct or standardized addresses are used along with nondescript envelopes.
- ☑ **Research any change of address that occurs within 30 days of account opening**. Frequent updates of an address on a reloadable card may point to possible fraud.
- ☑ **Evaluate requests for express delivery of cards for potential risks.** Expedited delivery requests may potentially be motivated by fraud.
- ☑ **Ensure that corporate clients have inventory controls and secure storage practices in place**. For instance, obtain signed agreements from corporate clients accepting responsibility for prepaid cards.

Attention should be paid to the following best practices:

- ☑ Mail cards in an inactive state and **require that an activation process be initiated by the cardholder** once the card has been received.
- ☑ **Commingle cards with other types of mail pieces** to reduce theft during the card-delivery process.
- ☑ **Drop-ship cards going to high risk areas** and use a delivery method that can be tracked.
- ☑ **Set thresholds for when gift cards should be mailed to the purchaser vs. the recipient.** For example, gift cards over a certain value, or orders of two or more gift cards that exceed a certain value, should be mailed to the purchaser. Gift cards with amounts under a certain value can be shipped directly to the recipient.

### Card Activation:

- ☑ **Only use secure card-activation methods**—e.g., use a secure web page where cardholders can validate information and activate cards.
- ☑ **Provide interactive voice response (IVR) validation** methods to positively identify cardholders.
- ☑ **Print unique activation codes on sales receipts that require activation via interactive voice response or voice response unit (IVR/VRU)** for cards sold but not activated at the point of sale.
- ☑ **In order to validate cardholders for the activation of cards or selection of PINs, do not use readily available information.** Use information that would be known only to the cardholder, such as a previous address or phone number, or data elements acquired from credit reports (e.g., monthly mortgage or car payment amounts) if legally permitted.

### PIN Fulfillment:

- ☑ Send mailers with **pre-selected temporary PINs** that require the cardholder to call and change the PIN via an IVR/VRU.
- ☑ Ensure that PIN mailers and cards are mailed separately, a minimum of two days apart.
- ☑ Mail PINs directly to the verified cardholder address.
- ☑ Use nondescript envelopes to mail PINs.

### 5.1.2 Prepaid Clearinghouse Service

All prepaid issuers are advised to participate in Visa's centralized Prepaid Clearinghouse Service (PCS)[5], a database that allows prepaid issuers and their agents to share prepaid card data such as enrollments, load funding, suspected fraudulent information, and previously reported fraud on existing card accounts. The PCS information sharing service will facilitate identification of fraudulent enrollments, funding, use, and other fraud schemes involving prepaid cards.

By participating in Prepaid Clearinghouse Service, participants will have access to a holistic view of prepaid fraud across the industry, enabling them to detect and protect their customers and their portfolios from fraud. **Depending on jurisdiction, it may be mandatory for a prepaid issuer to participate in PCS.** For more information about this service, contact your Visa Account Executive.

## 5.2 Storage and Transport

### 5.2.1 The Reason for Security

Visa prepaid products typically come in two varieties: personalized cards that have the name of the cardholder imprinted or embossed on the card just like standard Visa credit and debit cards, and non-personalized cards that do not bear the name of the cardholder.

In the non-personalized product category, the absence of an individual's name on a card, even if replaced by a generic identifier, can pose additional risks. **Because Visa prepaid cards may become counterfeit stock for card skimming or other types of fraud,** it is important for prepaid issuers to implement appropriate security controls centered on storage and transport of physical cards for personalized and non-personalized prepaid cards alike.

### 5.2.2 Physical Card Security

Issuers that contract with companies to store or distribute large amounts of commercially ready Visa prepaid cards **are fully responsible for all cards issued by them and distributed or stored by the companies with which they contract.** Some examples of such companies include:

- Companies responsible for the packaging of commercially-ready retail prepaid cards
- Warehouses that store and ship commercially-ready prepaid cards

[5] PCS may not be available in all regions. Check your region for availability.

Storage and shipment of non-personalized Visa products must be in accordance with the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*. As a component of this:

☑ **Appropriate steps to mitigate card inventory risk must be implemented, particularly at locations where Visa card inventory is out of the issuer's direct control.** Examples: employer for salary cards, corporate partner for incentive cards, retailers, fulfillment houses, or other third party agents.

☑ **The following security steps must be implemented to ensure card inventory remains safe:**

- Limit access to card inventory to select, authorized personnel.
- Use dual control for all card handling.
- Use accountability controls for card stock.
- Have procedures for the secure storage of cards and regular tracking of card inventory.
- Perform routine audits of card stock and intermittent spot checks.
- Implement a notification procedure for missing cards.

### 5.2.3 Working with Fulfillment Entities

The Visa Rules include requirements for entities responsible for the packaging, storing, and shipping of non-personalized Visa products (e.g., warehouses, wholesalers and logistics companies). These entities are known as Fulfillment Entities. Issuers contract with Fulfillment Entities to store or distribute non-personalized, commercially-ready Visa prepaid cards. When contracting with Fulfillment Entities not enrolled in the Visa Approved Vendor Program—specifically designated as Distribution Channel Vendors (DCVs)—issuers must comply with the following:

☑ Prepaid issuers using DCVs are required to **register them as third party agents,** as described in more detail in the "Use of Third Party Agents" section of this guide.

☑ DCVs are not enrolled in the Visa Approved Vendor Program (AVP); however, prepaid issuers may require DCVs to enroll or DCVs may enroll voluntarily to become Visa Approved Vendors.

☑ If a prepaid issuer contracts with DCVs, the issuer **must validate the DCVs' compliance with the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*.**

☑ **DCVs are not permitted to conduct manufacturing, printing, or personalization of plastics,** as they are not Visa Approved Vendors.

Entities such as retailers that store and ship prepaid products exclusively for their own programs are not required to register as agents; however, the warehouses where the retailers' prepaid products are

packaged or stored, and the methods used for shipping to retail outlets, must still meet the security standards of the *Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*.

## 5.3 Data Security

**Where third party agents provide functions requiring access to cardholder or card information (including the storage or transmission thereof), the prepaid issuer must:**

- ☑ **Ensure the agent is certified as PCI DSS compliant.** NOTE: This must be validated directly with the agent by means of obtaining a PCI DSS Attestation of Compliance (AOC), Report on Compliance (ROC) or equivalent; using Visa's online list of compliant agents alone is not sufficient.
- ☑ **Validate continued PCI DSS compliance of the agent on an annual basis.**
- ☑ **Register the agent under the correct agent type in accordance with the Visa Rules.** NOTE: If the agent transports and/or stores card information, the agent must be registered as a Third Party Servicer (TPS).
- ☑ **Limit access to cardholder data to the extent that it is required for providing the services for which the third party agent is engaged by the issuer.**
- ☑ **Ensure sensitive data is destroyed when no longer needed for providing services to the issuer in accordance with the PCI DSS.**
- ☑ **Ensure that ISO-PP agents are not permitted to handle card plastics or have access to account number information.**

# 6 Loss Prevention

## 6.1 Hold and Control of Funds

**Issuers must hold and control funds associated with their prepaid programs in order to meet Visa settlement obligations and protect their organization financially.** This includes making sure policies cover the responsibilities, timing, and liabilities for funds settlement, reserve amounts, and pre-funding requirements. Failure to properly control prepaid program funds can result in issuer losses. Therefore, Visa prepaid card issuers must:

☑ **Ensure all funds associated with prepaid card accounts, including any agent reserves, are held and controlled by the issuer's financial institution.** The following prepaid programs are excluded from this requirement:

- Prepaid issuers in countries where applicable laws or regulations require funds to be held in approved trust accounts.
- Issuers of Visa prepaid Health Savings Account programs in the Visa US region, where funds are held in an IRS-approved trust account.
- Issuers of Visa Mobile Prepaid, where funds are held with an issuer-approved Mobile Network Operator partner financial institution.

☑ **Make sure that card-loading funds are remitted to the issuer as quickly as possible, if not immediately.**

☑ **Make certain all prepaid funds are only used for valid presentments or cardholder service fees.**

Prepaid issuers must preserve and maintain all outstanding balances loaded onto any prepaid product and are prohibited from using prepaid balances for purposes other than described in this section.

## 6.2 Fraud Monitoring

### 6.2.1 Tracking Key Performance Metrics

To maintain control over their prepaid programs, **it is crucial that prepaid issuers continuously track key performance metrics as part of their fraud monitoring efforts.**

Once reporting standards are put in place, prepaid issuers must develop risk controls that flag any metrics that deviate beyond pre-defined risk thresholds indicating potential fraud activity. Once flagged, exception reports must be generated for the issuer to review and investigate.

**At a minimum, the prepaid issuer must:**

☑ **Track key performance metrics at a minimum on a monthly basis.** Prepaid issuers must monitor cardholder activity for each third party agent/program manager as well as their overall prepaid portfolios, tracking the following key performance metrics at a minimum:

- Load transaction count and amount
- Load losses
- Sales and cash transaction volume
- Negative balance losses
- Fraud transaction losses
- Account balances

☑ **Track and review daily exception reports to detect cardholder activity that could expose the issuer to losses.** Prepaid issuers must implement processes to detect and prevent losses by reviewing:

- Negative balances by account and number of days in negative position
- Additional activity on accounts with negative balance
- Transaction activity outside their geographic jurisdiction
- Large increase in loads (amount and frequency) by load source
- Cards with a high volume of returns
- Other high fraud risk transaction activity

☑ **Conduct daily monitoring of funding of accounts.** Controls must be established to ensure the following are reviewed on a daily basis:

- Load transaction count and amount by source
- Account funding balances

☑ **Track and reconcile outstanding balances on a daily basis.**

### 6.2.2 Communicating With Law Enforcement

An effective fraud-monitoring process includes establishing a convenient mechanism for law enforcement to contact issuers to report fraudulent or criminal activity. Communication with law enforcement agencies can be an effective means to detect criminal activity that may have circumvented issuer risk controls. To leverage this information, issuers are encouraged to provide a centralized contact point where law enforcement can alert issuers to suspicious activity, serve notice for legal actions, or advise on potential AML issues. This can be accomplished through establishment of a centralized contact point using a website or by creating a call option on an existing 24/7 customer service number listed on the back of the card.

## 6.3 Reserves: Mitigation Risk Exposure

In order to mitigate risk exposure when utilizing third party agents, prepaid issuers must safeguard themselves by requiring agents to have collateral on deposit to cover card transactions and Visa settlement obligations. However, such collateral is a balance sheet liability and should be held and accounted for accordingly. In order to properly manage agent reserves, prepaid issuers must:

- ☑ **Hold and control all agent reserves.** Separate reserve accounts must be established for each agent. The prepaid issuer must assign responsibility to designated employees for holding and controlling agent reserves.
- ☑ Implement procedures to monitor and reconcile reserve balances in order to **ensure that reserve amounts remain adequate compared to the risk each third party agent poses to the issuer.**
- ☑ Ensure that agent reserves are **only used to cover direct program losses.**
- ☑ Establish written policies and procedures to determine **how and when reserves are to be collected from and distributed to an agent.**

In addition to these requirements, prepaid issuers are encouraged to develop specific guidelines on the collecting of reserves. Such guidelines should be based on prepaid program metrics (such as funds-in-transit) and overall issuer risk exposure.

# 7 Operational On-site Reviews

## 7.1 Overview

To support compliance with the Visa Prepaid Issuer Risk Program, operational on-site reviews of both issuers and third party agents are conducted on a periodic basis.

The on-site review is based on requirements outlined in this guide and assesses the issuer's (or agent's) risk policies, procedures, and controls. Additionally, the review process includes the evaluation of an issuer's due diligence and oversight functions related to managing risks associated with the use of third party agents. In certain cases, Visa may mandate a review of other prepaid program-related areas as necessary.

## 7.2 Before a Review

When a prepaid issuer or agent is selected for an operational on-site review, a list of Visa-approved review vendors is provided from which the issuer or agent must select a reviewer. Issuers and agents are required to use a Visa-approved vendor and are solely responsible for the costs of the review. In the event the prepaid issuer or agent prefers to work with a vendor that is not pre-approved by Visa, it may enter a request for Visa to evaluate the qualifications and suitability of the proposed vendor to perform the review. Visa does not guarantee the approval of proposed vendor requests.

As part of the review notification, the prepaid issuer or agent will also receive a "List of Materials: Pre-review Required Documentation," which lists documentation to be provided in electronic format to both the review vendor and Visa. This documentation includes organizational information, policies and procedures, reporting, program metrics, and key performance indicators and must be delivered no less than two weeks prior to the commencement of the review.

## 7.3 Report and Remediation

Based on the on-site observations, interviews, and testing, the independent reviewer will complete the Visa Prepaid Issuer Risk Review Questionnaire (see Appendix B) and draft a report detailing the review findings identified during the operational review. The draft report is then delivered to the prepaid issuer and a copy is sent to Visa for review. Visa may concur with the findings or make

recommendations (such as which findings must be remediated and which findings are to be considered best practices), and the report is subsequently finalized.

Upon receipt of the final report, the issuer will be responsible for working with the vendor to develop a timely and effective remediation plan. The issuer will successively work on the implementation of the remediation plan while providing periodic updates to the vendor. Once the issuer has completed implementation of the remediation plan, it must be validated by the vendor as completed. A post-remediation check must be performed by the reviewer 90 days after the remediation plan was completed; if this is passed and no new violations have occurred, the review process will be closed.

## 7.4 Review Timeline

The timeline of the review process will be dictated in the on-site review notification sent to the prepaid issuer or agent by Visa. Typically the on-site review is required to be completed within 60 days of receipt of the notification. After the on-site review has been completed, a specific timeline is provided to present the findings report to Visa and to develop the remediation plan that addresses the review findings. The issuer is then responsible for remediating the findings in an expedient manner with completion of the remediation plan validation being conducted by the reviewer.

Once remediation has been validated as complete by the review vendor, a post-remediation period commences that normally lasts 90 days, after which a post-remediation check is performed. The purpose of the post-remediation period and check is to ensure that new procedures and other remediation items were properly implemented and adopted by the issuer or agent and not discontinued or abandoned shortly after the review was completed. The post-remediation check is comprised of the reviewer asking for itemized test work that illustrates and validates the proper implementation of remediation items. When the check is passed, Visa will be notified and a notification of review completion is sent to the issuer or agent.

This process is intended to be a beneficial and education experience for the issuer or agent, with the outcome being a more resilient Visa partner with a safe and sound Visa prepaid program.

# A Appendix: Agent Control Requirements

## A.1 Overview

Visa clients that use third party agents ("TPAs" or "agents") are obligated to comply with the *Third Party Agent Due Diligence Risk Standards* as part of their overall agent control environment. Pertinent sections from the *Third Party Agent Due Diligence Risk Standards* have been included in this Appendix for easy reference; however, **it is imperative that prepaid issuers obtain and read the complete version of the *Third Party Agent Due Diligence Risk Standards* when engaging in a relationship with a third party agent.**

## A.2 Agent Policies

The policy requirements set forth by the *Third Party Agent Due Diligence Risk Standards* dictate that at a minimum, a Visa client's third party agent policies must address oversight and control of agent programs, including the following:

- Agent program strategy
- Underwriting and monitoring
- Settlement, funding, and reserves
- Data security standards
- Regulatory and legal compliance
- Training and education

## A.3 Onboarding

When contracting with third party agents, specific requirements must be fulfilled as part of the agent onboarding process. These requirements include the initial due diligence and registration of third party agents by Visa clients. Per the *Visa Third Party Agent Due Diligence Risk Standards*, **Visa clients that use agents must comply with all of the following requirements**:

- Perform a thorough background check of the agent and its principals, including a review of any relevant past or pending litigation.
- Complete an adequate financial review of the agent, which includes a review of current financials and an outside party review—i.e., Dunn & Bradstreet, Experian, Better Business Bureau, SSAE16,

or equivalent type of report—if available. Where appropriate, the financial review should include an examination of the third party agent's principals.

- Check and review all current and previous issuing business relationships of the agent, including previous doing-business-as (DBA) or alternate names.
- Review the agent for adequate policies, procedures, and controls established as they pertain to the type of business the agent is engaged in. These policies, procedures, and controls may include processes for compliance with Visa Rules, regional, and country laws (e.g., anti-money laundering) and other regulatory requirements.
- Confirm the agent has established adequate and timely monitoring and exception reporting processes that are accessible by the client.
- Verify the information provided by a prospective agent is correct. Whenever feasible, conduct a physical inspection of the business premises of a prospective agent to ensure appropriate controls and business practices are implemented.
- Register third party agents with Visa prior to the performance of any contracted services or transaction activity.
- An appropriate senior officer of the Visa client must review all documentation and approve the agent. Approval must be based on sound business practices that will not compromise either the client or Visa, and may not be based solely on any purported limitation of the client's financial liability in any agreement with the agent.
- Any agent that stores, processes, or transmits cardholder data must be registered with Visa and validated for Payment Card Industry (PCI) Data Security Standard (DSS) compliance. Clients are held responsible for their agents' initial compliance and ongoing revalidation. If the agent is in the process of becoming PCI DSS compliant, the client can still register the agent; however, the client must confirm that the agent has contracted with a Qualified Security Assessor (QSA) and has an expected date of compliance or is in the process of completing a PCI DSS Self-Assessment Questionnaire (SAQ D).
- If an agent (ISO, ESO, or TPS PIN) deploys ATM, POS, or kiosk PIN-acceptance devices that process and accept cardholder PINs and/or manage encryption keys, the client must ensure that the on-site review of the agent's PIN security controls is conducted to validate compliance with the *PCI PIN Security Requirements,* the *PCI Payment Transaction Security (PTS) Point-of-Interaction (POI) Modular Security Requirements,* and the *Visa PIN Security Program Guide*.

Additional requirements exist for non-issuers; thus for a complete list of requirements, Visa clients should obtain the *Third Party Agent Due Diligence Risk Standards* publication for a complete list of requirements.

## A.4 Monitoring and Reporting

The *Third Party Agent Due Diligence Risk Standards* outline basic ongoing requirements for all Visa clients using third party agents that must be complied with; these requirements include the following:

- Confirmation that agents are compliant with Visa Rules, local, country, and regional laws or regulations.
- Establishment and execution of oversight procedures to control risks associated with third party agents. These include reviews of an agent's operations and business practices on an annual basis (or more frequent if needed) and the review of solicitation materials—e.g., websites, promotional collateral, cardholder applications, etc.—used by third party agents.
- Taking prompt and appropriate action if Visa risk monitoring programs identify an agent to be introducing substantial risk into the Visa payment system.
- Ensuring any services provided by agents on behalf of the client are performed by the agents themselves and are not subcontracted to other entities. If subcontracting is necessary for business reasons, the client must treat the subcontracted entity as a third party agent.

## A.5 Termination

Third party agents have a duty to conduct themselves in a professional manner and to protect the integrity of the Visa payment system. In the event a third party agent circumvents the Visa Rules, violates the law, or commits acts that harm the Visa brand, the agent may be removed from the system. Specific provisions must be included in agent contracts that allow the Visa client to terminate the relationship if the agent participates in any activities that violate the Visa Rules, laws, or generally operates in an unsound or unsafe manner.

**Visa clients are reminded that they are ultimately responsible for the conduct of the third party agents they sponsor. Ongoing oversight for compliance with the Visa Rules and other requirements is an integral part of the use of agents.**

## A.6 Additional Information

For more information and a complete list of requirements for Visa clients using third party agents, please refer to the *Visa Third Party Agent Due Diligence Risk Standards*, which is available as a Visa Supplemental Requirements publication and available from Visa Online.

# B Appendix: Prepaid Issuer On-Site Operational Review Questionnaire

This section complements the standards outlined within this guide and contains the questionnaire utilized as part of an on-site operational review. **Visa or approved review vendors may amend this questionnaire with additional requirements and inspections as mandated by the Visa Rules.**

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| **1: RISK POLICIES – Policy Requirements** | | | | |
| **1.1** | **The issuer is able to provide a copy of their prepaid program strategy.** | | | |
| **1.2** | **The issuer is able to provide a copy of their agent diligence and monitoring policy.** | | | |
| **1.3** | **The issuer's third party agent due diligence and monitoring policy specifically addresses the following areas:** | | | |
| 1.3.A | Initial due diligence | | | |
| 1.3.B | Agent agreements/contracts | | | |
| 1.3.C | Agent application requirements | | | |
| 1.3.D | Agent registration | | | |
| 1.3.E | Change in ownership requirements | | | |
| 1.3.F | Ongoing due diligence | | | |
| 1.3.G | Reporting standards for agents | | | |
| 1.3.H | Communication and training | | | |
| 1.3.I | Holding of funds | | | |
| 1.3.J | Agent termination | | | |
| **1.4** | **The issuer is able to provide a copy of their funding and reserve requirements policy.** | | | |
| **1.5** | **The issuer is able to provide a copy of their data security policy.** | | | |
| **1.6** | **The issuer is able to provide a copy of their regulatory and legal compliance policy.** | | | |
| **1.7** | **The issuer is able to provide a copy of their policy on education and training for third party agents.** | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| **1.8** | **The issuer is able to provide board resolutions, minutes, or other written documentation validating that the issuer's prepaid program policies have been formally approved by the Board of Directors or an applicable executive management committee.** | | | |
| **2: RISK POLICIES – Anti-Money Laundering Program** | | | | |
| **2.1** | **The issuer has a written prepaid Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) program and/or has incorporated prepaid card issuance into its existing written AML/ATF program** | | | |
| **2.2** | **The issuer's prepaid AML/ATF program includes at a minimum the following requirements, with which the issuer is in compliance:** | | | |
| 2.2.A | Written internal AML/ATF policies, procedures and controls over the issuer's prepaid program | | | |
| 2.2.B | Appointment of a designated "AML Officer" (or equivalent) responsible for the implementation and management of the AML/ATF program | | | |
| 2.2.C | Screening of trade-sanction watch-lists in accordance with applicable laws and regulations | | | |
| 2.2.D | Ongoing training of employees on the AML/ATF program | | | |
| 2.2.E | Ongoing independent testing of the AML/ATF program | | | |
| 2.2.F | If the issuer outsourcers any component of its AML/ATF program, it periodically audits its third parties' activities to ensure compliance with AML/ATF requirements | | | |
| **2.3** | **If reloadable cards or prepaid cards that allow for cash access are issued, the issuer maintains a written Customer Identification Program (CIP) that complies with all applicable regulatory requirements** | | | |
| **2.4** | **As part of its written Customer Identification Program (CIP), the issuer collects cardholder identifying information including at a minimum: name, physical address, DOB, government identification number for reloadable or prepaid cards that allow for cash access** | | | |
| **2.5** | **CIP must include procedures for determining whether the cardholder appears on any government sanctions lists before issuing cards and periodically afterwards** | | | |
| **2.6** | **The issuer maintains internal controls and monitoring processes to identify inappropriate card usages that pose potential AML/ATF risk including, but not limited to, the following:** | | | |
| 2.6.A | Controls to prevent issuance of prepaid cards in countries/regions outside the issuer's licensed jurisdiction, except when permitted by the Visa Rules | | | |
| 2.6.B | Controls to prevent the unintended bulk sale of cards or use of unintended distribution channels | | | |
| 2.6.C | Controls to limit the number of cards issued to each cardholder | | | |
| 2.6.D | Procedures for customer identification and due diligence reviews at account opening (for reloadable cards or prepaid cards that allow for cash access) | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 2.6.E | Procedures to screen cardholder information obtained through the CIP against government sanctions lists prior to account opening, during transaction processing, and periodically thereafter | | | |
| 2.6.F | Controls to block cash disbursements and quasi-cash transactions for non-reloadable cards when no cardholder information is on file | | | |
| 2.6.G | Controls to identify and block transactions occurring in countries designated as state sponsors of terrorism by the issuer's local government | | | |
| 2.6.H | Controls for velocity and transaction limits on account loads, withdrawals, and ATM cash and POS transactions (daily, weekly, monthly, and annually) | | | |
| 2.6.I | Procedures to for high-volume account funding transactions followed by cash withdrawals (either distributed over several locations or at one single site) | | | |
| 2.6.J | Card-usage pattern and program comparison controls—e.g., determine whether card usage is consistent with the specific card program and review card-to-card transfers within card programs | | | |
| **2.7** | **If the prepaid issuer uses third party agents, the issuer must ensure that each of their agents have sufficient AML/ATF controls in place to meet all relevant legal requirements including the following:** | | | |
| 2.7.A | Conducts appropriate due diligence to ensure agents abide by the issuer's AML/ATF policy, or have policies in place that the issuer has reviewed and approved | | | |
| 2.7.B | Communicates and trains its agents on the issuer's AML/ATF requirements on an ongoing basis | | | |
| 2.7.C | Monitors each agent's transaction activity directly rather than relying solely on agents providing monitoring data to the issuer. Periodically tests transaction activity to ensure card usage is commensurate with the type of prepaid programs | | | |
| 2.7.D | Requires agents to allow issuer access to Customer Identification Program records | | | |
| 2.7.F | Adopts a restricted-issuance policy that agents must use, which includes a list of prohibited industries based on an internal risk assessment | | | |
| **2.8** | **The issuer has included employee training as a primary component of its AML/ATF program and provides AML/ATF-related training for new employees and applicable staff members, annually at a minimum** | | | |
| **2.9** | **The employee AML/ATF training materials include the following subject matter:** | | | |
| 2.9.A | Updates to AML/ATF laws and regulations (when applicable) | | | |
| 2.9.B | Sanctions compliance | | | |
| 2.9.C | Customer Identification Program procedures | | | |
| 2.9.D | Monitoring and detection of unusual activity | | | |
| 2.9.E | Suspicious activity reporting requirements and procedures | | | |
| 2.9.F | AML/ATF oversight of third party agents | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| **2.10** | **The issuer has documented policy and procedures in place for investigating unusual or suspicious activity in accordance with all applicable regulations** | | | |
| **2.11** | **The issuer's suspicious activity policy and procedures include:** | | | |
| 2.11.A | Descriptions of what may constitute suspicious activity and the development of exception condition criteria | | | |
| 2.11.B | Processes on how to identify, investigate, track, and report suspicious activity | | | |
| **3: USE OF THIRD PARTY AGENTS – Initial Due Diligence** | | | | |
| **3.1** | **The issuer collects and completes the following items, at a minimum, as part of its third party agent due diligence process:** | | | |
| 3.1.A | The issuer is in compliance with the *Third Party Agent Due Diligence Risk Standards* (see Appendix A). | | | |
| 3.1.B | Agent application information and documentation is verified for accuracy. | | | |
| 3.1.C | Doing Business As (DBA) name | | | |
| 3.1.D | Third party agent legal name | | | |
| 3.1.E | Third party agent location information, including full physical address—not post office boxes. | | | |
| 3.1.F | Government-issued company identification numbers, such as tax identification numbers, and the source or issuing authority of the government identification numbers | | | |
| 3.1.G | Company legal status (e.g., corporation, partnership, sole proprietorship, or other) and location of legal filing | | | |
| 3.1.H | First and last names of company principals. If the agent is a sole proprietor, also collect middle initial and tax identification number. | | | |
| **3.2** | **The issuer conducts background checks of third party agents and their principal(s) to identify potential negative business practices that could impact the business relationship, and determines whether there has been a PCI DSS violation/breach or any other compliance issues in the past. The issuer's background checks include:** | | | |
| 3.2.A | References from various external third party entities, such as:<br>Government agencies and regulators<br>Suppliers and vendors<br>Trade associations and chambers of commerce<br>Creditors and banking relationships | | | |
| 3.2.B | AML/ATF review on the principal(s) as required by local law | | | |
| 3.2.C | Research of prior public business filings; e.g., bankruptcies and past civil litigations | | | |
| 3.2.D | Commercial or mercantile credit report | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 3.2.E | Detailed review of agent's website and screening of customer service phone number(s) | | | |
| 3.2.F | Internet complaint boards and consumer advocacy sites/forums | | | |
| **3.3** | **Physical site inspections of its agent's business are conducted to validate the suitability for the type of business the agents will engage in (e.g., follow the guidelines within the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendor* where applicable).** | | | |
| **3.4** | **The issuer conducts thorough reviews of its agent's financial condition and historical performance (e.g., examines financial statements, operational metrics and key performance indicators).** | | | |
| **3.5** | **The issuer obtains and reviews product or service marketing materials and any other advertising collateral in order to ensure they are compliant with the Visa Rules.** | | | |
| **3.6** | **If applicable, the issuer ensures a security assessment has been completed and findings were remediated, in order to protect the integrity of cardholder information in accordance with the PCI DSS. (Obtain a PCI DSS Report on Compliance or equivalent.)** | | | |
| **3.7** | **The issuer ensures all applicable registrations or licenses required are in place for the third party agent to conduct business.** | | | |
| **3.8** | **The issuer completes an adequate financial review of the agent's principals if they accept financial liability (e.g., personal guarantee).** | | | |
| **3.9** | **The issuer conducts quantitative and qualitative risk analyses to properly evaluate the risk exposure new agents pose and to underwrite agents for the specific role they will fulfill.** | | | |
| **4: USE OF THIRD PARTY AGENTS – Registration** | | | | |
| **4.1** | **The issuer has a contract in place with every third party agent.** | | | |
| **4.2** | **The issuer performs thorough due diligence reviews of agents prior to registering the agent.** | | | |
| **4.3** | **Agents are registered with Visa prior to the performance of any contracted services or transaction activity.** | | | |
| **4.4** | **The issuer pays registration fees for each registered agent, both initially and annually, where applicable.** | | | |
| **4.5** | **The issuer submits a *Prepaid Program Information Form* (PIF) to Visa in order to obtain approval for each new prepaid program prior to card issuance.** | | | |
| **4.6** | **The issuer informs agents that registration as a third party agent does not act as an endorsement of the agent's services by Visa; and that the registration of an agent is specific to each Visa prepaid issuer, and separate agent registrations are required for each agent/issuer business relationship.** | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| **5: USE OF THIRD PARTY AGENTS – Ongoing Due Diligence** | | | | |
| **5.1** | **The issuer carries out the following prescribed actions on an annual basis:** | | | |
| 5.1.A | Identifies each third party agent and designates its role and activities it is authorized to perform on the issuer's behalf. | | | |
| 5.1.B | Monitors ongoing compliance with the applicable agent oversight provisions in Appendix B, "Prepaid Issuer On-site Operational Review." | | | |
| 5.1.C | Ensures that third party agents have access to a current version of the *Visa Interchange Directory*, if the prepaid issuer uses the third party agent for processing of any of the following:<br>Chargebacks<br>Arbitrations<br>Compliance<br>Authorizations<br>Referrals<br>Fraud reporting<br>Settlement | | | |
| 5.1.D | Performs periodic financial reviews of third party agents to ensure continued solvency and the ability to support and maintain business operations by using the following:<br>Commercial or mercantile credit report<br>Updated financial statements<br>Recent income tax returns<br>Other financial information lawfully available to the issuer | | | |
| 5.1.F | Obtains a valid PCI DSS Report on Compliance (if applicable). | | | |
| 5.1.G | Conducts ongoing reviews of the agent's product or service marketing materials and other advertising collateral in order to ensure they are compliant with the Visa Rules. | | | |
| **6: USE OF THIRD PARTY AGENTS – Reporting and Controls** | | | | |
| **6.1** | **The issuer has defined and implemented reporting standards for its agents with the function of tracking each agent's overall performance.** | | | |
| **6.2** | **The issuer's reporting standards for its agents include the following:** | | | |
| 6.2.A | Key performance metrics to be reported | | | |
| 6.2.B | The manner in which reports are delivered to the issuer | | | |
| 6.2.C | Definition of how the issuer will have access to the agent's reporting systems (where allowable and in compliance with laws and regulations) | | | |
| 6.2.D | The frequency in which various reports are to be presented | | | |
| 6.2.E | The assignment of reporting responsibilities to specific employees in the third party agent's organization | | | |
| **6.3** | **The issuer collects summary-level reporting for each of its agents on a quarterly basis at a minimum and makes this available to Visa upon request.** | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| **6.4** | **The issuer ensures that all its agents have risk controls in place that include the following:** | | | |
| 6.4.A | The use of key performance metrics as pre-defined by the issuer's reporting standards | | | |
| 6.4.B | The assignment of specific thresholds for key performance metrics based on the issuer's risk tolerance | | | |
| 6.4.C | The generation of exception reports when thresholds are violated | | | |
| 6.4.D | A process outlining when and why specific exception reports are escalated to executive management for special handling | | | |
| 6.4.E | The remediation of what caused the threshold violation, mitigating any risk exposure | | | |
| **6.5** | **The issuer has direct access to its agent's systems (where legally permitted) to periodically monitor key performance metrics instead of relying on the agent's own monitoring.** | | | |
| **6.6** | **The issuer has agents provide direct access to exception reports so the issuer can verify highly suspicious exceptions as having been investigated and resolved.** | | | |
| **7: USE OF THIRD PARTY AGENTS – Contracts and Training** | | | | |
| **7.1** | **The third party agent contract must include the following elements:** | | | |
| 7.1.A | Clear assignment of all party's roles and responsibilities | | | |
| 7.1.B | Regulatory and legal compliance requirements for the agent | | | |
| 7.1.C | Issuer approval of all prepaid program marketing, signage, and solicitation materials before they are used by the agent | | | |
| 7.1.D | The issuer name—and city if Visa-owned marks are used—must be easily identifiable on marketing materials. | | | |
| 7.1.E | The agent's agreement to abide by the prepaid issuer's policies, the Visa Rules, the *Visa Prepaid Issuer Risk Program Standards* and applicable guidelines | | | |
| 7.1.F | Clearly stated control requirements, timing, and responsibilities for funding, settlement, and reserves | | | |
| 7.1.G | The agent's responsibility for compliance with the issuer's reporting standards | | | |
| 7.1.H | The rights of the issuer or Visa to monitor, investigate, review, audit, and inspect the premises, records, performance metrics, or procedures of the third party agent as legally permitted | | | |
| **7.2** | **The issuer contract with each third party agent contains the following clauses:** | | | |
| 7.2.A | Agent acknowledgement of its obligation to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS) and/or Payment Application Data Security Standard (PA-DSS) as applicable | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 7.2.B | Provision for immediate termination of an agent by the issuer for any significant circumstances that create harm or loss to the goodwill of the Visa payment system | | | |
| 7.2.C | Clarification of specific terms and conditions related to card shipping and storage | | | |
| **7.3** | **The issuer's contract with each third party agent:** | | | |
| 7.3.A | Prohibits card sales or issuance outside the licensed jurisdiction of the issuer unless in accordance with the Visa Rules. | | | |
| 7.3.B | Requires secure destruction of cardholder data after it is no longer needed. | | | |
| 7.3.C | Executes a confidentiality/non-disclosure agreement with the third party agent. The confidentiality/non-disclosure agreement specifically stipulates that: | | | |
| 7.3.C.1 | Visa confidential materials are not distributed to outside parties without written authorization from Visa. | | | |
| 7.3.C.2 | Third party agents must comply with all applicable privacy laws, regulations and PCI DSS in regards to any non-public (personal) information received by the third party agent under the program. | | | |
| **7.4** | **The issuer provides its agents with ongoing training to ensure agents are well versed on issuer and Visa policies, procedures, and regulations.** | | | |
| **7.5** | **The issuer provides training after executing a contract with a third party agent and ongoing at least on an annual basis.** | | | |
| **7.6** | **The issuer is actively engaged with its agents by providing necessary communications in order to support Visa prepaid programs.** | | | |
| **8: SECURITY PROCEDURES – Issuing, Fulfillment, and Storage** | | | | |
| **8.1** | **The following requirements have been established by the issuer to help mitigate risks associated with prepaid card fulfillment:** | | | |
| 8.1.A | The issuer uses secure card delivery methods as described in the *Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors.* | | | |
| 8.1.B | Cards are sent directly to an individual's verified address and not to a "ship to" address. | | | |
| 8.1.C | Any change of address that occurs within 30 days of account opening is researched. | | | |
| 8.1.D | Requests for express delivery of cards are evaluated for potential risks. | | | |
| 8.1.E | In case of corporate clients, the issuer ensures that the client has inventory controls and secure storage practices in place. | | | |
| **8.3** | **The following requirements have been established by the issuer to help mitigate risks associated with prepaid card activation:** | | | |
| 8.3.A | Only secure card activation methods are used. | | | |
| 8.3.B | Interactive voice response (IVR) validation methods are provided to positively identify cardholder. | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 8.3.C | For cards sold but not activated at the point of sale, unique activation codes are printed on the sales receipt that requires activation via interactive voice response or voice response unit (IVR/VRU). | | | |
| 8.3.D | No readily available information is used when validating cardholders for the activation of cards or selection of PINs. | | | |
| **8.4** | **The following requirements have been established to help mitigate risks associated with prepaid card PIN Fulfillment:** | | | |
| 8.4.A | Mailers are sent with pre-selected temporary PINs that require the cardholder to call and change the PIN via an IVR/VRU. | | | |
| 8.4.B | The issuer ensures that PIN mailers and cards are mailed separately, a minimum of two days apart. | | | |
| 8.4.C | PINs are mailed directly to the verified cardholder address. | | | |
| 8.4.D | Only nondescript envelopes are used to mail PINs. | | | |
| **8.5** | **Storage and shipment of non-personalized Visa products is performed in accordance with the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors.*** | | | |
| **8.6** | **The issuer has implemented appropriate steps to mitigate card inventory risk, particularly at locations where Visa card inventory is out of the issuer's direct control.** | | | |
| **8.7** | **The issuer has implemented the following security steps to ensure card inventory remains safe:** | | | |
| 8.7.A | Access to card inventory is limited to select, authorized personnel. | | | |
| 8.7.B | Dual control is used for all card handling. | | | |
| 8.7.C | Accountability controls for card stock are used. | | | |
| 8.7.D | Procedures exist and are used for the secure storage of cards and regular tracking of card inventory. | | | |
| 8.7.E | Routine audits of card stock and intermittent spot checks are performed. | | | |
| 8.7.F | A notification procedure for missing cards has been implemented. | | | |
| **8.8** | **If the issuer has contracted with Distribution Channel Vendors (DCVs), it is in compliance with the following:** | | | |
| 8.8.A | The issuer has registered DCVs as third party agents. | | | |
| 8.8.B | The issuer has taken steps to ensure that the DCVs adhere to the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors.* | | | |
| 8.8.C | The issuer has ensured that the DCVs are not permitted to conduct manufacturing, printing, or personalization of plastics. | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| **9: SECURITY PROCEDURES – Data Security** | | | | |
| **9.1** | **If the issuer has third party agents providing functions that require access to cardholder or card information (including the transmission or storage thereof), the prepaid issuer:** | | | |
| 9.1.A | Ensures such agents are certified as PCI DSS compliant. NOTE: This must be validated directly with the agents by means of obtaining a PCI DSS Attestation of Compliance (AOC), Report on Compliance (ROC), or equivalent; using Visa's online list of compliant agents alone is not sufficient. | | | |
| 9.1.B | Validates continued PCI DSS compliance of the agent on an annual basis. | | | |
| 9.1.C | Registers such agents under the correct agent type. E.g., if any agent transports and/or stores card information, the agent has been registered as a Third Party Servicer (TPS). | | | |
| 9.1.D | Ensures access to cardholder data is limited to the extent that it is required for providing the services for which third party agents are engaged by the issuer. | | | |
| 9.1.E | Ensures sensitive data is destroyed when no longer needed for providing services to the issuer in accordance with the PCI DSS. | | | |
| 9.1.F | Ensures that ISO-PP agents are not permitted to handle card plastics or have access to account number information. | | | |
| **10: LOSS PREVENTION – Hold and Control** | | | | |
| 10.1 | **The issuer has full control over the funds associated with its prepaid programs in order to meet Visa settlement obligations.** | | | |
| 10.2 | **All funds associated with prepaid card accounts, including any agent reserves, are held and controlled by the issuer's financial institution (unless the prepaid program is excluded from this requirement as defined under the "Hold and Control" section of this guide).** | | | |
| 10.3 | **The issuer makes sure that card load funds are remitted to the issuer as quickly as possible, if not immediately.** | | | |
| 10.4 | **The issuer only uses prepaid funds for valid presentments or cardholder service fees.** | | | |
| **11: LOSS PREVENTION – Monitoring** | | | | |
| **11.1** | **The issuer tracks the following key performance metrics at a minimum on a monthly basis, monitoring cardholder activity for each third party agent/program manager as well as their overall portfolio:** | | | |
| 11.1.A | Load transaction count and amount | | | |
| 11.1.B | Load losses | | | |
| 11.1.C | Sales and cash transaction volume | | | |
| 11.1.D | Negative balance losses | | | |

| Questionnaire Section and Compliance Statement | | Finding | | |
|---|---|---|---|---|
| | | Yes | No | N/A |
| 11.1.E | Fraud transaction losses | | | |
| 11.1.F | Account balances | | | |
| **11.2** | **The issuer has implemented processes that track and review daily exception reports on the following parameters in order to detect and prevent losses:** | | | |
| 11.2.A | Negative balances by account and number of days in negative position | | | |
| 11.2.B | Additional activity on accounts with negative balance | | | |
| 11.2.C | Transaction activity outside its geographic jurisdiction | | | |
| 11.2.D | Large increase in loads (amount and frequency) by load source | | | |
| 11.2.E | Cards with high volume of returns | | | |
| 11.2.F | Other high fraud risk transaction activity | | | |
| **11.3** | **The issuer has controls established to ensure the following are reviewed on a daily basis:** | | | |
| 11.3.A | Load transaction count and amount by source | | | |
| 11.3.A | Account funding balances | | | |
| **11.4** | **The issuer tracks and reconciles unused funds and account balances on a daily basis.** | | | |
| **12: LOSS PREVENTION – Reserves** | | | | |
| **12.1** | **If the prepaid issuers is holding agent reserves, the issuer is in compliance with the following:** | | | |
| 12.1.A | The issuer holds and controls all agent reserves. | | | |
| 12.1.B | Separate reserve accounts are established for each agent. | | | |
| 12.1.D | The issuer has implemented procedures to monitor and reconcile reserve balances to ensure reserve amounts remain adequate compared to the risk each third party agent poses to the issuer. | | | |
| 12.1.E | Agent reserves are only used by the issuer to cover direct program losses. | | | |
| 12.1.F | As part of the issuer's "Holding of funds" policy (see 1.3.I of this questionnaire), the issuer has specific procedures to determine how and when reserves are to be collected from and distributed to an agent. | | | |
| **13: Prepaid Issuer Self-Assessment Questionnaire** | | | | |
| **13.1** | **The issuer completes the Prepaid Issuer Self-Assessment Questionnaire (see Appendix C, *Prepaid Issuer Self-Assessment Questionnaire*) on an annual basis.** | | | |

# C Appendix: Prepaid Issuer Self-Assessment Questionnaire

The Prepaid Issuer Self-Assessment Questionnaire (SAQ) must be completed by a prepaid issuer upon the inception of a prepaid card program and on an annual basis thereafter. The issuer must provide a copy of the completed SAQ when requested by Visa.

| Topic and Question | | Performance | | |
|---|---|---|---|---|
| | | Pass | Fail | N/A |
| **Policies** | | | | |
| 1 | Do you have formal underwriting, due diligence, monitoring, and control policies governing agents (ISOs, third-party servicers, or fulfillment entities) that support your Visa prepaid card program? | | | |
| 2 | Has the Board of Directors or an executive management committee formally approved and adopted such policies, governing use of agents that manage components of your prepaid card programs? | | | |
| 3 | Have you implemented a functional AML/ATF program or incorporated prepaid card issuing into your existing AML/ATF program, inclusive of procedures and controls that address AML/ATF, the screening of trade-sanction watch lists, and employee training on your AML/ATF program? | | | |
| **Registration** | | | | |
| 4 | If you use third party agents that fulfill any component of your Visa prepaid card program, have you registered each agent with Visa? | | | |
| 5 | Has a *Prepaid Program Information Form (PIF)* been submitted to Visa in order to obtain approval for each new prepaid program prior to card issuance? | | | |
| **Security** | | | | |
| 6 | If any of your Visa prepaid cards are being distributed from a remote location under the direction of an agent, does your contract with the agent include required card inventory management controls? | | | |
| 7 | Have you conducted an initial review or an ongoing due diligence review for each agent within the past twelve months? | | | |
| 8 | Have you ensured that all applicable agents are certified as PCI DSS compliant for their appropriate levels? NOTE: This must be validated directly with the agent; using Visa's online list of compliant agents alone is not sufficient. PCI DSS compliance of the agent is continuously validated by the issuer on an annual basis. | | | |
| 9 | Is agent access to cardholder data expressly limited to that required for providing the services for which the third party agent or service provider is engaged? | | | |
| 10 | Do you formally require agents to securely destroy cardholder data when it is no longer needed for the contracted services? | | | |

| Topic and Question | | Performance | | |
|---|---|---|---|---|
| | | Pass | Fail | N/A |
| 11 | Is any agent that is not enrolled in the Visa Approved Vendor Program annually validated to comply with the *Visa Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors*? | | | |
| 12 | Do you restrict ISOs from physically handling plastics and having access to account number information? | | | |
| **Activity Monitoring and Reporting** | | | | |
| 13 | Have you implemented reporting standards for your agents with the function of tracking each agent's key performance metrics, including loads, transactions, losses and balances, for each agent at least on a monthly basis? | | | |
| 14 | Do you have access to each agent's system and the ability to create or view key reports (if permitted by laws and regulations)? | | | |
| 15 | In conjunction with the reporting standards implemented for your agents, do you have pre-defined risk controls in place in order to quickly detect deviations in performance metrics, indicating a potential risk threat to your card program(s)? | | | |
| **Funds and Reserves** | | | | |
| 16 | Are all Visa prepaid funds and agent reserves held and controlled by your institution? | | | |
| 17 | Are monitoring reports on agent reserves and account funding available? | | | |
| 18 | Do you have policy and procedures to determine the specific conditions to collect reserves from or release reserves to an agent? | | | |
| 19 | Have you established controls to ensure that agent reserves may only be used to cover direct program losses? | | | |
| 20 | Do you have controls in place to ensure prepaid funds are only used for valid presentments and cardholder service fees? | | | |
| **Issuance and Fulfillment** | | | | |
| 21 | Have you implemented policies and procedures to ensure cards are only issued to residents within your licensed jurisdiction(s)? | | | |
| 22 | Card storage and delivery methods are only performed as described in the *Global Physical Security Validation Requirements for Data Preparation, Encryption Support and Fulfillment Card Vendors.* | | | |
| 23 | Do your reloadable cards require activation that validates a cardholder's identity? | | | |
| 24 | Are card-activation methods secure—e.g., do they use a web page that can authenticate the cardholder before activating the card? | | | |
| **Risk Controls** | | | | |
| 25 | Do you have specific thresholds assigned to key performance metrics based on your calculated risk tolerances? | | | |
| 26 | Do you track and review key exceptions, including unusual loads and accounts with negative balances? | | | |

| Topic and Question | | Performance | | |
|---|---|---|---|---|
| | | Pass | Fail | N/A |
| 27 | Do you block all cash disbursement and quasi-cash transactions for non-reloadable cards when no cardholder information is on file? | | | |
| **Statutory and Regulatory Considerations** | | | | |
| 28 | Do you perform load screening to prevent doing business with individuals or countries prohibited by your local government to engage in commerce with? | | | |
| 29 | Have you established policies or procedures to file suspicious activity reports (SARs) or equivalent for losses when circumstances warrant? | | | |
| 30 | Do you perform customer identification and due diligence reviews at account set-up (for reloadable cards or prepaid cards that allow for cash access)? | | | |

# Glossary

| Term | Definition |
|---|---|
| **A** | |
| **Account Number** | An Issuer-assigned number that identifies an account in order to post a Transaction. |
| **Address Verification Service (AVS)** | A VisaNet service through which a Merchant can verify a Cardholder's billing address before completing a Transaction under specific conditions. |
| **Agent** | An entity that acts as a VisaNet Processor, a Third Party Agent, or both. |
| **AML/ATF** | Anti-Money Laundering and Anti-Terrorist Funding. |
| **Automated Teller Machine (ATM)** | An unattended Magnetic-Stripe or Chip-reading Terminal that has Electronic Capability, accepts PINs, and disburses currency. |
| **Authorization** | A process where an Issuer, a VisaNet Processor, or Stand-In Processing approves a Transaction. This includes Offline Authorization. |
| **Authorization Code** | A code that an Issuer, its VisaNet Processor, or Stand-In Processing provides to indicate approval of a Transaction. The code is returned in the Authorization Response message and is usually recorded on the Transaction Receipt as proof of Authorization. |
| **Authorization Request** | A Merchant or Acquirer request for an Authorization. |
| **B** | |
| **Bank Identification Number (BIN)** | A 6-digit number assigned by Visa and used to identify a Member or VisaNet Processor for Authorization, Clearing, or Settlement processing. |
| **C** | |
| **Card Verification Value (CVV)** | A unique check value encoded on the Magnetic Stripe of a Card to validate Card information during the Authorization process. The Card Verification Value is calculated from the data encoded on the Magnetic Stripe using a secure cryptographic process. |

| Term | Definition |
|---|---|
| **Card Verification Value 2 (CVV2)** | A unique check value printed on the back of a Card, which is generated using a secure cryptographic process, as specified in the Payment Technology Standards Manual. |
| **Cardholder** | An individual who is issued and authorized to use either or both a Card or Virtual Account |
| **Cash Disbursement** | Currency, including travelers cheques, paid out to a Cardholder using a Card, excluding Cash-Back. |
| **Clearing** | All of the functions necessary to collect a Clearing Record from an Acquirer in the Transaction Currency and deliver it to the Issuer in the Billing Currency, or to reverse this transaction, or to process a Fee Collection Transaction. |
| **Customer Identification Program (CIP)** | A regulatory program related to collecting information on financial institution customers as part of AML/ATF measures. Also referred to as "Know Your Customer" or "KYC." |
| **D** | |
| **Decline Response** | An Authorization Response where the Transaction was declined. |
| **Distribution Channel Vendor (DCV)** | A Third Party Agent responsible for the packaging, storing, and shipping of pre-manufactured, commercially ready Visa Products (for example: warehouses, card packagers, logistics companies). "Pre-manufactured, commercially ready" refers to non-personalized Visa Products that have already been manufactured, encoded, embossed/printed and are ready for sale or distribution to Cardholders. |
| **F** | |
| **Fulfillment Card Vendor** | A company that is responsible for the packaging, storing and shipping of non-personalized Visa products (e.g., warehouses, wholesalers, logistics companies). |
| **Fulfillment Entity** | A type of Fulfillment Card Vendor that is enrolled in the Visa Approved Vendor Program and therefore can work with any issuer and is not subject to agent registration. |

| Term | Definition |
|---|---|
| **I** | |
| **Independent Sales Organization (ISO)** | An organization whose bank card-related business relationship with a Member or third party involves any of the following:<br>• Merchant solicitation, sales, or service<br>• Merchant Transaction processing solicitation<br>Cardholder solicitation or Card application processing services. |
| **Issuer** | A Member that enters into a contractual relationship with a Cardholder for the issuance of one or more Card products. |
| **M** | |
| **Member** | A client of Visa U.S.A., Visa International, Visa Worldwide, or Visa International Servicios de Pago España, S.R.L.U. or a customer that has entered into a Services Agreement with Visa Canada. Requirements for membership are defined in the applicable Visa Charter Documents. |
| **Merchant** | An entity that accepts a Visa Card for the sale of goods or services and submits the resulting Transaction to an Acquirer for Interchange, directly or via a Payment Facilitator. A Merchant may be a single Merchant Outlet or represent multiple Merchant Outlets. |
| **Merchant Agreement** | A direct contract between a Merchant and an Acquirer or between a Sponsored Merchant and a Payment Facilitator, containing their respective rights, duties, and obligations for participation in the Acquirer's Visa or Visa Electron Program. |
| **Merchant Category Code (MCC)** | A code designating the principal trade, profession, or line of business in which a Merchant is engaged, as specified in the Visa Merchant Data Standards Manual. |
| **P** | |
| **Partial Authorization** | An Authorization for an amount less than the amount requested by a Merchant for a Transaction on a Visa Card. |

| Term | Definition |
|---|---|
| **Point-of-Transaction Terminal** | A device used at the Point-of-Transaction that has a corresponding Point-of-Transaction Capability. The Visa Rules refer to the following types of Point-of-Transaction Terminals:<br>• Account-Number-Verifying Terminal (US Region)<br>• ATM<br>• Chip-Reading Device<br>• Contactless Payment Terminal (US Region)<br>• Magnetic-Stripe Terminal<br>• Unattended Cardholder-Activated Terminal |
| **Prepaid Account** | An account established by an Issuer, with previously deposited, authorized, or transferred funds, which is decreased by purchase Transactions, Cash Disbursement, or account fees. |
| **Processor** | See VisaNet Processor. |
| **S** | |
| **Settlement** | The reporting and funds transfer of Settlement Amounts owed by one Member to another, or to Visa, as a result of Clearing. |
| **T** | |
| **Third Party Agent** | An entity, not defined as a VisaNet Processor, that provides payment-related services, directly or indirectly, to a Member and/or stores, transmits, or processes Cardholder data.<br>No financial institution eligible to become a Principal Member of Visa may serve as a Third Party Agent.<br>A Third Party Agent does not include:<br>• Financial institutions that perform Agent activities<br>• Affinity Co-Brand Partners or Global Co-Branding Partners<br>• Card manufacturers<br>• Card personalizers |
| **Transaction Record** | A paper record issued by, or in connection with, a Point-of-Sale Acceptance Device. |

| Term | Definition |
|---|---|
| **V** | |
| **Visa Prepaid Card** | A Visa Card used to access funds in a Visa Prepaid Account or a Card where monetary value is stored on a Chip. |
| **Visa Prepaid Card Transaction** | The act between a Cardholder using a Visa Prepaid Card and a Merchant or an Acquirer resulting in a Transaction Receipt. |
| **VisaNet** | The systems and services, including the V.I.P. System, Visa Europe Authorization Service, and BASE II, through which Visa delivers Online Financial Processing, Authorization, Clearing, and Settlement services to Members, as applicable. |
| **VisaNet Processor** | A Member, or Visa-approved non-Member, that is directly connected to VisaNet and that provides Authorization, Clearing, or Settlement services to Merchants and/or Members. |