Visa Public

VISA SCAM DISRUPTION

# Detecting, investigating, and disrupting scams

Using advanced technologies and partnerships with financial institutions and law enforcement to proactively investigate and dismantle scam operations.

# Executive Summary

The Visa Scam Disruption (VSD) initiative is a comprehensive effort aimed at protecting consumers and organizations within the payments ecosystem from various scam operations. By leveraging advanced technologies, strategic partnerships, and a multidisciplinary team, VSD proactively investigates and dismantles scam networks to stop further impacts to payments organizations

- **Advanced Detection Methods:** Utilizing a multi-layered approach, VSD employs client-reported scams, dark web intelligence, and proprietary technologies to identify scam signals and fraudulent merchant processing patterns. Generative AI modeling powered by Visa's network-level data helps detect complex scam behaviors and uncover hidden relationships at scale.
- **Proactive Investigations**: VSD's investigations are driven by Visa's proprietary network-level technology, which analyzes merchant transaction patterns to uncover scam activity. Specialized tools and partnerships expand visibility into scam infrastructure, while intelligence platforms and subject matter experts assign threat actor attribution to tangible fraud losses.
- **Actionable Intelligence**: VSD delivers tailored intelligence referrals through global and regional collaboration, enabling clients to take informed action against scam activity. Impacted clients receive bespoke alerts detailing the nature of the scam, recommended remediation steps, and ongoing support through direct engagement with the VSD team.
- **Significant Impact**: VSD has identified more than $1.6 billion in fraud attempts since its inception just a year ago. As a result, we've worked closely with our clients and law enforcement to dismantle more than 25,000 scam merchants.

The VSD initiative not only strengthens ecosystem-wide defenses but also protects cardholders by reducing exposure to fraudulent merchants and scam tactics. Through intelligence sharing and alerts, clients can understand emerging threats and take early action to prevent widespread fraud. We're not stopping there; to help fight scams we've strengthened one of our core ecosystem protection programs — the Visa Integrity Risk Program — to further support our client banks in their detection of deceptive merchant practices. Combatting scams requires collaboration across the entire ecosystem and a 360-degree approach that places equal, if not greater, emphasis on prevention as on mitigation.

© 2025 Visa. All rights reserved.

# The State of Scams

Scammers in the payments ecosystem are increasingly targeting cardholders directly, using sophisticated techniques to exploit trust and urgency. With the rise of AI-driven tools, fraudsters can now craft highly convincing phishing messages, deepfake voices, images, and videos, and realistic fake websites that mimic legitimate institutions. This technological leap has made it harder for consumers to distinguish real from fraudulent activity, amplifying the risk of financial and personal data loss.

## Impacts and emerging trends in scams

eCommerce scammers create fake online stores or intercept legitimate transactions to trick cardholders into paying for goods that never arrive.

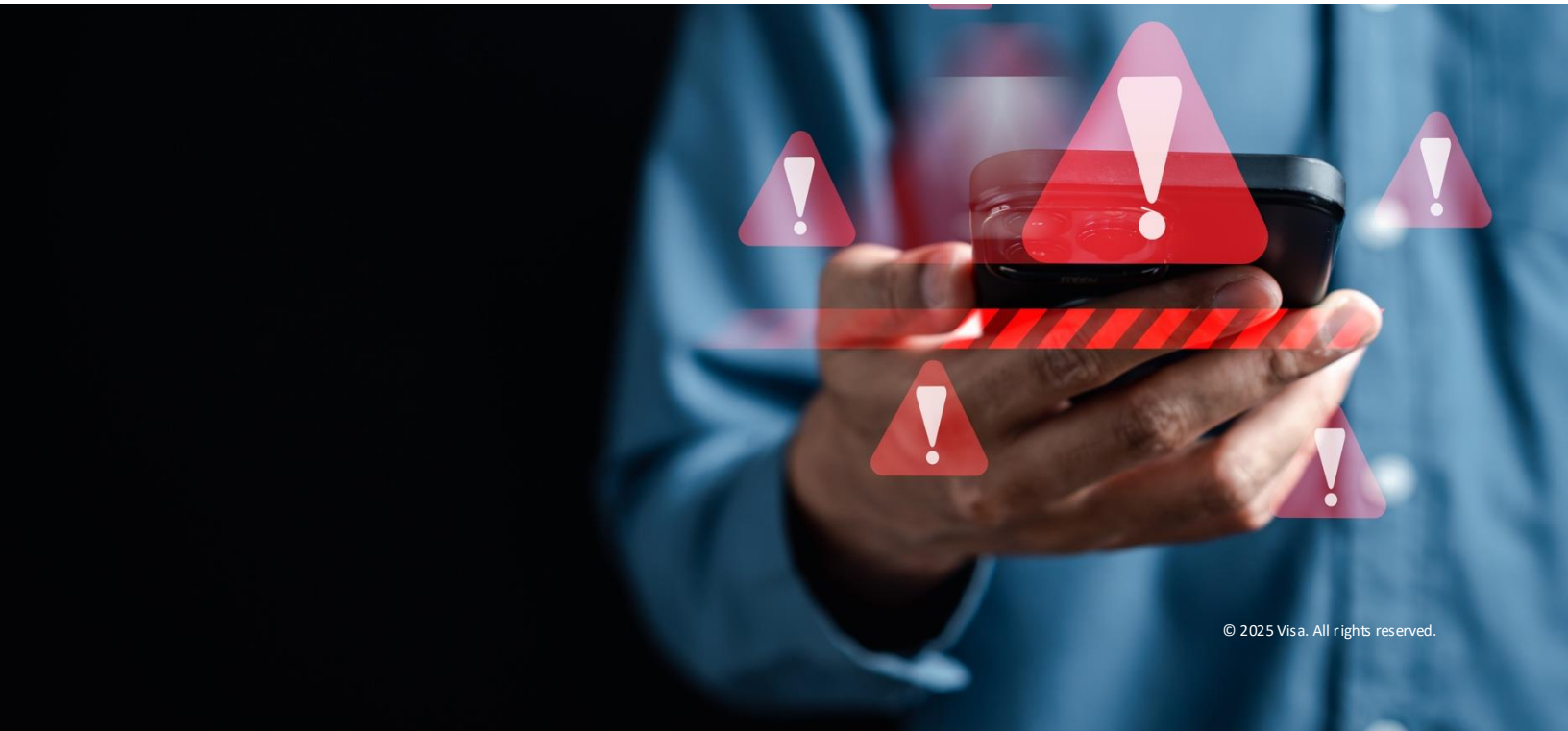
Fraudsters pose as government officials or agencies, often using urgent language to pressure cardholders into sharing sensitive information or making payments.

Deep fake AI-generated audio or video is used to convincingly mimic trusted individuals, leading cardholders to believe fraudulent requests are legitimate.

Social engineering and phishing operations that weaponize AI to mimic real people

Scammers exploit social media platforms to spread phishing links, impersonate friends or influencers, and lure cardholders into giveaways or investment traps.

Criminals spoof bank communications—emails, texts, or calls—to convince cardholders to verify accounts or authorize fraudulent transfers.



© 2025 Visa. All rights reserved.

## Introducing Visa Scam Disruption

Visa Scam Disruption (VSD) is a comprehensive initiative designed to protect consumers and organizations across the payments ecosystem by harnessing Visa's advanced technologies, deep expertise, and strategic partnerships.

It combines proactive scam investigations, cutting-edge detection tools, and a multidisciplinary team—including AI developers, former law enforcement, and threat analysts—to identify and mitigate scams before they cause significant harm. Through collaboration with financial institutions, law enforcement, and third-party partners, VSD works to dismantle scam networks at their source and help prevent future fraudulent activity.

### Visa Scam Disruption helps:

Identify and mitigate scams early through proactive investigations and proprietary technologies

Links scam infrastructure to fraud by attributing losses and driving enforcement

Acts on intelligence through alerts, referrals, and law enforcement engagement to disrupt scam operations

## Visa Scam Disruption: How it works

### Detection

VSD begins by identifying scams through transaction monitoring, intelligence collection and proprietary technology, tracking suspicious activity using structured case management and incident response protocols.

This early detection helps surface emerging threats before they escalate.

### Investigation & Analysis

VSD investigates scam patterns and infrastructure through open-source research, dark web intelligence, transaction analysis, and collaboration with internal and external partners.

Attribution links fraudulent behavior to infrastructure and quantifies losses through evidence-based reporting.

### Intelligence Action & Reporting

VSD transforms insights into action by publishing security alerts, acquirer referrals, and law enforcement escalations based on the impact of scam activity.

These efforts help disrupt scam operations and strengthen defenses across the payments ecosystem.

Visa Scam Disruption identifies emerging scams, investigates their infrastructure and patterns, and transforms intelligence into actionable steps to protect the ecosystem.

© 2025 Visa. All rights reserved.

## Advanced, multi-layered scam detection:


**Transaction monitoring**
To identify merchant history, suspicious patterns, and processing information

**Client reporting**
Allows VSD to collaborate with clients and provide a channel to report scam activity

**Dark Web monitoring**
To identify new and emerging scams, threat actors chatter, and the sale of scam infrastructure

**Threat Intelligence**
On emerging threats in payments ecosystem

**Proactive threat hunting**
Enabling VSD to identify new scams before they expand throughout the ecosystem

**Gen AI modeling**
Based on Visa network level data and Gen AI insights to proactively identify scam merchants in the ecosystem

## Objectives and scope: Visa's commitment to clients with Visa Scam Disruption

Visa Scam Disruption (VSD) is committed to protecting clients by proactively identifying and dismantling scam operations across the payments ecosystem. The Visa Scam Disruption practice has identified more than $1.6 billion in fraud attempts since its inception just a year ago. As a result, we've worked closely with our clients and law enforcement to dismantle more than 25,000 scam merchants. These efforts help Visa deliver actionable intelligence and strengthen defenses for financial institutions and consumers.

Visa continues to invest in proprietary technologies to help clients stay ahead of evolving scam tactics and strengthen theirdefenses.

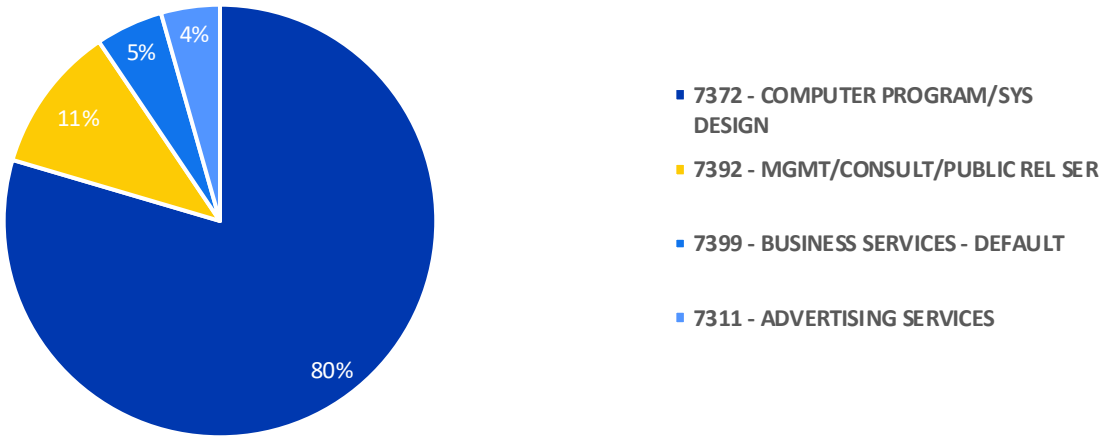

© 2025 Visa. All rights reserved.

# Illustrative use cases

## Marketing Scams

VSD investigated a sophisticated marketing scam targeting individuals attempting to start online businesses. Fraudsters charged victims thousands of dollars for business setup services, coerced them into opening new credit accounts, and misused their personal information to apply for credit cards and enroll them in recurring billing schemes. The scam was identified by an issuing client who identified suspicious merchant activity, including high-dollar charges on newly opened credit lines and recurring billing activity. Victims were often exposed via social media ads, and the scam involved collusive marketing companies that misled victims over several months. VSD worked with clients to flag anomalous activity, enforce merchant monitoring protocols, and educate clients on scam indicators. VSD also engaged with Law Enforcement to help disrupt threat actor operations. Recommendations included real-time authorization monitoring, velocity checks, and use of tools like Visa Merchant Screening Service (VMSS) to prevent onboarding of fraudulent merchants.

Top 4 MCCs Observed in Marketing Scams by Volume




Visa Scam Disruption incorporates unique data from scam cases—such as merchant behavior, infrastructure patterns, and transaction signals—into its detection models. Using Generative AI and proprietary modeling, VSD proactively identifies similar scam merchants across the network, enabling earlier intervention and stronger protection for clients and cardholders.

## Investigation Results

Following Visa Scam Disruptions comprehensive investigation, and close cooperation with our acquiring clients, the merchants accounts were terminated and removed from the payments ecosystem.

## *Attempted Fraud Detected

# ~$62.74M

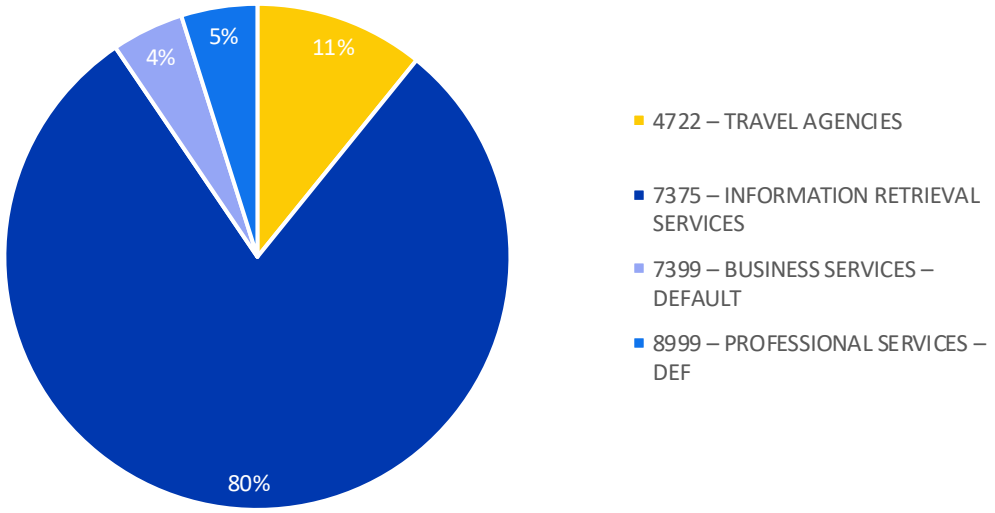
*Presumed fraud is based on the full authorized payment volume of all merchants involved in a scam over the past six months, while confirmed fraud reflects only the TC40-reported volume

© 2025 Visa. All rights reserved.

## Government Impersonation

Government impersonation scams—fraudulent schemes that mimic official agencies to extract money or sensitive data—have surged dramatically in recent years, with the FTC reporting over 160,000 such scams in 2023 alone, resulting in $618 million in losses. Visa Scam Disruption detected several of these scams, including one involving a merchant impersonating the US Treasury's FinCEN platform for Beneficial Ownership Information Reports. The site used domain spoofing, visual impersonation, and social engineering to deceive business owners into paying $149–$350 for a service that is free through the legitimate government portal. Sites like this exploit regulatory confusion and urgency to mislead users, harvest sensitive data, and erode trust in digital government services—contributing to the $1.1 billion in combined losses from business and government impersonation scams in 2023, more than triple the amount reported in 2020. Visa Scam Disruption identified this scam early through network monitoring and worked directly with acquiring partners to investigate the merchant's activity and terminate its access to the payment ecosystem. This case highlights the critical role of proactive fraud detection and acquirer collaboration in disrupting scams before they scale.

Top 4 MCCs Observed in Government Impersonation Scams by Volume




Visa Scam Disruption can detect scam merchants early and work with clients to remove scam merchants from the ecosystem.

### Tactics and Techniques:

- Domain spoofing
- Social engineering
- Illicit search engine optimization
- Data harvesting
- Phishing

### *Attempted Fraud Detected:

~$40.98M

### Shared intelligence could include:

- An acquirer referral explaining the scam and how it is impacting their portfolio
- Investigations team coordinates one on one meetings with acquirers to discuss contents of the referral
- Acquirer should investigate the referral, confirm if the merchant is fraudulent and take the necessary remediation steps

*Presumed fraud is based on the full authorized payment volume of all merchants involved in a scam over the past six months, while confirmed fraud reflects only the TC40-reported volume

© 2025 Visa. All rights reserved.

# Scam Mitigation Best Practices

## Issuer Best Practices

- Monitor authorizations in real time to detect unusual transactions.
- Flag merchants with high fraud rates and report fraud to Visa using TC40.
- Watch for large or unusual transactions on new credit lines, especially when limits are quickly reached.
- Apply enhanced fraud screening for common scam Merchant Category Codes (MCC)
- Educate cardholders on safely sharing payment information.

## Acquirer Best Practices

- Use proper tools to detect and decline fraudulent merchant applications in underwriting.
- Adopt the Auto-Boarding Best Practices.
- Use velocity checks to detect sudden surges in new applications or applications with similar characteristics and shared personal information.
- Upon detection of suspect activity, consider suspending merchant's settlement funding until properly investigated.
- Act timely on merchants generating excessive fraud advices and/or disputes.

© 2025 Visa. All rights reserved.