Payment Facilitator and Marketplace Risk Guide

How to Identify and Manage Risk in Today's Payment Ecosystem

April 2021
Visa Public

Table of Contents

1. About This Guide

In today's world where payments and technology have merged, many financial technology companies—known as Fintechs—have entered the payments industry as payment facilitators or marketplaces. As third party agents, they play a unique role with respect to enabling commerce between buyers and sellers. However, being a payment service provider presents inherent risk. It is therefore critical that payment facilitators and marketplaces are equipped with the expertise and capabilities to appropriately address and mitigate such risk. Payment facilitators and marketplaces must manage these risks on behalf of themselves, their acquirers, and the payment ecosystem.

Visa developed this guide with the intention of having acquirers share it with the payment facilitators and marketplaces they sponsor.

Visa developed this guide with the intent to have acquirers share it with the payment facilitators and marketplaces they sponsor. Payment facilitators and marketplaces should be familiar with the information provided in this guide and use it to aid in the deployment and operation of a sound and adequate risk control environment. The guide contains risk management information aimed to assist those new to the payment system as well as seasoned organizations. Content of this guide applies to traditional "pull" payments, when a merchant accepts Visa for payment, as well as "push" payments (e.g., Visa Direct) where cardholders or merchants use Visa payment credentials to send money to recipients, which may include other Visa, bank account, or non-Visa payment credentials.

PURPOSE OF THE PAYMENT FACILITATOR AND MARKETPLACE RISK GUIDE

To assist acquirers, payment facilitators, and marketplaces with their risk management obligations, Visa has developed the ***Payment Facilitator and Marketplace Risk Guide*** to serve the following purposes:

- ✔ Provide acquirers with a reference to address the various risks associated with the sponsorship of payment facilitators and marketplaces.
- ✔ Educate payment facilitators and marketplaces on common payment ecosystem risks and provide information about how to mitigate those risks.
- ✔ Aid acquirers in assessing the risk management capabilities of their sponsored payment facilitators and marketplaces.
- ✔ Provide additional details on Visa's risk management expectations for payment facilitators, marketplaces, and the acquirers that sponsor them.

2. Payment Facilitator and Marketplace Basics

A fundamental facet of managing risk, as it relates to payment facilitators and marketplaces, is that one must understand each entity's distinctive role in the payment ecosystem.

2.1 Definitions and Roles

The Acquirer

An acquirer is a Visa client operating under a Visa-approved license agreement, permitting it to contract with merchants for the provision of Visa payment acceptance. The acquirer's primary role with respect to payment facilitators and marketplaces is to maintain complete oversight over those it sponsors. An acquirer must continuously monitor payment facilitators and marketplaces to ensure compliance with the *Visa Core Rules and Visa Product and Service Rules* ("Visa Rules"), the *Visa Global Acquirer Risk Standards* (GARS), the acquirer's own policies, and applicable laws. Additionally, the acquirer must constantly affirm that payment facilitators and marketplaces—as well as their underlying sponsored merchants and retailers—do not pose an undue risk to the integrity of the Visa payment system.

Visa designates payment facilitators and marketplaces as third-party agents, which require sponsorship and registration by an acquirer.

Third Party Agents

Third party agents (a.k.a. TPAs or agents) are entities—generally not directly connected to VisaNet—that contract with Visa clients to solicit or provide payment related services on behalf of those Visa clients. This is inclusive of organizations that store, process, or transmit Visa transaction data on behalf of Visa clients and/or merchants. Visa designates payment facilitators and marketplaces as third party agents, which require sponsorship and registration by an acquirer. An acquirer's responsibilities and accountabilities remain the same whether merchants are signed directly or through third party agents.

Payment Facilitators and Sponsored Merchants

Also known as a "PayFac" or merchant aggregator, a payment facilitator is a third party agent that contracts with an acquirer to

THE ACQUIRER
A Visa Client licensed to provide card acceptance services.

THIRD PARTY AGENT
An entity that provides payment related services on behalf of a Visa Client.

PAYMENT FACILITATOR
A type of agent that provides payment acceptance services on behalf of an acquirer.

MARKETPLACE
A type of agent that brings together buyers and retailers on a common platform.

provide payment services and solutions on its behalf. In certain cases, a Visa client can also act as a payment facilitator. In turn, payment facilitators enter into payment services contracts (a.k.a. merchant agreements) with sponsored merchants in order to provide payment services.

As the acquirer is not a direct party to such payment services contracts (with certain exceptions), merchants solely contracted by payment facilitators are designated as "sponsored merchants."

An acquirer will deposit settlement funds directly to the payment facilitator. The payment facilitator subsequently settles those funds to its sponsored merchants.

IMPORTANT:
Visa treats a payment facilitator's sponsored merchant as a merchant of the payment facilitator's acquirer.

Marketplaces

A marketplace is a third party agent that brings together buyers and retailers via a single marketplace-branded platform—i.e., an electronic commerce website and/or mobile application. Therefore, marketplaces exclusively process card-absent transactions and are not permitted to operate in a card-present environment.

Marketplaces process payments and receive settlement proceeds on behalf of retailers; entities that do not process transactions on behalf of retailers are not considered marketplaces. In this context, it is the marketplace that contracts with the acquirer for payment acceptance and is treated as "the merchant of record"—not the underlying retailers. The marketplace also manages the primary customer experience, accepting the payment on behalf of the retailer and issuing a transaction receipt in the name of the

marketplace, even if the customer is buying from multiple retailers in a single transaction. The marketplace also administers refunds and disputes between the buyer and retailer.

Marketplaces may operate with retailers in a single line of business (e.g., food delivery or ride-share services). In such instances, it must be assigned the Merchant Category Code (MCC) that best describes the majority of its business. However, because marketplaces can also accept Visa payments on behalf of a variety of retailers offering diverse goods and services, they can be assigned a unique Merchant Category Code—MCC 5262 (Marketplaces)—which covers all lines of business that are not otherwise classifiable under a single MCC, akin to a department store.

An acquirer may only contract with a payment facilitator or marketplace it has screened for risk exposure.

2.2 Acquirer Responsibility

Acquirers fulfill a vital role in maintaining the integrity of the Visa payment system by ensuring their merchants and third party agents comply with the Visa Rules and applicable laws. They play an important gatekeeping role by preventing bad elements from entering the payment system. These elements include entities that operate in violation of applicable laws and regulations, as well as those engaged in fraud, deceptive sales and marketing practices, or other violations of the Visa Rules. Such illicit activities may expose an acquirer, payment facilitator, or marketplace to compliance action, financial loss, reputation damage, or potential disqualification from the Visa payment system.

IMPORTANT:
An acquirer that contracts with a payment facilitator or marketplace is responsible for all acts, omissions, and other adverse conditions caused by the payment facilitator and its sponsored merchants or the marketplace and its retailers.

An acquirer may only contract with a payment facilitator or marketplace it has screened for risk exposure. Acquirers must ensure the payment facilitators and marketplaces they sponsor—and their underlying sponsored merchants and retailers—employ safe and sound risk management practices. An acquirer must maintain ongoing oversight to protect the Visa payment system from undue risk.

IMPORTANT:
This guide may collectively refer to merchants, sponsored merchants and retailers as "sellers."

3. Payment Ecosystem Risk

The categories of risk outlined in this chapter generally apply to any participant in the payment ecosystem. It is critical to understand each category as many of the threats and risks faced by payment facilitators and marketplaces—described in Section 4 of this guide—fall under one or more of these categories.

3.1 Operational Risk

An acquirer must monitor and periodically review or audit payment facilitators and marketplaces for risk exposure.

Operational risk generally refers to the threat of loss, litigation, compliance/regulatory action, or reputation damage resulting from inadequate or failed internal business processes, personnel, or systems. This pertains to payment service providers in the sense that such entities must have the proper business processes, controls, and systems in place combined with capable personnel.

Payment facilitators and marketplaces must therefore ensure they have competent risk management personnel, effective systems, and reporting in place before engaging in payment operations. Examples of key business processes and controls pertinent to mitigating operational risk are merchant underwriting and risk monitoring, as outlined in Sections 7 and 8 of this guide. An acquirer must monitor and periodically review or audit payment facilitators and marketplaces for operational risk exposure. Such reviews or audits must include affirmation of compliance with the Visa Rules, the *Visa Global Acquirer Risk Standards* (GARS), and the acquirer's own policy.

3.2 Regulatory and Compliance Risk

Various authorities play a role in the regulation of the payments industry. These authorities include banking and finance regulators, consumer protection agencies, and the payment networks themselves. It is essential that companies operating in the payments industry comply with applicable laws and regulations and cooperate with the appropriate authorities.

Banking regulators (such as central banks and related government agencies) are generally concerned with the safety and soundness of the banking system—which includes the payments industry. In addition, there are numerous laws that directly apply to the financial services sector and payments industry. Examples of laws common in most jurisdictions include Anti-Money Laundering (AML) and Know-Your-Customer (KYC) laws. Laws also dictate what constitutes legal or illegal activity, and identify goods and services that are unlawful to sell or purchase in a given jurisdiction. Consumer protection agencies play a role in protecting customers—generally cardholders—from questionable merchants. The payment system is also governed by its own standards, such as the *Payment Card Industry Data Security Standard* (PCI DSS). In addition, Visa governs its payment system, and holds participants accountable through the enforcement of its membership agreement, Bylaws, the Visa Rules and other applicable documents.

3.3 Credit Settlement Risk

Credit settlement risk is a type of financial risk inherent to merchant acquiring. Acquirers are obligated to pay the settlement obligations of their merchants and third party agents on a timely basis. For example, if a merchant or third party agent is unable to honor disputes resulting from previously submitted sales drafts due to a lack of funds, the acquirer must continue to honor all financial settlement obligations when due. In turn, acquirers require payment facilitators and marketplaces to honor the settlement obligations of their sellers. As such, it is critical that acquirers, payment facilitators, and marketplaces possess proper controls to mitigate financial losses.

3.4 Brand & Reputation Risk

The beliefs or opinions held about a brand can have an impact on the ability of a company to attract or retain customers and partners. Trust in the secure processing of payments by participants in the Visa network can benefit the entire payment ecosystem and help drive commerce. Similarly, risks introduced into the ecosystem can erode trust and extend beyond payments and impact brand and reputation. Visa and Visa payment system participants must safeguard against risks that may negatively affect their brand or reputation. This includes facilitating payments for entities involved in illegal activity or deceptive marketing practices.

Visa and Visa payment system participants must safeguard against risks that may negatively affect their brand or reputation.

4. Risks Pertaining to Payment Facilitators and Marketplaces

Acquirers, payment facilitators and marketplaces should educate themselves on an ongoing basis about the evolving risks they may face. Knowing the latest trends and keeping ones control environment up-to-date are effective practices in mitigating such risks.

4.1 Third Party Agent Risk

If mismanaged, third party agents could pose a substantial risk to their sponsoring acquirers, to themselves and the payment system in general.

A lack of agent oversight can potentially prove catastrophic for acquirers.

A lack of agent oversight can potentially prove catastrophic for acquirers, resulting in financial losses, brand damage, regulatory intervention or in extreme cases, the revocation of their Visa license. Some of the common situations that can place an acquirer at risk from third party agents include:

- Non-Compliance with the *Visa Global Acquirer Risk Standards*
- Questionable Agents

Non-Compliance with *Visa Global Acquirer Risk Standards*

The GARS provide minimum requirements for acquirers to mitigate payment acceptance risk. The standards include a requirement that acquirers enact proper oversight of their agents. Acquirers may delegate authority to payment facilitators and marketplaces to enable sellers with payment acceptance privileges. It is therefore crucial that the acquirer and its agents have mechanisms in place to ensure that merchant onboarding processes comply with the GARS, the Visa Rules, and the acquirer's own policy. In addition, acquirers, payment facilitators, and marketplaces have a duty to monitor their sellers for ongoing compliance and suspect activity. Acquirers may share the GARS with their payment facilitators and marketplaces, and periodically assess them for compliance.

IMPORTANT:
The Global Acquirer Risk Standards (GARS) are an extension of the Visa Rules.

Questionable Agents

While third party agents fulfill a valuable role in the payment system, there have been occurrences where certain agents engaged in questionable business practices. Such agents may leverage the payment system primarily for their own gains by allowing illicit sellers and even criminals to process payments. This may be a profitable venture for the agent, but it represents a severe risk to the acquirer and the Visa payment system. On the surface, questionable agents may appear legitimate. Often such agents go to significant lengths to hide their own bad conduct as well as the illicit transaction activity of their sellers. Since the acquirer is responsible for the conduct of its sponsored payment facilitators and marketplaces, it is essential that an acquirer is vigilant in detecting and terminating questionable agents. To mitigate this risk, acquirers are required to perform proper due diligence and ongoing monitoring of their agents—including payment facilitators and marketplaces—as outlined in the GARS.

4.2 Merchant Risk

Merchant (or seller) risk refers to the potential for financial losses, regulator/compliance enforcement, litigation, law enforcement action, or reputation/brand damage due to the actions or inactions of a seller.

Payment facilitators and marketplaces generally manage and control the underwriting and onboarding of sellers—the process where merchant risk is initially assessed. Prospective sellers must be onboarded in compliance with the Visa Rules, the GARS, and the acquirer's own underwriting policy. In addition, payment facilitators and marketplaces must monitor their sellers for ongoing compliance as well as any indications of increased risk and take immediate action if warranted. Specific risks involving sellers include:

- Questionable or Unsound Business Practices
- High-Brand Risk Merchants
- Sellers Involved in Fraud or Illicit Activity

Questionable or Unsound Business Practices

Unfortunately not all businesses act in a principled or ethical manner. Some sellers may conduct customer billing practices in a negligent or deceptive manner—e.g., billing customers without their proper consent or making it difficult to cancel recurring payments. Sellers with negligent or deceptive business practices harm consumers and negatively affect the payment system.

A common example is the use of deceptive marketing practices—for example, sellers making unreasonable guarantees or false claims concerning the results, capabilities, actual cost or billing terms of a product or service. Sellers that employ free trials must comply with the applicable Visa Rules requiring proper disclosure of terms, explicit cardholder consent, and a simple way for customers to opt out or cancel. Sellers that mismanage free trials or discounted/promotional subscription offers will often face elevated disputes from their customers. It is important that payment facilitators and marketplaces only sign prospective sellers after validating that they conduct business in an ethical and sound manner. Adequate ongoing monitoring for excessive disputes and consumer complaints must be in place to protect the acquirer, cardholders, and the Visa payment system from undue harm.

High-Brand Risk Merchants

Visa has classified a set of merchant types as "high-brand risk" when accepting card-absent payments, as these businesses present an elevated risk to the payment system—specifically due to higher levels of disputes or brand/reputation risk. These merchant types are also typically highly regulated with some deemed illegal in certain jurisdictions.

IMPORTANT:
Acquirers must obtain a High-Brand Risk Acquirer Registration from Visa prior to contracting with a high-brand risk merchant. A payment facilitator must be registered as a High Risk Internet Payment Facilitator (HRIPF) with Visa before signing high-brand risk merchants.

Visa defines a high-brand risk merchant as a merchant outlet accepting or sending card-absent (and in some cases specifically

cross-border) payments, required to be classified with one of the following Merchant Category Codes (MCC):

MCC	DESCRIPTION
5122	Drugs, Drug Proprietaries, Druggist Sundries
5912	Drug Stores and Pharmacies
5962	Direct Marketing – Travel-Related Arrangement Services
5966	Direct Marketing – Outbound Telemarketing Merchant
5967	Direct Marketing – Inbound Teleservices Merchant (Digital Adult Content)
5993	Cigar Stores and Stands
7273	Dating Services
7995	Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks

Acquirers are required to implement adequate controls to ensure merchants do not process illegal payments.

In the cases below, Visa designates particular activities to be high-brand risk, as opposed to classifying the entire MCC they operate in as high-brand risk:

ACTIVITIES DESIGNATED AS HIGH BRAND RISK
MCC 4816: Computer Network / Information Services Cyberlockers and similar remote digital file-sharing services where uploaded content is accessible to the public or the service pays uploaders for content.
MCC 5816: Digital Goods—Games Games of skill such as daily fantasy sports gaming where consumers pay a fee to enter and the outcomes of the game is determined by skill instead of luck.
MCC 6051: Non-Financial Institutions Purchase of cryptocurrency, funding of crypto wallets or funding of initial coin offerings (ICO).

As Visa makes periodic updates to its high-brand risk merchant classifications—please consult the Visa Rules for the most up-to-date information.

IMPORTANT:
Payment facilitators are prohibited from signing sponsored merchants belonging to certain high-brand risk MCCs—consult the Visa Rules for details. Marketplaces are prohibited from soliciting high-brand risk merchants.

Visa operates the Global Brand Protection Program, a compliance program that monitors the Visa payment system for illegal activity or merchants with miscoded MCCs. The *Visa Global Brand Protection Program (GBPP) Guide* is an extension of the Visa Rules and requires acquirers to implement adequate controls to ensure merchants do not process payments that are illegal and/or may adversely affect the reputation of Visa or its affiliates. In addition, it outlines what acquirers and their agents must do to effectively control the elevated risk associated with high-brand risk merchants.

Acquirers and High-Risk Internet Payment Facilitators (HRIPF) approved to sign high-brand risk merchants must be familiar and comply with content of the GBPP guide. Compliance violations associated with the GBPP may result in non-compliance assessments.

Sellers Involved in Fraud or Illicit Activity

Criminals often intend to access the payment system as sellers to conduct fraud or other illicit activity as mentioned in this section. It also occasionally occurs that a legitimately signed seller resorts to fraud or illicit activity, typically for financial gain. Such sellers may engage in various schemes that cause harm to the payment system; these include processing of illegal transactions, transaction laundering, or the resale of cardholder account information. These and other fraud schemes are further described in Section 4.6 of this guide.

The payment facilitator, marketplace, or acquirer must terminate sellers engaged in activity harmful to the payment system or in willful violation of the Visa Rules. Sponsored merchants terminated for such activity must be added to the Visa Merchant Screening Service[1] (VMSS) in accordance with the Visa Rules.

4.3 Illegal Activity

Sellers involved in illegal activity pose a severe risk to the payment ecosystem.

Sellers involved in illegal activity pose a severe risk to an acquirer, payment facilitator, marketplace, and the payment ecosystem in general. Sometimes the risk is not immediately evident, as criminals often deploy elaborate schemes to conceal their activities. Payment facilitators and marketplaces must assume an active role in protecting the payment system from the threat of illegal activity. Visa upholds the integrity of its payment system by detecting illegal activity violations through the Global Brand Protection Program (GBPP).

IMPORTANT:
A payment facilitator or marketplace must not accept any transaction from a seller—for submission into the Visa payment system—that is illegal.

Visa prohibits any type of activity in violation of applicable law from entering the Visa payment system. Because laws can vary by jurisdiction, certain goods or services—and associated transactions—may be legal in one region but could be illegal in another. It is essential that payment facilitators and marketplaces ensure that their sellers only submit transactions that are legal in the jurisdiction of both the buyer (cardholder) and the seller (sponsored merchant or retailer). The following are examples of commonly identified illegal activity:

- Unlawful Sale of Prescription Drugs
- Intellectual Property (IP) Violations
- Illegal or Miscoded Gambling
- Online Sale of Tobacco Products
- Rogue Cyberlocker Merchants
- Prohibited Adult Content

Unlawful Sale of Prescription Drugs

Illegitimate pharmaceutical merchants may attempt to dispense medications online without a prescription, often in violation of the law in the consumer's jurisdiction. In some cases, these transactions involve prescription-only controlled substances; medications that have an accepted medical use but possess a high potential for abuse. If dispensed to individuals without a medical prescription, these controlled substances could represent a substantial health risk to those who consume them. Illegal online pharmacies often circumvent applicable licensing requirements and sell medications (including counterfeit or adulterated substances) in violation of health and safety laws in the jurisdiction where they operate. Such illicit pharmacy merchants transgress a multitude of laws and regulations in many jurisdictions. Facilitating transactions on behalf of illegal pharmacies—in any capacity—could expose those participating to reputation/brand risk, civil litigation, criminal prosecution, and financial risk and may contribute to the serious injury or death of an individual.

Payments involving the sale of illegal narcotics, recreational drugs, or chemical analogs of controlled substances (a.k.a. designer drugs) are strictly prohibited from entering the Visa payment system.

[1] *Where required and available, or use a comparable Terminated Merchant File.*

Intellectual Property (IP) Violations

With the advent of ecommerce, the sale of counterfeit or IP-infringing products has expanded globally, presenting increased litigation and regulatory risk to acquirers and their agents. Counterfeit goods span across various industries including but not limited to media, apparel, accessories, electronics, pharmaceuticals, and medical devices. Copyright, patent, and trademark laws regulate and prohibit the sale or distribution of counterfeit products or licensed material without the appropriate authorization from the rights holder.

IMPORTANT:
Payment facilitators and marketplaces must have processes in place to effectively address and respond to rights-holder complaints stemming from sellers marketing counterfeit or IP-infringing goods.

Illegal or Miscoded Gambling

Gambling is a regulated industry in many jurisdictions, especially when conducted online. Moreover, while online gambling is legal in a variety of regions, many other markets prohibit it. To help card issuers comply with applicable laws, acquirers and agents are required to ensure gambling transactions are identified with the correct Merchant Category Codes (MCC) and Point-of-Sale Condition Codes. The intentional miscoding of online gambling transactions can be lucrative for agents that seek to facilitate entry of illegal merchants and transactions into the payment system. Entities that miscode MCCs of gambling merchants are in violation of the Visa Rules and subject to non-compliance assessments or other enforcement action. Mobile and/or digital wallets, where the end use of funds is intended for illegal gambling, also fall under this category.

Online Sale of Tobacco Products

Cigarettes and loose tobacco are regulated globally and often subject to taxes by local government authorities. Given this, certain card-absent merchants have established illicit business models that seek to circumvent or evade government taxes by selling tax-free cigarettes into markets with licensing or tax-stamp requirements. Acquirers or agents that sign merchants who sell cigarettes and other tobacco products must take steps to ensure compliance with laws in the jurisdictions of both buyer and seller. Acquirers and agents with merchants that ship to or within the United States are specifically required to ensure their merchants comply with individual state and federal law.

Rogue Cyberlocker Merchants

As online file sharing services or cyberlockers continue to evolve, illegal merchants have emerged using cyberlockers as a means to distribute copyright-protected digital content (e.g., pirated movies, music and software shared without rights-holder authorization or proper licensing). In extreme cases, such content may include prohibited adult content (e.g., Child Sex Abuse Material (CSAM), child exploitation, bestiality, rape, or violent imagery). Rogue cyberlocker merchants often use elaborate business models to conceal their illicit activities. Hence, when onboarding cyberlocker merchants, they require careful review to ensure such services are only used for legitimate purposes. Additionally, cyberlockers require continued monitoring while processing payments.

Prohibited Adult Content

In addition to complying with prohibitions in the buyer and seller's jurisdiction, Visa prohibits the purchase or trade of certain photographs, video imagery, computer-generated images, cartoons, simulation or any other media or activities. This includes but is not limited to CSAM, bestiality, rape (or any other non-consensual sexual conduct), or non-consensual mutilation of a person or body part.

IMPORTANT:
For more information on prohibited or illegal activity, please consult the *Visa Global Brand Protection Program Guide*.

4.4 Transaction Laundering

Also known as "factoring," transaction laundering occurs when an illicit business surreptitiously uses payment services through a front-organization posing as a legitimate merchant. By hiding the nature of payment activity, transaction laundering allows illegitimate businesses to accept payments for illicit goods or services. Additionally, it gives the sellers of illicit goods and services a way to launder "dirty" money by clandestinely entering their sales receipts into the payment system.

Spurred by the growth of ecommerce and the anonymity afforded by the internet, the use of transaction laundering is surging worldwide. Illicit businesses commonly use transaction laundering to accept payments clandestinely related to illegal gambling, illegitimate online pharmacies, illegal drugs, and counterfeit merchandise. In order to uphold the integrity of the payment system, Visa employs monitoring and controls to interdict transaction laundering by holding acquirers, payment facilitators and marketplaces accountable for the illicit actions of the sellers they onboard.

IMPORTANT:
Merchant agreements used to contract sellers must explicitly prohibit all transactions that did not result from an act between a cardholder and a seller.

Payment facilitators and marketplaces must possess controls to detect and block transaction laundering activity.

Payment facilitators and marketplaces must possess controls to detect and block transaction laundering activity. This is primarily achieved through robust underwriting and the ongoing monitoring for sellers exhibiting transaction laundering characteristics. In addition, many acquirers and agents contract with third parties known as Merchant Monitoring Service Providers (MMSPs), which use algorithms and machine-learning technology to detect suspect merchants and activity.

4.5 Financial Loss Exposure

Payment facilitators and marketplaces assume a level of financial risk when enabling sponsored merchants and retailers to accept payments. In essence, they provide an unsecured line of credit to their sellers. Sellers often receive the settlement proceeds from their transactions in advance of the customer receiving their goods or services. This is in accordance with the understanding and agreement that the seller will deliver the goods or services for which it received settlement funds.

Should there be a problem with customers not receiving their goods or services, or with the goods or services themselves after delivery, it may result in a seller having to credit the funds back to the cardholder. In such cases, the seller generally processes a refund; in other events, the seller must return the funds if a cardholder files a dispute. In the event of fraud transactions, the seller is obligated to credit the funds back to the legitimate cardholder, often facilitated by means of a fraud dispute. A customer has the ability to dispute a payment for up to 120 days after the original purchase date in most cases, and in some up to 540 days. Payment facilitators and marketplaces should factor this in when assessing financial risk of prospective and existing sellers. Sellers that accept payments well in advance of delivering their goods or services—for travel, event ticket sales, or annual memberships for example—should be closely evaluated for financial risk exposure. If such a seller is unable to deliver, all goods or services paid for in advance and not received by cardholders as agreed may be subject to consumer disputes.

The inability of a seller to pay the cardholder back—e.g., due to a lack of funds or no longer being in business—will obligate the payment facilitator or marketplace to fund disputes and other settlement obligations on behalf of the seller. This scenario would potentially expose a payment facilitator or marketplace to losses.

IMPORTANT:
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. The acts and omissions of a retailer will be treated as those of the marketplace, and the acquirer is fully liable for any losses to Visa, its clients, or other stakeholders caused by a marketplace or its retailers.

4.6 Fraud Schemes

The payment ecosystem has faced fraud threats since its inception. However, the evolving scope and sophistication of fraud schemes could have significant consequences for acquirers and agents unprepared to prevent or mitigate them.

Criminals tend to seek out and target businesses with inadequate fraud prevention controls. The resulting fraud events have the capacity to expose acquirers, agents, and sellers to financial losses, regulatory inquiries, and damaged reputations. This section will cover common present-day threats to the payment ecosystem. However, it is critical that payment facilitators, marketplaces, and their sellers continuously remain educated on the ever-evolving fraud landscape and prevention practices.

Fraudulent Merchant Applications

Criminals posing as legitimate businesses will attempt to apply for payment services with the intent to commit fraud once granted access to the payment system. They will often use synthetic or stolen identities, obtained through data breaches or social engineering.

Businesses that cannot gain approval to sell certain types of high-risk goods or services, or who may have been previously declined or terminated, may attempt to obtain payment services by misrepresenting the information on their merchant applications. A prominent factor compounding the risk of onboarding fraudulent merchants is the widespread adoption of automated onboarding or "auto-boarding" by payment facilitators and marketplaces. Auto-boarding, if not properly managed and controlled, could increase the risk of approving fraudulent merchant applications.

MITIGATION TIPS:

- ✔ Adopt the Auto-Boarding Best Practices as outlined in the *Visa Global Acquirer Risk Standards* (GARS).
- ✔ Use proper tools to detect and decline fraudulent merchant applications in underwriting, such as: third party validation, negative databases, device fingerprinting, and geolocation checks (e.g., matching the IP address location used to fill out the application to the merchant's physical address).
- ✔ Use velocity checks to detect sudden surges in new applications or applications with similar characteristics.

Enumeration or Account Testing Schemes

Enumeration or account testing are schemes where criminals leverage bots and other technology to obtain or validate payment card information. By illicitly obtaining access to payment services, criminals systematically submit low-amount authorization attempts (test transactions) while iterating through various combinations of card values. Issuers decline the authorization attempts until the right combination of card values returns an approval response. An approved authorization response is indicative that the criminal has obtained a combination of card values—such as Primary Identification Number (PAN), expiration date, postal code, and Card Verification Value 2 (CVV2)—to derive valid payment card information. Fraudsters subsequently sell the valid payment card information (often on the dark web) or use the information to make fraudulent purchases.

A common trait of enumeration or card testing are high-velocity authorization attempts. Sometimes criminals deploy a "low-and-slow" approach by using low-velocity repeated authorization attempts. Authorizations regularly contain PANs with the same Bank Identification Number (BIN) or have identical PANs with various expiration dates, postal codes, or CVV2 values.

As previously stated, criminals must gain access to payment services in order to perpetrate this scheme, typically achieved by using a legitimate seller's payments webpage, Account Take-Overs (ATOs), or fraudulent applications. Therefore, the primary method effective in mitigating these schemes is to prevent criminals from gaining access to payment services. The secondary method is the rapid detection and blocking of suspect activity.

MITIGATION TIPS:

- ✔ Employ proper controls to detect fraudulent merchant applications, account take-overs, or other methods criminals use to gain illicit access to the payment system.
- ✔ Payment facilitators and marketplaces must monitor for transaction activity and velocity with enumeration characteristics and act rapidly to block it (see Section 8.2).
- ✔ Sellers must use controls such as CAPTCHA[2] and velocity-checks to prevent criminals from using their payment webpages for enumeration attacks.

[2] *A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a tool used on a website to differentiate between human users and automated or computerized users, such as bots.*

Force-Post Fraud

Force-post and purchase return activity should be closely monitored.

A force-posted (a.k.a. offline) transaction allows a merchant to bypass the online authorization process by manually entering an authorization code received through a previous authorization. Because forced transactions are directly routed into clearing without an authorization attempt at the time they are submitted, the issuer has no means to decline or reject them—hence they are "force-posted." By using this method to circumvent the authorization process, fraudsters initiate sales or purchase returns with counterfeit, stolen, or even fictitious card information. Attacks involving force-posted transactions often comprise large transaction amounts and if unmitigated can expose payment facilitators, marketplaces, and sellers to significant losses.

As a legacy function of the payment system, the legitimate-use cases for submitting forced transactions have greatly diminished. However, many point-of-sale (POS) devices and payment gateways may still support this functionality. The failure to control the use of force-posted transactions can expose payment facilitators, marketplaces, and sellers to undue risk.

MITIGATION TIPS:

- ✔ Tightly control the enabling of sellers with force-post functionality.
- ✔ Only grant force-post functionality to sellers if they have a legitimate use case.
- ✔ Closely monitor for suspect force-post activity and block it from clearing when detected.

Purchase Return Fraud and Purchase Return Authorizations

A seller submits a purchase return (a.k.a. credit voucher) transaction to refund a customer for a previous sale. In this scenario, funds flow from a seller back to a customer's payment account. When committing purchase return fraud, criminals gain access to payment services—commonly through Account Take-Overs (ATOs), fraudulent applications, or merchant cloning (covered later in this section). Once having gained access to the payment system, fraudsters submit purchase returns, typically to debit or prepaid cards under their control. When the funds are posted to the cards, the illicit proceeds are quickly cashed out at bank branches or ATMs. In other cases, fraudsters will use the ill-gained funds to buy merchandise.

Because purchase returns also require authorizations (similar to sales drafts), it is essential for payment facilitators and marketplaces to monitor Purchase Return Authorization (PRA) velocity and act to block excessive authorizations and the clearing of fraudulent purchase returns. It is important to understand the nature of PRAs and that an approval from an issuer does not necessarily mean that the transaction is without risk. A PRA approval simply means that the issuer has the payment account on file and is ready to receive funds. PRAs may not be subject to the same fraud and risk controls as sales draft authorizations. Even when approved by an issuer, the payment facilitator or marketplace submitting the subsequent purchase returns is liable for any fraud.

MITIGATION TIPS:

- ✔ Closely monitor for unusual PRA and purchase return activity (e.g., transaction amounts and counts), specifically to prepaid or debit cards.
- ✔ Based on monitoring results, block suspect purchase returns from clearing.
- ✔ Monitor for purchase returns without offsetting sales.

Merchant Bust-Out Schemes

A merchant bust-out scheme is a tactic that typically involves a relatively new seller that processes normal payment volumes for some time to build up a good reputation. Once having established a satisfactory payment processing history, the seller will suddenly submit a large number of fraudulent transactions—typically using stolen card data. Such bust-out sellers will then quickly disappear after they have been funded the proceeds of the fraudulent transactions. In some cases, a fraudster will set up payment services to sell goods or services it never intends to fulfill. Once having accumulated a certain amount of sales proceeds, they will quickly disappear with the funds before customers start inquiring about their missing goods or services.

MITIGATION TIPS:

- ✔ Use proper risk monitoring as covered in Section 8 of this guide—specifically use velocity checks to monitor newly onboarded sellers.
- ✔ Upon detection of suspect activity, suspend a seller's settlement funding until properly investigated.
- ✔ Consider suspending payment services when a bust-out scheme is suspected.
- ✔ Act timely on sellers generating excessive fraud advices and/or disputes.

4.7 Account Take-Overs and Merchant Cloning

As previously stated, many fraud schemes require criminals to gain access to payment services in order to submit fraudulent transactions. It is therefore vital that payment facilitators, marketplaces, and their underlying sellers, make it a priority to block any unauthorized access to their payment services and the payment system in general. That said, one should not underestimate the resourcefulness and persistence of criminals to circumvent security measures preventing unauthorized access to the payment system. While there are various ways for criminals to gain access—such as fraudulent merchant applications covered previously—other prominent methods include:

- Account Take-Overs
- Merchant Cloning

Account Take-Overs

Fraudsters will attempt to obtain credentials to access a payment account a seller has established with their payment facilitator or marketplace. Once accessed, fraudsters will take over the payment account to submit fraudulent transactions. Common methods used by criminals to steal a seller's credentials are phishing attacks or social engineering. In some cases fraudsters have gathered sufficient information through social engineering to dial into a payment facilitator's or marketplace's customer service center to have a seller's password reset and gain access.

MITIGATION TIPS:

- ✔ Educate sellers about phishing schemes and the importance of keeping their credentials secure.
- ✔ Payment facilitator and marketplace call centers must use appropriate Identification and Validation (ID&V) controls to authenticate callers as legitimate customers.
- ✔ Facilitate periodic password resets for sellers.

A data breach due to lapses in security is often avoidable.

Merchant Cloning

Another method employed by criminals to gain access to the payment system is cloning POS acceptance devices and payment gateways (a.k.a. spoofing). Fraudsters will program a POS acceptance device or payment gateway they control to make it appear like it belongs to a legitimate seller. In order to program a POS acceptance device or payment gateway with sufficient information to function, fraudsters will obtain various data elements from an unsuspecting seller. These data elements commonly include the seller's Merchant Identification Number (MID) and Terminal Identification Number (TID). Criminals use these values to derive processor host information—the processor's network computer to which devices connect. Once connected to the host, fraudsters will submit fraudulent transactions.

Criminals will obtain merchant data elements for cloning through various means. Common methods involve their obtaining MIDs and TIDs from transaction receipts, or probing processor hosts for live MID and TID combinations through enumeration.

MITIGATION TIPS:

- ✔ Do not print a seller's MID and/or TID on transaction receipts.
- ✔ If acting as a payment processor (a.k.a. VisaNet end-point), deploy proper security protocols to authenticate and limit host connectivity to POS acceptance devices and gateways belonging to legitimate sellers.
- ✔ Utilize unique cryptographic transaction keys and/or Point-To-Point Encryption (P2PE) for all host connectivity.

4.8 Data Breaches

At its core, the payment system runs on information. Organizations participating in the payment system receive, store, and/or transmit sensitive data that must remain secure. A data breach at a payment facilitator, marketplace, or its underlying sellers due to lapses in security is often both devastating and avoidable. Such data breaches consequentially lead to fraud and other crimes, potentially affecting other institutions and countless consumers.

Most payment facilitators and marketplaces operate their own technology platforms that store and transmit sensitive payment data. Hence, acquirers must ensure their sponsored agents comply with the Payment Card Industry Data Security Standard (PCI DSS) and any other applicable security requirements or standards.

5. Conditions, Restrictions, and Prerequisites

Payment facilitators and marketplaces must contract with a qualified and approved acquirer in order to provide payment services. Visa stipulates that certain conditions, restrictions, and prerequisites apply in order for an acquirer to sponsor and contract with a prospective payment facilitator or marketplace. Acquirers should also consult the Visa Rules for more detailed information pertaining to these conditions, restrictions, and prerequisites.

5.1 Contracting with Payment Facilitators and Marketplaces

Before an acquirer can contract with a payment facilitator or marketplace, it must meet the following conditions:

- It is financially sound (as determined by Visa).
- It operates in compliance with the Visa Rules, including all aspects of the Global Acquirer Risk Standards (GARS).
- It is in good standing in all Visa risk-compliance programs (see Section 8.6).

5.2 Capital Requirements for Acquirers

In order to sponsor a payment facilitator or marketplace, an acquirer must meet minimum Tier 1 capital requirements as outlined in the Visa Rules. These capital requirements vary based on factors such as the payment facilitator or marketplace's region and sales volume. Additionally, separate Tier 1 capital requirements exist to register a high-risk internet payment facilitator that intends to solicit high-brand risk merchants.

5.3 Cross-Border Acquiring

Visa issues licenses to acquirers that are applicable to a specific jurisdiction or region. Thus acquirers may only contract with payment facilitators or marketplaces that are located within their licensed jurisdiction.

IMPORTANT:
An acquirer must only accept and submit transactions from payment facilitators, marketplaces and sponsored merchants located within the Acquirer's licensed jurisdiction.

Acquirers may only contract with payment facilitators or marketplaces that are located within their licensed jurisdiction.

Payment Facilitator and Sponsored Merchant Location Requirements

A payment facilitator must only contract with a sponsored merchant located inside the country in which the payment facilitator and its acquirer are located—meaning all three parties must be located in the same country. An acquirer must determine the correct location of its payment facilitator as the country of the payment facilitator's principal place of business. Please consult the Visa Rules as to what constitutes "principal place of business" and any related requirements.

Marketplace and Retailer Location Requirements

A marketplace submits transactions and receives settlement proceeds on behalf of its underlying retailers. Under this model, Visa considers the marketplace as the merchant. While the Visa Rules permit marketplaces to accept transactions from retailers that are located outside the acquirer's jurisdiction, the marketplace must be located within the licensed jurisdiction of the acquirer. For detailed requirements concerning the permissible location of a marketplace, or additional locations, please consult the Visa Rules.

5.4 Marketplace Qualifications and Visa Approval

Acquirers may only register entities as marketplaces if they meet Visa's marketplace qualification requirements as outlined in the Visa Rules, and further explained in Section 2.1 of this guide. Once it has established that the prospective entity meets the requirements, the acquirer must obtain written approval confirmation from Visa that the prospective entity qualifies as a marketplace.

IMPORTANT:
A marketplace is financially liable for all disputes and must resolve disputes between buyers and sellers.

An acquirer that contracts with a marketplace must recertify annually that the information it provided to obtain written approval from Visa remained materially unchanged. Acquirers must inform Visa immediately if there is a material change in the information provided to obtain approval from Visa to treat the entity as a marketplace. Visa may withdraw marketplace approval if the acquirer fails to comply with this requirement.

6. Onboarding of Payment Facilitators and Marketplaces

When prerequisites have been met for a prospective payment facilitator or marketplace to enter into business relationship with an acquirer, the due diligence phase begins. Acquirers must perform proper due diligence on prospective payment facilitators and marketplaces to assure that the agent is suitable as a participant of the Visa payment system. Once a due diligence review has established the prospective agent as satisfactory, the acquirer may contract with, register, and onboard the prospective payment facilitator or marketplace.

6.1 Due Diligence Review Requirements

Before an acquirer may contract with, and register a prospective payment facilitator or marketplace, it must perform a due diligence review of the prospective third party agent. Due diligence on a prospective payment facilitator or marketplace must include, but is not limited to, the following:

- A review determining that the entity is financially responsible and adheres to sound business practices and applicable laws and regulations, which in some jurisdictions may include holding money-transmission licenses.
- A review of the payment facilitator or marketplace's business strategy, merchant solicitation materials, collateral, and online presence. The review must establish the existence of sound sales and marketing practices.
- A background investigation[3] to verify the financial and fiduciary responsibilities of the principal ownership and ensure no significant derogatory information exists (e.g., present or previous litigation or regulatory action).
- An onsite inspection of the payment facilitator's or marketplace's business operations and operational risk policies, procedures, and controls—including underwriting, risk monitoring, and data security requirements.
- A review to ensure that the prospective payment facilitator or marketplace complies with the Visa Rules relating to sponsored merchants and retailers.
- A query of the Visa Merchant Screening Service[4] (VMSS) to determine whether the Payment Facilitator or marketplace has been previously terminated for cause.

IMPORTANT:
An acquirer must perform a due diligence review compliant with the Visa Rules, the Third Party Due Diligence Risk Standards, and the *Visa Global Acquirer Risk Standards* (GARS).

A senior officer of the acquirer must review and accept all documentation and make a determination that the prospective agent complies with all requirements and does not pose an undue risk to the acquirer and the Visa payment system.

[3] *If applicable laws or regulations prohibit background checks (including financial reviews) on individuals, the acquirer must note this when registering the third party agent including other due diligence procedures it undertook to ensure that it completed due diligence.*
[4] *Where required and available, or use a comparable Terminated Merchant File.*

6.2 Contracting

An acquirer must execute a written contract with each third party agent that solicits merchants and/or stores, processes, or transmits payment or transaction data on its behalf. Third party agent contracts—to the extent permitted by applicable laws and/or regulations—must comply with all of the content requirements as specified in the Visa Rules and the *Visa Global Acquirer Risk Standards* (GARS).

The acquirer must receive a registration confirmation from Visa before submitting transactions on behalf of the payment facilitator or marketplace.

IMPORTANT:
Specific terms and conditions are required to be included in contracts with payment facilitators and marketplaces. Please consult the Visa Rules and the GARS for details.

A senior officer of the acquirer must execute all contracts with payment facilitators or marketplaces.

6.3 Third Party Agent Registration

After attesting to Visa of a satisfactory due diligence review, the acquirer must register the payment facilitator or marketplace using the Visa Program Request Management (PRM) system. The acquirer must receive a registration confirmation from Visa before it can begin to submit transactions on behalf of the payment facilitator or marketplace. If a payment facilitator intends to solicit and provide payment services to high-brand risk merchants, it must be registered with Visa as a High-Risk Internet Payment Facilitator (HRIPF) even if that payment facilitator has previously been registered with Visa.

IMPORTANT:
An acquirer submitting transactions on behalf of a payment facilitator or marketplace it did not register, is in violation of the Visa Rules.

6.4 Transaction Identifier Requirements

Acquirers must use Visa-assigned identifiers for payment facilitators and marketplaces before they may submit transactions. Additionally, payment facilitators must assign their own unique identifiers for each sponsored merchant. The identifiers must be included in all transactions and will result in more effective monitoring of the activity of sponsored merchants that operate under a payment facilitator and of the transactions that occur at a registered marketplace.

7. Merchant Underwriting and Onboarding

Providing sellers with access to the payment system requires a high level of responsibility and accountability. Therefore, the merchant underwriting and onboarding process is an integral component of a payment facilitator and marketplace's risk control environment.

The underwriting process is an integral component of a payment facilitator and marketplace's risk control environment.

To ensure sound underwriting capabilities, it is important that a payment facilitator and marketplace can demonstrate all of the following:

- ✔ Possession of written underwriting policy and procedures.
- ✔ Use of acquirer-approved merchant agreements.
- ✔ Proper collection of seller information.
- ✔ Proper due diligence to ensure every prospective seller meets the Merchant Qualification Standards.
- ✔ Applications from prohibited sellers are rejected.
- ✔ High-brand risk merchants are subject to enhanced due diligence (HRIPFs only).
- ✔ Use of VMSS and/or a comparable Terminated Merchant File (PFs only).
- ✔ Use of Auto-Boarding Best Practices.

Each of these capabilities is crucial in mitigating risk and further explained in this section.

IMPORTANT:
Payment facilitators and marketplaces act as "gatekeepers" to the payment system and must ensure that only qualified and responsible sellers are provided access.

7.1 Underwriting Policy and Procedures

Payment facilitators and marketplaces must possess sound merchant underwriting policies in compliance with the Visa Rules, the GARS, and the Visa Mobile P2M Push Payments Underwriting Standards (if applicable). In addition, payment facilitators and marketplaces must conduct their merchant underwriting in accordance with the acquirer's own underwriting policy and merchant acceptance criteria. Underwriting Policies must be used as the foundation of a payment facilitator or marketplace's underwriting procedures.

A component of the underwriting Policy should be a clear framework of approval authority. This entails the establishment of a hierarchy of underwriters with cascading approval limits specific to various type of seller risk categories. By categorizing prospective sellers from higher to lower risk characteristics, sellers can be assigned specific underwriting authority rules for approval. Acquirers should also have controls in place to provide approval concurrence for sellers that pose a higher risk (based on MCC or sales volume) before agents may onboard them.

7.2 Merchant Agreements

A payment facilitator or marketplace may only submit transactions from sponsored merchants or on behalf of retailers with which it has a valid and executed contract. Such contract—referred to as a merchant agreement or payment service agreement—must include content, terms, and

conditions as outlined in the Visa Rules and the GARS. These terms and conditions include prohibiting sellers from submitting illegal transactions and requiring compliance with the Visa Rules and applicable laws or regulations.

A payment facilitator must ensure the acquirer is party to any merchant agreement where the sponsored merchant's payment volume exceeds the limits as described in the Visa Rules.

The seller must not be engaged in any activity that could cause harm to the Visa payment system or the Visa brand.

IMPORTANT:
The acquirer must approve the merchant agreement that a payment facilitator or marketplace will use to sign sellers and approve any subsequent updates.

7.3 Collection and Validation of Merchant Information

In order to validate and authenticate a prospective seller for payment services, payment facilitators and marketplaces must collect pertinent public and non-public information. Data collection and validation must be carried out in compliance with applicable laws and regulations. This includes Anti-Money Laundering (AML) and other applicable laws or regulations pertaining to the "Know Your Customer" (KYC) process, as well as local privacy laws.

Visa has separated the collection of merchant information into data elements that are "required" and elements that should be collected as a "best practice." Consult the GARS for a full list of required data elements, as well as data elements that should be collected as a best practice to the extent permissible under local law.

Payment facilitators and marketplaces must collect information of prospective sponsored merchants and retailers via a merchant application. Once collected, the information must be validated, and the merchant must be authenticated to prevent fraudulent merchant applications.

Following this, once all required and pertinent information has been collected, the payment facilitator or marketplace must render an underwriting decision to approve, conditionally approve, or decline a new seller application.

7.4 Due Diligence and the Merchant Qualification Standards

A core component of the merchant underwriting process is the performance of due diligence on prospective sellers to establish if they meet the Merchant Qualification Standards. All sellers must meet the following Merchant Qualification Standards at a minimum:

- Financial responsibility
- Posing no harm to the Visa Payment System
- Operating within an allowed jurisdiction

Financial Responsibility

Payment facilitators must determine that a sponsored merchant does not pose an undue financial risk as sponsored merchants submit their own transactions. Since a marketplace accepts and submits transactions on behalf of its retailers, it acts as the merchant of record and absorbs any financial risk. Nevertheless, it would be prudent for marketplaces to take a risk-based approach and screen appropriate retailers for financial responsibility.

No Harm to the Visa Payment System

A seller must not be engaged in any activity that could cause harm to the Visa payment system or

the Visa brand. This includes any illegal activity or involvement in fraudulent, questionable or unsound business practices.

Operating Within an Allowed Jurisdiction

The seller is not misrepresenting its location and is operating within the permitted jurisdiction of the payment facilitator or marketplace.

In addition to the standards above, a payment facilitator must also determine that there is no significant negative background information about any of the sponsored merchant's principals as legally permitted.

7.5 Prohibited Merchant Types

Visa prohibits marketplaces from signing and onboarding specific merchant categories. Merchant categories ineligible to be a retailer under a marketplace include all high-brand risk merchant categories, franchises, and travel agents. Marketplaces are also prohibited from signing retailers that exceed the purchase volume limits as stipulated in the Visa Rules.

Payment facilitators are prohibited from providing payment services to outbound telemarketers, other payment facilitators, and marketplaces. Payment facilitators are restricted from onboarding certain types of digital wallets. When signing a digital wallet, a payment facilitator must ensure that the intended end use does not fund a prohibited merchant type.

Payment facilitators and marketplaces must also be following their acquirer's merchant acceptance criteria. The acquirer may deem additional merchant categories as prohibited (do not onboard) or restricted (may onboard under certain conditions).

7.6 Underwriting High-Brand Risk Merchants

High-brand risk merchants pose an elevated risk to the payment system. Such merchants have the potential to inflict brand or reputation risk if not properly vetted, managed, and controlled. Therefore, high-brand risk merchants require an enhanced level of due diligence. This should include a detailed review of the goods or services offered, how they are marketed and sold, validation of the merchant location, and review of previous processing history (if applicable). The underwriting process should include checks of consumer complaint boards. It is additionally important to ascertain a high-brand risk merchant's compliance with the Visa Rules and applicable laws.

Only duly registered High-Risk Internet Payment Facilitators are permitted to solicit high-brand risk merchants.

IMPORTANT:
Marketplaces are prohibited from soliciting high-brand risk merchants.

Only duly registered High-Risk Internet Payment Facilitators (HRIPFs) are permitted to solicit high-brand risk merchants in accordance with the Visa Rules and their acquirer's underwriting policy and merchant acceptance criteria.

7.7 The Visa Merchant Screening Service (VMSS)

The VMSS is a database product that acquirers and their designated agents use to list merchants that have had their payment services terminated for presenting an undue risk to the payment system.

Payment facilitators must query the VMSS[5] for each prospective seller applicant to determine if it was previously terminated for cause. The information obtained via the VMSS should be used in consideration with all other merchant due diligence and should not be the sole basis for declining a merchant for payment acceptance privileges. Please consult the Visa Rules on use of VMSS and regional availability. If VMSS is not available, a comparable Terminated Merchant File must be used.

7.8 Auto-Boarding Best Practices

Many payment facilitators and marketplaces leverage technology to facilitate the rapid and frictionless onboarding of new sellers. Instead of using traditional underwriters to review merchant applications, the merchant underwriting and onboarding process is largely automated (hence called auto-boarding) through utilization of rule logic and machine learning. However, if this process is not properly controlled and managed in accordance with sound underwriting policy and procedures, it could invite fraudulent applications and illicit sellers. It is critical that payment facilitators and marketplaces who use auto-boarding avoid shortcuts when it comes to crucial checks aimed to authenticate prospective sellers and validate the goods or services they sell. In addition, controls must be used to detect anomalous application activity, such as velocity checks on new applications, as fraudsters often target weak auto-boarding controls to gain illicit access to the payment system.

IMPORTANT:
Visa strongly recommends that payment facilitators and marketplaces adopt the "Auto-Boarding Best Practices" as outlined in the GARS.

[5] *Where required and available, or use a comparable Terminated Merchant File.*

8. Risk Monitoring and Controls

Risk monitoring and the proper application of controls are critical functions in mitigating risk. Therefore, payment facilitators and marketplaces must continuously monitor the transactions and behavior of sellers for risk exposure and suspect activity. In addition, monitoring must occur to ensure sellers remain in compliance with the Visa Rules and applicable laws.

Payment facilitators and marketplaces must continuously monitor sellers for risk exposure and suspect activity.

Payment facilitators and marketplaces must be able to identify and investigate activity indicative of increased risk exposure at the earliest possible moment. The monitoring of daily and monthly transaction activity can help recognize any unusual or sudden changes in normal seller activity in order to prompt mitigating action.

To ensure sound risk-monitoring practices, it is important that a payment facilitator and marketplace can demonstrate all of the following:

- ✔ Possession of written risk-monitoring policy and procedures.
- ✔ Use of transaction monitoring, velocity checks, and fraud detection.
- ✔ Use of exception reporting and investigations.
- ✔ Proper monitoring of seller websites.
- ✔ Knowledge and avoidance of Visa risk-compliance programs.
- ✔ Proper and appropriate use of merchant reserves (payment facilitators).
- ✔ Use of a terminated merchant file (payment facilitators).
- ✔ Proper termination of sponsored merchants and retailers.
- ✔ Use of adequate reporting.

8.1 Risk-Monitoring Policy

Payment facilitators and marketplaces must possess sound merchant risk-monitoring policies in compliance with the Visa Rules and the GARS. Similarly, payment facilitators and marketplaces must conduct their risk monitoring in accordance with their acquirer's risk-monitoring policies.

8.2 Transaction Monitoring and Fraud Detection

Payment facilitators and marketplaces must monitor the daily transaction activity associated with their sellers. In addition, sellers must be monitored for signs of unusual or suspect activity. While this guide outlines the various parameters to monitor, periodically consult the Visa Rules and the GARS for complete and up-to-date risk-monitoring requirements.

Velocity Checks

A key component of risk monitoring involves the ability to detect abrupt or unusual deviations in the aspects of a seller's normal transaction pattern. Transaction velocity checks generally involve the use of parameters that are assigned unique threshold limits for sellers. At a minimum, payment facilitators and marketplaces should monitor the velocity of the following parameters for each seller as well as its entire portfolio:

- Monthly Sales Amount (Volume)
- Average Transaction Amount
- Purchase Return Amount (Volume)
- Sales-to-Purchase Return Ratio
- Real-time Authorization Attempt Count
- Real-time Declined Authorization Count
- Dispute Count and Amount Ratios (compared to Sales Count and Amount)
- Fraud Advice Amount and Ratio (compared to Sales Amount)

- Card-Absent to Card-Present Sales Amount Ratio
- Cross-Border to Domestic Sales Amount Ratio
- Force-Posted Transaction Amount

When alerted of transaction activity that exceeds velocity thresholds, a payment facilitator or marketplace must investigate the activity and take appropriate risk-mitigation actions.

Fraud Detection and Loss Prevention

Fraud detection and loss prevention controls aim to identify early indications of fraud or potential loss exposure. In events that involve fraud or other potential for loss exposure, early detection through velocity checks and rapid mitigation are key. In the event of fraud, it must be rapidly determined whether the seller has fallen victim to fraud, exhibits unsound acceptance practices causing customers to claim fraud, or is directly involved in committing fraud.

IMPORTANT:
Payment facilitators and marketplaces are responsible for fraudulent and/or unauthenticated transactions submitted by sponsored merchants and retailers, and any related losses.

In addition to fraud, sellers engaged in questionable business practices also possess the potential to expose payment facilitators and marketplaces to losses by generating excessive disputes. Therefore, coupled with velocity checks, payment facilitators and marketplaces should address unusual or suspect activity as part of their risk control environment. When velocity checks detect unusual activity, the payment facilitator or marketplace should determine the root cause and act to remediate it. Following are examples of unusual activity and what risks they may pose. A quick-reference card with this information is available in the Quick Reference Appendix.

- **Sudden Spikes in Sales Volume or Transaction Amounts**
  When a seller abruptly exceeds predetermined sales volume and/or transaction amount thresholds, the seller may pose a financial risk. It should be ascertained whether the sudden increase is justified and the seller has sufficient capital liquidity to cover the associated risk, such as the ability to fund a potential increase in disputes. Significant spikes in transaction amounts may also be indicative that the seller is accepting payments for goods or services they do not normally sell or involvement in a bust-out scheme.

- **Elevated Dispute Activity**
  Dispute activity is a key indication of merchant risk. While disputes are common in the payment system, sellers exhibiting elevated or excessive disputes must be investigated. There are a variety of reasons for such elevated activity, often related to unsound acceptance practices, deceptive marketing, or fraud. It is important to note that sellers generating excessive disputes negatively impact issuers and their cardholders; payment facilitators and marketplaces must address such instances in a prompt manner.

- **Elevated Fraud Advices**
  Often driven by cardholder claims, a fraud advice (also known as a TC40) is initiated by an issuer when it has reason to believe that a transaction was fraudulent. In many cases, a fraud advice may be followed up by a fraud dispute. Payment facilitators and marketplaces must monitor for sellers that generate excessive fraud and take immediate action to address the activity.

IMPORTANT:
All sellers must be monitored for fraud and dispute activity approaching the *Visa Fraud Monitoring Program* (VFMP) and *Visa Dispute Mentioning Program* (VDMP) thresholds in order to avoid compliance violations.

- **Purchase Return Volume**
  Payment facilitators and marketplaces must investigate sellers that exhibit excessive purchase return (a.k.a. credit voucher) volume or ratios—primarily to ascertain the reason for customers requiring an unusual amount of refunds—often indicative of unsound business or sales practices. Such scenarios can quickly turn into excessive disputes should the merchant fail to refund its customers for any reason. It is important to ensure sellers use purchase returns only to reverse a previous (or offsetting) sale. Any purchase returns that cannot be linked to an offsetting sale pose a risk and must be investigated (see *Purchase Return Fraud and Purchase Return Authorizations* in Section 4.6).

- **Authorization Activity**
  A spike in authorization attempts and decline responses may be indicative of an enumeration attack (see *Enumeration or Account Testing Schemes* in Section 4.6). Such instances should trigger an immediate investigation. When suspecting an enumeration attack, the authorization activity must be rapidly blocked. Both sales draft and Purchase Return Authorizations (PRAs) must be monitored. A spike in purchase return authorizations may be indicative of purchase return fraud (see *Purchase Return Fraud and Purchase Return Authorizations* in Section 4.6).

- **Force-Posted Transactions**
  Since there is a high propensity to abuse the force-posting of transactions, providing sellers with this functionality significantly elevates risk exposure. Few sellers have the actual need to force transactions, therefore payment facilitators must only grant this functionality to sponsored merchants on an exception basis and in compliance with the Visa Rules. Marketplaces should not enable retailers with force-post functionality. Force-posted transactions must be closely monitored for potential fraud. In the event fraud is suspected, force-posted transactions must be blocked from clearing.

Suspicious Transaction Activity

Payment facilitators and marketplaces must also monitor for activity that seems suspicious when deviating from a seller's regular processing pattern. This type of activity must be investigated to ascertain if a seller is not being defrauded, or if the seller itself is not participating in a fraud scheme or illicit activity. Below are examples of suspicious activity. See the Quick Reference Appendix for a chart of these monitoring functions.

- **Card-Present vs. Card-Absent Volume**
  This is pertinent to sellers that generally accept payments face-to-face in a retail environment. Transaction activity should be investigated when a card-present seller suddenly submits an elevated volume in card-absent transactions. In some cases, retail sellers are contacted by fraudsters, often asked to ship expensive goods overseas with fraudulent payment information accepted via email or telephone.

- **Transactions with Rounded Amounts**
  Payment facilitators and marketplaces should investigate sudden high occurrences of transactions with rounded amounts (e.g., USD 500.00 or USD 1,000.00) if it deviates from a seller's regular activity. Such transactions may be an indication that a seller is processing payments not related to their business, such as cash disbursements or transaction laundering. Rounded amount transactions involving the same card in a short timeframe may also be an indication of a seller splitting a transaction into smaller amounts to circumvent detection by risk-monitoring systems.

- **High Volume of Micro-Transactions**
  Visa monitors the payment system for instances of excessive fraud or dispute activity. It operates a suite of risk-compliance programs; including the Visa Dispute Monitoring Program (VDMP) and Visa Fraud Monitoring Program (VFMP), see Section 8.6. Each program comes with predetermined thresholds that, when exceeded, will identify sellers in violation. In rare cases, Visa has encountered sellers that inflate transaction counts with one- or two-cent transactions using prepaid cards in order to artificially remain below program thresholds. It is therefore important to detect instances of sellers processing high-volume micro-transactions, as it may be an attempt to obfuscate illicit payment activity.

- **Repeated Sales on the Same Card**
  Repeated transactions involving the same card in a short succession may be an indication of fraudsters realizing they are able to purchase goods with stolen card information from a seller. Because the first attempt was successful, fraudsters will attempt to purchase more goods with the same card within a short timeframe. Payment facilitators and marketplaces should detect and treat repeated transactions on the same card in short succession as suspicious activity.

- **Unusual Cross-Border Activity.** Seller activity should be monitored for sudden spikes in transactions outside the regular service area of the seller, specifically cross-border sales activity. There are legitimate reasons for sellers to accept payments from other regions. However, a surge in such activity should be investigated as it may point to a fraud attack (e.g., force-post or purchase-return fraud) as those attacks often involve cross-border transactions.

- **Dormant Sellers with Sudden Activity Spikes** Fraudsters may attempt to sign up for payment services, and when successful they will refrain from activity until an opportune moment arises. In such cases, fraudsters may secure a high number of payment accounts to use simultaneously in a coordinated fraud attack. To mitigate the risk of fraudulent activity, payment facilitators and marketplaces should monitor sellers that are dormant for an extended period and suddenly show a surge in volume. Exceptions can be made if the seller is known to operate a seasonal business.

- **Load Balancing** Some sellers that generate an excessive amount of dispute or fraud activity may resort to load balancing. Load balancing occurs when sellers distribute their payments and dispute or fraud activity across a number of payment accounts, with the aim to remain undetected by risk-monitoring systems or Visa's compliance programs. Sellers are permitted to utilize multiple payment accounts to separate distinct sales or business channels, often assigned with unique merchant descriptors. However, using multiple payment accounts for the same sales or business channel—often with identical merchant descriptors—should be investigated for potential load balancing.

Risk management staff must rapidly act on all exception reports by investigating the root cause and mitigate any associated risks.

8.3 Exception Reporting and Investigations

Payment facilitators and marketplaces must use exception reports and investigate them when a seller exceeds velocity checks tolerances or when detecting usual or suspect activity. Risk management staff must rapidly act on all exception reports by investigating the root cause and take appropriate action to mitigate any associated risks. Exception reports are best addressed through a case-management system that documents the resulting actions taken by risk management personnel, also providing subsequent reporting. During an exception report investigation, and when appropriate, a payment facilitator or marketplace may temporarily suspend a seller's settlement proceeds when it has reason to believe that funding the seller may result in loss exposure. If the investigation concludes favorably, the funds held in suspense must be released to the seller. If an investigation reveals that releasing settlement funds may likely result in a financial loss, settlement funds may be diverted into a designated reserve account, pursuant to contract terms with the seller and the Visa Rules.

8.4 Website Monitoring

Payment facilitators and marketplaces must monitor the ecommerce websites of their sellers on an ongoing basis. An important responsibility is to ensure that sellers are not engaged in any activity or displaying items that pose a risk to the payment system or could cause harm to the Visa brand. Payment facilitators and marketplaces may contract with third parties that specialize

in screening seller sites for illegal or illicit goods and services. However, it is the responsibility of the payment facilitator or marketplace to select the third party most suitable for them; and the accountability for compliance remains with the payment facilitator, marketplace, and acquirer. As part of the monitoring process, websites must be screened for signs of illegal activity or transaction laundering as well as deceptive marketing practices. This especially holds true for high-brand risk merchants.

Screen seller websites for signs of illegal activity, transaction laundering, or deceptive marketing practices.

8.5 Visa Risk-Compliance Programs

Visa operates a suite of compliance programs aimed to uphold the integrity of the payment system. These programs monitor the payment system for merchants with a disproportionate amount of fraud and/or disputes, as well as signs of illegal activity. Visa also monitors acquirer merchant portfolios—and third party agents by extension—for the same type of activity. When a Visa risk-compliance program identifies a merchant for excessive fraud, disputes or illegal activity, Visa holds the acquirer responsible. The acquirer is required to engage the identified merchant immediately in order to remediate the situation. In many instances, these compliance programs carry non-compliance assessments levied on acquirers for program violations. Examples of Visa compliance programs applicable to acquirers, payment facilitators, and marketplaces are described in the table below.

VISA RISK COMPLIANCE PROGRAMS APPLICABLE TO PAYMENT ACCEPTANCE
Visa Dispute Monitoring Program (VDMP) Identifies merchants exceeding predetermined program thresholds based on a merchant's monthly dispute count and the dispute count to transaction count ratio.
Visa Fraud Monitoring Program (VFMP) Monitors to identify merchants exceeding predetermined program thresholds based on a merchant's monthly fraud amount and the fraud amount to sales amount ratio.
Visa Acquirer Monitoring Program (VAMP) Identifies Acquirers, and indirectly their agents, exceeding predetermined thresholds based on aggregated merchant portfolio fraud and dispute activity.
Global Brand Protection Program (GBPP) Monitors the payment system for illegal, prohibited, or brand-damaging activity.
Transaction Laundering Detection (TLD) Detects merchants with signs pointing to a high probability of transaction laundering using payment system data and machine learning.

IMPORTANT:
Payment facilitators and marketplaces must monitor their own transaction activity as well as their individual sellers to ensure they do not approach Visa compliance program thresholds.

8.6 Merchant Reserves

Acquirers must avail themselves of reporting pertaining to merchant onboarding and risk monitoring conducted by their payment facilitators and marketplaces.

Payment facilitators may employ the use of merchant reserves as a mechanism to mitigate loss exposure. Payment facilitators should apply merchant reserves by using a risk-based approach. Examples when reserves may be applicable include sponsored merchants that offer delayed delivery of goods or services—e.g., travel-related businesses, event ticketing, or merchants offering annual memberships. While payment facilitators may require a sponsored merchant to establish a reserve account, Visa prohibits payment facilitators from holding and controlling merchant reserves. Reserve funds are the property of the sponsored merchant—only drawn upon pursuant to applicable clauses in the payment services agreement with the sponsored merchant—and must be held and controlled by the acquirer.

It is important to note that merchants should be underwritten based on their merits, and reserves are only an added measure to mitigate risk—not a justification to onboard unreasonably high-risk merchants.

8.7 Sponsored Merchant Terminations

Upon terminating a sponsored merchant for cause—such as excessive disputes or fraud—a payment facilitator must add that merchant to the Visa Merchant Screening Service (VMSS)[6]. This will notify other payment service providers of the termination should that sponsored merchant apply for services in the future.

8.8 Reporting Obligations

Acquirers are required to maintain appropriate oversight of the payment facilitators and marketplaces they sponsor. Acquirers must therefore avail themselves of ongoing reporting pertaining to transaction activity, merchant onboarding, and risk monitoring conducted by the payment facilitators and marketplaces. Under certain conditions stipulated by the Visa Rules, payment facilitators and marketplaces are required to provide Visa with similar reporting. Therefore, payment facilitators and marketplaces must retain information required for oversight purposes and provide it upon request to their acquirer or to Visa.

[6] *Where required and available, or use a comparable Terminated Merchant File.*

9. Conclusion and Additional Resources

An acquirer, payment facilitator, or marketplace has an obligation to protect and uphold the integrity of the Visa payment system. This guide provides an overview of what Visa expects from each party in order to mitigate and control the risks related to payment acceptance. Knowing and applying its content in combination with information provided in the reference materials below will help payment facilitators and marketplaces to better manage those risks.

For additional information, payment facilitators and marketplaces should contact their acquirer. Acquirers should contact their regional Visa Risk team or relationship manager.

ADDITIONAL RESOURCES

Some links may require access to Visa Online (VOL) or resources may be obtained through your acquirer.

Visa Core Rules and Visa Product and Service Rules
Public Version • *Full Version (VOL)*

Visa Global Acquirer Risk Standards Guide

Visa Global Brand Protection Program Guide (VOL)

Visa Online Pharmacy Guide for Acquirers (VOL)

Risk Best Practices Resources (VOL)

Visa Direct Risk Resources (VOL)

Visa Mobile P2M Push Payment Underwriting Standards (VOL)

Visa Acquirer Monitoring Program (VOL)

Visa Fraud Monitoring Program (VFMP) Guide

Visa Dispute Monitoring Program (VDMP) Guide

QUICK REFERENCE APPENDIX

Fraud Detection & Loss Prevention

Unusual Business Practices and the Risks They May Pose

Sudden Spikes in Sales Volume or Transaction Amounts

When a seller abruptly exceeds predetermined sales volume and/or transaction amount thresholds, the seller may pose a financial risk. It should be ascertained whether the sudden increase is justified and that the seller has sufficient capital liquidity to cover the associated risk, such as the ability to fund a potential increase in disputes. Significant spikes in transaction amounts may also be indicative that the seller is accepting payments for goods or services they do not normally sell or involvement in a bust-out scheme.

Elevated Dispute Activity

Dispute activity is a key indication of merchant risk. While disputes are common in the payment system, sellers exhibiting elevated or excessive disputes must be investigated. There is a variety of reasons for such elevated activity, often related to unsound acceptance practices, deceptive marketing, or fraud. It is important to note that sellers generating excessive disputes generally present a negative impact on issuers and their cardholders; payment facilitators and marketplaces must address such instances in a prompt manner.

Elevated Fraud Advice

Often driven by cardholder claims, a fraud advice (also known as a TC40) is initiated by an issuer when it has reason to believe that a transaction was fraudulent. In many cases, a fraud advice may be followed up by a fraud dispute. Payment facilitators and marketplaces must monitor for sellers that generate excessive fraud and take immediate action to address the activity.

Purchase Return Volume

Payment facilitators and marketplaces must investigate sellers that exhibit excessive purchase return (a.k.a. credit voucher) volume or ratios—primarily to ascertain the reason for customers requiring an unusual amount of refunds—often indicative of unsound business or sales practices. Such scenarios can quickly turn into excessive disputes should the merchant fail to refund its customers for any reason. It is important to ensure sellers use purchase returns only to reverse a previous (or offsetting) sale. Any purchase returns that cannot be linked to an offsetting sale pose a risk and must be investigated (see *Purchase Return Fraud and Purchase Return Authorizations* in Section 4.6).

Authorization Activity

A spike in authorization attempts and decline responses may be indicative of an enumeration attack (see *Enumeration or Account Testing Schemes* in Section 4.6). Such instances should trigger an immediate investigation. When suspecting an enumeration attack, the authorization activity must be rapidly blocked. Both sales draft and Purchase Return Authorizations (PRAs) must be monitored. A spike in purchase return authorizations may be indicative of purchase return fraud (see *Purchase Return Fraud and Purchase Return Authorizations* in Section 4.6).

Force-Posted Transactions

Since there is a high propensity to abuse the force-posting of transactions, providing sellers with this functionality significantly elevates risk exposure. Few sellers have the actual need to force transactions, therefore payment facilitators must only grant this functionality to sponsored merchants on an exception basis and in compliance with the Visa Rules. Marketplaces should not enable retailers with force-post functionality. Force-posted transactions must be closely monitored for potential fraud. In the event fraud is suspected, force-posted transactions must be blocked from clearing.

QUICK REFERENCE APPENDIX

Suspicious Transaction Activity

Monitor for activity that seems suspicious or deviations from a regular processing pattern

Card-Present vs. Card-Absent Volume

This is pertinent to sellers that generally accept payments face-to-face in a retail environment. Transaction activity should be investigated when a card-present seller suddenly submits an elevated volume in card-absent transactions. In some cases, retail sellers are contacted by fraudsters, often asked to ship expensive goods overseas with fraudulent payment information accepted via email or telephone.

Transactions with Rounded Amounts

Payment facilitators and marketplaces should investigate sudden high occurrences of transactions with rounded amounts (e.g., USD 500.00 or USD 1,000.00) if it deviates from a seller's regular activity. Such transactions may be an indication that a seller is processing payments not related to their business, such as cash disbursements or transaction laundering. Rounded amount transactions involving the same card in a short timeframe may also be an indication of a seller splitting a transaction into smaller amounts to circumvent detection by risk-monitoring systems.

High Volume of Micro-Transactions

Visa monitors the payment system for instances of excessive fraud or dispute activity. It operates a suite of risk-compliance programs; including the Visa Dispute Monitoring Program (VDMP) and Visa Fraud Monitoring Program (VFMP), see Section 8.6. Each program comes with predetermined thresholds that, when exceeded, will identify sellers in violation. In rare cases, Visa has encountered sellers that inflate transaction counts with one- or two-cent transactions using prepaid cards in order to artificially remain below program thresholds. It is therefore important to detect instances of sellers processing high-volume micro-transactions, as it may be an attempt to obfuscate illicit payment activity.

Repeated Sales on the Same Card

Repeated transactions involving the same card in a short succession may be an indication of fraudsters realizing they are able to purchase goods with stolen card information from a seller. Because the first attempt was successful, fraudsters will attempt to purchase more goods with the same card within a short timeframe. Payment facilitators and marketplaces should detect and treat repeated transactions on the same card in short succession as suspicious activity.

Unusual Cross-Border Activity

Seller activity should be monitored for sudden spikes in transactions outside the regular service area of the seller, specifically cross-border sales activity. There are legitimate reasons for sellers to accept payments from other regions. However, a surge in such activity should be investigated as it may point to a fraud attack (e.g., force-post or purchase-return fraud) as those attacks often involve cross-border transactions.

Dormant Sellers with Sudden Activity Spikes

Fraudsters may attempt to sign up for payment services, and when successful they will refrain from activity until an opportune moment arises. In such cases, fraudsters may secure a high number of payment accounts to use simultaneously in a coordinated fraud attack. To mitigate the risk of fraudulent activity, payment facilitators and marketplaces should monitor sellers that are dormant for an extended period and suddenly show a surge in volume. Exceptions can be made if the seller is known to operate a seasonal business.

Load Balancing

Some sellers that generate an excessive amount of dispute or fraud activity may resort to load balancing. Load balancing occurs when sellers distribute their payments and dispute or fraud activity across a number of payment accounts, with the aim to remain undetected by risk-monitoring systems or Visa's compliance programs. Sellers are permitted to utilize multiple payment accounts to separate distinct sales or business channels, often assigned with unique merchant descriptors. However, using multiple payment accounts for the same sales or business channel—often with identical merchant descriptors—should be investigated for potential load balancing.