WHITE PAPER
MAY 2025

Building digital trust by combating scams and fraudulent merchants

Contents

Foreword

In a world where digital platforms offer us greater connectivity and convenience, these same channels have become avenues for advanced scams. Whether it's an unsuspecting individual coerced into handing over their personal information or a fraudulent business accepting a legitimate payment, behind these acts are fraudsters skilled at exploiting human trust.

At the highest level, a scam can be defined as "the use of deception or manipulation intended to achieve financial gain".[1] Fraudsters mislead consumers by selling goods or services that are either non-existent or of poor quality. These fraudulent activities can potentially result in financial loss, identity theft, and brand damage, as fraudsters often extract a significant amount of money and then disappear, making recovery difficult for victims.

One of the biggest concerns in today's digital environment is the speed and complexity with which scam operations evolve. Fraudsters leverage sophisticated websites, advanced social engineering techniques, and even stolen identities to pass themselves off as legitimate businesses. Their success not only results in direct financial harm to consumers but also to businesses. Furthermore, every instance of fraud erodes public confidence in digital commerce, stalling growth and innovation in an industry with tremendous potential to enhance global trade.

According to the Global Anti-Scam Alliance and Feedzai's 2024 Global State of Scams report, scammers have siphoned more than $1.03 trillion worldwide in 2024 alone.

Mastercard is committed to creating a secure, reliable environment where consumers and business alike can thrive. From artificial intelligence-powered scam prevention technology and tools to industry collaboration, this paper will explore how the ecosystem can come together and maintain trust in digital payments. By fostering transparency, sharing real-time information, and continually educating stakeholders, we can create a trusted digital world.

1. The Federal Reserve, Defined Scams to Fight Scams.

Introduction

In today's interconnected world, e-commerce has revolutionized how businesses and consumers engage in buying and selling. With a few clicks or taps, a consumer can purchase products or services from companies all over the world. This unparalleled level of access has opened opportunities for reputable merchants, elevating growth and competition in the digital marketplace. However, the accessibility that has driven innovation and convenience has also created an environment exploitable by scam websites set up with the sole intention of committing fraud.

Fraudulent merchants operate by leveraging vulnerabilities that exist across various points in the payments ecosystem. They may take advantage of weaknesses in acquirer onboarding procedures or the anonymity of online platforms. In many cases, these fraudulent actors appear to be legitimate businesses with professional-looking websites, sophisticated advertising campaigns, and appealing product offers. Beneath the surface, however, their aim is to deceive consumers into sharing payment details or making purchases for goods and services that are never delivered. In 2024, scams emerged as the most prevalent type of fraud, overtaking digital payment fraud. Scam-related fraud surged by 56%, while financial losses from scams soared by 121%.[2]

Fraudulent merchants can lead to high chargeback rates as cardholders dispute unauthorized charges. When these merchants are closed or disappear after collecting payments, both acquirers and issuers are left to handle a surge in disputes and financial losses. The impact of such scams extends beyond immediate financial losses; it undermines consumer trust in digital commerce, damages the reputation of financial institutions and networks, and places legitimate businesses at a competitive disadvantage.

Tackling this challenge requires a collaborative, multi-layered approach. Mastercard plays a pivotal role by establishing standards and best practices for merchant onboarding, transaction monitoring, and dispute resolution. Issuing and acquiring institutions are equally critical, as they must implement strict Know Your Customer (KYC) protocols and maintain robust fraud detection systems. Merchants themselves bear responsibility for safeguarding their platforms with security measures that minimize the risk of account takeovers (ATO) and data breaches. Such ATO attacks can allow fraudsters to gain access to merchant accounts and use it for scam-related purposes such as obtaining credit card details from unsuspecting customers. Once the legitimate account is compromised, the fraudulent merchant processes unauthorized transactions, leaving both consumers and financial institutions to deal with the consequences. Lastly, consumers can become the first line of defense by learning how to identify suspicious sites, scrutinize deals that seem too good to be true, and report suspicious activity promptly.

Throughout this paper, the challenges posed by fraudulent merchants will be explored, illustrating both the scope and scale of their activities. Real-world examples will be examined that underscore the challenges, while highlighting the Mastercard Standards that shape fraud prevention efforts. A spotlight on the Mastercard tools and best practices designed to combat these bad actors at every stage of the payment life cycle will also be emphasized. This information provides all stakeholders with best practices and a strong framework to effectively mitigate fraud and maintain trust in digital transactions.

2. PYMNTS, Scam-Related Fraud Jumped 56% in 2024, Surpassing Digital Payment Crimes, December 10, 2024.

Industry challenges in combating scam websites

Scam websites are a major challenge in today's global e-commerce environment. The "on demand" nature of a consumer's desire for digital goods and services delivered also allows for fraudulent merchant proliferation within the payment ecosystem. Quick checkout solutions through digital wallets, instant downloads, and worldwide shipping options have all increased consumer expectations, while making it easier for fraudsters to slip through conventional controls.

As consumer demand for digital goods and services increases, so do opportunities for fraudsters to leverage underwriting gaps, technological deficiencies, and human trust to create fraudulent businesses at scale. According to the Better Business Bureau, reports have shown a 125% increase in fraud from 2023 with fraudsters tricking consumers into buying fake or misleading online advertisements, in part driven by items often popular on social media.

Social media scams continued to grow in 2024, with research indicating that the majority of scam types reported originated from either social media or tech platforms.[3] Various social media and messaging apps have become common channels for small businesses, as well as scammers. Fraudsters taking advantage of these channels can either create new business pages or compromise existing commercial pages and run ads targeting specific demographics with misleading offers. With minimal due diligence from certain platform operators, these scam websites may attract thousands of customers before encountering any serious scrutiny.

In many cases, fraudsters leverage social media advertising, low-cost website builders, and even official-looking payment gateways to portray the illusion of credibility. Fraudsters can register new domain names at a low cost, often in locations with minimal oversight, and leverage prebuilt e-commerce platforms or drop-shipping services with little verification required. These Fraud-as-a-Service or "FaaS" packages reduce the technical expertise needed to create seemingly legitimate websites, accelerating the pace at which scam operations can begin processing payments.[4]

Scam websites may advertise free trials or heavily discounted items, enabling impulse buys and making it more likely that customers complete a transaction before fully verifying the legitimacy of the business. Additionally, flaws in merchant onboarding processes, where due diligence might be minimal or inconsistent, allow for illegitimate accounts to remain active far longer than they should.

Scam operations often overlap other forms of digital fraud. Phishing, identity theft, and synthetic identities can all feed into fraudulent merchant activity, aiding criminals in bypassing key security protocols. Technological gaps, such as a lack of real-time transaction monitoring, outdated risk-scoring models, or lack of two-factor authentication, allows scam websites to blend in with genuine merchants until losses reach thresholds that require immediate attention.

The damage inflicted by these scam operations are seen through financial losses, reputational harm, and a growing erosion of trust in online commerce. Beyond the immediate monetary impact, there is a profound effect on consumer sentiment. Shoppers who fall victim to non-delivery scams or who unknowingly share personal data on compromised sites may hesitate to engage in future e-commerce transactions. Issuers, acquirers, and merchants bear the cost of chargebacks, operational overhead, and brand damage. For genuine merchants, every headline highlighting large-scale fraud can cast doubt on trustworthy businesses, leading to increased consumer skepticism.

Addressing these issues requires a collaborative, multi-layered effort that unites Mastercard, financial institutions, regulators, and merchants in a commitment to greater oversight, improved risk monitoring, and comprehensive education campaigns for both businesses and consumers. By strengthening each link in the e-commerce chain, the industry can mitigate the profound financial harm and reputational fallout that scam operations so often bring.

3. Fnextra, One-in-five consumers lost money to scammers in 2024, January 6, 2025.
4. Ravelin, FaaS: What is it and why is Fraud-as-a-Service trending?, March 4 2024.

Rapid proliferation of scam websites

Scam websites are a result of onboarding process deficiencies, fast-evolving technology, and human behavior. Recent reporting underscores the size and scope of fraudulent merchant activity within the payments ecosystem, highlighting the need for a stronger, more coordinated global response to the issue. In 2024, the Federal Trade Commission (FTC) reported that overall fraud losses surpassed $12 billion across the United States, a 25% increase over the prior year. Investment scams were the top fraud category, surpassing online shopping.

Another factor is the global reach of digital platforms. For example, some fraudsters concentrate on regions where consumer protection laws are weak or poorly enforced. Others deliberately target countries with high credit card usage, knowing that the high volume of transactions can make detecting unauthorized patterns of traffic more challenging. A 2024 investigation by *The Guardian* revealed that more than 800,000 people in Europe and the U.S. fell victim to a network of fraudulent online designer shops reportedly operated from China. These sites enticed consumers with heavily discounted products, only to steal their card details or fail to deliver legitimate merchandise. The sheer scale of this operation demonstrates how easily scammers can build extensive global networks when cross-border regulations and enforcement are inconsistent or slow to react.

In April 2024, Recorded Future identified the "ERIAKOS" scam campaign, a network of over 600 fraudulent e-commerce sites exploiting social media ads to target mobile users. Using brand impersonation and malvertising, scammers stole financial and personal data while evading detection. Payments were processed through major card networks and Chinese Payment Service Providers (PSPs), making enforcement more challenging.

Payment processors, acquirers, and even digital wallet providers may lack the resources, or the incentive, to detect and block all fraudulent merchant accounts upfront. Although most reputable payment networks have implemented standard monitoring programs, the overall volume of newly-created businesses each month allows fraudulent businesses to bypass early-stage verification checks. By the time the scam operation is uncovered, the threat actors have often already siphoned a significant amount of money and disappeared.

Diverse fraud attack vectors

The variety of attack vectors utilized by threat actors highlights the complexity of the proliferation of fraudulent merchants throughout the payments ecosystem.

Phishing and social engineering

Threat actors create elaborate phishing emails or text messages using generative artificial intelligence (GenAI), email spoofing, domain impersonation, and social engineering that impersonate trusted brands. Additionally, attackers use malicious attachments and hidden redirects to trick recipients into revealing sensitive information or downloading malware. These messages lure victims into providing sensitive information or clicking on malicious links, ultimately allowing fraudsters to hijack accounts or steal payment credentials. According to 2024 Federal Trade Commission data, email was the most common method fraudsters used to target consumers in the United States. Furthermore, advanced social engineering scams employed by fraudsters to target consumers directly in the U.S. has increased 56% since 2023.[5]

Skimming and embedded malware

Some fraudulent operations involve injecting malicious scripts into checkout pages of legitimate online stores, essentially "skimming" card details. These compromised sites might be entirely unaware that they are facilitating data theft. Victims believe they are purchasing from a credible merchant, yet their payment data gets diverted to scam operators. In 2024, the volume of Magecart e-skimmer infections, which are malicious scripts injected into websites to steal payment data surged, reaching nearly 11,000 unique e-commerce domains, which tripled from 2023.[6]

5. PYMNTS, Social Engineering Scams Prove Costly to Consumers and Bank Bottom Lines, November 22, 2024.
6. Record Future, Annual Payment Fraud Intelligence Report: 2024, January 21, 2025.

Account takeover (ATO)

In some cases, fraudsters do not even need to create new merchant accounts. By hacking into existing, reputable accounts, there is a built-in brand and consumer trust that is inherited. Stolen credentials can be acquired through phishing attacks, data breaches, or on the dark web. Once in control, scammers can quickly change bank routing details, intercept customer payments, and exploit the trust previously built by a legitimate merchant. Password reuse across accounts can also lead to credentials being repurposed to exploit other platforms, making it even easier for attackers to scale their fraud.

Enumeration attacks

Enumeration attacks allow threat actors to systematically test and validate payment credentials, which they later use to conduct fraudulent transactions through fake or deceptive merchants.

First party misuse and synthetic identities

While first party misuse typically refers to consumers who file illegitimate chargebacks, it also can be used by fraudulent merchants pretending to be their own "customers." These fraudsters initiate unauthorized refunds or use synthetic identities where fragments of real personal data are pieced together to create a seemingly legitimate individual to challenge legitimate transactions or funnel funds through multiple accounts. The blending of first party misuse and synthetic IDs complicates the dispute process and drains resources from legitimate merchants and financial institutions.

Multi-channel tactics

With the rise of mobile e-commerce and social commerce, fraudsters can engage victims across platforms and channels. They might advertise on social media, direct users to a legitimate looking website, and then process payments through yet another service. This multi-layered approach complicates efforts to trace funds and identify the actual origin of malicious activity.

Challenges in tracking and monitoring scam websites

From a consumer's perspective, identifying scam websites is more difficult than ever. Fraudsters use sophisticated tactics such as website impersonation, social engineering, and deceptive marketing, making fraudulent schemes appear legitimate and difficult to distinguish from real businesses. Scam websites rarely provide consistent or verifiable contact information, physical addresses, or phone numbers. Even if consumers are suspicious of the purchase made, they cannot easily request returns from the merchant due to the anonymity these sites maintain. Furthermore, as cross-border e-commerce becomes more common, consumers may be lured by deals on foreign sites. When issues arise, language barriers or unfamiliar consumer protection laws prevent consumers from effectively seeking recourse.

Tracking and monitoring scam transactions presents challenges for issuers, particularly when scams result in low-value chargebacks under "Goods Not Delivered" disputes. Many scam transactions are less than $100, leading to underreporting by consumers to their issuers, as consumers may see the loss as insignificant or feel embarrassed about being deceived.

Fraudsters exploit this by keeping transaction amounts low, making scams harder to detect and less likely to trigger fraud alerts. Additionally, fraudulent merchants frequently change names and merchant descriptors, making it difficult for issuers to identify repeat offenders. The high volume of small disputes strains issuer resources, as processing costs may exceed the transaction value.

Furthermore, the emotional impact of being scammed is a significant challenge that cannot be overstated. Victims often feel angry or ashamed, particularly if the scam seems blatantly obvious in hindsight. This emotional component can delay or prevent individuals from reporting incidents to their issuing bank or law enforcement, allowing scam operations a longer lifespan before detection.

Industry scam classifications

The lack of clear standardization for defining and tracking scams has been a significant industry challenge. Recognizing that inconsistent definitions and fragmented reporting impact effective enforcement, the Federal Reserve introduced in 2024 the ScamClassifier℠ model, which was developed to drive more consistent and detailed classification, reporting, analysis and identification of trends in scams.

As an active working group member, Mastercard helped shape and define the scam definition and classification model to drive more consistency in how the industry identifies, tracks and mitigates scams. Moreover, Mastercard is engaging key industry participants to educate and enable them to utilize the ScamClassifier℠ model and helping to address the key issues the industry is facing with respect to scams.

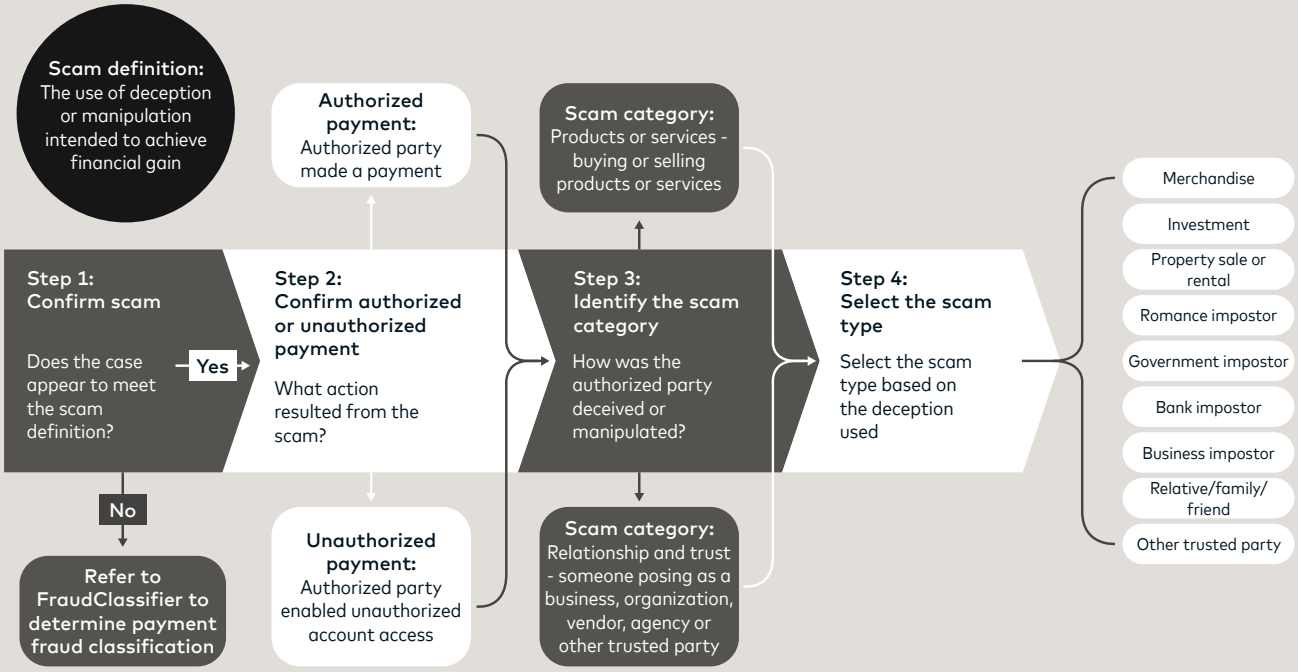
A common classification model can facilitate broader data exchange between banks, Mastercard, law enforcement agencies, and technology partners.

By developing consistent naming conventions and typologies for different scam types, including purchase scams, romance scams, and impersonation scams, ScamClassifier℠ reduces ambiguity in reporting and data analysis. This shared language enables financial institutions and payment networks to accurately categorize and track fraudulent schemes.

Furthermore, the Euro Banking Association (EBA) Fraud Taxonomy standardizes fraud classification across Europe, enabling consistent data sharing and collaboration among PSPs. Developed by the EBA it categorizes fraud types for account-to-account and card payments, detailing fraudster tactics and transaction initiators. This framework enhances fraud detection, prevention, and collective defense in the European payments ecosystem.[7]

7. The Paypers, Fraud intelligence sharing with the EBA fraud taxonomy: creating a pan-European ecosystem, November 26, 2024.

ScamClassifier



The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the ScamClassifier model throughout the industry is encouraged, any adoption of the ScamClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the ScamClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Key terms and definitions

Authorized payment

A payment entered or requested by a legitimate account owner or user from the owner's account.

Unauthorized payment

A payment entered or requested by a third party who has no legitimate right to move money from another entity's account.

Scam categories and definitions

Products or services

A situation involving a transfer of funds in exchange for a product or service, irrespective of the nature of the relationship between the two parties, in which the receiver of the funds does not deliver the product or service or delivers a grossly inferior product or service than the one advertised or promised.

Relationship or trust

A situation involving a transfer of funds to a trusted party, or an impostor acting as a trusted or authoritative party, where there is no expectation or promise of merchandise in exchange for the transferred funds. The seemingly trustworthy party can be an existing or emerging relationship or a party pretending to be an authority or reputable company.

Scam type definitions and examples

Merchandise scam

Purchase of merchandise that is never delivered or is substantially different from the advertised description or quality.

Scam examples: Online purchase scams, puppy and pet scams, and sales of fake sports or concert tickets, counterfeit prescription drugs or anti-aging remedies.

Investment scam

An investment in a financial asset with expectation of a high return rate based on false promises.

Scam examples: Investments in fake business opportunities, fake cryptocurrency purchases or buying precious metals that do not exist.

Property sale or rental scam

The purchase or rental of a home, apartment, or property that was fictitious, was not made available, or was not rightfully owned by the offering party or agent.

Scam examples: Making a down payment for a new home purchase or rental that is not for sale/rent by the real owners. Paying for a fake rental property offered online.

Romance impostor scam

The use of a fictitious online identity to establish a trusted relationship (romance or friendship) with another person with the intent to request money by using a false situation to create a sense of urgency.

Scam examples: Travel expenses requested for a visit to further the relationship, money requested for medical bills, car or home repairs, family emergencies or to access restricted funds.

ScamClassifier

The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the ScamClassifier model throughout the industry is encouraged, any adoption of the ScamClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the ScamClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Source: fedpaymentsimprovement.org.

Government impostor scam

A person poses as an employee of a government agency, law enforcement, or a trusted authority like a court representative to deceive an authorized party to make a payment or provide sensitive information often based on the potential for negative consequences like arrest, financial penalties or reputational harm.

Scam examples: IRS back taxes, arrest warrant issued, agency penalties or fines, government refund offers, Medicare/benefits coverage offers.

Bank impostor scam

A person poses as a legitimate financial institution, bank department or bank representative to deceive individuals or businesses into revealing confidential banking information or as a bank impostor, instructing a customer to make a payment to protect the customer's money.

Scam examples: Posing as a fraud department, bank security department or bank customer service representative to request funds be moved to a secure account, request login credentials or obtain a one-time passcode from an account holder.

Business impostor scam

A type of deception where an individual poses as a legitimate business, company or brand to deceive a victim into making payments or providing sensitive information.

Scam examples: Tech support, business email compromise (BEC), lottery/prizes, employment offer, adoption scam, advanced fee scam, fake healthcare offers, prepaid funeral expenses, CEO/treasurer impostor, mortgage/title company down payment or closing costs, fake invoice payment scam, airline/travel offer scam, shipping/delivery company scam.

Relative/family/friend scam

A person poses as a family member or someone representing a family member who contacts a relative to request money to help the family member based on a false situation or emergency.

Scam examples: Grandparent scam, fake kidnapping, fake travel issues or accidents, fake arrests.

Other trusted party scam

A person poses as a specific role to engage another person to request money based on a false expectation.

Scam examples: Charity/disaster relief impostor scams, babysitter scam (posing as a potential customer).

Learn more about ScamClassifier model at fedpaymentsimprovement.org

ScamClassifier

The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the ScamClassifier model throughout the industry is encouraged, any adoption of the ScamClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the ScamClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Source: fedpaymentsimprovement.org.

Mastercard standards — issuer reporting

Fraud reporting

A leading challenge in mitigating the proliferation of fraudulent merchants is the lack of standardization around the tracking of the types of scams that consumers are experiencing.

To combat scams more effectively, in Mastercard's Fraud and Loss Database new subtypes are available globally under the broader "Scams" fraud type of Fraud Reason Code 56 – Manipulation of Cardholder (RC56). These subtypes offer finer granularity in tracking and categorizing specific scam patterns, facilitating a more data-driven and targeted focus.

The new subtypes include:

- **Purchase scam — subtype code H**
  A common online shopping fraud where consumers pay for goods or services that are never delivered or are significantly different from what was advertised. Classifying disputes as "Purchase Scams" highlights the need for more stringent merchant vetting and transaction monitoring.
- **Investment scam — subtype code V**
  Fraudsters promote bogus investment opportunities often promising high returns to entice victims to transfer funds. Marking disputes as "Investment Scams" under RC56 helps differentiate these frauds from other commercial disputes and provides clearer data for risk modeling.
- **Advance fee scam — subtype code A**
  Victims are asked to pay an upfront fee in return for a loan, employment, or other promised benefit that never materializes. By recording such incidents under RC56 and labeling them as "Advance Fee" issuers and acquirers gain valuable insight into how these scams originate and how often they occur.
- **Romance scam — subtype code R**
  Fraudsters exploit emotional or romantic connections to request money or valuable information from unsuspecting victims. Labeling disputes such as "Romance Scams" allows issuers to identify emerging patterns in dating platforms or social media environments.
- **Impersonation scam — subtype code I**
  Fraudsters pose as legitimate entities, such as government agencies, charities, corporate representatives, or close family members like a grandchild to trick victims into handing over money or sensitive data. Capturing these scenarios as "Impersonation Scams" helps Mastercard and financial institutions to quickly recognize large-scale events.

By categorizing reported fraud under RC56, issuers promptly alert acquirers and Mastercard to potential fraudulent merchants. This targeted reporting enables Mastercard to track scam-related claims in aggregate, identify patterns of bad actors, and enforce appropriate actions against noncompliant entities. The clarity offered by RC56 also supports faster investigations, better performance of products and services that prevent scams, and more effective industry-wide collaboration in shutting down scam operations. Furthermore, issuers will also be able to select the existing subtype "Unknown" in the Fraud and Loss Database in instances where they are unable to determine the most accurate sub-type.

The diverse scam classifications outlined in the ScamClassifier℠ model align with Mastercard's fraud subtypes, providing a range of use cases for identifying and addressing various scam-related activities. Scam classifications serve various purposes across different industries, helping enhance security, minimize financial losses, and improve user trust.

Chargeback process implications

Issuers must carefully evaluate each scam scenario to determine if the specific nuances of the transaction(s) justify a chargeback under the existing chargeback rules. This involves a thorough assessment of the circumstances surrounding the transaction, including the nature of the scam, the behavior of the merchant, and the documentation provided by the cardholder.

By meticulously analyzing these factors, issuers can ensure that chargebacks are appropriately filed and that the chargeback process remains fair and effective. It is crucial for issuers to adhere to the established guidelines and leverage the available chargeback rules to address fraudulent activities while minimizing the risk of abuse or misuse of the chargeback system. Issuers also want to ensure that they are getting as much evidentiary documentation from the cardholder as possible to prove that the cardholder was scammed by the merchant.

Fighting back against fraudsters

Best practices for acquirers

Acquirers play a pivotal role in ensuring that only legitimate, compliant merchants gain access to the payments ecosystem. By adhering to the requirements in the Mastercard Security Rules and Procedures manual and implementing robust underwriting, monitoring, and education practices, acquirers can reduce the risk of onboarding or maintaining relationships with fraudulent merchants. For acquirer assistance, below are recommended strategies and references to key Mastercard requirements:

Rigorous underwriting processes

- **Enhanced due diligence**

  Verify the merchant's business model, historical payment processing activity, and beneficial ownership. Section 7.1.1 of the Mastercard Security Rules and Procedures manual sets forth minimum requirements for identifying and verifying each merchant.

- **Mastercard MATCH Pro**

  Ensure use of the Mastercard MATCH (Member Alert to Control High-Risk Merchants) Pro system to determine if a prospective merchant has been previously terminated for non-compliance, fraud, or excessive chargebacks. Checking of MATCH Pro and utilization of retroactive MATCH Pro inquiries regularly may prevent re-onboarding of known bad actors.

Merchant site inspections and compliance validation

- **Ongoing website reviews**

  Check the merchant's website or app periodically to confirm it aligns with the information provided during underwriting (e.g., product offerings, terms and conditions, and branding).

- **Prohibited merchants and high-risk MCCs**

  Verify that the merchant's category code (MCC) matches the type of goods or services they provide. Monitor for prohibited or high-risk MCCs, such as illegal gambling or adult content where additional controls and specialty merchant registration is required.

Ongoing merchant monitoring

- **Transaction pattern analysis**

  Implement real-time monitoring tools that track abnormal spikes, suspicious refund patterns, or inconsistent average ticket sizes. Refer to Section 6 of the Mastercard Security Rules and Procedures manual for guidance on additional Acquirer Authorization Monitoring Requirements.

- **Monitoring sub-merchants by payment facilitators**

  As recent large-scale consumer scams have involved payment facilitators managing multiple sub-merchants, each operating hundreds of websites and URLs, making fraud detection more challenging, acquirers should ensure that payment facilitators:

  - Are carefully onboarding and monitoring each sub-merchant's URL using web crawlers, Merchant Monitoring Service Providers, and tools that track adverse media and web traffic flows.
  - Limit the number of URLs a sub-merchant can use, ideally to a maximum of three.
  - Assign a Unique Merchant ID to each sub-merchant for authentication.

Chargeback management

- **Mastercard Acquirer Chargeback Monitoring Program (ACMP)**

  To ensure a positive cardholder experience and protect the Mastercard ecosystem, it is important that acquirers and merchants take swift action when fraud and chargeback levels become excessive. To help acquirers monitor merchants that exceed established thresholds, Mastercard established the Acquirer Chargeback Monitoring Program which includes the Excessive Fraud Merchant (EFM) program and the Excessive Chargeback Program (ECP). Acquirers should align their oversight with program guidelines to identify merchants who exceed chargeback thresholds. When a merchant is flagged, initiate immediate corrective measures such as targeted reviews or hold back reserves to mitigate future potential losses.

- **Ethoca Alerts**

  Leverage Ethoca Alerts to get near real-time notification of incoming disputes and fraud. These solutions enable merchants to proactively address issues before they escalate into chargebacks, helping to reduce dispute volume and financial losses.

Collaboration with issuers and Mastercard

- **Shared fraud intelligence**

  Create direct communication channels with issuers to exchange data on emerging scams or questionable transaction activity. Mastercard encourages all stakeholders to participate in industry consortiums and working groups that address evolving fraud patterns. An acquirer approached by an issuer with a High Impact/Critical Fraud management request is recommended to collaborate with the issuer to the best of its ability as outlined in Section 6 of the Mastercard Security Rules and Procedures manual.

Data security and incident response

- **Payment Card Industry Data Security Standard (PCI DSS) enforcement**

  Ensure that merchants meet the required data security standards for storing, processing, and transmitting cardholder information. If a merchant suffers a data breach, follow the guidelines in the Mastercard Account Data Compromise (ADC) Program and the Security Rules and Procedures to coordinate response efforts and investigations.

- **Incident escalation plans**

  Develop escalation protocols for suspected scam websites, including immediate risk assessments, site take-down procedures, and potential cooperation with law enforcement. Document findings and share relevant intelligence with Mastercard to aid broader ecosystem protection.

Merchant education and awareness

- **Awareness training**

  Provide merchants with easy-to-understand guides on PCI DSS requirements, dispute resolution best practices, and red flags for fraudulent orders. Fraudsters often create new accounts with incomplete or suspicious details, such as random names, free email domains, or mismatched contact information, to place fraudulent orders. They may also generate multiple accounts with slight variations (e.g., similar email addresses or shared phone numbers) to bypass detection and carry out repeat scams.

- **Business review sessions**

  Offer periodic check-ins or webinars on compliance updates, particularly when there are revisions to the Mastercard Publications and relevant Bulletin announcements.

- **Transparency on consequences**

  Clearly communicate that merchants who fail to comply with security rules or who exhibit excessive fraud will face potential fines, account termination, or placement in MATCH Pro.

Best practices for issuers

To protect cardholders and reduce exposure to fraudulent transactions, issuers should implement measures to identify and mitigate fraudulent merchant activity. Adopting some of the following best practices can help issuers strengthen their fraud prevention efforts:

Data driven fraud prevention

- **Real-time fraud detection**

  Employ advanced AI and machine learning solutions to identify unusual cardholder or merchant activity. Immediate alerts to cardholders can mitigate losses. By analyzing transaction velocity, geolocation anomalies, and historical purchase behaviors, issuers reduce false positives and accelerate the detection of genuine threats.

- **Dynamic authorization controls**

  Tailor authorization thresholds based on cardholder profiles and risk factors, declining or flagging high-risk transactions in real time. Adaptive risk scoring, based on transaction location, merchant category, and historic spending patterns, minimizes friction for legitimate transactions while catching unusual activity earlier.

Chargeback and dispute management

- **Speed up the dispute resolution process**

  Issuers should leverage collaborative tools that alert merchants quickly when a cardholder disputes a transaction as fraud. This can help deflect disputes quickly before the costly and time-consuming chargeback process even begins.

- **Coordinated fraud response**

  If an issuer is approached by an acquirer with a High Impact/Critical Fraud management request, they should collaborate with the acquirer to the best of their ability as outlined in Section 6 of the Mastercard Security Rules and Procedures manual.

Consumer awareness and customer engagement

- **Proactive cardholder communication**

  Notify customers of irregular spending patterns via SMS or email. Quick confirmations or denials of suspicious transactions help reduce fraud exposure. Encouraging cardholders to report potential scams promptly not only prevents further unauthorized transactions but also helps issuers obtain metrics to refine risk models.

- **Educate and empower cardholders**

  Offer resources that teach cardholders how to spot scams, secure their personal data, and report questionable charges immediately. Regularly updated educational materials via emails, social media channels, and in-app alerts can keep consumers informed about evolving scam tactics.

- **Overcoming embarrassment and stigma**

  Some cardholders, especially those who fall victim to scams that may feel "obvious" in hindsight, are too embarrassed to admit they were deceived. As a result, they may avoid informing their banks or filing a dispute. Issuers can address this by:

  - **Creating a supportive environment:** Clearly communicate that scam incidents are increasingly sophisticated and that even vigilant cardholders can be targeted.
  - **Dedicated hotlines or points of contact:** Providing confidential and empathetic reporting channels encourages cardholders to come forward without fear of judgment.
  - **Regular awareness campaigns:** Reinforcing the message that timely reporting is crucial for containing fraud and possibly recovering funds, thereby normalizing the act of seeking help.

Preventing scams is crucial in today's digital age. Issuers can communicate some effective strategies to cardholders:

Recognize common scam signs

- **Impersonation:** Scammers often pretend to be from trusted organizations, like government agencies or well-known companies. Be cautious of unsolicited calls or messages.
- **Urgency:** If someone pressures you to act quickly, it's likely a scam. Legitimate businesses will give you time to think.
- **Payment methods:** Be wary of requests for payment via gift cards, cryptocurrency, or wire transfers. These are common red flags.

Protect personal information

- **Don't share unsolicited information:** Never provide personal or financial information in response to unexpected requests. Legitimate organizations won't ask for sensitive information this way.
- **Don't share** a one-time password, PIN, online credentials, or social security number.
- **Verify contacts:** If you receive a suspicious message, contact the organization directly using a known phone number or website.

Use technology wisely

- **Strong passwords:** Use complex passwords and change them regularly. Consider using a password manager.
- **Two-factor authentication:** Enable this feature on sensitive accounts for an extra layer of security.

Stay informed

- **Educate yourself:** Familiarize yourself with common scams and how they operate. Knowledge is a powerful tool against fraud.

Here are some of the **latest consumer scams** to be aware of:

AI-powered scams: Scammers are increasingly using artificial intelligence to create more convincing phishing emails and deepfakes. This includes impersonating friends or relatives to solicit money or impersonating employers to extract personal information.[8]

Student loan forgiveness scams: With ongoing changes in student loan policies, scammers are exploiting this by creating fake application sites or making unsolicited calls, often asking for personal information or fees to process loan forgiveness applications. Remember, applying for forgiveness should never require a fee.

Phone scams: These include robocalls that can sound surprisingly natural, impersonation scams where callers pose as IRS agents or delivery personnel, and attempts to install malicious apps. Be cautious of any unsolicited calls asking for personal information.

Person to person (P2P) scams: Scammers are targeting users of payment apps by pretending to be bank representatives. They may instruct you to send money to yourself to "fix" a supposed issue, but the money actually goes to the scammer.

Disaster relief scams: Scammers pretending to be charitable organizations. Look into the agency to which donations are being provided to ensure it is legitimate.

Text message scams (Smishing): Text scams are on the rise, with scammers impersonating banks or delivery services to trick you into clicking links or providing personal information.

Gift card scams: Do not put money on a gift card and give someone the card number.

Wire transfer fraud: Know the person you are sending money too. Fraudsters will tell you to wire money to them.

QR code scams: While QR codes are convenient, scammers are placing fake codes that lead to malicious sites or prompt unauthorized purchases. Always verify the source before scanning.

What to do if you encounter a scam

- **Report it:** If you suspect a scam, report it to the Federal Trade Commission (FTC) or your local consumer protection agency.
- **Talk to someone you trust:** If something feels off, discuss it with a friend or family member. They might provide a different perspective and help you see potential red flags.
- **Stay informed:** Regularly check resources like the FTC's website for updates on common scams and prevention tips.

By staying vigilant and informed, you can significantly reduce your risk.

8. Experian, The Latest Scams You Need to Be Aware of in 2025.

How Mastercard is helping

Scam Protect

Mastercard continues its ongoing efforts of safeguarding the payments ecosystem, providing stakeholders with a variety of tools, guidelines, and educational resources to keep pace with rapidly evolving scam tactics. In April 2024, Mastercard announced Scam Protect, an initiative designed to transform the fight against scams by delivering an end-to-end framework that protects stakeholders across a growing spectrum of fraudulent schemes. This program is built on three core pillars:

- **Technology solutions**

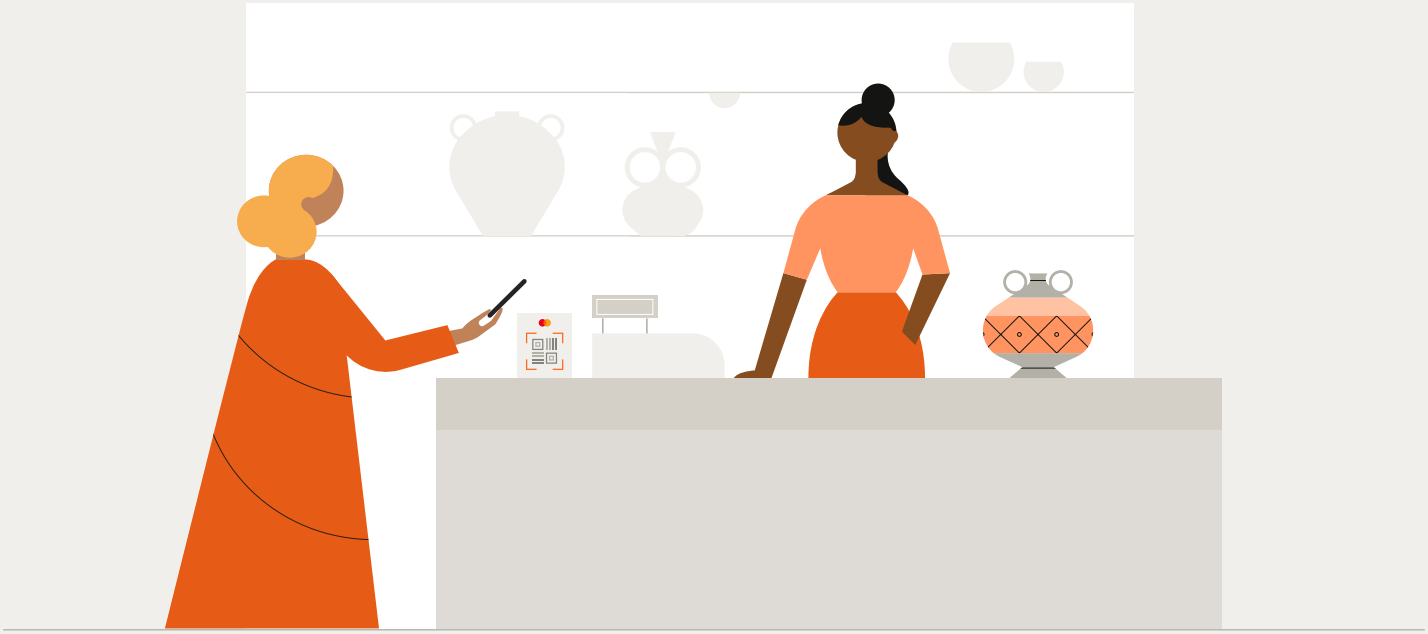
  Powered by cutting-edge AI, Mastercard's suite of specialized solutions helps identify suspicious transaction patterns and block scams in real time. By leveraging the global scale of Mastercard's network data, these tools offer insights into emerging fraud typologies, ensuring that stakeholders can rapidly adapt to new threats.

- **Market education**

  Recognizing that consumer awareness is crucial in preventing scams, Mastercard works with and through a network of collaborators to share knowledge, training, and tools. These educational resources empower financial institutions and consumers to adopt safer practices while also working to remove the stigma of fraud victimization, creating a supportive environment that encourages prompt reporting and proactive prevention.

- **Industry collaboration**

  Mastercard proactively partners with organizations operating across various industries to prevent scams ensuring that payments remain safe for all participants.



Technology solutions

At Mastercard, we've been developing and using AI for two decades. Our AI models are trained on our global network intelligence, one of the largest payments data sets in the world, making their projections both powerful and accurate. Mastercard marries the transformative potential of AI with responsible development and deployment through our guiding principles, governing framework, and ongoing responsibility initiatives. Our teams embed privacy and responsibility safeguards into the design and creation of all our products and services, so you and your customers know your data is safeguarded.

Mastercard's unique and comprehensive suite of AI-powered solutions can help identify and prevent scams at all stages of a scam lifecycle from merchant onboarding to when a user carries out a transaction. We are continuously investing in product development to consistently improve the efficacy of our data and capabilities to detect and combat scams.

Acquirer tools

Mastercard equips acquirers with a comprehensive set of tools to assess and manage merchant risk, both during onboarding and through ongoing monitoring. These tools are provided via various delivery methods, including a user-friendly dashboard and authorization message responses, to facilitate effective risk management and monitoring.

Onboarding capabilities

- **Onboard Risk Check:** Provides a centralized and comprehensive view of potential merchant risk, enabling acquirers to make faster, more efficient and informed merchant onboarding decisions. Acquirers can augment existing risk management tools by identifying potential vulnerabilities within a merchant's online environment and improving merchant underwriting.
- **MID Check:** Leveraging Mastercard's data resources, MID Check assigns a score based on a merchant's historical risk factors, allowing acquirers to incorporate additional intelligence into their onboarding assessments. This helps filter out known scam operations or merchants with patterns of non-compliance.

Ongoing monitoring capabilities

- **Merchant Risk Predict (MRP):** Offers segmented risk perspectives, in which Ghost Merchant and Merchant Fraud Attrition specifically highlight scam risk. The Ghost Merchant score gauges the likelihood of a brand-new merchant account existing solely for short-term fraud, while the Merchant Fraud Attrition score addresses established merchants that may pivot into scam activity. MRP scores appear within the authorization response for dual-message transactions as well as in a dashboard, enabling acquirers to spot warning signs in real time.
- **Small Business Credit Analytics (SBCA):** SBCA provides weekly metrics and monthly benchmarks related to merchant transaction volume, channels, and cyclical spending patterns. This granular view assists acquirers in constructing detailed risk profiles and spotting abnormal shifts indicative of potential scams.

Many of these onboarding and ongoing monitoring capabilities are offered through Mastercard's Acquirer Security Program (ASP).

Issuer tools

Effective decision-making is key to managing fraud risks, especially in identifying scam fraud patterns. Issuers should use advanced decision models that assess transaction risk in real time to effectively combat fraud, optimize the approval process, and enhance authentication measures. By incorporating real-time risk analysis, issuers can ensure that each transaction is thoroughly vetted, while simultaneously strengthening authentication to confirm the legitimacy of the cardholder, leading to a more secure and seamless experience.

Authentication capabilities

Mastercard's Smart Authentication platform considers a merchant's fraud history, tracking those with a significant record of fraud, to provide risk-based recommendations. This information influences the transaction scores assigned which in turn impacts the score provided to issuers via their ACS server (3DS), as well as the Digital Transaction Insights score utilized during the authorization process.

Transaction fraud and decisioning capabilities

Mastercard Transaction Fraud & Decisioning tools leverage advanced AI technology and insights from Mastercard's global network-level consortium:

- **Decision Intelligence (DI):** Offers real-time decision scoring, unique cardholder and transaction-level insights, and reason codes to contextualize risk. DI's AI models evaluate thousands of data points from Mastercard's network-level consortium, including historical and real-time merchant insights (such as average ticket, fraud rate, velocity count).
- **Fraud Rule Manager:** Comprehensive fraud mitigation rule writing solution that empowers issuers to manage their fraud strategy with the best-in-class rules, cases, and performance insights.
- **Rule Discovery Tool:** A tool that optimizes the fraud mitigation rule writing process and generates actionable results. It provides a data visualization interface with a navigable workflow that enables refining of rules. Each visual within the tool's dashboard acts as a rule condition.

Mastercard's On Behalf Rules Services help issuers maximize the value of Mastercard's decisioning solutions through seamless implementation of fraud mitigation rules. The team creates and maintains consortium-based Rule Cartridges to address regional fraud trends and challenges, ensuring issuers can navigate evolving risk landscapes.

In addition to region-specific cartridges, the team has developed standalone Rule Cartridges targeting specific fraud vulnerabilities. Currently, there are two available: The Money Transfer Cartridge and the Authentication Cartridge. A new cartridge is being developed to detect suspicious merchant activities with high-risk patterns.

Market education

Guidance and training: Mastercard recognizes that education for acquirers, issuers, merchants, and consumers is one of the most effective strategies against fraudulent merchant operations. Mastercard offers training programs and resources that support each stakeholder in understanding and responding to emerging threats.

Key initiatives and platforms include:

Mastercard Academy

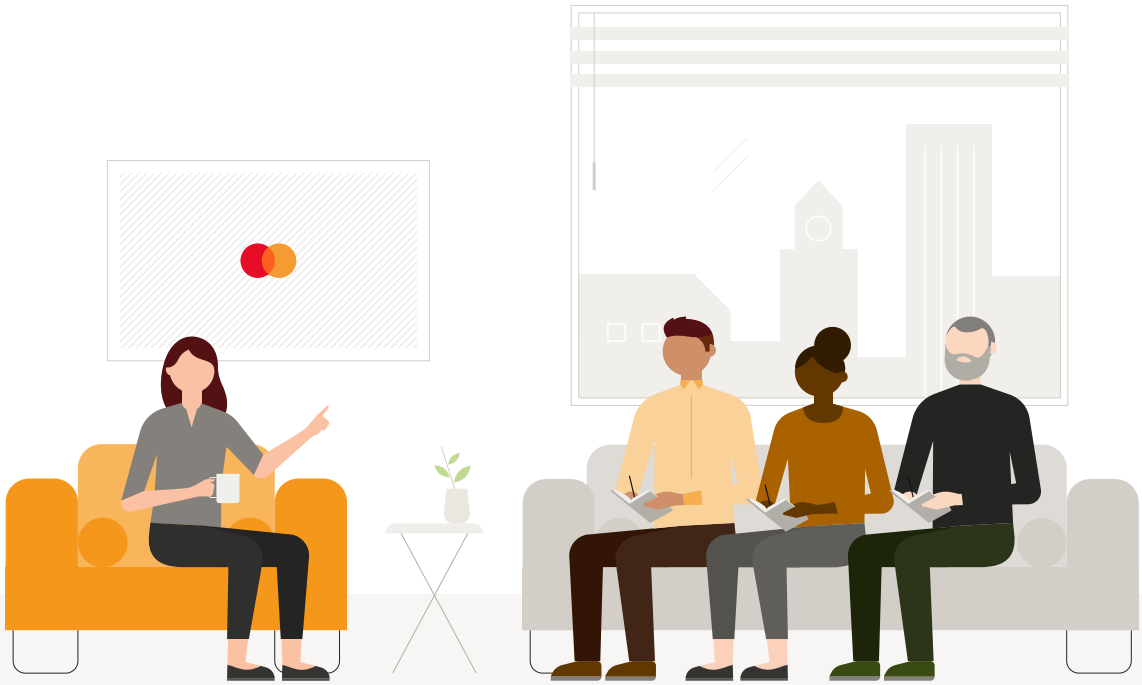
- **Structured learning pathways:** Through the Mastercard Academy, participants can enroll in a series of targeted courses designed to cover a spectrum of topics ranging from the fundamentals of card acceptance and fraud prevention to dispute resolution management.
- **Emerging fraud trends:** Regularly scheduled webinars highlight emerging methods used by fraudulent merchants, such as phishing, friendly fraud, and advanced account takeover while offering best practices for early identification.

Franchise and consulting services

- **Franchise Customized Partner Engagements:** Drawing on Mastercard's expertise, financial institutions can receive specialized training that addresses various fraud risks. This includes strategies for dispute resolution optimization, as well as ensuring compliance with Mastercard Standards along with best practices for implementing uniform security measures.
- **Mastercard Advisors Consulting:** Provides support in the development of a scam prevention strategy, including communication tactics and detection techniques.

Marketing services

- **Security Awareness Acceleration Marketing (SAAM) program:** Helps issuers warn end consumers against critical security risks and educate them about the best ways to prevent impact. SAAM comes as a safety and security themed communication toolkit, delivered quarterly and consistent with multiple assets, including:
  - **Turnkey email and social media templates** that can be easily adjusted to host Issuers' logo and distinctive branding elements;
  - **A deployment playbook** with detailed instructions on how to leverage the turnkey assets;
  - **Webinars** to help issuers stay on top of key trends and latest updates on the program features.
- **Customer education:** Marketing Services can also design a custom communication program based on the financial institution's needs to educate consumers and employees on critical scams and security threats.



Industry collaboration

Mastercard collaborates across industries, partners, and organizations worldwide to secure the digital ecosystem, ensuring payments are safe for all. Combating the growing threat of scams demands a collective effort. Some notable efforts include:

- Mastercard is a Foundation member of the Global Anti-Scam Alliance, which aims to protect consumers worldwide against scams. Together with the Global Anti-Scam Alliance, Mastercard shares knowledge and defines joint actions to advocate for safe and secure ways to transact, interact, and protect consumers.
- Mastercard is also an inaugural member of the Aspen Institute Financial Security Program (Aspen FSP) National Task Force for Fraud and Scam Prevention, an initiative that brings together leading stakeholders from government, law enforcement, private industry, and civil society to develop a nation-wide strategy aimed at helping prevent fraud and scams in the U.S. The Task Force builds on and advances participant organizations' work to address fraud and scams by strengthening consumer advocacy and education, improving information-sharing mechanisms, and advancing technology and policy solutions.
- The United Nations Development Programme (UNDP) and Mastercard have signed a Memorandum of Understanding to collaborate towards deepening the understanding of the impact of digital scams, and ways to detect and address them.

Compliance and Standards

Mastercard plays a crucial role in maintaining the integrity of the global payments ecosystem by enforcing its compliance programs and security standards that help identify, prevent, and eliminate fraudulent merchant activity. These standards ensure that acquirers and merchants adhere to policies that protect consumers, reduce fraud, and maintain trust in digital transactions.

Rules and compliance: Mastercard employs a multi-layered enforcement strategy to ensure that acquirers and issuers quickly identify, monitor, and take action against merchants engaging in fraudulent or scam-like behavior. Through programs such as the Acquirer Chargeback Monitoring Program (ACMP), Business Risk Assessment and Mitigation (BRAM), and various global investigation initiatives, Mastercard enforces compliance, reduces financial risk, and protects consumers from deceptive merchants. Violations of the Mastercard Standards may lead to potential assessments, stricter monitoring, or request of termination of merchant accounts.

Conclusion: How to build trust

Building and maintaining trust in the digital payments ecosystem is a multi-faceted effort that requires ongoing vigilance, collaboration, and innovation from all industry participants, from Mastercard to merchants, issuers, acquirers, payment networks, and regulators alike. The scope and sophistication of fraudulent merchant activity demonstrates that the industry must adopt a holistic framework that addresses prevention, detection, enforcement, and education.

A crucial component of this framework involves coordination among stakeholders. Mastercard plays a critical role in setting guidelines, establishing rules, and providing tools that help card issuers and acquirers detect anomalies, identify scam patterns, and take decisive action. Collaboration extends further when cross-industry alliances, such as the Global Anti-Scam Alliance, Aspen FSP National Taskforce for Fraud and Scam Prevention and the Federal Reserve Bank's initiative to develop the ScamClassifier℠ model, come into play. These partnerships unify and standardize definitions of scams, streamline data sharing, and empower institutions to detect threats more quickly, ultimately reinforcing consumer protection.

In addition to following the guidance and mandates of Mastercard, financial institutions should remain informed about emerging national or regional frameworks, such as the Federal Reserve's cross-industry working group that standardize scam definitions and reporting practices. When all parties adhere to a shared set of best practices, fraudsters have fewer gaps to exploit.

Finally, trust is sustained through continuous evolution. Scam methods will keep adapting as technology advances. The payments ecosystem must respond by refining strategies, enhancing collaboration channels, and adopting solutions that can scale to meet new fraud scenarios. By focusing on transparency, consumer education, cross-sector coordination, and innovative security technologies, the industry can build and preserve a resilient, trustworthy environment in which digital commerce thrives. In doing so, legitimate participants are protected, consumer confidence remains high, and the collective fight against fraudulent merchants becomes progressively more effective.

Final thoughts

While industry efforts, supported by stringent rules, best practices, and advanced technology, have helped mitigate some scam websites and fraudulent activity, significant challenges remain. As fraudsters continue to evolve their tactics, ongoing vigilance and adaptation are essential to staying ahead of emerging threats.

Mastercard's suite of tools, combined with the industry's commitment to following best practices, sets a foundation for tackling fraud. By maintaining transparency, investing in detection and prevention measures, and prioritizing education, the payment ecosystem can grow securely, ensuring that trust is reinforced at every step of the transaction journey. Together we can sustain a secure, reliable environment where consumers and business alike can thrive.