Visa Acceptance Risk Standards (VARS)

October 2024

Visa Public

Introduction

As a global leader in digital payments, Visa connects consumers, businesses, and financial institutions to enable secure growth, so that businesses can thrive, while customers are protected and satisfied. The proliferation of digital payments has offered significant opportunity for business growth, and with it introduced greater security threats. To keep pace with the challenges, Visa is dedicated to staying ahead of the rapidly evolving threat landscape through making strategic investments and enhancements. This includes efforts to reduce fraud, enumeration, illegal activity, and disputes.

Visa and our clients share a common objective: to enable secure growth through upholding the security and integrity of the Visa Payment System. Visa is updating and enhancing requirements for Acquirers, due to the increasing complexity of players involved and technological advancements in payment methods, and the resulting rise of compromising activities. Compliance with these standards will assist Acquirers, Third-Party Agents, and Merchants in developing processes and tools that support innovation and facilitate secure growth. Strengthening an Acquirer's risk controls helps minimize activities that adversely affect the ecosystem and its participants. It also helps reduce friction for the consumer.

The Visa Ecosystem Risk Program guide aims to mitigate the risks associated with the payment environment. The program consists of four main components: **Visa Acceptance Risk Standards (VARS), Visa Integrity Risk Program** (VIRP)**, Visa Monitoring Programs, and Account Information Security Program.**

The **Visa Acceptance Risk Standards (VARS)** is a risk control framework designed to help safeguard Acquirers and the Visa payment system. The clients include Acquirers and Money Movement Entities, who use the Visa Payment Network (VisaNet).

The **Visa Integrity Risk Program** (VIRP) is a framework and set of requirements to deter, detect, and remediate illegal activity from the Visa Payment System. It helps Acquirers, their TPAs, and their Merchants maintain proper controls and oversight to prevent illegal activity. It includes a registration process for Acquirers in High Integrity Risk processing.

Visa Monitoring Programs are the tools and processes that Visa uses to assess the performance and compliance of its clients against the VARS, other Visa Rules, and regulations. The programs include reviews, and reports that provide feedback and guidance to the clients on how to improve their risk posture and address any issues or gaps.

© 2024 Visa. All rights reserved. Visa Public

Account Information Security Program are the requirements and best practices that Visa and its clients must follow to protect the confidentiality, integrity, and availability of cardholder data and payment transactions. These include adhering to the Payment Card Industry Data Security Standard (PCI DSS) and reporting any incidents of data breach or compromise to Visa.

The guide is intended to help Visa clients understand their roles and responsibilities in the Visa Ecosystem Risk Programs and provide them with the necessary information and resources to meet the expectations and requirements. The Visa clients can gauge their performance and success in fulfilling these roles and responsibilities through key performance indicators outlined in the Visa Ecosystem Risk programs. Appendix J: for Successful key performance indicators.

© 2024 Visa. All rights reserved. Visa Public

Table of Contents

© 2024 Visa. All rights reserved. Visa Public

Appendix

© 2024 Visa. All rights reserved. Visa Public

1 Visa Acceptance Risk Standards Overview

The **Visa Acceptance Risk Standards (VARS)** is a risk control framework designed to help safeguard the Visa payment system. The most recent version, which is periodically updated, is accessible via Visa Access. This document has replaced the **Global Acquirer Risk Standards (GARS).**

All participants involved in the Visa Payments System, either directly or indirectly, share the responsibility of minimizing risks to ensure customer trust and safety. Direct participants include Acquiring entities and Money Movement Entities, and indirect participants include Third-Party Agents (e.g., Payment Facilitators, ISOs), Merchants, and Third-Party Reviewers.

Complying with VARS helps Acquirers, their Third-Party Agents, and their Merchants develop strategies and tools to monitor risk events, while promoting innovation, and encouraging business growth.

The Visa Core Rules and Visa Product and Service Rules collectively known as the Visa Rules, hold the Acquirer responsible for Merchant and Third-Party Agent oversight and any losses incurred by either entity. **The VARS is a supplementary document to the** Visa 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.

1.1 Guide Purpose

The VARS is designed to help Acquirers:

- Understand their accountabilities and responsibilities to the Visa payment system.
- Implement required controls and consider adopting recommended controls where applicable.
- Manage and control their relationships with Merchants and TPAs.
- Effectively and efficiently mitigate risks related to payment security (fraud) and integrity.

1.2 How This Guide is Organized

The VARS guide is organized as follows:

Section 1: VARS Overview explains the background and purpose for the VARS.

Section 2: Key Attributes of VARS explains the Acquirer archetypes and control approach.

Section 3: Ensuring Compliance explains the control requirements' compliance process.

Section 4: Risk Domains and Controls by Archetype is the main content on risk domains, control requirements and mandatory/recommended controls for Acquirer archetypes.

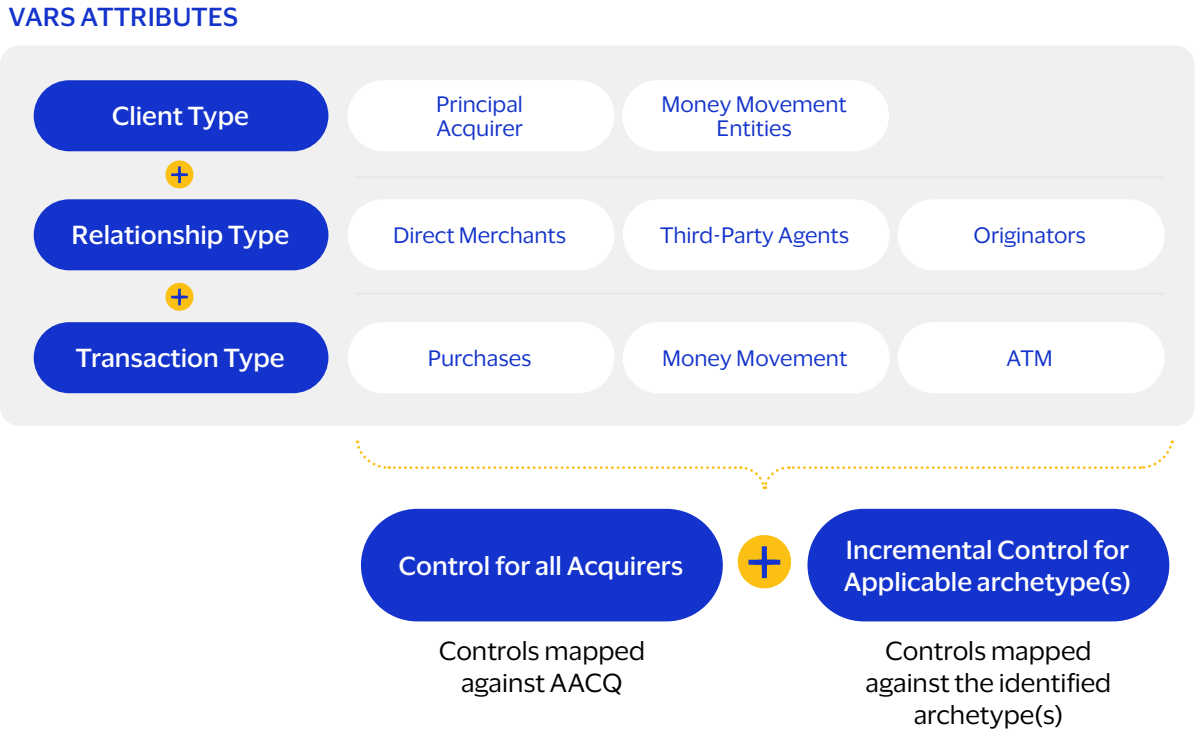
Section 5: VARS Reviews explains the process to conduct a control review to ensure adherence to VARS, followed by a post-review remediation process.

© 2024 Visa. All rights reserved. Visa Public

2 Key Attributes of VARS

2.1 Defining Acquirer Archetypes

To reflect different business models, we have defined Acquirer archetypes. These are based on the type of Visa Client, Acquirer Relationship, and Transactions, as seen in the graphic below.



Refer to Appendix A: Types of Visa Client, Acquirer Relationship and Transactions for key definitions of the terms listed above.

NOTE: For this document, the term **"Acquirers"** refers to Principal Acquirers and/or Money Movement Entities offering acquiring services, unless otherwise specified.

© 2024 Visa. All rights reserved. Visa Public

Acquirer archetypes are listed below. Each of these archetypes require a unique set of risk controls.

ACRONYM	ACQUIRER ARCHETYPE	DESCRIPTION
AACQ	All Acquirers	All Acquirers regardless of their portfolio and business characteristics
ATPA	Acquirers sponsoring TPAs	Acquirers who do not directly interact with Merchants but contract with a TPA. Refer to Appendix E.2 for TPA Types
AHIR	Acquirers processing for High Integrity Risk Transaction Merchants	Visa-licensed Acquirer and their TPAs, who sponsor and process transactions for High Integrity Risk Merchants.
AATM	Acquirers processing for ATMs	Acquirers who provide acquiring services to ATM Operators.
AVDC	Money Movement Entities originating Visa Direct transactions	Money Movement Entities who originate money movement transactions using Visa Direct rails.

2.2 Identifying Acquirer Archetypes

Acquirers can determine the archetype(s) applicable to them by reviewing the following questions. **The archetypes are not mutually exclusive, i.e., Acquirers can have more than one archetype that is applicable to their business.**

AACQ is applicable to all Acquirers. If an Acquirer's answers "Yes" for below questions, then the respective archetype applies.

ARCHETYPE QUESTIONNAIRE

	ACQUIRER RESPONSE	ARCHETYPE
Visa Client		
Are you a Money Movement Entity and originate Visa Direct transactions?	Yes	**AVDC**
Acquirer Relationships		
Do you contract with TPAs?	Yes	**ATPA**
Acquirer Transaction Type		
Do you process for High Integrity Risk Transaction Merchants?	Yes	**AHIR**
Do you provide ATM acquiring services?	Yes	**AATM**

© 2024 Visa. All rights reserved. Visa Public

2.3 Control Approach

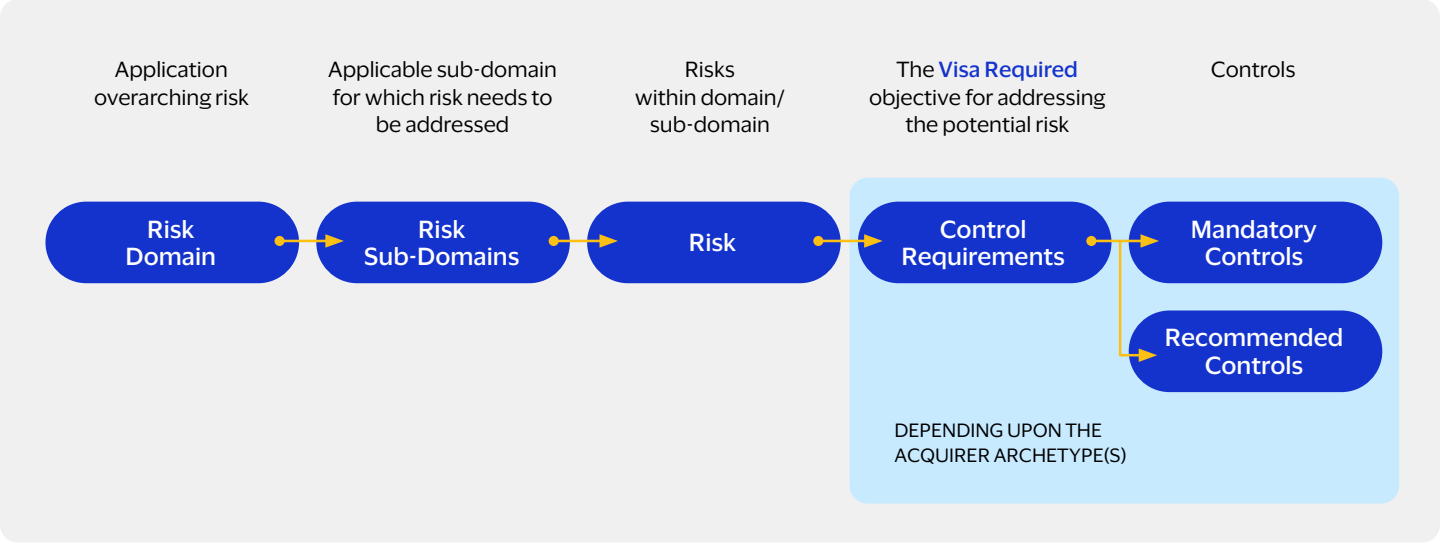
Key risks in the acquiring/acceptance activities have been defined along with their control requirements.

- **Risk Taxonomy (Risk Domain/Sub-domain)** are the types of risk that apply to Acquirers, and include Business, Operational, or Legal & Regulatory Risk.
- **Control Requirements** are specific requirements that must be fulfilled by the relevant Acquirer archetype(s) to minimize potential risk.

Included with each control requirement is the background on the necessity of the control and details on mandatory and recommended controls.

- **Mandatory Controls:** Acquirer must comply with to satisfy the Control Requirement. These mandatory controls are the minimum requirements, but they do not ensure all risk is eliminated
- **Recommended Controls:** Optional controls which are shaped by each Acquirer's program in line with their risk tolerance, and regulations.

LAYOUT FOR VARS CONTROLS



© 2024 Visa. All rights reserved. Visa Public

2.4 Risk Taxonomy

VARS is structured around three risk domains: **Business, Operational,** and **Legal & Regulatory Risk**. Controls should be implemented in a manner that is commensurate with the level of risk the Visa Rules, applicable regulatory requirements, and the Acquirer's risk appetite. The risk domains are broken into sub-domains as below:

Refer to Appendix C: Risk Taxonomy for key definitions of the risk domains and sub-domains from the VARS purview.

© 2024 Visa. All rights reserved. Visa Public

3 Ensuring Compliance

3.1 VARS Compliance: Meeting Control Requirements

To mitigate risks, Acquirers must ensure that control requirements are met.

- All Acquirers must comply with the control requirements applicable to **AACQ (all Acquirers),** as outlined in Section 4.1.
- If an Acquirer contains an additional archetype, they must comply with the control requirements outlined in that archetype's section. (Acquirer archetype: AACQ - ATPA - AHIR - AATM - AVDC)
- Acquirers are able to implement alternative solutions, if it equally meets all applicable requirements.

Key Notes:

- All Acquirers must comply with the applicable laws and regulations in addition to the Visa Rules.
- For any region or country specific requirements, refer to the Visa Rules **and the Acquirer's legal team**
- Acquirers are liable for the actions of their Merchants, TPAs, and employees.

© 2024 Visa. All rights reserved. Visa Public

4 Risk Domains and Control Requirements by Archetype

This section outlines the risks, control requirements, mandatory controls and recommended controls by archetypes.

4.1 All Acquirers (AACQ)

The following control requirements are applicable for **all Acquirers**. The control requirements have been categorized under overarching risks and related sub-domains.

4.1.1 Business Risk

We define Business risk as the risk that the Acquirer does not achieve its business objectives as a result of its risk strategy, and/or risk management execution against its strategy.

Risk Appetite and Policy Framework

1	6	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

The absence of a clearly defined Acquirer risk appetite or tolerance, thorough Acquiring policy documents, uniform implementation procedures, and skilled staff could lead to a decline in operational or financial performance, which may result in potential fraud and regulatory noncompliance.

CONTROL REQUIREMENT #1

AACQ.C1

Acquirers must maintain a defined risk appetite/tolerance as well as risk management capabilities that are adequate for their business model.

AACQ.C1.1 – Alignment Between Business Plans and Risk Policies

Maintaining an evolving risk management approach that aligns with the Acquirer's business plan involves implementing up-to-date risk policies and effective controls. Rigorous due diligence is crucial in this process, aiding in the identification and assessment of the risks associated with different Merchant activities across different jurisdictions. As the business plan and risk profiles evolve, it is imperative to adapt the risk policy and controls accordingly to ensure operational effectiveness and sustainability.

© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. Acquirers must define a **risk tolerance/appetite,** inclusive of risk policies and approval procedures by merchant activity segments, including those that are permissible, conditionally restricted, and prohibited. In addition, the plan must specify the countries from which the Acquirer aims to conduct different business activities.
2. The Acquirer must have well developed **risk policies** that define the Acquirer's approach on risk management, including roles & responsibilities, Merchant underwriting and risk monitoring, Merchant termination and incident investigation / response, settlement management, complaint handling, exception reporting, data security and data retention, business continuity planning, and disaster recovery. Policies will typically include:
    a. A risk policy that defines the Acquirer's overall risk appetite, tolerance or strategy that is aligned with the business plan.
    b. An underwriting policy crafted for various business segments (defined by merchant activities, countries, origination channel), including defined requirements, submission/approval process, and signing authority matrix.
    c. If applicable, a TPA policy that determines requirements, responsibilities including oversight and monitoring capabilities.
3. Risk policies must be documented and **approved** by the Board of Directors or an Executive Level Committee. The policy must be subject to version controls, and periodically reviewed.
4. Acquirers must have a governance process in place to manage and **oversee the implementation of risk policies**. This includes driving awareness across the organization, implementing adequate controls, measuring performance and managing exceptions.
5. Acquirers must establish Key Risk Indicators (KRIs) and/or Key Performance Indicators (KPIs) to **measure their performance against the defined risk appetite**. These may include approval rates, decline reasons, dispute and fraud rates, payment volume trends, credit and operational losses, level of noncompliance identifications (e.g., under Visa risk programs).
6. The **competencies and training of staff** must align with the business plan, with clear organizational responsibilities that support the execution of the Acquirer's strategy.

© 2024 Visa. All rights reserved. Visa Public

4.1.2 Operational Risk

We define Operational risk as the risk of loss due to internal/external events, external relationships, or inadequate/failed internal processes.

Written Agreements

3	5	1
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

The absence of a written agreement for Acquirers can lead to misunderstandings, legal vulnerabilities, insufficient evidence in case of disputes, potential financial losses, and reputational damage.

CONTROL REQUIREMENT #1

AACQ.C2

Acquirers must have contractual binding agreements with Merchants/ TPAs that assures compliance with the acquiring strategy.

AACQ.C2.1 - Merchant Agreement Content

A Merchant agreement is a direct contract between a Merchant and an Acquirer containing their respective rights, duties, and obligations for participation in the Visa's Acquiring Program. The Agreement may be tailored by the Acquirer for Merchants in different MCCs or lines of business, and in totality may include requirements from other payment networks, as long as the requirements for accepting Visa payments are included. Acquirers should consult their internal Legal teams while constructing the written agreements, in accordance with Visa's standards.

Mandatory Controls:

1. Acquirers must have a Merchant Agreement with each of its Merchants to accept Visa Payments. The agreement must require the Merchant to:
   a. Adhere to the Acquirer's policies and procedures as per their defined risk tolerance, and training that they have received and acknowledged.
   b. Fulfill its responsibilities in accordance with applicable laws and regulations.

© 2024 Visa. All rights reserved. Visa Public

c. Comply with the Visa Rules.

d. Refrain from knowingly submitting any transactions that are illegal or that the Merchant should have known were illegal.

e. Recognize Visa's right to limit or terminate the Acquirer's agreement with the Merchant.

f. In the event of an ongoing investigation at the time the Merchant Agreement is signed, the Merchant must fully cooperate with the investigation until its completion, in compliance with local laws and regulations and as per the instructions in What to Do If Compromised.

2. The agreement must have a clause that allows for the revocation of Visa acceptance of a Merchant by the Acquirer for any activity that may create harm or loss to the goodwill of the Visa payment system. The agreement must have a clause to support Acquirer action.

   a. After verifying that Visa has prohibited a Merchant from participating in Visa acceptance programs, Acquirers must suspend all Visa processing no later than the date specified by Visa (if applicable).

   b. The Merchant must be notified in writing if the Acquirer terminates the Merchant agreement.

   c. In case where the Merchant is terminated for cause, they are listed on the Terminated Merchant File (e.g., Visa Merchant Screening Service (VMSS).

3. The Merchant agreement should outline the following prohibitions:

   a. Resubmission of previously disputed charges: One cannot submit a transaction that has been previously disputed and returned to the Merchant.

   b. Submission or execution of fraudulent or unauthorized transactions: It is not acceptable to knowingly submit a fraudulent or unauthorized transaction into the payment system.

   c. Transaction laundering (TL): Transactions that are knowingly intended to hide the true source and nature of the transaction by layering them through what appear as low risk but in fact it is prohibited goods or services as per the Visa Rules.

   d. Data security breach: Unauthorized storage, processing, or transmission of payment data through non-approved software and processes are prohibited, as is the failure to enforce data security requirements for Merchants/TPA.

   e. Acquirer Disclosure: This includes a disclosure page or section that identifies the Acquirer and its responsibilities when a TPA is part of the agreement.

Recommended Controls:

1. Consider the following elements in the Merchant agreement:

   a. Transaction terms: This includes the conditions necessary for the completion of payment, delivered directly to the Merchant. The details of the financial institution where the Acquirer deposits funds for Visa transaction payments are also included.

   b. Fee Differentiation: This section separates fees associated with Visa transactions from those linked to other card transactions for clarity.

© 2024 Visa. All rights reserved. Visa Public

c. Information Provision to Visa: This includes all required and suitable rights under applicable laws, regulations, privacy policies, or agreements to share Merchant information with Visa,and the use of a Merchant's logo presented alongside the Merchant transaction details in digital formats (for example, in a cardholder's digital statement), to aid cardholders in identifying transactions and to minimize instances of disputes due to unrecognized transactions.

d. Although not required, acquirers may choose to reference the Visa risk standards in their Merchant agreements. Any Merchant agreement executed on or before October 20, 2024 may reference the Global Acquirer Risk Standards (GARS) and does not need to be updated. However, any Merchant agreement executed on or after October 21, 2024 must reference the Visa Acceptance Risk Standards (VARS).

Risk Statement

Failure to mitigate exposure during an acquisition of new Merchant could lead to financial losses.

CONTROL REQUIREMENT #2

AACQ.C3

Acquirers must have a clause in their contractual binding agreements with Merchants/TPAs that enables exposure mitigation coverage.

AACQ.C3.1 – Exposure Mitigation

It is critical to include a clause in an Acquirer's contractual binding agreement with Merchants/TPAs on exposure mitigation when using reserves, personal/corporate/bank guarantees, or account/transaction level holds.

Mandatory Controls:

1. The clause in an Acquirer's contract with a Merchant outlines the below points to enable exposure mitigation using reserve or other means such as personal or bank guarantees, and account level holds or transactions level holds for all direct and indirect relationships with an Acquirer:
   a. If the Acquirer is using Merchant reserves, they must explain that these are collateral that are property of the Merchant, which is held and controlled by the Acquirer in a unique deposit account in the Merchant's or Sponsored Merchant's name or other means that ensure segregation of funds.
   b. Acquirers explain the different types of exposure mitigation usage and ensure clarity on the reconciliation process.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Failure to settle funds timely and as agreed upon in the contractual binding agreements could lead to financial losses, regulatory noncompliance, reputational damage, and legal issues.

CONTROL REQUIREMENT #3

AACQ.C4

Acquirers must settle funds to the Merchant/TPA as per the terms described in the contractual binding agreement and take any applicable withholdings into consideration.

AACQ.C4.1 – Settlement of Funds

Acquirers have a responsibility for settlement. It is important for Acquirers to fund or credit Merchants, Marketplaces, Sponsored Merchants, Payment Facilitators (PayFacs), or Digital Wallet Operators (DWOs) promptly after the clearing of a transaction.

Mandatory Controls:

1. The Merchant Agreement stipulates that the Acquirer settles funds in accordance with regulations to the signing party:
   a. Acquirers must promptly pay or credit its Merchant's, Marketplace's, Sponsored Merchant's, PayFac's, DWO's, or Ramp Provider's account after transaction deposit. These payments are equal the Transaction totals, deducting any Credit Transactions or Original Credit Transactions, relevant discounts, Disputes, other agreed fees, or Merchant reserve funds (if applicable) accumulated to secure the Merchant's, Sponsored Merchant's, Marketplace's, PayFac's, or DWO's payment system obligations to the Acquirer.
   b. Acquirers settle within market-based timelines, provided there are no mandated holding periods (e.g., Future Service Merchants) or ongoing investigations. Acquirers retain settlements to offset any Disputes or financial losses directly associated with the Merchant.
   c. The Merchant Agreement states that Acquirers are responsible for providing settlement funds to the Merchant. Ensuring the security and proper handling of Merchant funds is a fundamental responsibility of Acquirers.

© 2024 Visa. All rights reserved. Visa Public

Onboarding

3	12	4
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Acquirers that have ineffective onboarding standards could onboard Merchants involved in illegal activities, deceptive practices, and/or have elevated Dispute activity. This could lead to financial losses, reputational damage, and legal issues.

CONTROL REQUIREMENT #1

AACQ.C5

Acquirers must have an onboarding standard that enables risk-based due diligence processes.

AACQ.C5.1 – Underwriting Policy

An onboarding standard for all Merchants put in place by the Acquirer enables risk-based due diligence processes and can protect Acquirers from financial and legal risk.

Mandatory Controls:

1. Acquirers establish an onboarding policy that is risk-based and appropriately segments Merchants into risk categories such as low (e.g., small/individual Merchants), medium, and high (e.g., Future Sales activity, VIRP High Integrity Risk merchant categories, Enterprise entities or Pay by link Merchants). All TPAs (regardless of risk-level) and Merchants in high integrity risk categories are underwritten to confirm:
   a. Credit worthiness and that their business model aligns with the Acquirer's defined risk tolerance.
   b. Controls are in place to detect and prevent activities that may potentially harm the Visa payment system, the Visa brand, or submitting illegal transactions to VisaNet.
   c. Merchants/TPAs operate within the allowed jurisdiction(s) and are compliant with all relevant regulations.
   d. Merchant Outlet locations are not misrepresented.

© 2024 Visa. All rights reserved. Visa Public

2. Acquirers assign the MCC to a Merchant Outlet that most accurately describes its business.
3. Acquirers assign 2 or more MCCs to a Merchant Outlet if either:
   a. The Merchant Outlet has deployed an automated fuel dispenser and sells fuel or other goods or services in a face-to-face environment.
   b. Separate lines of business are located at the same Merchant Outlet and one or more of the following applies:
      i. A separate Merchant agreement exists for each line of business.
      ii. Multiple Merchant Outlets on the same premises display different Merchant names.
      iii. An e-commerce Merchant Outlet contains a link to a separate e-commerce website, and each website qualifies for a different MCC.
4. Acquirers assign a unique Card Acceptor Identification (CAID) number to each Merchant/TPA, as specified in the Visa Rules.
5. Acquirers must consult both their internal lists of terminated and declined profiles, as well as external resources such as the Terminated Merchant File (e.g., VMSS), before finalizing a contract with a prospective Merchant. If a match is found with a Merchant listed on the Terminated Merchant File, Acquirers:
   a. Conduct the search using Legal Entity name, contacts, and owner details as available.
   b. Verify if the Merchant in question is the same one for whom the inquiry was made.
   c. Engage with the Acquirer who listed the Merchant to understand the reasons behind their inclusion in the file.
   d. Make an informed decision about accepting the merchant, based on a thorough investigation using the Terminated Merchant File, credit reports, local business registries, and other relevant sources.
6. Acquirers must develop a risk-based underwriting process to help identify, assess, and manage the risks associated with onboarding new Merchants either through automated systems or enhanced due diligence review process. The policy and process must be reviewed and updated periodically to reflect changes in regulatory requirements, industry best practices, and the organization's risk appetite.
   a. Acquirers enhance their underwriting process by utilizing automated systems and use diverse models which can efficiently verify a merchant's identity, evaluate credit ratings, conduct fraud checks, and validate the business intent as per the submitted application, making the process more precise and efficient. Underwriting process must include the following steps:
      i. **Implement a robust verification process:** This is to confirm seller authenticity, including verification of name, address, email, phone number, business registration checks, and document verification.

© 2024 Visa. All rights reserved. Visa Public

ii. **Assess the creditworthiness of the Merchant:** This involves analyzing credit history, financial statements, and performance, existing debts, and public records to assess their ability and likelihood to fulfill financial obligations.

iii. **Assess Business Activity:** Acquirers assess the Merchant's business plan, review URLs (if applicable), type of goods or services offered, delivery methods, return policies, and detect templated or counterfeit websites that lack real traffic and fulfilling the services or goods for the engaged consumers. High Integrity Risk Merchants may require additional due diligence to assess compliance with the requirements as defined in the VIRP.

iv. **Assess Compliance:** The Merchant must comply with all relevant laws and regulations, including those related to data security and privacy. This also includes compliance with card network rules.

v. **Assess Merchant Business Location:** The Merchant business location is evaluated. Certain locations may present higher risks based on factors such as local laws and levels of fraud.

vi. **Assess Merchant's Service Provider(s):** Identifying the service provider(s) used by Merchant to process, transmit, or store Cardholder data. Ensure the service provider is registered as a TPA with Visa and compliant with Payment Card Industry Data Security Standard (PCI DSS), per the Visa Account Information Security Program requirements.

vii. **Assess Merchant's Business History:** The Merchant's business history, including any previous merchant accounts and processing history, is reviewed. Any history of instances of termination (screening VMSS or other Terminated Merchant Files), excessive chargebacks, fraud, or illegal activity can impact the underwriting decision.

viii. **Issue decision on the Merchant application:** Approve, Decline or Conditional approval which might involve exposure mitigation strategies such as reserves, holds, limitations on business activity, or guarantees.

ix. **Auto-Boarding (Automated Onboarding):** Automated underwriting and onboarding will often result from the use of decision or risk models, which may also include the use of artificial intelligence (AI). Model risk should be evaluated, and a fit-for-purpose model risk management framework should ensure model risk is properly assessed. If the decision on the Merchant application is based on auto-boarding process, and the Acquirer contracts with a TPA, Acquirer needs to comply with applicable regulatory requirements and refer to Visa's Payment Facilitator and Marketplace Risk Guide for more auto-boarding best practices.

x. In the event of a significant risk event involving an auto-boarded or manually onboarded Merchant, Acquirers must assess if deficiencies or flaws in the onboarding process could have contributed and remediate any findings to prevent future occurrences.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

A lack of KYC/KYB procedures could lead to an increase in illegal activities, which may result in financial losses, potential fraud, regulatory noncompliance, reputational damage, and legal issues.

CONTROL REQUIREMENT #2

AACQ.C6

Acquirers must execute KYC/KYB checks in accordance with applicable jurisdictional laws and regulations.

AACQ.C6.1 – KYC/KYB Data Collection

Collecting KYC/KYB data from Merchants and conducting regular updates allows Acquirers to have the most up-to-date information and provide the same to Visa.

Mandatory Controls:

1. Acquirers must collect and provide to Visa (when requested) the required information for each Merchant, Marketplace, Sponsored Merchant, or Ramp Provider. current and in the format specified by Visa:
   a. T/A (trading as) or DBA (doing business as) name.
   b. Full legal name (if different from DBA name). For a sole proprietor, the information must include the sole proprietor's full first and last name, including the middle initial.
   c. Merchant Outlet address (including street address, city, state/province, and postal code (or country equivalent).
   d. Telephone number (not required for Sponsored Merchants).
   e. Acquirer-assigned Merchant ID (Card Acceptor ID).
   f. Merchant business registration number or tax identification number.
   g. PayFac name (for Sponsored Merchants only).
   h. PayFac identifier assigned by Visa and Sponsored Merchant identifier assigned by the PayFac, as applicable.
   i. Ramp Provider identifier assigned by Visa and Conversion Affiliate identifier assigned by the Ramp Provider, as applicable.

© 2024 Visa. All rights reserved. Visa Public

AACQ.C6.2 – KYC/KYB Veri ications

Performing KYC/KYB verifications allows Acquirers to verify data, which will help mitigate potential risk exposure.

Mandatory Controls:

1. Acquirers conduct KYC/KYB verifications, which include:
   a. **Collecting and Verifying Principal/Director information:** Obtain the name, address, government identification number, email address, and telephone number of each principal/director involved in the business. Where applicable under law, collect information on the nationality and residency of the principals. Use Identity Verification Services to help verify the identities of Merchants by cross-checking their provided information against multiple data sources.
   b. **Ownership information:** Obtain the percentage of ownership held by each principal representing at least material ownership.
   c. **Business license or registration:** Obtain a business license or registration certificate. When appropriate, perform a search with the appropriate business bureaus to verify that the Merchant owns or operates a legitimate business.
2. Acquirers screen Merchants against all applicable economic and government trade-sanction watch-lists in accordance with applicable laws and regulations.
3. Acquirers collect and verify additional elements for e-Commerce Merchants. This includes:
   a. A listing of URLs used by the Merchant to promote its business, sell products, and accept payments.
   b. Verification that the Merchant is the registered owner of these domains and websites.

VISA

Risk Statement

Onboarding processes that lack proper underwriting could lead to onboarding, transactional, and overall fraud, which may result in financial losses, operational damage, and reputational damage.

CONTROL REQUIREMENT #3

AACQ.C7

Acquirers must conduct fraud checks when onboarding a Merchant.

AACQ.C7.1 – Fraud Detection and Prevention

Conducting fraud checks when onboarding a Merchant enhances due diligence and continuous monitoring and is a key factor in the potential reduction of fraudulent activity.

Mandatory Controls:

1. Acquirers have systems in place to detect fraudulent behaviour and potential fraud linked to the Merchant during the onboarding process.
2. Acquirers utilize tools such as Address Verification Service (AVS), Card Verification Value (CVV), Visa Secure, machine learning algorithms, fraud scoring, geolocation, velocity checking, biometric authentication, and more to identify and prevent fraudulent transactions.

Recommended Controls:

1. Using a mix of tools is recommended for a robust fraud prevention strategy as detailed below:
   a. **Two-Factor Authentication (2FA):** This adds an extra layer of security by requiring Merchants to provide two different authentication factors to verify themselves.
   b. **IP Address Tracking:** This helps to identify if multiple accounts are being operated from the same device or location, which can be a signal of fraudulent activity.
   c. **Device Fingerprinting:** This involves collecting information about a device for the purpose of identification.
   d. **Behavioral Biometrics:** This involves tracking and analyzing a Merchant's behaviour, such as typing rhythm and mouse movements to identify fraudulent activity.
   e. **Risk-Based Authentication:** This involves varying the authentication requirements based on the Merchant's risk profile.

© 2024 Visa. All rights reserved. Visa Public

2. Acquirers conduct first- and third-party data verifications using web crawling, negative news scanning, beneficial owner research, Merchant domicile and activities, in addition to Merchant industry and geography.
3. Acquirers implement processes/systems to store and manage evidence related to fraud incidents/investigations for audit trails as per local laws and regulations.
4. Acquirers should mitigate redirecting of URLs for any processing of transactions to prevent unauthorized access to Merchant checkout (e.g., Pay by link Merchants).

Monitoring

4	8	2
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Lack of portfolio oversight across processed transactions and Merchant activity could lead to processing transactions that may be fraudulent/ illegal, which may result in financial losses, regulatory noncompliance, and reputational damage.

CONTROL REQUIREMENT #1

AACQ.C8

Acquirers must monitor transaction and Merchant activity to detect threats, unusual or suspicious activities/ transactions and use exception reporting to act upon deviations.

AACQ.C8.1 – Portfolio Monitoring

Acquirers must adopt a risk management-focused monitoring strategy for their Merchants, beginning with successful onboarding and continuing until partnership termination. The monitoring aims to detect and mitigate various risks such as fraud/collusion, credit issues, disputes, anti-money laundering (AML), brand-damaging and illegal activities.

VISA
© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. **Documentation:** Acquirers must maintain clear process/procedure documentation outlining their review stages, supported by a dedicated and competent team.
2. **Monitoring Strategies:** Acquirers must develop monitoring capabilities that meet the following requirements:
   a. Build the capability to monitor for changes or anomalies in various merchant transaction attributes: transaction velocity, high occurrences of rounded sales draft amounts, forced transaction activity, new or inactive Merchant activity, sudden changes in account contact information, spikes in authorization attempts, changes in sales volume, changes in the ratio of card-present vs. card-absent sales, and discrepancies in cross-border activities.
   b. Establish models or other analytical methods that will alert the Acquirer to sudden or unexpected changes in the Merchant's activity. This can be achieved by establishing and regularly updating a baseline of normal daily activity, against which the most recent activity is compared.
   c. Adequate monitoring requires the Acquirer to retain daily data such as gross sales volume, average transaction amount, number of transactions received, average time between transaction and settlement dates, and number of disputes. Perform ongoing monitoring of the daily data for any spikes or irregularities and ensure that there is an established escalation process in place in case an investigation is needed.
   d. Carry out ongoing AML due diligence including sanction, politically exposed persons (PEPs) & derogatory media screening, regulatory license monitoring (when applicable), and oversight of compliance with AML responsibilities agreed during onboarding.
   e. Review business activity including URLs, products or services sold, delivery methods, and scan for products or services, review any hyperlinks directing Cardholders to other websites that violate the Visa Rules or laws.
   f. Monitor VMSS alerts against active Merchants to compare against initial onboarding approval.
3. **Review of Reports:** Acquirers periodically review payment intelligence security alerts, Payment Threat Disruption Biannual Reports, and Pressure Gauge.

VISA
© 2024 Visa. All rights reserved. Visa Public

AACQ.C8.2 – Portfolio Monitoring – Fraud Risk

Analyzing data through comprehensive fraud detection and prevention tools helps monitor for suspicious activity at Merchant/TPA/Sponsored Merchant level relating to fraud/disputes.

Mandatory Controls:

1. Acquirers possess the following capabilities to detect and prevent fraudulent activity:
   a. **Fraud Detection:** Acquirers are equipped with rules or models that can identify suspicious or confirmed fraudulent behavior.
   b. **Fraud Prevention:** Throughout the Merchant's lifecycle, Acquirers employ various tools and techniques to curtail fraudulent activity. These can include AVS, CVV2, machine learning algorithms, fraud scoring, geolocation, velocity checking, and biometric authentication.

Recommended Controls:

1. Acquirers use a comprehensive multi-layered approach to prevent fraud which includes checking Merchant data and profile at the onboarding stage and continuous assessment throughout their lifecycle:
   a. **For a robust fraud prevention strategy,** the security measures mentioned in AACQ. C7.1 – Fraud Detection and Prevention are utilized.
   b. **Data Verification:** Acquirers use web crawling, negative news scanning, beneficial owner research, and checks on Merchant domicile, activities, industry, and geography to verify first- and third-party data.
   c. **Attack Detection:** Acquirers monitor for enumeration or BIN attacks by observing for inconsistencies in Merchant's IP addresses, identifiers, total fraud rate, and differences in authorization and clearing data elements. They also keep an eye on transaction velocity and alerts on authorization and authentication.
   d. **Visa Ecosystem Utilization:** Acquirers adopt Visa's ecosystem-level best practice procedures and alerting resources, including Visa Account Attack Intelligence Service, Account Testing and Enumeration Procedures, Anti-Enumeration and Account Testing Best Practices for Acquirers and Merchants, and Visa Ecosystem Alerting.
   e. **First-Party Fraud Monitoring:** Acquirers work with Visa to identify suitable fraud solutions (e.g., Issuers'/Prepaid Clearinghouse Service (ICS/PCS)) and leverage Order Insight from Verifi, a comprehensive chargeback and fraud protection solution that helps validate sales and combat first-party fraud.

© 2024 Visa. All rights reserved. Visa Public

AACQ.C8.3 – Exception Reporting and Investigation

Exception reports are generated when there is a deviation from, not limited to but including, the average activity of daily transactions, number of daily deposits, gross amount of daily deposits, average transaction amounts, number of daily disputes, the average elapsed time between the Processing Date and either the Transaction Date or the Settlement Date for a Transaction (counting each as one day) exceeds 15 calendar days.

Mandatory Controls:

1. Acquirers must investigate a Merchant that appears on an exception report immediately and report the result of the investigation and actions taken to Visa.
2. If the investigation reveals Merchant involvement in illegal or fraudulent activity, Acquirers must:
   a. Take appropriate legal action to minimize losses.
   b. Cooperate with Visa, Issuers, and law enforcement agencies.
   c. Hold all available settlement funds, if possible. Acquirers validate that their Merchant agreement allows Acquirers to hold funds in this scenario.
   d. Attempt to make the Merchant responsible for the transaction.
   e. Initiate criminal and civil proceedings against the Merchant, if applicable.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Not assisting with fraudulent activity investigations could lead to undetected fraud, which may result in financial losses, regulatory noncompliance, and reputational damage.

CONTROL REQUIREMENT #2

AACQ.C9

Acquirers must support fraudulent investigations by providing comprehensive details on the Merchant and/or transactions to the relevant party/authorities.

AACQ.C9.1 – Assistance with Fraudulent Activity Investigation

Acquirers have an obligation to protect the Visa payment system and assist in fraudulent activity investigations by providing the required information, when asked by Visa, law enforcement agencies, or other Acquirers, as per internal rules, processes, and local regulations. This aids in limiting their risk exposure, protecting consumers, and preventing similar incidents.

Mandatory Controls:

1. Acquirers must aid other Visa Clients in investigating fraudulent activities by undertaking the following tasks:
   a. **Interviews:** Conducting discussions with Merchants, Sponsored Merchants, and any other relevant party.
   b. **Evidence Collection:** Assisting law enforcement in obtaining all physical or electronic evidence.
   c. **Information Sharing:** Providing necessary information (such as device fingerprinting) to the applicable authorities as per local laws and regulations.
   d. **Additional Assistance:** Offering any other reasonable investigative assistance.
   e. **Suspension of Settlement:** Choosing to suspend settlement of Merchant funding during the investigation period.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Failure to report suspicious activity could lead to an increased risk of fraudulent transactions, which may result in financial losses, regulatory noncompliance, and reputational damage.

CONTROL REQUIREMENT #3

AACQ.C10

Acquirers must report suspicious activity to help prevent fraud, comply with regulations, protect finances, and maintain their reputation.

AACQ.C10.1 – Reporting of Suspicious Activity

Suspicious activity reports help detect and report suspected violations of law by financial institutions subject to the regulations, making it easier to investigate any concerns. Transactions may be suspicious because they are caused by compromised systems including exposure of PAN.

Mandatory Controls:

1. Acquirers must immediately report any data breaches and include a remediation plan, as specified in What to Do If Compromised. The report must be thorough, complete, and submitted in the format specified.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Ineffective monitoring of changes in Merchant creditworthiness could lead to the Merchant being unable to fulfill their committed goods/services to Cardholders, which may result in Acquirers facing financial losses, operational damage, and reputational damage.

CONTROL REQUIREMENT #4

AACQ.C11

Acquirers must have the ability to proactively monitor and act on changes in credit risk.

AACQ.C11.1 – Portfolio Monitoring – Credit Risk

The Acquirer should monitor the credit risk of Merchants (e.g., Future-service Merchants) and take appropriate action. Merchant agreements should detail which actions the Acquirer can take, such as changing reserve requirements, adding holds on funds, and conducting additional reviews.

Recommended Controls:

1. When monitoring Merchant credit risk, Acquirers:
   a. **Evaluate Creditworthiness:** This involves assessing financial and credit reports (e.g., bankruptcy, liquidation, increased payment defaults) with external vendors and establishing an enhanced due diligence process for review and necessary action.
   b. **Monitor Merchant Performance:** Look for anomalies in specific MCCs, downward trends in Purchase Volume (PV), increases in refunds and/or disputes, unusual cardholder/issuer concentration, inconsistencies in business activity compared to history, and changes to delivery periods in comparison to initial underwriting.
   c. **Tailor Review Process:** Depending on the Merchant's category, type (such as online or brick-and-mortar stores), projections, and jurisdiction, adjust the review process. Emphasize enhanced due diligence for high-risk segments.
   d. **Align Mitigation Strategy:** Ensure the Merchant's exposure mitigation strategy is in line with their risk appetite and policies. If there are shortcomings in the Merchant's credit policies, make up for these by increasing reserves or applying other mitigation options.
   e. **Adjust Settlement Procedures:** If necessary, the settlement procedures are revised to better manage risk.

VISA
© 2024 Visa. All rights reserved. Visa Public

f. **Periodic Credit Exposure Assessment:** The credit exposure of the Acquirer portfolio is evaluated on a monthly, quarterly, and yearly basis.

g. **Monitor Dispute Patterns:** Ensure that the Merchant's dispute patterns are in line with their operating sectors. For instance, non-future service or cryptocurrency merchants should not have an elevated level of disputes or refunds.

Chargeback/Dispute

1	1	4
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Inadequate dispute management throughout the transaction process could lead to considerable financial vulnerability, which may result in financial losses.

CONTROL REQUIREMENT #1

AACQ.C12

Acquirers must have access to dispute management solutions and be able to manage and respond to disputes within the timelines specified by Visa.

AACQ.C12.1 – Dispute Management Process

When Acquirers effectively manage disputes, they can mitigate risks associated with excessive disputes. This includes ensuring accurate data collection, analyzing trends, and taking proactive measures to address issues. Creating investigation cases for flagged Merchants exceeding specified thresholds is essential for Acquirers to effectively manage risks, protect the payment ecosystem, and maintain trust and reputation within the industry.

Mandatory Controls:

1. Acquirers must adhere to the dispute requirements as per the Visa Rules including
   a. Acquirers handling procedures for a response during a dispute resolution process.
   b. Dispute timelines for Acquirers.

© 2024 Visa. All rights reserved. Visa Public

Recommended Controls:

1. Acquirers utilize various tools and resources to manage disputes effectively and improve Risk Monitoring detection:
   a. **Dispute Management Platforms:** Implementation of in-house or third-party dispute management platforms.
   b. **TC40 Fraud Reports:** Utilization of TC40 fraud reports for analysis and insights.
   c. **Standard Operating Procedures (SOP):** Definition of SOPs, detailing the process, owners, and timeline for streamlining dispute management.
   d. **Training:** Ensuring that the Acquirer's chargeback/dispute teams are trained and updated about changes included in the Visa Business Newsletters (VBNs).
   e. **Merchant Education:** Providing training workshops and materials to keep Merchants updated with best practices to avoid disputes, and to educate staff on dispute resolution.
   f. **VAMP Thresholds:** For Merchants that exceed VAMP thresholds, Acquirers flag these Merchants and generate a monthly report on disputes by Merchant category and Merchant level.
2. Acquirers must investigate and retain the following information for a minimum of 2 years, or as long as specified by law in the Acquirer's jurisdiction:
   a. Investigation details (type, date, etc.)
   b. Event description and analysis.
3. An Acquirer ensures a Marketplace:
   a. Discloses the country of the Marketplace retailer within the sequence of pages that the Cardholder accesses during the purchase process. A link to a separate web page does not meet this requirement.
   b. Makes available to the Cardholder for at least 120 days from the Processing Date:
      i. The name of the retailer, Transaction Date, and Transaction amount.
      ii. If the retailer is responsible for answering questions about the purchase of the goods, an easy means for the Cardholder to contact the retailer.
4. Acquirers must review Merchants with high dispute rates for deceptive or misleading sales/marketing practices or insufficient cardholder interaction/communication. In cases when Issuer documents indicate that merchant activity is not in line with MCC assigned, Acquirer must also review merchant business activity to understand the reasons of the discrepancy and take appropriate measures.

© 2024 Visa. All rights reserved. Visa Public

Data Integrity/Quality

1	1	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Failure to validate Merchant's data elements with the Merchant's registered details could lead to accepting transactions from unlawful or previously terminated Merchants. This may result in financial losses, potential fraud, operational damage, and reputational damage.

CONTROL REQUIREMENT #1

AACQ.C13

Acquirers must implement controls on Merchant names to maintain consistency throughout the transaction lifecycle, thereby safeguarding against unauthorized or illegal use.

AACQ.C13.1 – Consistency in Merchant Data Elements

Verifying that a Merchant's data elements align precisely with the Merchant's registered details on file with the Acquirer confirms the legitimacy of the transaction, which reduces the risk of fraudulent activity or unauthorized transactions.

Mandatory Controls:

1. Acquirers, along with their TPAs, are obligated to maintain uniformity in the use of key identifiers such as Registered Merchant Names, Merchant Logos, CAID, MCC, Merchant ID, Merchant DBA, Terminal ID, Merchant data, and Merchant performance throughout the transaction lifecycle, including authentication, authorization, clearing, settlement, collections data, fraud and dispute reporting. Consistency in these identifiers is essential for accurate record keeping, smooth transaction processing, and effective dispute resolution and fraud detection.

VISA
© 2024 Visa. All rights reserved. Visa Public

Data Security

2	7	2
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Ineffective data management procedures and supervision, in accordance with the Visa Rules and jurisdictional requirements, can lead to data loss, theft, or compromise, which may result in financial losses, reputational damage, and legal issues.

CONTROL REQUIREMENT #1

AACQ.C14

Acquirers must comply with the Visa Account Information Security Program and jurisdiction regulations for data handling.

AACQ.C14.1 – PCI DSS Compliance

Validating that service providers are compliant with PCI DSS ensures data is secured and secure technology capabilities are in place.

Mandatory Controls:

1. Acquirers safeguard all materials or records, regardless of form, which contains account or Transaction Information. Access is restricted to authorized personnel, as outlined in the PCI DSS.
2. Acquirers guarantee that contracts and agreements with TPAs and Merchants clearly define their responsibilities to adhere to Visa standards, the liabilities for noncompliance, and the obligation to permit inspections by the Acquirer or Visa.
3. Acquirers ensure compliance with PCI DSS by all TPAs and Merchants who have access to account or transaction information.
4. Acquirers ensure that post-authorization all TPAs and Merchants refrain from storing:
   a. Complete data extracted from the magnetic stripe (on a Card, in a Chip, or elsewhere).
   b. CVV2.

© 2024 Visa. All rights reserved. Visa Public

c. PIN or the encrypted PIN block.
d. Token Authentication Verification Value (TAVV).
e. Dynamic Token Verification Value (DTVV).
f. Visa Secure Cardholder Authentication Verification Value (CAVV).

5. Acquirers ensure that all Merchants and TPAs utilize Payment Applications that are compliant with the PCI Software Security Framework (SSF) Standards.
6. Upon request, Acquirers provide certification to Visa that TPAs and Merchants comply with PCI DSS.
7. Acquirers abide by, and ensure that its Merchants, TPAs, and other third parties with access to account or transaction information comply with the Account Information Security Program requirements. Acquirers must also ensure that its Merchants:
   a. Implement and uphold all Account Information Security Program requirements.
   b. If utilizing a TPA, ensure that the TPA implements and upholds all security requirements outlined in the Account Information Security Program.

Risk Statement

Lack of business continuity planning could lead to disruptions in operations, which may result in financial losses and reputational damage.

CONTROL REQUIREMENT #2

AACQ.C15

Acquirers must have a business continuity plan and resume operations within their specified timeline, in case of unforeseen events like natural disasters, and avoid disruption in critical payment operations.

AACQ.C15.1 – Business Continuity and Resilience Plan

A tested business continuity and resilience plan with considerations for resource allocation, contingency of storage site, tools, software and solutions are critical to payment operations, and it is especially important it outlines resumption timelines to ensure minimum disruption to payment operations.

Recommended Controls:

1. Acquirers outline:
   a. A business continuity plan to protect and preserve sensitive and vital data, regain critical systems, and resume normal operations following unforeseen incidents.
   b. Well defined recovery point objectives (RPOs) and recovery time objectives (RTOs).

© 2024 Visa. All rights reserved. Visa Public

c. A plan incorporating the use of a secondary site, designed to ensure that critical information technology systems can resume operations within pre-defined RPO and RTO requirements following disruptive events.

2. Acquirers maintain geographically dispersed recovery sites adhering to legal and regulatory requirements and conduct a routine check to test recovery plans and mechanisms. This may be dependent on the Acquirer's size and its recovery processes.

Network and Scheme Compliance

1	3	2
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Failure to ensure ongoing compliance to Visa Rules or technical standards, which are updated periodically, can result in financial losses, operational damage, and reputational damage.

CONTROL REQUIREMENT #1

AACQ.C16

Acquirers must ensure their operational, sales & technical functions remain compliant with all Visa requirements, as regularly updated.

AACQ.C16.1 – Visa's requirements and policies

Visa's rules & technical standards are designed to minimize risks and provide a common, convenient, secure, and reliable global payment experience while supporting country-specific nuances that allow for variations and unique marketplace needs.

The Visa Rules contain fundamental rules that apply to all Visa system participants and specify the minimum requirements applicable to all clients to uphold the safety, security, soundness, integrity, and interoperability of the Visa system. The Visa Rules include policies that apply to use of a product, service, the Visa-Owned Marks, VisaNet, the dispute resolution process, and other aspects of the Visa payment system.

Visa Supplemental Requirements are separate documents or websites that contain requirements beyond the content of the Visa Rules, for example, VisaNet technical requirements, and Visa Product Brand Standards.

© 2024 Visa. All rights reserved. Visa Public

Global, regional & country-specific communications are prepared by Visa to announce changes that have been approved but are not yet incorporated into the Visa Rules or Visa Supplemental Requirements. These communications have the full authority of the Visa Rules, and the contents are effective on the date of publication, or any effective date specified in the communication. While Visa may distribute these communications, clients are responsible for obtaining and referring to this information on Visa Access.

Mandatory Controls:

1. Acquirers must ensure that Visa's requirements & policies are embedded into acquirers' overall operating structure and risk appetite, as updated periodically.
2. Acquirers must ensure that acquirer's & all other parties in their ecosystem, remain compliant to Visa's technical standards, as updated periodically.
3. Acquirers must ensure that updated Visa Rules & technical standards are adopted in line with the Effective Dates communicated in applicable communications.

Recommended Controls:

1. Acquirers should establish a dedicated group of employees who are responsible for understanding Visa's requirements & policies; this group should:
    a. Be a l SMEs for other groups to ensure business policies & operational structures support Visa's requirements. This may include:
        i. Access to Visa Access and regular reviews of which internal employees have access to Visa Access and the level of access they have, removing colleagues who may no longer need Visa Access access
        ii. Access to Visa Acess from each region that acquirer operates in
        iii. Regular interaction with their local Visa representatives in each country or region the acquirer operates in. Developing such interactions with Visa will give acquirers foresight to forthcoming Visa announcements which may not be advertised via Visa Access
        iv. Knowledge of the content of Visa Access will also give the acquirer knowledge of the range of Visa products available to assist the acquirer with their business needs.
        v. Information on Visa Training courses, either online or via the Visa University can be found on Visa Access
    b. Be a dedicated contact point for receiving Visa's regular (weekly) communications, announcing forthcoming updates to Visa Rules, requirements & technical standards. These communications are typically retrieved through accessing Visa Access and pulling new items for internal review. Acquirer will need to access the regional Visa Access for each region they acquire in.

© 2024 Visa. All rights reserved. Visa Public

c. Develop measures and controls to periodically review and circulate announcements for updated Visa Rules, technical standards & other requirements across the Acquirer's organization to ensure upcoming updates are known & understood by business owners.

d. As Visa documentation maybe confidential in status, develop internal practices of communications to share that information with relevant stakeholders such as merchants and other third parties without circumventing any Visa confidentiality controls.

2. Acquirers should continuously ensure business policies & operational structures support Visa's requirements, as updated periodically, through periodic internal audits & analysis.

4.1.3 Legal & Regulatory Risk

Miscoding/Transaction Laundering

1	-	2
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Processing illegal transactions (or transactions related to prohibited goods and services) that may be caused by miscoding or transaction laundering could lead to financial losses, reputational damage, and legal issues.

CONTROL REQUIREMENT #1

AACQ.C17

Acquirers must implement controls during underwriting and monitoring for potentially concealed illegal transactions to ensure no illegal transactions enter the Visa ecosystem.

AACQ.C17.1 – Monitoring Illegal Transactions

Transaction laundering, also known as factoring, is a sophisticated form of money laundering where an unknown business uses an approved Merchant's payment credentials to process card payments for undisclosed goods or services. Detecting and preventing transaction laundering requires a combination of manual checks, automated systems, and data analysis.

© 2024 Visa. All rights reserved. Visa Public

Recommended Controls:

1. Effective monitoring for illegal transactions includes utilizing web crawling tools, if needed, that helps Acquirers monitor and protect themselves against illegal transactions. Some of these controls include:
   a. **Regularly Review Transaction Data:** Regularly review transaction data for any unusual patterns. This could include an unusually high number of transactions, transactions with similar amounts, or transactions that do not match the nature of the underwritten Merchant.
   b. **Website and cyber analytics-based tools:** These tools help to identify transaction tunnels like mobile apps and fraudulent mobile payments through cyber intelligence.
   c. **Behavioural analytics-based tools:** Real-time monitoring of Merchant behaviour and traffic flow together and alerts the Acquirer. Use advanced analytics and machine learning algorithms to identify patterns that might indicate transaction laundering. This could include looking for patterns in the transaction data, such as recurring transactions from the same IP address or geographic location.
   d. **Verify Merchant Websites:** Regularly verify the websites of your Merchants to ensure that they are only selling the products or services they have declared. In addition, verify that the website has a checkout process and an ability to process payments. Transaction laundering often involves selling products or services that are not declared to the payment processor.
   e. **Database and website analytics-based tools:** External databases are used for pattern detection within traffic, website, and transactions.
   f. **Additional monitoring requirements:** Acquirers also monitor for any mismatch in Merchant identifiers such as Merchant names, MCC, identification of suspicious connections to the URL and backlinks, and conduct investigation upon violation.

AACQ.C17.2 – Transaction Laundering/Miscoding Knowledge and Skills

By providing targeted education and training opportunities, Acquirers empower stakeholders with the knowledge and skills needed to mitigate transaction laundering and miscoding risks effectively and uphold the integrity of the payment system.

Recommended Controls:

1. Acquirers remain up to date on the latest developments in transaction laundering and transaction miscoding through Visa's PFD communications, V-Alerts, Pressure Gauge, the Payment Threat Disruption biannual report, and through any additional sources of information based upon advice from Acquirer's Legal team.

© 2024 Visa. All rights reserved. Visa Public

Regulatory Risk

1	2	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Acquirer's acquiring and risk policies that are not aligned to jurisdictional and regulatory requirements could lead to financial losses and regulatory noncompliance.

CONTROL REQUIREMENT #1

AACQ.C18

Acquirer's acquiring and risk policies must align with all applicable jurisdictional laws and regulations, which must be shared with Merchants/TPAs.

AACQ.C18.1 – Compliance with all Applicable Jurisdictional Laws, Regulations, and the Visa Rules

Effective Acquirer risk profile and applicable policy documentation are reflective of all applicable jurisdictional laws and are aligned to the requirements outlined in the Visa Rules. As the local market, regulations, and laws change, ensuring that policies are current is particularly important in order protect emerging Acquirers and Acquirers that work across multiple jurisdictions.

Mandatory Controls:

1. Acquiring and risk policies comply with all applicable jurisdictional laws and regulations, including AML and sanctions compliance requirements.
2. Acquirers ensure that all transactions are legal in both the Merchant and Cardholder's jurisdictions.

© 2024 Visa. All rights reserved. Visa Public

4.2 Acquirers Sponsoring with TPAs (ATPA)

The following control requirements are mandated for **Acquirers sponsoring TPAs**. The control requirements have been categorized under overarching risks and related sub-domains. The control requirement is the required objective that must be met by the Acquirer, through the mandatory and recommended controls.

Refer to Appendix E.2 TPA Types for details on various TPA types and sub-types covered as part of this archetype.

4.2.2 Operational Risk

Written Agreements

2	4	2
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

The absence of written agreements between Acquirers and TPAs could lead to misunderstandings, legal vulnerabilities, insufficient evidence in case of disputes, which may result in financial losses and reputational damage.

CONTROL REQUIREMENT #1

ATPA.C1

Acquirers must have contractual binding agreements with TPAs that assures compliance with their acquiring strategy.

ATPA.C1.1 – TPA Agreement

TPA agreements are an integral element of the legal relationship between an Acquirer and TPA. The purpose of a TPA agreement is to provide a "terms of use" contract containing each party's respective rights, duties, and obligations for participation in the Visa Acceptance Program. The Agreement may be tailored by the Acquirer for Merchants in different MCCs or lines of business, and may include requirements from other payment networks, as long as the requirements for accepting Visa payments are included.

© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. Acquirers have an obligation to enter into a written agreement with each TPA that performs Cardholder or Merchant solicitation, or stores, processes, or transmits Cardholder or Transaction data on their behalf. The agreement must contain the following provisions:
   a. **Standards:** The contract incorporates the minimum standards established by Visa, including policies, procedures, service levels, and performance standards.
   b. **Visa's Rights and Authority:** The contract permits Visa to conduct financial and procedural audits and general reviews at any time. It requires the TPA makes Cardholder and Merchant information accessible to Visa and regulatory agencies. The contract must also include a termination notice clause and grant Visa the right to determine and impose risk conditions on the TPA. The agreement must also grant Visa the right to limit or terminate the Acquirer's agreement with the TPA.
   c. **Compliance:** Acquirers ensure TPAs do not knowingly submit any transaction that is illegal or that the Merchant should have known was illegal.
      i. The TPA must comply with the Visa Rules and the applicable laws or regulations.
      ii. TPAs must adhere to the policies and procedures of the Acquirer and the requirements of the Visa Account Information Security Program and any relevant data security standard.
   d. **Cooperation:** Acquirers ensure the TPA, fully cooperates with a forensic investigation until it is completed as per the What to Do If Compromised.
   e. **Security Compliance:** The TPA must comply with PCI DSS, where applicable.
   f. **Termination:** The agreement includes a provision that allows the Acquirer or its Merchant to terminate the contract if the TPA participates in any activities described in the Visa Rules, or if the Acquirer or its Merchant becomes insolvent. Termination of Sponsored Merchant and PayFac Agreement must follow the steps below:
      i. After verifying that Visa has prohibited a Sponsored Merchant or PayFac from participating, Acquirers must ensure Visa processing for the PayFac is suspended no later than the date specified by Visa.
      ii. The Sponsored Merchant or PayFac will be notified in writing if the Acquirer terminates the agreement, depending upon whether it is a direct or tri-party agreement.
   g. **Settlement of Funds:** The TPA agreement states that Acquirers must pay or credit its TPA's account promptly after transaction deposit. The TPA agreement prohibits deposit of transactions on behalf of another TPA. Acquirers must directly pay only a Sponsored Merchant for its portion of the deposit, if the Acquirer also contracts with the PayFac.

© 2024 Visa. All rights reserved. Visa Public

h. Acquirers may allow a TPA to place its own contact name, phone number, and its logo on the application. This information must not be more prominent than the Acquirer contact information and should not discourage the merchant from contacting the Acquirer to report service deficiencies. If the TPA's logo is present on the merchant application, the Acquirer's logo must also be present.

Recommended Controls:

1. Acquirers using TPAs remain responsible for setting up and maintaining proper risk controls and procedures. Their contractually binding agreement with TPAs:
   a. **Primary Party:** Identifies the Acquirer as a primary party to the contract, affirming that the Acquirer extends the acceptance of Visa products to Merchants. Clearly define the duties and responsibilities of both the TPA and Acquirer, including responsibilities for transaction monitoring, website monitoring, detection of transaction laundering.
   b. **Transfer/Assignment:** Allows for the transfer or assignment of a Sponsored Merchant/TPA agreement to another Acquirer.
   c. **Merchant Agreements:** Establishes a method for examining Merchant agreements utilized by the TPA.
   d. **Responsibilities:** Clearly defines the duties and responsibilities of both the TPA and Acquirer, including responsibilities for transaction monitoring, website monitoring, detection of transaction laundering.
   e. **Addendum:** Ensures that all modifications are documented in an addendum, which must be accepted and signed by the principal owner or compliance officers of the TPA. This addendum is then utilized for training the TPA's staff.
   f. **Restrictions:** Restricts TPAs from registering other TPAs (PayFac, Marketplaces, Ramp Providers) that are not permissible by Visa Rules.

ATPA.C1.2 – TPA Agreement for PayFac or DWO

TPA agreements are an integral element of the legal relationship between an Acquirer and a PayFac or DWO. The acts and omissions caused by a Sponsored Merchant will be treated as those of the Payment Facilitator and those caused by a Payment Facilitator or a Sponsored Merchant as those of the Acquirer. Acquirers should use separate templates of agreements with PayFac and Merchant.

Mandatory Controls:

1. Acquirers must ensure that both PayFac and DWO agreements contain the following provisions:
   a. Both the PayFac, its Sponsored Merchants, or the DWO must adhere to the Visa Rules.

© 2024 Visa. All rights reserved. Visa Public

b. The PayFac is obligated to establish a contract with each Sponsored Merchant.

c. The Acquirer reserves the right to immediately terminate an agreement with a Sponsored Merchant, PayFac, DWO, or a retailer under a DWO due to valid reasons, fraudulent actions, other activities, or upon Visa's request.

d. The PayFac or DWO must:

   i. Accept liability for all actions, neglect, Cardholder disputes, and other Cardholder-related customer service issues caused by the PayFac's Sponsored Merchants or the retailer under a DWO.

   ii. Take responsibility and financial liability for each transaction processed for the Sponsored Merchant, or any disputed transaction or credit.

   iii. Refrain from transferring its financial liability by asking or requiring Cardholders to waive their dispute rights.

   iv. Prevent a Sponsored Merchant from trying to transfer its financial liability by asking or requiring Cardholders to waive their dispute rights.

   v. Not process transactions on behalf of another PayFac. Acquirers ensure that PayFacs deposit a transaction between the Cardholder and a Sponsored Merchant of the PayFac only.

   vi. Avoid contracting with a Sponsored Merchant or a retailer under a DWO, if their contract to accept transactions was terminated by Visa or a government agency.

   vii. Provide the names of principals and their country of domicile for each of its Sponsored Merchants or retailers under a DWO and provide Transaction reports to its Acquirer and Visa when requested.

   viii. Ensure that its Sponsored Merchants adhere to PCI DSS and PCI SSF Standards.

   ix. Ensure PayFacs & Staged Digital Wallet Operators (SDWOs) do not process transactions from Sponsored Merchants or retailers under a DWO outside the Acquirer's jurisdiction.

2. Acquirers who are in a contract with a Payment Facilitator are required to establish a direct Merchant Agreement with any Sponsored Merchant that has an annual Transaction volume exceeding USD 1 million, as outlined below:

   a. For a new Sponsored Merchant application.

   b. For an existing Sponsored Merchant which is due for renewal or within 2 years after the Sponsored Merchant's annual Transaction volume exceeds USD 1 million.

   c. The PayFac may continue to provide payment services (including settlement) to the Merchant.

NOTE: Additional exceptions based on the Sponsored Merchant's MCC & tenure of relationship are included in the Visa Rules.

© 2024 Visa. All rights reserved. Visa Public

ATPA.C1.3 – TPA Agreement for Marketplaces

An Acquirer that contracts with a Marketplace is liable for all acts, omissions, and other adverse conditions caused by the Marketplace and its retailers.

Mandatory Controls:

1. Acquirers must ensure that Marketplace agreements contain the following provisions:
    a. The Marketplace and its retailers comply with the Visa Rules.
    b. The Marketplace enter into a contract with each retailer before it deposits Transactions on the retailer's behalf.
    c. The Acquirer's right to prohibit individual retailers from participating in the Visa system and to immediately stop depositing Transactions for any individual retailer for good cause or upon Visa request.
    d. Statements specifying that the Marketplace:
        i. Is permitted to process Transactions for retailers located in a different country to the Marketplace and must ensure that Transactions are legal in the country of the Marketplace and of the retailer.
        ii. Is liable for all acts, omissions, Cardholder disputes, and other Cardholder customer service-related issues caused by the Marketplace's retailers.
        iii. Is responsible and financially liable for each Transaction processed on behalf of a retailer.
        iv. Must not transfer or attempt to transfer or permit the retailer to transfer or attempt to transfer, its financial liability by asking or requiring Cardholders to waive their dispute rights.
        v. Must deposit Transactions only on behalf of retailers of goods and services that use the Marketplace's website or application.
        vi. Must not knowingly contract with a retailer whose contract to accept Transactions was terminated at the direction of Visa or a government agency.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Delayed recording of terminated TPAs, especially those terminated for just cause due to misuse, deception, and/or processing illegal transactions may result in potential fraud, operational damage, reputational damage, and legal issues.

CONTROL REQUIREMENT #2

ATPA.C2

Acquirers must have a contractually binding agreement with TPAs that includes that TPAs terminated for just cause are reported in line with Visa practices.

ATPA.C2.1 – TPA Reporting Terminated Merchants

TPA agreements must ensure that TPAs are following the required standards for terminated merchants.

Recommended Controls:

1. Acquirers ensure TPAs check the Terminated Merchant File (e.g., VMSS) for any match to the Sponsored Merchants. If there is a positive match, Acquirers ensure that the TPA:
   a. Verifies if the Merchant in question is the same one for whom the inquiry was made.
   b. Engages with the Acquirer who listed the Merchant to understand the reasons behind their inclusion in the file.
   c. Makes an informed decision about accepting the merchant, based on a thorough investigation using the Terminated Merchant File, credit reports, local business registries, and other relevant sources.

© 2024 Visa. All rights reserved. Visa Public

Onboarding

5	14	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

When participating in the acquiring of TPAs, Acquirers have lower visibility into the end Merchant. This could lead to potential gaps in policy implementation, and may result in financial losses, operational damage, reputational damage, and legal issues.

CONTROL REQUIREMENT #1

ATPA.C3

Acquirers must have a TPA specific onboarding process and underwrite all TPAs prior to onboarding.

ATPA.C3.1 – TPA Underwriting Requirements

A TPA specific onboarding process creates a well-controlled relationship between an Acquirer and a TPA, and can reduce the possibility of bank failure, minimize risk of loss to the payment system. In addition, registering TPAs with Visa mitigates the risk of unregistered Merchants in the Visa payment system and facilitates the tracking and monitoring of TPAs. For TPA categories outside of ISO, consult the Third-Party Agent Due Diligence Risk Standards.

Mandatory Controls:

1. Acquirers must run a comprehensive underwriting process for each TPA before signing the contract and integrating them for onboarding, complying with the Third-Party Agent Due Diligence Risk Standards. This process must include:
   a. Conducting an enhanced due diligence review, which may include a site visit to the business or other suitable alternatives.
   b. Assessing the TPA's creditworthiness by analyzing their credit history, financial statements, previous processor history (chargeback performance), business operations, existing debts, and public records.
   c. Conducting a background investigation to verify the principals' identities and ensure there's no significant derogatory information. If certain checks are prohibited by laws or regulations, alternative due diligence procedures must be undertaken and documented.

© 2024 Visa. All rights reserved. Visa Public

d. Check TPA listing in Terminated Merchant File (e.g., VMSS)
e. Examining the TPA's business strategy, considering any past Merchant accounts, terminations, chargebacks, instances of fraud, or illicit activities.
f. Verifying the TPA's onboarding procedures for Sponsored Merchants and scrutinize sample files to confirm both the Acquirer's and TPA's policies are being followed. This includes ensuring the Merchant outlet location is accurately represented and the Merchant maintains a legal presence within the Acquirer's country of jurisdiction.
g. Controlling the approval and review of Merchants, the approval of Cardholder applications, and the establishment of Merchant fees for transactions. This can be accomplished by shadow onboarding the Merchant application.
h. Confirming the TPA's capability to provide Visa with quarterly reports detailing the goods or services each of the Sponsored Merchants is doing business on its behalf, if requested.
i. Verifying the TPA's compliance with all relevant laws and regulations, including those related to data security, privacy, and card network rules.
j. Ensuring the TPA has policies and procedures (e.g., Merchant onboarding, Merchant activity monitoring, Merchant written agreements) in place that align with their business plan and confirm that training is provided to the Sponsored Merchants.
k. Reviewing a TPA's use of any solicitation materials, such as advertisements, stationery, business cards, sales brochures, and website and/or application promotional content.

Risk Statement

When participating in the acquiring of TPAs, Acquirers have lower visibility into the end Merchant. This could lead to potential gaps in policy implementation, and may result in financial losses, operational damage, reputational damage, and legal issues.

CONTROL REQUIREMENT #2

ATPA.C4

Acquirers must conduct additional underwriting for PayFacs prior to onboarding.

ATPA.C4.1 – TPA Underwriting Requirements for PayFacs

For a PayFac's underwriting process, Acquirers must conduct additional steps as defined in ATPA.C3.1 – TPA Underwriting Requirements.

© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. If an Acquirer partners with a PayFac, the Acquirer:
   a. Confirms with the PayFac that they are in good standing in all Visa risk management programs.
   b. Ensures the Payfac is financially stable and creditworthy. This involves analyzing credit history, financial statements, and performance, existing debts, and public records to assess their ability and likelihood to fulfill financial obligations.
   c. Ensures the registration of its PayFac, including the due diligence review attestation, is confirmed by Visa before submitting transactions on behalf of the PayFac or its Sponsored Merchant. If the PayFac is considered high-integrity risk, it must be registered as a High-Risk Internet PayFac, even if it has been previously registered with Visa.
   d. Obtains a unique PayFac identifier from Visa that must be assigned by the Acquirer to each PayFac for transaction processing.
   e. Ensures that the PayFac assigns a unique identifier to each Sponsored Merchant.
   f. Ensures every transaction contains the PayFac identifier and the Sponsored Merchant identifier as follows:
      i. In an Authorization record, both the PayFac identifier and the Sponsored Merchant identifier is present.
      ii. In a Clearing Record, only the PayFac identifier is included.
   g. Assigns a unique CAID number to each PayFac when processing transactions in a card-absent environment, as specified in the Visa Rules.
2. Acquirers must assign the correct location of its PayFac as the country of the PayFac's principal place of business.

VISA
© 2024 Visa. All rights reserved. Visa Public

Risk Statement

When participating in the acquiring of TPAs, Acquirers have lower visibility into the end Merchant. This could lead to potential gaps in policy implementation, and may result in financial losses, operational damage, reputational damage, and legal issues.

CONTROL REQUIREMENT #3

ATPA.C5

Acquirers must conduct additional underwriting for DWOs and SDWOs prior to onboarding.

ATPA.C5.1 – TPA Underwriting Requirements for DWOs and SDWOs

For a DWO's and SDWO's underwriting process, Acquirers must conduct additional steps as defined in ATPA.C3.1 – TPA Underwriting Requirements.

Mandatory Controls:

1. Acquirers partnering with a DWO that runs a SDWO must adhere to the following requirements:
   a. Maintain good standing in all Visa risk management programs.
   b. Register the SDWO as a TPA with Visa.
   c. Assign a unique CAID number to the SDWO for processing transactions in a Card-Absent Environment, as specified in the Visa Rules.
   d. Get a Merchant Verification Value (MVV) for each SDWO.
   e. Deposit the proceeds from transactions conducted via the SDWO into a bank account located in the SDWO's country of operation.
2. Acquirers must set the primary location of a SDWO as the country of the SDWO's Principal Place of Business.
3. Acquirers must assign an additional SDWO location in the instance where the following conditions are all met within each country:
   a. The SDWO has a permanent location where it manages the tasks related to the digital wallet.
   b. The SDWO is taxed on revenue earned from providing wallet services to Cardholders and acceptance services to retailers that were signed up by the SDWO, if such taxes are applicable in that country.
   c. The SDWO is subject to the local laws and regulations.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

When participating in the acquiring of TPAs, Acquirers have lower visibility into the end Merchant. This could lead to potential gaps in policy implementation, and may result in financial losses, operational damage, reputational damage, and legal issues.

CONTROL REQUIREMENT #4

ATPA.C6

Acquirers must conduct additional underwriting for Marketplaces prior to onboarding.

ATPA.C6.1 – TPA Underwriting Requirements for Marketplaces

For a Marketplace's underwriting process, Acquirers must conduct additional steps as defined in ATPA.C3.1 – TPA Underwriting Requirements.

Mandatory Controls:

1. Acquirers must confirm the following Marketplace qualification requirements:
   a. The Marketplace connects Cardholders and retailers via an e-commerce website or mobile application.
   b. The Marketplace's name or brand(s) is prominently displayed on the website or mobile application, is more visible than the names and brands of retailers using the Marketplace and is a part of the mobile application name or URL.
   c. The Marketplace manages payments for sales and refunds on behalf of the retailers that sell goods and services through the Marketplace and receives settlement for transactions on their behalf.
   d. The Marketplace is financially responsible for Disputes and resolves disagreements between Cardholders and retailers by offering either a mutually binding decision, or a money-back guarantee financed by the Marketplace.
2. Acquirers must assess the Marketplace's creditworthiness by analyzing their credit history, financial statements, previous processor history (chargeback performance), business operations, existing debts, and public records.
3. Acquirers must ensure the Marketplace complies with the Visa Rules.
4. Acquirers must examine the Marketplace's business strategy, considering any past Merchant accounts, terminations, chargebacks, instances of fraud, or illicit activities.
5. Acquirers must assign the correct location of its Marketplace as the country of the Marketplace's Principal Place of Business.
6. Acquirers must review onboarding policies and how Marketplaces conduct due diligence of their sellers.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

When participating in the acquiring of TPAs, Acquirers have lower visibility into the end Merchant. This could lead to potential gaps in policy implementation, and may result in financial losses, operational damage, reputational damage, and legal issues.

CONTROL REQUIREMENT #5

ATPA.C7

Acquirers must conduct additional underwriting for Ramp Providers prior to onboarding.

ATPA.C7.1 – TPA Underwriting Requirements for Ramp Providers

For a Ramp Provider's underwriting process, Acquirers must conduct additional steps as defined in ATPA.C3.1 – TPA Underwriting Requirements.

Mandatory Controls:

1. Acquirers must assign the correct location of a Ramp Provider as the country of the Ramp Provider's Principal Place of Business.
2. Acquirers must assign additional locations for a Ramp Provider if all the following conditions are met in each country:
   a. The Ramp Provider has a permanent location where its employees or agents conduct business activities directly related to providing services to the Conversion Affiliates.
   b. Cardholder correspondence and judicial processes are sent to or delivered by the Ramp Provider.
   c. The Ramp Provider pays taxes on revenue earned from providing services to Cardholders and Card acceptance services to Conversion Affiliates if such taxes are applicable in that country.
   d. The Conversion Affiliate is subject to the local laws and regulations of the country.

© 2024 Visa. All rights reserved. Visa Public

Monitoring

3	16	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Inadequate monitoring of transaction-level, Merchant-level and/or TPA-level illegal, suspicious, and/or deceptive practices could lead to financial losses, regulatory/compliance issues, and reputational damage.

CONTROL REQUIREMENT #1

ATPA.C8

Acquirers must monitor TPA transaction activity to detect threats and unusual or suspicious activity and act upon any identified deviations.

ATPA.C8.1 – Portfolio Monitoring of TPAs

Restricting transactions to only valid transactions, i.e., true Cardholder and true Merchants/ Sponsored Merchants, reduces the opportunity for fraudulent transactions. Prohibiting a Merchant or Sponsored Merchant from submitting a transaction representing sales of goods or services fulfilled by another Merchant or Sponsored Merchant curtails the risk of transaction laundering. For TPAs, Acquirers must conduct additional steps to the portfolio monitoring process as defined in AACQ.C8.1.

Mandatory Controls:

1. Acquirers must implement:
   a. **Regular Monitoring:** Analyze transaction patterns and volumes regularly to detect any unusual or suspicious activity. This could involve monitoring for sudden changes in volumes, unusual refund patterns, or transactions that do not fit the normal profile of the TPA's business. Regular sampling of Sponsored Merchant activity (e.g. on a monthly/quarterly basis) should be conducted to ensure ongoing TPA compliance.
   b. **Fraud Detection:** Use advanced fraud detection systems to identify potentially fraudulent transactions. This could involve machine learning algorithms that can identify patterns of fraud.
   c. **Compliance Checks:** Ensure that TPAs are complying with all relevant laws, regulations, and card network rules. This includes data security standards, AML regulations, and rules relating to chargebacks and refunds.

© 2024 Visa. All rights reserved. Visa Public

   d. **Risk Assessment:** Regularly assess the risk profile of the TPA against risk appetite/ KRI's, considering factors such as their business model, geographic location, and the types of transactions they process.
   e. **Reporting:** Generate regular reports on the TPA's transaction activity, share these with relevant stakeholders, and report suspicious activity to the authorities.

2. Acquirers ensure that they settle the proceeds of the transactions submitted into a bank account that this is in the jurisdiction of the acquirer and in line with the agreement with the TPA, and Sponsored Merchants.
3. Acquirers must ensure that a PayFac contracts with a Sponsored Merchant that is outside the country in which the PayFac is located only if both:
   a. The Acquirer and Sponsored Merchant are in the same country.
   b. Settlement to the Sponsored Merchant is performed in the Acquirer's jurisdiction via one of the following:
   c. A local settlement account owned and controlled by the PayFac.
   d. A local settlement account owned by the Acquirer but controlled by the PayFac (e.g., an "on behalf of" account).
   e. Direct settlement from the Acquirer to the Sponsored Merchant.
4. Acquirers must grant access to the TPA for the Terminated Merchant File (e.g., VMSS) and other similar tools to support monitoring for any changes in their Merchant portfolio in case of positive matches to the terminated files.
5. Acquirers must ensure that all Sponsored Merchants are using the correct MCC(s) and are registered with Visa if applicable.
6. Acquirers must evaluate that the TPA is only submitting transactions into interchange within the Acquirer jurisdiction, only from DWO, Merchants, Marketplaces, and Sponsored Merchants within that Acquirer's jurisdiction.
7. Acquirers must perform an annual review of the TPA to confirm ongoing compliance with applicable regional due diligence standards, laws and regulations.
   a. **Financial Statements:** Review the TPA's most recent financial statements to determine its financial condition.
   b. **Ownership Changes:** Document any changes in ownership and perform due diligence on the new owners, if applicable.
   c. **Use of Acquirer's Policies and Procedures:** Examine the TPA's internal policies and procedures and how they align with the Acquirer's own. Also, conduct tests to verify PayFac' s compliance with the Acquirer's onboarding and monitoring policies/requirements.
   d. **PCI DSS Compliance:** If the TPA handles Cardholder data (storing, transmitting, or processing), review the most recent compliance report validating the TPA's compliance with the PCI DSS. TPAs must attest to comply with the PCI DSS and other data security requirements for the protection of Cardholder information and transaction data.

© 2024 Visa. All rights reserved. Visa Public

e. **Review of Merchant Complaints:** Review the TPA's complaint log, any written complaints received from Merchants, and online complaint boards to ensure the TPA is maintaining high service standards.

8. Acquirers ensure remediation plans are implemented to mitigate any imminent risk to Visa Payment System. For any such investigations, reports are shared with Visa as per the Recommend Controls outlined in AACQ.C12.1 – Dispute Management Process.

ATPA.C8.2 – Monitoring Fraud Risk for TPAs

Analyzing data through comprehensive fraud analytics, fraud detection and prevention tools, helps monitor for suspicious activity relating to fraud/disputes. This will ensure that activity is in line with risk appetite/ fraud KRI's.

Mandatory Controls:

1. Acquirers must possess the capabilities, as outlined in AACQ.C8.2 – Portfolio Monitoring – Fraud Risk to detect and prevent fraudulent activity.

ATPA.C8.3 – Reporting of Suspicious Activity by TPAs

Suspicious activity reports help detect, and report known, or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations, making it easier to investigate any concerns. Transactions may be suspicious because they are caused by compromised systems including exposure of PAN.

Mandatory Controls:

1. An Acquirer must immediately report any suspicious activity by a TPA to Visa and include a remediation plan, as specified in What to Do If Compromised:
   a. An Acquirer must immediately report to Visa the suspected or confirmed:
      i. Loss, theft, compromise, or misuse of Visa account information, Cardholder information or Visa.
      ii. Transaction Information, systems, or equipment by one of its Merchants/TPAs.
      iii. Fraud and/or laundering of a transaction.
   b. The report must be thorough, complete and submitted in the formats specified.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Inadequate monitoring of transaction-level, Merchant-level and/or TPA-level illegal, suspicious, and/or deceptive practices could lead to financial losses, regulatory noncompliance, and reputational damage.

CONTROL REQUIREMENT #2

ATPA.C9

Acquirers must regularly check the credit risk of TPAs and adjust their exposure mitigation strategy when needed.

ATPA.C9.1 – Monitoring Credit Risk for TPAs

Where changes in credit risk occur, at the TPA level, an Acquirer's ability to act shall be unhindered for controllable factors. Monitoring help dictate these actions where necessary. Implementing detection capabilities for changes in reserve requirements, adding holds on funds, and conducting reviews helps protect against changes in credit risk.

Mandatory Controls:

1. Acquirers must provide Visa, upon request and within 5 business days, with the following information regarding its Merchants, PayFacs, Marketplaces, DWOs, or any other entity for which the Acquirer is responsible:
   a. A comprehensive overview of its underwriting process for any given entity.
   b. A complete breakdown of its current Visa exposure, and any collateral held against Visa-related positions with Merchants and other entities.
   c. A detailed breakdown of its risk monitoring policy, must, at a minimum, include:
      i. Minimum financial requirements for any given entity.
      ii. How an entity's financial position is determined.
      iii. How the Acquirer protects itself against potential failure of any given entity.
      iv. Policy for managing credit risk on an acquiring portfolio and determining collateral taken.
      v. Exact collateral volumes maintained for potential dispute exposure, for future service Merchants.
      vi. The process for terminating a relationship with any given entity.
2. Acquirer's process for withholding funds from an entity, where the Acquirer has reason to believe that the entity is unable to meet its Visa obligations, provide a future service, or is facing insolvency.

© 2024 Visa. All rights reserved. Visa Public

Risk Statement

Inadequate TPA performance reviews could lead to financial losses and operational damage.

CONTROL REQUIREMENT #3

ATPA.C10

Acquirers must periodically review TPA data and ensure the accuracy of the information entered in Visa systems.

ATPA.C10.1– Reporting Changes in TPA Data

Effective monitoring of TPAs data ensures compliance with the Visa Rules and the Acquirer's policies and procedures.

Mandatory Controls:

1. Acquirers must use the Program Request Management application or the appropriate form to notify Visa of any change in a TPA's principals or business relationship (including change of ownership or termination of contract). The Acquirer must submit the notice to Visa within 5 business days of the change or knowledge of the change. The Acquirer must forward to Visa requests for correction.

© 2024 Visa. All rights reserved. Visa Public

Data Integrity/Quality

1	3	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Insufficient recordkeeping and retention policies and/or procedures could impact the ability to manage TPA information and portfolios, which may result in operational damage and legal issues.

CONTROL REQUIREMENT #1

ATPA.C11

Acquirers must have a clearly defined record keeping and retention policy in line with applicable jurisdiction, pertaining to TPAs as part of their risk management.

ATPA.C11.1 – Data Collection and Retention

Verifying that data elements align precisely with the registered details on file confirms the legitimacy of the transaction. This reduces the risk of fraudulent activity or unauthorized transactions.

Mandatory Controls:

1. Acquirers must ensure TPAs maintain a complete, well-documented file containing Merchant records, including any information connected to an investigation, for at least 2 years after Merchant Agreement termination.
2. Acquirers of a TPA that is undergoing a forensic investigation must also notify Visa when it receives notice.
3. Acquirers collect data and records in line with the Visa Rules and maintain those records in line with local jurisdictional laws and regulations and Dispute resolution standards.

© 2024 Visa. All rights reserved. Visa Public

4.3 Acquirers Processing for High Integrity Risk Transaction Merchants (AHIR)

The following control requirements are mandated for **Visa-licensed Acquirers and their TPAs, who sponsor and process transactions for High Integrity Risk Transaction Merchants.** The control requirements have been categorized under overarching risks and related sub-domains. The control requirement is the required objective that must be met by the Acquirer, through the mandatory and recommended controls.

4.3.3 Legal & Regulatory Risk

Legal & regulatory risk is the risk of potential losses due to noncompliance with laws or regulations, or due to legal or regulatory changes.

Integrity Risk

1	3	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Inadequate controls while processing High Integrity Risk transactions could lead to financial losses, reputational damage, and regulatory noncompliance.

CONTROL REQUIREMENT #1

AHIR.C1

Acquirers and their designated TPAs (if applicable) must maintain proper controls and oversight processes to deter illegal transactions from entering the Visa Payment System, as per the VIRP.

AHIR.C1.1 – Compliance with the VIRP

Acquirers and their TPAs that support High Integrity Risk Merchants and transactions maintain proper controls and oversight to identify and deter illegal transactions from entering the Visa Payment System. These controls are designed to accommodate the complexity of local regulations and the potential for illicit activities in certain areas. It also helps define the mechanisms of accepting and acquiring legal, High Integrity Risk transactions.

The VIRP contains detailed requirements and identifies t he scope of High Integrity Risk Merchants and transactions.

© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. Acquirers have a fundamental obligation to operate in a legal and compliant manner. As such, Acquirers ensure their TPAs and Merchants operate in a legal manner and in compliance with all Visa Rules, including:
   a. Comply with all applicable laws, regulations, and other legal requirements.
   b. Maintain sufficient oversight to ensure each of their TPAs involved in the solicitation, onboarding, and servicing of Merchants and Sponsored Merchants (e.g., ISOs, PayFacs, and DWO) complies with all applicable laws, regulations, and other legal requirements applicable to each country in which the TPAs operate.
   c. Use and maintain appropriate controls and processes to ensure their Merchants and Sponsored Merchants only submit transactions that are legal in the buyer's and seller's jurisdictions.
   d. In accordance with the VIRP, establish and implement enhanced due diligence and processes for all High Integrity Risk Merchants, for as long as they are able to accept Visa payments.
2. To apply for a High Integrity Risk Acquirer Registration, Acquirers:
   a. Complete and submit the High Integrity Risk Acquiring Registration Application and associated required documents, depending on the chosen registration tier(s), to Visa.
   b. Provide written attestation that no Merchant transactions that falls into one of the categories within the VIRP have been or will be entered into the Visa Payment System until the High Integrity Risk Acquiring Registration has been approved.
   c. Submit the designated one-time, non-refundable application fee.
   d. Comply with the Visa Rules, requirements, and policies.
   e. Be in good standing in all Visa Risk Management Programs.
3. Depending on the risk tier of the business types the Acquirer is applying for, comply with the requirements listed in the table below:

TIER 1 RISK ACQUIRER	TIER 2 RISK ACQUIRER	TIER 3 RISK ACQUIRER
Undergo an initial control assessment for the specific High Integrity Risk Merchant Tier 1 category for which the Acquirer intends to acquire. Acquirers will be subject to periodic reassessments (up to annually at Visa's discretion). Complete an annual control self-assessment for each approved High Integrity Risk Merchant Tier 1 category.	Undergo and initial control assessment for High Integrity Risk Merchant Tier 2 business types. Acquirers will be subject to periodic reassessments (up to annually at Visa's discretion). Complete an annual control self-assessment for High Integrity Risk Merchant Tier 2 acquiring.	Register to process High Integrity Risk Merchant Tier 3 business types with Visa. Upon request, complete a control self-assessment for High Integrity Risk Merchant Tier 3 acquiring and submit to Visa.

© 2024 Visa. All rights reserved. Visa Public

4.4 Acquirers Processing for ATMs (AATM)

The following control requirements are applicable for **Acquirers processing for ATMs.** The control requirements have been categorized under overarching risks and related sub-domains. The control requirement is the required objective that must be met by the Acquirer through the mandatory and recommended controls.

4.4.1 Business Risk

We define Business risk as the risk that the Acquirer does not achieve its business objectives as a result of its risk strategy, and/or risk management execution against its strategy.

Risk Appetite and Policy Framework

1	4	5
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Misaligned acquiring and risk policies with the risk profile of ATM Operators could lead to a decline in performance, potential fraud, and reputational damage.

CONTROL REQUIREMENT #1

AATM.C1

ATM Acquirers must have documented acquiring and risk policies, outlining the applicable controls, as per the risk profile of ATM Operators.

AATM.C1.1 – Alignment of Acquirer Risk Policies with ATM Network Risk Profile

ATMs are susceptible to fraud and theft. Aligning the Acquirer's risk policies to the ATM Operator's risk profile is essential to ensure fraud and potential losses are mitigated. ATM Operator risk profiles are impacted by both the ATM geographic location and card fraud rates in those jurisdictions/geographies. These factors impact risk mitigation policies.

VISA
© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. In their defined risk/appetite/tolerance, Acquirers must state if they plan to be acting as an ATM Acquirer (including Acquirers that process through a VisaNet Processor with an existing VisaNet endpoint).
2. Before acting as an ATM Acquirer, Acquirers:
   a. Comply with applicable licensing and processing requirements.
   b. Are certified to participate in Custom Payment Services/ATM or be a Full-Service Acquirer.
3. Acquirers conduct ongoing or periodic monitoring of rates and metrics, as defined in the Acquirer's policies and the Visa Rules.
4. Acquirers ensure fraud reporting requirements and policies are in line with the Visa Rules to ensure Issuers, ATM Operators, Sponsoring Banks, and other relevant stakeholders are informed.

Recommended Controls:

1. Acquirers establish a risk acceptance tailored to the ATM network risk profile, encompassing aspects such as limits, assignment of liability, and countermeasures for physical theft and card fraud.
2. Acquirers monitor market concentration limits, measured as the percentage of volume tolerance by market/geography, and make sure both inter- and intra-jurisdiction concentration risks are mitigated.
3. Acquirers evaluate suitable performance metrics for each ATM network risk profile, including factors like cash withdrawal limits, approval rates, reasons for declines, fraud rates, and suspicious activity and act on alerts that detect anomalies compared to regular performance.
4. Acquirers implement robust anti-skimming strategies at ATMs to prevent theft of credit card information. This includes using specialized hardware and software, encrypting data, conducting regular inspections, and educating consumers.
5. Acquirers ensure that ATM Operators comply with the relevant data security standards and requirements such as PCI DSS to prevent compromise of data though various methods such as ATM jackpotting*.

*ATM jackpotting is a sophisticated theft method where hackers force an ATM to dispense all its cash, similar to hitting a jackpot. It requires extensive technical knowledge and can lead to significant financial losses.

© 2024 Visa. All rights reserved. Visa Public

4.4.2 Operational Risk

We define Operational risk as the risk of loss due to internal/external events, external relationships, or inadequate/failed internal processes.

Written Agreements

1	1	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

A lack of contractual binding agreements with ATM Operators could lead to noncompliance and an inappropriate liability assignment, which may result in financial losses, a lack of recourse, operational damage, regulatory noncompliance, and legal issues.

CONTROL REQUIREMENT #1

AATM.C2

ATM Acquirers must have a contractually binding ATM Operator agreement with each of their ATM Operators and must only process Visa ATM Network Transactions from an ATM Operator with which it has a valid agreement.

AATM.C2.1 – ATM Operator Agreement Content

ATM Operator agreements are an integral element of the legal relationship between an Acquirer and an ATM Operator. The purpose of an agreement is to provide a "terms of use" contract containing each party's respective rights, duties, and obligations.

Mandatory Controls:

1. Acquirers have a written agreement with ATM Operators. The agreement:
   a. Includes the ATM Acquirer's name, location, and contact information, and language stating that the ATM Operator may be terminated for failure to comply with the ATM Operator agreement.
   b. Must not contain contractual details regarding pricing arrangements.
   c. States that the ATM Operators must comply with the Visa Rules.

© 2024 Visa. All rights reserved. Visa Public

Onboarding

1	4	1
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Inadequate KYC and KYB verifications could lead to an increase in susceptibility to money laundering and illegal activities, which could lead to financial losses, regulatory noncompliance, and legal issues.

CONTROL REQUIREMENT #1

ATM.C3

ATM Acquirers must conduct KYO (Know-Your-Operator) verifications for ATM Operators.

AATM.C3.1 – Underwriting Requirement for ATM Operators

Onboarding ATM Operators requires different due diligence requirements given their unique risk profile. Whether directly or indirectly through an ISO, onboarding ATM Operators requires understanding the ATM Operator's business model, terminal network, volumes, and bank relationships.

Mandatory Controls:

1. ATM Acquirers maintain documented policies and procedures to manage their TPAs.
2. ATM Acquirers validate its TPA's compliance with the ATM Acquirer Solicitation and Qualification Standards on a periodic basis.
3. ATM Acquirers collect the following information from its ATM Operators and TPAs:
   a. DBA name.
   b. ATM Operator legal name.
   c. ATM Operator outlet location, including street address, city, state, and postal code.
   d. Full first and last name and middle initial of principals (e.g., of corporations, partnerships, sole proprietors).
   e. Incorporation status (e.g., corporation, partnership, sole proprietor, non-profit).
4. ATM Acquirers ensure that a prospective ATM Operator has no significant derogatory background information about any of its principals.

© 2024 Visa. All rights reserved. Visa Public

Recommended Controls:

1. Acquirers gather additional information for enhanced ATM Operator due diligence, which includes:
   a. Clear statement of the business model.
   b. Outlining corresponding fee and pricing model.
   c. Current ATM network and future ATM network plans, which includes specific ATM addresses.
   d. Ensuring ATM Operators have appropriate reporting tools for transaction identification (e.g., source TID).
   e. Sponsor Bank relationships and strategies.
   f. Annual attestations by Sponsor Banks of their portfolios of TIDs and Transactions.
   g. Physical verifications of ATM locations and installation of security measures such as security cameras. Ensure ATM locations are compliant with safety guidelines in terms of visibility of location, lighting within the ATM kiosks etc.).
   h. Onboarding KYB/KYC due diligence and validation of responsibility under PCI PIN Transaction Standards.

Monitoring

1	3	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Inadequate monitoring of ATM-level fraudulent, illegal, suspicious, and/or deceptive practices could lead to financial losses, regulatory noncompliance, and reputational damage.

CONTROL REQUIREMENT #1

AATM.C4

ATM Acquirers must monitor transaction activity to detect threats, unusual and/or suspicious activity and use exception reporting to act upon deviations.

AATM.C4.1 – Portfolio Monitoring for ATM Terminals

Each ATM Operator, ATM Acquirer, and any Service Providers (or other TPAs acting on their behalf) ensure controls, resources, and monitoring systems for the prompt detection and reporting of fraud and unusual or suspicious activity, to prevent and effectively respond to potential threats to ATM activity.

© 2024 Visa. All rights reserved. Visa Public

Mandatory Controls:

1. ATM Acquirers accept all valid cards for all transaction functions in which the Acquirer has elected to participate through the Visa Global ATM Network.
2. ATM Acquirers must track and report any suspicious ATM transactions. In collaboration with ATM Operators, their associated banks, and any TPAs, Acquirers proactively detect potential threats and monitor for any fraudulent or suspicious activities and taking remediation action for confirmed or suspected fraud. Their monitoring scope includes:
   a. Detection of unusual patterns in ATM deposits or withdrawal volumes at a specific ATM.
   b. Tracking repeated instances of high withdrawal volumes at the same ATM(s) by multiple cards from a single Issuer.
   c. Monitoring for excessive charges applied for minor withdrawals or at various ATMs. Acquirers investigate the activity and request the ATM Operator to act if needed.
3. In case of an incident, Acquirers:
   a. Determine and relay the real-time (or near real-time) location of the ATM terminals to the law enforcement agencies.
   b. Ensure the protection of video recordings, if any, captured by the targeted ATMs. Wherever legally possible, these are shared with law enforcement agencies to support their investigation.

© 2024 Visa. All rights reserved. Visa Public

4.4.3 Legal & Regulatory Risk

Legal & regulatory risk is the risk of potential losses due to noncompliance with laws or regulations, or due to legal or regulatory changes.

Regulatory Risk

1	1	-
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Acquirer's acquiring and risk policies that are not aligned to jurisdictional and regulatory requirements could lead to financial losses and regulatory noncompliance.

CONTROL REQUIREMENT #1

AATM.C5

ATM Acquirers must ensure ATM Operators are compliant with jurisdictional laws and regulations.

AATM.C5.1 – Compliance with Jurisdictional Laws and Regulations

ATM Operators must comply with applicable jurisdictional laws and regulations, which may vary in comprehensiveness, depending upon the locations and jurisdictions.

Mandatory Controls:

1. Acquirers display Visa ATM and Plus Acceptance Marks on all ATMs within 30 days from the date the Acquirer begins accepting Visa Cards and Plus enabled Cards.

VISA
© 2024 Visa. All rights reserved. Visa Public

4.5 Visa Direct Clients (AVDC)

The following control requirements are applicable for **Money Movement Entities who accept Visa Direct transactions.** Additionally, it will also be applicable to non-member Money Movement Entities which sponsor Originators. The control requirements have been categorized under overarching risks and related sub-domains. The control requirement is the required objective that must be met by the Acquirer through the mandatory and recommended controls.

For the purpose of this section**, "Acquirers"** are referred as **"Money Movement Entities"**, unless otherwise specified.

4.5.2 Operational Risk

We define Operational risk as the risk of loss due to internal/external events, external relationships, or inadequate/failed internal processes.

Onboarding

1	-	4
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Money Movement Entities that have ineffective onboarding standards could onboard Originators involved in illegal activities, deceptive practices, and/or have elevated Dispute activity. This could lead to financial losses, reputational damage, and legal issues.

CONTROL REQUIREMENT #1

AVDC.C1

Money Movement Entities must have additional onboarding standards for Originators.

AVDC.C1.1 – Underwriting Requirements for Originators

Collecting and verifying additional information for Originators enables Enhanced Due Diligence (EDD) procedures and decreases the potential for fraudulent/deceptive activity to occur.

© 2023 Visa. All rights reserved. Visa Public

Recommended Controls:

1. A Money Movement Entities' due diligence ensures coverage of the associated risk profile for Visa Direct transactions.
2. Money Movement Entities have an approved Program Information Form (PIF) to conduct Visa Direct transactions and obtain PIF approval for their programs before their BINs are enabled for OCTs and AFTs.
3. To establish a legitimate business model and a clear nature of the transaction, Money Movement Entities request website URLs and/or mobile device applications that are used by the Originators/Originating Entities. Originators/Originating Entities business model expected volumes and controls (such as velocity limits) are requested by Money Movement Entities.
4. Money Movement Entities ensure registration of the service provider(s) the Money Movement Entities use to process, transmit, or store Cardholder data as a TPA and ensure the service provider is compliant with PCI DSS, per the Visa Account Information Security Program requirements.

Monitoring

1	-	5
CONTROL REQUIREMENTS #	MANDATORY CONTROLS #	RECOMENDED CONTROLS #

Risk Statement

Increased scam-based fraud in person-to-person use cases places undue liability on Money Movement Entities or other ecosystem stakeholders, which may result in financial losses and legal issues.

CONTROL REQUIREMENT #1

AVDC.C2

Money Movement Entities must monitor for scams and their evolving nature when acquiring Visa Direct transactions to detect targeted scams or Originator-level scams.

© 2023 Visa. All rights reserved. Visa Public

AVDC.C2.1 – Portfolio Monitoring for Fraud Risk

Scams continually evolve in nature, particularly in P2P money movement, taking on various shapes in OCT and AFT transactions. Scammers use social engineering and hacking to obtain pertinent information at the Cardholder and Issuer level to initiate and complete fraud.

In addition, evolving regulations globally place additional liability on Issuers and Money Movement Entities to protect Cardholders from such scams, necessitating additional diligence and scrutiny by Money Movement Entities.

Recommended Controls:

1. Money Movement Entities deploy monitoring capabilities as outlined in AACQ Monitoring. These capabilities include behavioral, biometric, digital, authentication, graph analytics, and rules-based decision-making among other strategies for scam detection, automated decision-making, and near-real-time action.
2. Money Movement Entities monitor for:
    a. Account opening fraud by reviewing trends in personal information accuracy, card/account details, and behavioural data.
    b. Scams that may take on several fraud types:
        i. **Account Takeover (ATO):** Money Movement Entities monitor for Phishing trends and behaviours, such as one time passcode (OTP) usage and behaviours, transaction amounts, transaction types, recipient account, age of recipient account, standing data and changes in Cardholder profile, among other factors, to detect ATO attempts. This fraud type can also present as vishing, smishing, viruses/malware, data breaches, brute force, and man-in-the-middle attacks.
        ii. **Authorized Push Payments (APP):** Money Movement Entities monitor for Social Engineering trends and behaviours, such as login/data entry velocity, age of recipient account, unrelated recipient account, among other factors, to detect APP attempts. This fraud type can also present as romance scams, investment scams, purchase scams, invoice scams, and bank staff impersonation.
        iii. **Unauthorized Card Usage:** Money Movement Entities monitor for suspicious activity, trends, and behaviours, such as dark web monitoring for exposed card details, recently added cards to wallets, IP addresses, geolocation, age of recipient accounts, compromised card credentials.
3. Money Movement Entities' monitoring capabilities include email/phone number reputation analysis, KYC checks, sanctions, and PEP checks, ID verification, behaviour analysis, rule-based decisioning, including using predictive models.
4. Money Movement Entities ensure fraud reporting procedures are enhanced to capture and report OCT fraud to Visa to ensure Issuer visibility on potentially fraudulent activity which may prevent further fraud.
5. To ensure the Visa Direct program is operating in line with the approved PIF supplied to Visa when the Visa Direct program was initiated, Money Movement Entities perform continuous monitoring of the Originator's business model and relevant program. If the Originator's business model changes over time, Visa is contacted, or the PIF is updated.

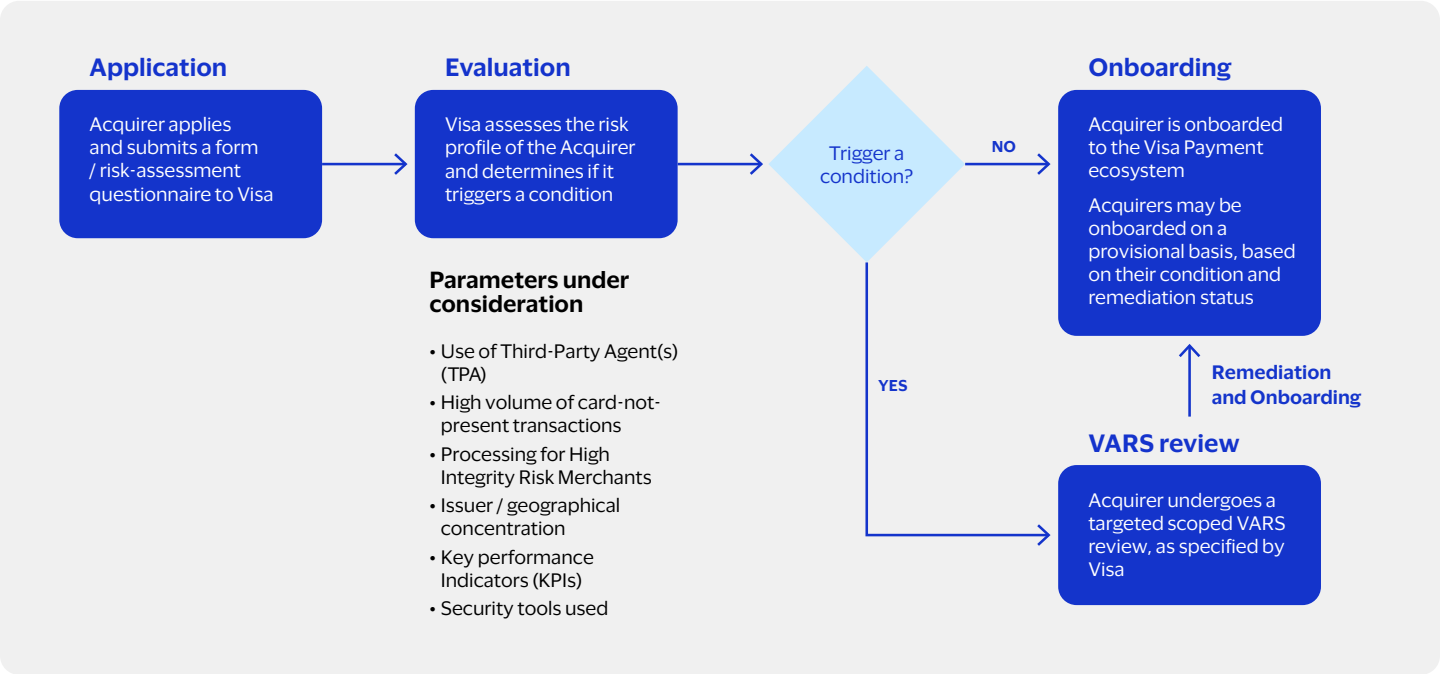
© 2023 Visa. All rights reserved. Visa Public

5 VARS Reviews

5.1 Reviews

VARS serves as a set of controls to identify potential risks both at the application and on an ongoing basis to identify deviations to pre-defined thresholds.

NEW ACQUIRERS: ONBOARDING PROCESS



During the initial application, an Acquirer's preliminary profile will be captured based on the details provided and information available with other Visa teams. The Acquirer's profile will be reviewed against the high-level criteria defined for a VARS review, including their relationship with TPAs, High Integrity Risk Merchants, involvement with alternative payment methods, and other requirements as applicable. Based on the outcome of the high-level assessment, the Acquirer will be either be subject to a VARS review or initiated into the onboarding process.

© 2024 Visa. All rights reserved. Visa Public

Existing Acquirers are monitored on an ongoing basis and may trigger a VARS review on a risk-based approach. Below represents illustrative criteria (not exhaustive):

- Consistent violations (e.g., VIRP, VAMP, AML, etc.)
- Changes in acquiring profile (e.g., high integrity risk Merchants, expansion into a new geography, Frisco Score)
- Changes in key metrics (e.g., disputes, transaction volumes)

Acquirers must **identify their archetype(s)** prior to determining the scope of the review, and the **reviewer must confirm** that the identified archetype(s) correctly depict the Acquirer's business model.

Acquirers will be responsible for the cost of a VARS review and are accountable for sharing the final review report with Visa.

VARS reviews must be completed by Visa Staff **or through a selected third party reviewers with Visa oversight.**

5.2 VARS Review Remediation

Following the review, a findings report will be developed to identify control gaps and corrective actions, and the reviewer will work with the Acquirer on developing a remediation plan. Acquirers are expected to work on appropriate remediations as suggested, based on the review outcome. The reviewer will continue to track the Acquirer's progress, and if an Acquirer fails to implement an approved remediation plan within the agreed-upon timeframe, Visa may impose Member Risk Reduction Requirements as specified in the Visa Rules.

© 2024 Visa. All rights reserved. Visa Public

Appendix A: Types of Visa Clients, Acquirer Relationship and Transactions

VISA CLIENT	**A client is a financial institution or entity that is in a direct contractual relationship with Visa (e.g., VisaNet, Visa Direct).**
Principal Acquirer	A financial institution or entity that is a member of Visa and is authorized to directly connect to Visa's network to process credit or debit card transactions. They enable acceptance of the card payments and manage the transactions process, including authorization and settlement.
Money Movement Entity	A financial institution or entity leveraging Visa Direct for money movement among different transacting parties.
ACQUIRER RELATIONSHIP	**Acquirers engage in a relationship with a Merchant or Originator either directly or through a TPA.**
Merchant	An Acquirer has a direct relationship with a Merchant to provide access to the Visa Payment network. Refer to Appendix E.1: Merchant Types for more information.
Third-Party Agent (TPA)	An entity, not defined as a VisaNet Processor or Visa Scheme Processor, which provides payment-related services, directly or indirectly, to an Acquirer and/or its Merchants or Sponsored Merchants. Refer to Appendix E.2: TPA Types for more information
Originator	An Acquirer (Money Movement Entity) who engages with Originators that initiate Visa Direct transactions.
TRANSACTION	**A card-present or card-absent transaction indicates an exchange of value between two parties, typically involving the transfer of funds from one party to another facilitated by the ecosystem of players including, Issuer, payment network, Acquirer etc.**
Purchase	The act of acquiring goods or services using various methods of payments.
Money Movement	The transfer of funds between two parties/mediums electronically.
Automated Teller Machine (ATM)	An electronic banking device that enables cardholders to complete transactions, such as cash withdrawals, deposits, funds transfers, and balance inquiries. ATM Transactions are monetary (Withdrawals and Deposits) and non-monetary (Balance Inquiry, PIN Change, Mini Statements, and Transfers).

© 2024 Visa. All rights reserved. Visa Public

Appendix B: Control Requirements by Archetype

The table below provides a summary of control requirements across the Acquirer archetypes:

THEME	AACQ	ATPA	AHIR	AATM	AVDC
Risk Policies	AACQ.C1			AATM.C1	
Contractual Agreements	AACQ.C2	ATPA.C1		AATM.C2	
Exposure Mitigation	AACQ.C3				
Settlement of Funds	AACQ.C4				
Reporting Terminated Merchants		ATPA.C2			
Underwriting Requirements	AACQ.C5	ATPA.C3 ATPA.C4 ATPA.C5 ATPA.C6 ATPA.C7		AATM.C3	AVDC.C1
KYC/KYB	AACQ.C6				
Fraud Detection and Prevention	AACQ.C7				
Portfolio Monitoring/Exception Reporting	AACQ.C8	ATPA.C8		AATM.C4	AVDC.C2
Fraudulent Activity Investigation	AACQ.C9				
Reporting of Suspicious Activity	AACQ.C10	ATPA.C8			
Monitoring Credit Risk	AACQ.C11	ATPA.C9			
Dispute Management Process	AACQ.C12				
Data Elements/Data Collection & Retention	AACQ.C13	ATPA.C10 ATPA.C11			
PCI DSS Compliance	AACQ.C14				
Business Continuity and Resilience	AACQ.C15				
Visa's Requirements and Policies	AACQ.C16				
Monitoring Illegal Transactions	AACQ.C17				
Compliance	AACQ.C18		AHIR.C1	AATM.C5	

© 2024 Visa. All rights reserved. Visa Public

Appendix C: Risk Taxonomy

Below are key definitions of the risk domains and sub-domains from the VARS purview:

RISK TAXONOMY	DESCRIPTION
1. Business Risk	We define business risk as the risk that the Acquirer does not achieve its business objectives as a result of its risk strategy, and/or risk management execution against its strategy.
1.1 Risk Appetite and Policy Framework	The risk of being unable to align the Acquirer's policies with the risk appetite.
2. Operational Risk	We define operational risk as the risk of loss due to internal/external events or inadequate/failed internal processes.
2.1 Written Agreements	The risk of improper disclosure of the obligations and/or violations of the contractual binding agreements.
2.2 Onboarding*	The risk of onboarding and underwriting gaps, including insufficient due diligence, inability to identify suspicious traits, regulatory noncompliance, and operational disruptions.
2.3 Monitoring*	The risk of inadequate monitoring standards, leading to noncompliance, excessive fraud, and chargebacks etc.
2.4 Chargeback/Dispute	The risk of excessive disputes beyond the Acquirer's risk appetite and the Visa Acquirer Program rates (VAMP).
2.5 Data Integrity/Quality	The risk of a Merchant/TPA misrepresenting information during onboarding, period of contract, and offboarding.
2.6 Data Security	The risk that Payment and Cardholder data is lost, stolen, or otherwise compromised.
2.7 Network and Scheme Compliance	The risk of failure to comply with Visa Rules and/or technical standards, which are updated periodically
3. Legal & Regulatory Risk	The risk of potential losses due to noncompliance with laws or regulations, or due to legal or regulatory changes.
3.1 Miscoding/Transaction Laundering	The risk an Acquirer faces due to concealed illegal transactions such as miscoding.
3.2 Regulatory Risk	The risk of noncompliance with new or existing regulations.
3.3 Integrity Risk	The risk of gaps in registering for high-integrity risk processing and/or processing illegal transactions (Refer to the VIRP).

*Fraud and Credit Risk are covered as part of Operational Risk under Onboarding and Monitoring sub-domains.

© 2024 Visa. All rights reserved. Visa Public

Appendix D: Stakeholders Involved

The various stakeholders (primary and secondary) and their roles in the context of VARS is as follows:

Primary stakeholders are those who are directly involved in the VARS process, either as an Acquirer, or a Money Movement Entity complying with the VARS requirements, or as Visa, ensuring that Acquirers comply with the requirements outlined in the VARS.

PRIMARY STAKEHOLDERS	ROLE
Acquirers	Comply with the VARS requirements in a timely and ongoing manner (wherever applicable) to mitigate potential risks impacting the Visa ecosystem.
Money Movement Entities	Comply with the VARS requirements in a timely and ongoing manner (wherever applicable) to mitigate potential risks impacting the Visa ecosystem, pertaining to accepting Visa Direct transactions.
Visa	Provide the required support/clarifications to the Acquirers to complete their review process in an efficient manner.

Secondary stakeholders are those who are not directly involved in the compliance or review process of the VARS, but they have a relationship to the primary stakeholders to ensure enforcement of VARS.

SECONDARY STAKEHOLDERS	ROLE
Third-Party Reviewers	Conduct an unbiased review of the VARS compliance by the Acquirer or its TPAs.
TPAs	Support the Acquirer in complying with the VARS in a timely and ongoing manner (wherever applicable).
Merchants	Support the Acquirer in complying with the VARS in a timely and ongoing manner (wherever applicable).

© 2024 Visa. All rights reserved. Visa Public

Appendix E: Merchant and TPA Types

E.1 Merchant Types

Marketplaces and Ramp Providers are registered as TPAs, but otherwise behave as a Merchant/ Sponsored Merchant.

- For more information on Marketplaces, refer to **Third-Party Agent Registration Program – TPA Types and Functional Descriptions**.
- For more information on Ramp Providers, refer to **Digital Currency Transactions Guide – Ramp Provider Program Requirements**.

E.2 TPA Types

The various TPA types and sub-types are listed below. For more information and functional descriptions, refer to **Third-Party Agent Registration Program – TPA Types and Functional Descriptions**.

INDEPENDENT SALES ORGANIZATIONS (ISO)				
ISO Merchant (ISO – M)	ISO Cardholder (ISO – C)	ISO ATM (ISO – ATM)	ISO Prepaid (ISO – PP)	ISO High Risk (ISO – HR)
ENCRYPTION SUPPORT ORGANIZATIONS (ESO)				
THIRD-PARTY SERVICERS (TPS)				
Payment processing	Value added services	Datacentre housing	Secure storage facilities	Managed services
Monitoring services	Network service provider	Managed firewall/ router provider	Statement printing	Call Center provider
Token service provider	Corporate T&E charge reporting	Acquirer token service providers	POS services	Software as a Service (SaaS)
Platform as a Service (PaaS)	Infrastructure as a Sercice (IaaS)			

© 2024 Visa. All rights reserved. Visa Public

MERCHANT SERVICERS (MS)				
Payment Gateways and online shopping cart	Payment processing	POS services	Value added services	3DS Service Provider
Datacentre housing	Secure storage facilities	Managed services	Monitoring services	Network service provider
Managed firewall/ router provider	Statement printing	Call Center provider	Token service providers	Corporate T&E charge reporting
Acquirer token service providers	Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)	
CORPORATE FRANCHISE SERVICERS (CFS)				
PAYMENT FACILITATORS (PF)				
HIGH INTEGRITY RISK PAYMENT FACILITATORS (HIRPF)				
MARKETPLACES				
STAGED DIGITAL WALLET OPERATORS				
DISTRIBUTION CHANNEL VENDORS (DCV)				
INSTANT CARD PERSONALIZATION AND ISSUANCE AGENT (ICPIA)				
DYNAMIC CURRENCY CONVERSION (DCC)				
VISA RECOGNIZED THIRD PARTIES – DOES NOT REQUIRE REGISTRATION				

© 2024 Visa. All rights reserved. Visa Public

Appendix F: Control Requirements Checklist

This is a comprehensive list of mandatory control requirements. This checklist can be used to tracking compliance with the control requirements.

Reiterating, all Acquirers must satisfy the control requirements under AACQ (All Acquirers), irrespective of any additional archetype(s). Acquirers must also meet the additional control requirements as listed under their respective archetype.

RISK DOMAIN	SUB-DOMAIN	CR ID	CONTROL REQUIREMENT	COMPLIANT		
AACQ (All Acquirers)				**Yes**	**No**	**N/A**
Business	**Risk Appetite and Policy framework**	**AACQ.C1**	Acquirers must maintain a defined risk appetite/ tolerance as well as risk management capabilities that are adequate for their business model.			
Operational	**Written Agreements**	**AACQ.C2**	Acquirers must have contractual binding agreements with Merchants/TPAs that assures compliance with the acquiring strategy.			
Operational	**Written Agreements**	**AACQ.C3**	Acquirers must have a clause in their contractual binding agreements with Merchants/TPAs that enables exposure mitigation coverage.			
Operational	**Written Agreements**	**AACQ.C4**	Acquirers must settle funds to the Merchant/ TPA as per the terms described in the contractual binding agreement and take any applicable withholdings into consideration.			
Operational	**Onboarding**	**AACQ.C5**	Acquirers must have an onboarding standard that enables risk-based due diligence processes.			
Operational	**Onboarding**	**AACQ.C6**	Acquirers must execute KYC/KYB checks in accordance with applicable jurisdictional laws and regulations.			
Operational	**Onboarding**	**AACQ.C7**	Acquirers must conduct fraud checks when onboarding a Merchant.			
Operational	**Monitoring**	**AACQ.C8**	Acquirers must monitor transaction and Merchant activity to detect threats, unusual or suspicious activities/transactions and use exception reporting to act upon deviations.			

© 2024 Visa. All rights reserved. Visa Public

RISK DOMAIN	SUB-DOMAIN	CR ID	CONTROL REQUIREMENT	COMPLIANT		
Operational	**Monitoring**	**AACQ.C9**	Acquirers must support fraudulent investigations by providing comprehensive details on the Merchant and/or transactions to the relevant party/authorities.			
Operational	**Monitoring**	**AACQ.C10**	Acquirers must report suspicious activity to help prevent fraud, comply with regulations, protect finances, and maintain their reputation.			
Operational	**Monitoring**	**AACQ.C11**	Acquirers must have the ability to proactively monitor and act on changes in credit risk.			
Operational	**Chargeback / Dispute**	**AACQ.C12**	Acquirers must have access to dispute management solutions and be able to manage and respond to disputes within the timelines specified by Visa.			
Operational	**Data Integrity / Quality**	**AACQ.C13**	Acquirers must implement controls on Merchant names to maintain consistency throughout the transaction lifecycle, thereby safeguarding against unauthorized or illegal use.			
Operational	**Data Security**	**AACQ.C14**	Acquirers must comply with the Visa Account Information Security Program and jurisdiction regulations for data handling.			
Operational	**Data Security**	**AACQ.C15**	Acquirers must have a business continuity plan and resume operations within their specified timeline, in case of unforeseen events like natural disasters, and avoid disruption in critical payment operations.			
Operational	**Network and Scheme Compliance**	**AACQ.C16**	Acquirers must ensure their operational, sales & technical functions remain compliant with all Visa requirements, as regularly updated.			
Legal & Regulatory	**Miscoding / Transaction Laundering**	**AACQ.C17**	Acquirers must implement controls during underwriting and monitoring for potentially concealed illegal transactions to ensure no illegal transactions enter the Visa ecosystem.			
Legal & Regulatory	**Regulatory**	**AACQ.C18**	Acquirer's acquiring and risk policies must align with all applicable jurisdictional laws and regulations, which must be shared with Merchants/TPAs.			

© 2024 Visa. All rights reserved. Visa Public

RISK DOMAIN	SUB-DOMAIN	CR ID	CONTROL REQUIREMENT	COMPLIANT		
ATPA (Acquirers sponsoring TPAs)				**Yes**	**No**	**N/A**
Operational	**Written Agreements**	**ATPA.C1**	Acquirers must have contractual binding agreements with TPAs that assures compliance with their acquiring strategy.			
Operational	**Written Agreements**	**ATPA.C2**	Acquirers must have a contractual agreement with TPAs that includes that TPAs terminated for just cause are reported in line with Visa practices.			
Onboarding	**Onboarding**	**ATPA.C3**	Acquirers must have a TPA specific onboarding process and underwrite all TPAs prior to onboarding.			
Onboarding	**Onboarding**	**ATPA.C4**	Acquirers must conduct additional underwriting for PayFacs prior to onboarding.			
Onboarding	**Onboarding**	**ATPA.C5**	Acquirers must conduct additional underwriting for DWOs and SDWOs prior to onboarding.			
Onboarding	**Onboarding**	**ATPA.C6**	Acquirers must conduct additional underwriting for Marketplaces prior to onboarding.			
Onboarding	**Onboarding**	**ATPA.C7**	Acquirers must conduct additional underwriting for Ramp Providers prior to onboarding.			
Onboarding	**Monitoring**	**ATPA.C8**	Acquirers must monitor TPA transaction activity to detect threats and unusual or suspicious activity and act upon any identified deviations.			
Onboarding	**Monitoring**	**ATPA.C9**	Acquirers must regularly check the credit risk of TPAs and adjust their exposure mitigation strategy when needed.			
Onboarding	**Monitoring**	**ATPA.C10**	Acquirers must periodically review TPA data and ensure the accuracy of the information entered in Visa systems.			
Onboarding	**Data Integrity / Quality**	**ATPA.C11**	Acquirers must have a clearly defined record keeping and retention policy in line with applicable jurisdiction, pertaining to TPAs as part of their risk management.			

© 2024 Visa. All rights reserved. Visa Public

RISK DOMAIN	SUB-DOMAIN	CR ID	CONTROL REQUIREMENT	COMPLIANT		
AHIR (Acquirers processing for High Integrity Risk Transaction Merchants)				**Yes**	**No**	**N/A**
Legal & Regulatory	**Integrity**	**AHIR.C1**	Acquirers and their designated TPAs (if applicable) must maintain proper controls and oversight processes to deter illegal transactions from entering the Visa Payment System, as per the VIRP.			
AATM (Acquirers processing for ATMs)				**Yes**	**No**	**N/A**
Business	**Risk Appetite and Policy Framework**	**AATM.C1**	ATM Acquirers must have documented acquiring and risk policies, outlining the applicable controls, as per the risk profile of ATM Operators.			
Operational	**Written Agreements**	**AATM.C2**	ATM Acquirers must have a contractually binding ATM Operator agreement with each of their ATM Operators and must only process Visa ATM Network Transactions from an ATM Operator with which it has a valid agreement.			
Operational	**Onboarding**	**AATM.C3**	ATM Acquirers must conduct KYO (Know-Your-Operator) verifications for ATM Operators			
Operational	**Monitoring**	**AATM.C4**	ATM Acquirers must monitor transaction activity to detect threats, unusual and/or suspicious activity and use exception reporting to act upon deviations.			
Legal & Regulatory	**Regulatory**	**AATM.C5**	ATM Acquirers must ensure ATM Operators are compliant with jurisdictional laws and regulations.			
AVDC (Visa Direct Clients)				**Yes**	**No**	**N/A**
Operational	**Onboarding**	**AVDC.C1**	ATM Acquirers must have documented acquiring and risk policies, outlining the applicable controls, as per the risk profile of ATM Operators.			
Operational	**Monitoring**	**AVDC.C2**	Money Movement Entities must monitor for scams and their evolving nature when acquiring Visa Direct transactions to detect targeted scams or Originator-level scams.			

© 2024 Visa. All rights reserved. Visa Public

Appendix G: Visa Direct Use Cases

There are two types of Visa Direct transactions:

- **Account Funding Transactions (AFT):** Pull transactions used to move funds from a funding source to a card or used to pull funds into a recipient account from a card.
- **Original Credit Transactions (OCT):** Push transactions used to transfer funds from originating card/account to recipient card/account in the form of a credit to the recipient. OCTs are most used in the simple P2P (card-to-card or account-to-account) use case.

Within the above two types, below is a set of Visa Direct use cases, inserted here for familiarity. The list below is representative and not comprehensive. Visa Direct may add new use cases:

TRANSACTION USE CASE	DESCRIPTION
AFT to fund a subsequent P2P transaction	Use AFT to pull funds from a card/account to further push funds for a follow-on transaction
AFT to load/reload a prepaid card	Use AFT to pull funds and load or reload a prepaid card
AFT to fund an external account (e.g., brokerage)	Use AFT to debit a card to send to an account (bank, brokerage)
AFT to pre-fund a Digital Wallet	Use AFT to pull funds from a card that can then be credited (OCT) to a Digital Wallet
AFT to acquire digital currency/liquid assets	Use AFT to acquire/"purchase" digital currency (e.g., cryptocurrency) or liquid assets (e.g., shares)
OCT for P2P	Receive-side of Person-to-person transfers
OCT for Digital Wallet payout	Use OCT for P2P transfers from a Digital Wallet to a card/Digital Wallet
OCT for Merchant settlements	Use OCT for payouts from Merchant accounts with PSPs to beneficial owners' card
OCT for remittances	Use OCT for P2P transactions with payout in x-currency (most often)
OCT for earned wage access	Use OCT to initiate early payroll payout from payroll/EWA provider to recipient card
OCT for loyalty payments	Use OCT to payout from loyalty/rewards account to recipient card/wallet/account

© 2024 Visa. All rights reserved. Visa Public

TRANSACTION USE CASE	DESCRIPTION
OCT for funds disbursement	Use OCT to payout from a business/institution (e.g., insurance company) into recipient card/wallet/account
OCT for refunds/merchandise returns	Use OCT to return funds to a customer linked to a previous purchase
OCT for B2B Payment	Use OCT to push funds where a POS solution does not exist, standing in for a purchase transaction.
OCT for B2B Payment	Use OCT to push funds from a third-party biller collecting payment on behalf of the supplier from the buying business as a purchase followed by an OCT to the supplier.

For more on Visa Direct transactions, visit Visa Access.

© 2024 Visa. All rights reserved. Visa Public

Appendix H: Glossary

Below is a glossary for the VARS. It is recommended to use this glossary in conjunction with the glossary in Visa Access.

ACRONYMS	FULL FORM
3DS	3D Secure
AACQ	All Acquirers
AATM	Acquirers processing for ATMs
AFT	Account Funding Transactions
AHIR	Acquirers processing for High Integrity Risk Transaction Merchants
AML	Anti-Money Laundering
ARPU	Average Revenue Per User
ATF	Anti-Terrorist Financing
ATM	Automated Teller Machine
ATO	Account Take-Over
ATPA	Acquirers sponsoring TPAs
AVDC	Money Movement Entities accepting Visa Direct transactions
AVS	Address Verification Service
BIN	Bank Identification Number
BBB	Better Business Bureau
BTC	Bitcoin
CAVV	Cardholder Authentication Verification Value
CDD	Customer Due Diligence

© 2024 Visa. All rights reserved. Visa Public

ACRONYMS	FULL FORM
CFT	Combating the Financing of Terrorism
CRM	Customer Relationship Management
CSR	Credit Settlement Risk
CTR	Chargeback-to-Transaction Report
CVV	Card Verification Value
DBA	Doing Business As
DDA	Demand Deposit Account
DR	Disaster Recovery
DTVV	Dynamic Token Verification Value
DWO	Digital Wallet Operators
E-Commerce	Electronic Commerce
EDD	Enhanced Due Diligence
EUR	Euro
FATF	Financial Action Task Force
FAQ	Frequently Asked Questions
HIRPF	High Integrity Risk Payment Facilitator
ICS	Issuers' Clearinghouse Service
ID	Identification
IP	Internet Protocol
ISO	Independent Sales Organization

© 2024 Visa. All rights reserved. Visa Public

ACRONYMS	FULL FORM
KYB	Know Your Business
KYC	Know Your Customer
MCC	Merchant Category Code
MID	Merchant ID
MO	Mail Order
MVV	Merchant Verification Value
NFT	Non-Fungible Token
NCA	Non-compliance assessment
OCT	Original Credit Transaction
OTP	One Time Passcode
P2P	Person-to-Person
PA DSS	Payment Application Data Security Standard
Pay by Link Merchant	A Merchant who sends a link to a cardholder via chat, social media, email, or another preferred channel; when the cardholder clicks the link it takes the cardholder to a payment page where the payment is performed. This allows merchants to sell their products even without having their own website that is connected to a payment gateway.
PayFac	Payment Facilitator
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PCS	Prepaid Clearinghouse Service
PEP	Politically Exposed Person
PFD	Payment Fraud Disruption

© 2024 Visa. All rights reserved. Visa Public

ACRONYMS	FULL FORM
PII	Personal Identifiable Information
PIF	Program Information Form
PIN	Personal Identification Number
POS	Point-of-Sale
PSP	Payment Service Provider
PV	Present Value
RACI	Responsible Accountable Consulted Informed
RPO	Recovery Point Objective
PSP	Payment Service Provider
RTO	Recovery Time Objective
SMB	Small and Medium Businesses
SDWO	Staged Digital Wallet Operator
SOP	Standard Operating Procedures
T/A	Trading As (Trading Names)
T1C	Tier 1 Capital
TAVV	Token Authentication Verification Value
TC40	Fraud reports submitted by the Issuers
TID	Terminal ID
TLD	Transaction Laundering
TO	Telephone Order
TPA	Third-Party Agent

© 2024 Visa. All rights reserved. Visa Public

ACRONYMS	FULL FORM
USDC	US Dollar Coin
URL	Uniform Resource Locator
VAMP	Visa Acquirer Monitoring Program
VARS	Visa Acceptance Risk Standards
VBN	Visa Business Newsletter
VIRP	Visa Integrity Risk Program
VMSS	Visa Merchant Screening Service
VA	Visa Access (a regional Visa tool and access is dictated at BID level. Acquirers which operate in more than one Visa region will need to arrange separate regional accesses to Visa Access.)

COMMON VARS TERMS	DESCRIPTION
Risk Appetite	The level of risk that an organization is prepared to accept in pursuit of its objectives before action is deemed necessary to reduce the risk.
Risk Domain	Applicable overarching risk: Business, Financial, Operational, Legal & Regulatory
Risk Sub-domain	Applicable sub-domain for which risk needs to be addressed
Risk	Risks within each pair of domains and sub-domains
Control Requirement	Required objective to be met by the applicable Acquirer archetype(s) for addressing the risk.
Context	Additional background on the control.
Implementation Guidance	Outlines Mandatory Controls that are required to be implemented by the Acquirer. Additional Recommended Controls are included as best practices.

© 2024 Visa. All rights reserved. Visa Public

Appendix I: VIRP

The VIRP ensures that Acquirers, and their designated TPAs, maintain proper controls and oversight processes to deter illegal transactions from entering the Visa Payment System. Access the VIRP through Visa Access.

Appendix J: Successful Key Performance Indicators (KPI)

VISA ECOSYSTEM RISK PROGRAM NAME	KPI
VIRP	No VIRP identification, or confirm TLD cases for illegal or miscoded activity,
VAMP	Acquirers maintain the Program threshold below 30bps, and their Merchants doesn't exceed 150bps
Enumeration	Acquirers enumerated authorization attempts is below 2000bps.
Account Information Security	PCI DSS Compliance

© 2024 Visa. All rights reserved. Visa Public

Appendix H: Assess Business Activity

VISA ECOSYSTEM RISK PROGRAM NAME	URL/WEBSITE REVIEW
Detect Templated/ Counterfeit	1. Check the URL closely for spelling mistakes 2. Inspect the site's security certificate, and also the subdomains 3. Consider how you found the website in the first place 4. Use Safe Browsing tools or a website checker 5. Look for spelling, grammar, and formatting issues 6. Be wary of poor-quality design or photos – copied, with no detailed description. 7. Check the domain age and ownership – reputable entities are usually around for years and so it is website is also long standing and not few months old. 8. Search for user reviews and potential scams. You can use the scam tracker database using one or many available under the "Lookup Scam By). 9. Check the "About," "Shipping," and "Privacy Policy" pages as in most cases it lacks the details to explain the terms and conditions. 10. 1Research the company's social media and online presence sharing more details on public available forums 11. Look for payment red flags – example use of unusual payment methods such as gift cards or cryptocurrency, prices are too good to be true when compared to industry average price mark.
Prevent URL Re-direct	1. Create a whitelist with all the URLs that are approved as part of the detailed website review. 2. Link the payment processing to the whitelist approval URLs/Websites 3. Decline any payment process where the URLs are not in your approved list

© 2024 Visa. All rights reserved. Visa Public