

Biannual Threats Report

Fall 2026

A Payment Ecosystem Report by

Visa Payment Ecosystem Risk and Control

Table of Contents

1 Advanced Intrusion
2 Executive Summary
3 Increased **Sophistication** of Fraud Attacks
9 Increased **Scale** of Fraud Attacks
17 Increased **Precision** of Fraud Attacks
27 How Visa Helps



Advanced Intrusion: AI-Enabled Threats Across the Payment Lifecycle

Visa Payment Ecosystem Risk and Control (PERC) continues its mission to safeguard the global payments ecosystem from evolving threats. Over the prior six-month period (Jan-June 2026), the landscape of fraud and cybercrime threats saw a continuation of trends in large-scale scam activities and ransomware incidents, precise enumeration and token provisioning attacks, and threat actors' interest in the malicious use of artificial intelligence (AI) to facilitate sophisticated fraud and cybercrime operations. Overall, Visa PERC observed a common theme of threat actors leveraging AI tools throughout their operations, leading to a new definition of AI: Advanced Intrusion. AI is not inherently harmful; rather, risk arises when bad actors misuse it or when it is deployed without appropriate safeguards. In this context, AI has allowed threat actors to increase the sophistication, scale and precision of fraud attacks. These fraud attack techniques observed by Visa PERC are not new, but rather enhanced with AI, providing threat actors with advanced intrusion capabilities, regardless of their available resources, expertise or geographic location. This report provides an overview of how threat actors have conducted "Advanced Intrusion" attacks in the previous six months. Some of the notable findings in this report include:

© 2026 Visa. All rights reserved. Visa Public



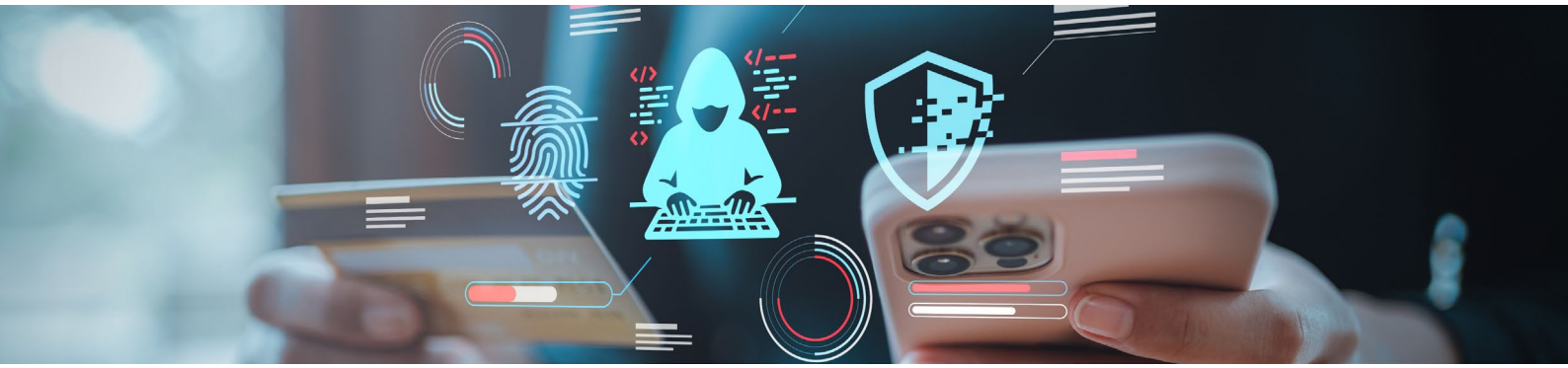
Third-party providers have become high-value force multipliers. Cybercriminals increasingly target payment processors, eCommerce platforms, and other third-party providers because one successful intrusion can expose numerous downstream merchants and millions of potential payment accounts. Third-party agent incidents increased **62%** vs. the prior six months.

Fraud attacks are operating at greater scale and geographic reach. AI-enabled translation, synthetic identities, deepfakes, automated phishing, and scalable infrastructure allow ransomware groups and scam networks to target large victim populations across languages and regions simultaneously. Visa Scam Disruption (VSD) identified more than **US$1.4B in attempted fraud**, a **40% increase** over the prior six-month period.

Attack tactics are becoming more precise and control-aware. Threat actors are probing authorization, authentication, token-provisioning, and eCommerce environments to discover specific processing gaps, including invalid or missing CVV2 handling, velocity thresholds, tokenization controls, and low-friction transaction pathways. These insights allow attackers to tailor transaction timing, values, merchants, and cashout methods to avoid detection.

AI is accelerating the full attack lifecycle. Threat actors are using AI agents and advanced models to automate reconnaissance, identify vulnerabilities, generate or refine malicious code, adapt tactics in real time, and execute multi-stage intrusions with significantly less human involvement.

Defenses must become adaptive, proactive, and AI-enabled. Static controls are increasingly insufficient against autonomous attacks that continuously test and modify their behavior. Visa is responding by "fighting AI with AI," to identify probing activity, simulate emerging fraud scenarios, and remediate vulnerabilities before they are exploited at scale.



Executive Summary

During the first half of 2026, Visa PERC observed a significant evolution in the payments threat landscape as cybercriminals increasingly leveraged AI tools, agentic systems, and advanced automation to conduct more sophisticated fraud attacks across the global payments ecosystem. Rather than relying on opportunistic attacks, threat actors focused on identifying specific vulnerabilities, misconfigurations, and weak points within payment processes, authentication systems, and third-party service providers. This shift enabled threat actors to execute advanced intrusions against organizations that serve as payments ecosystem force multipliers, including payment processors, cloud providers, hospitality technology vendors, and eCommerce platforms. As a result, large-scale compromises exposed millions of payment accounts and potentially indicate how a single successful intrusion can create downstream impacts across hundreds of organizations.

At the same time, Visa PERC saw AI dramatically increasing the scale, speed, and precision of fraud operations. Threat actors used AI to automate reconnaissance, generate convincing phishing and social engineering campaigns, conduct fraud probing against authorization systems, and identify exploitable gaps in token provisioning, authentication, and payment processing controls. Large ransomware groups, industrialized scam networks, and payment fraud actors benefited from these capabilities, allowing them to conduct attacks across multiple regions and languages simultaneously while continuously adapting tactics to evade detection. Visa PERC assesses that the convergence of AI-driven automation, advanced intrusion techniques, and increasingly precise fraud targeting represents a fundamental shift in cybercriminal operations.

© 2026 Visa. All rights reserved. Visa Public

Increased Sophistication of Fraud Attacks

Over this last six-month period, Visa PERC has observed threat actors conducting more sophisticated fraud attacks across the entire global payments ecosystem. These advanced attacks have, in large part, been facilitated through the deployment of AI tools and models to assist threat actors with performing reconnaissance on victims and identifying potential vulnerabilities which can be exploited as initial attack vectors. Namely, cybercriminals have focused on targeting third-party providers and other entities across the supply chain that provide services to numerous downstream merchants or process payments for multiple entities in order to compromise payment account data and perform fraudulent activities.

Compromised Account Fraud

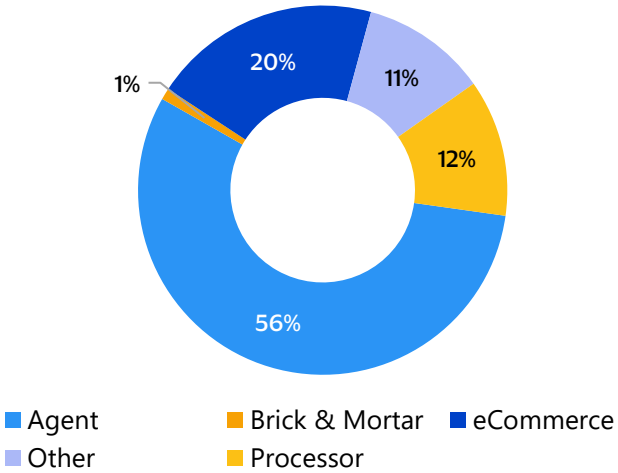
Evolving Threat Landscape



Over the six-month period of Jan-June 2026, Visa PERC observed new tactics used by threat actors to compromise payment account data with threat actors heavily targeting third-party providers or third-party agents who provide payment or eCommerce platform and other technology services across the payments ecosystem. Threat actors have become more sophisticated in how they attack vulnerable third-party providers to obtain access to the largest population of payment account data for the least required effort as noted by third-party agent related incidents increasing 62% when compared to the prior six months. Additionally, Visa PERC identified systemic eCommerce platform risks posed by merchants onboarded to eCommerce platforms that lacked sufficient merchant vetting practices, monitoring and enforcement controls. These risks impact acquirers, processors and the greater ecosystem as they provide threat actors with the opportunity to incorporate fake or otherwise collusive merchants into the payments ecosystem.

Lastly, Visa PERC investigated and actioned several large data breaches where millions of recovered accounts were analyzed and distributed by Visa PERC to clients. When compared to the prior six-month period, the total number of recovered Primary Account Numbers (PANs) from data breaches increased over 1,200% from the Jan-June 2026 period. Recovered payment accounts were the primary driver of compromised PANs during this period versus other methods, such as merchant compromise or network intrusion. When payment accounts are compromised, the Visa Global Risk Investigations team (GRI) manages the payment data breach process, notifying clients when Visa identifies compromised and recovered accounts.

Percentage of Compromised PANs by Entity Type

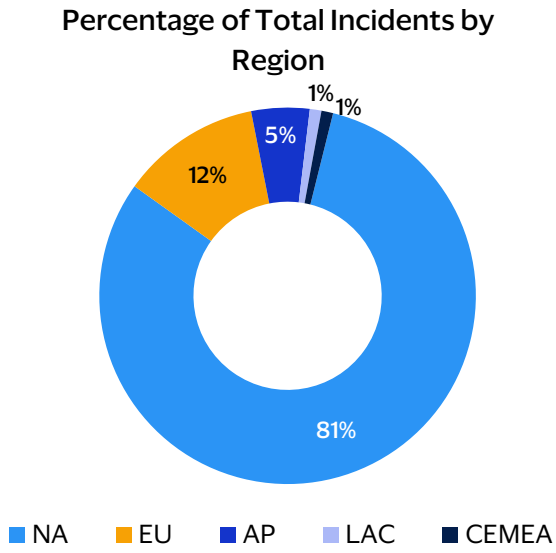


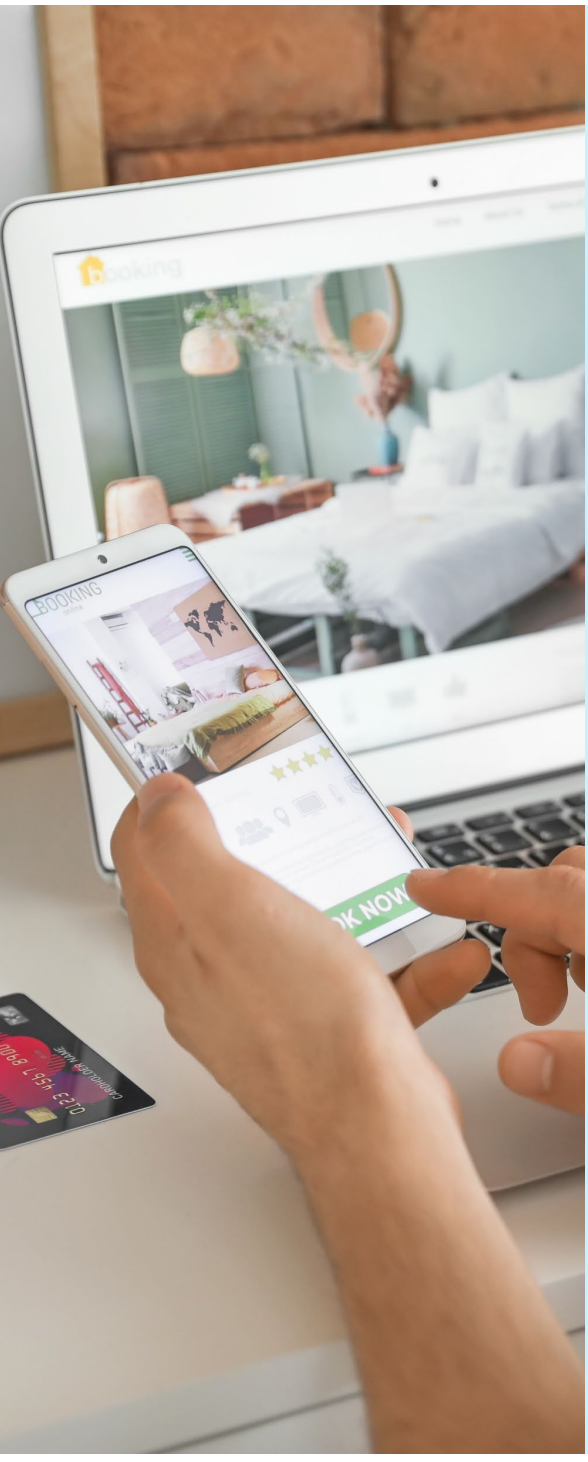
Fraud Trends in Compromised Accounts

In Visa PERC's continued efforts to protect the payments ecosystem from threat actors' efforts to compromise payment account data, Visa PERC investigated several data breach incidents and reported potentially compromised payment accounts to impacted issuers. The targeting of third-party providers and agents during Jan-June 2026 accounted for approximately 56% of the total compromised PANs.. This is likely because threat actors are able to obtain a high number of potentially valid payment accounts by attacking one organization versus targeting several merchants. The targeting of third-party providers and agents will likely continue as threat actors will seek to obtain the highest amount of PANs with the least amount of effort.

© 2026 Visa. All rights reserved. Visa Public

Across the globe, the GRI team investigated incidents mostly stemming from data breaches or compromises of US-based organizations and entities, with North America (NA) accounting for 81% of the total compromises investigated by GRI where PAN data was at-risk. The next highest region, EU, only had 12% of incidents and the AP region had 5%. While threat actors may target victims from around the world, the frequent attacks conducted against US-based organizations is not all that unsurprising given the majority of third-party providers and agents and eCommerce merchants that were targeted were based in the US. Visa PERC also observed a trend where the most frequently attacked third-party providers during this six-month period were in the hospitality industry.





Targeting of Hospitality Third-Party Service Providers

In this last six-month period, Visa PERC investigated several incidents where a third-party service provider for the hospitality industry was targeted in attacks to obtain payment account data. While the targeting of third-party providers has continued from prior periods, the repeated attacks against those in the hospitality industry is a notable development. Particularly, threat actors targeted vulnerabilities within these third-party providers' reservation platforms which were used by numerous downstream hospitality or travel agency merchants for cardholders to book and reserve travel and/or accommodations. This trend demonstrates threat actors recognize third-party providers as force multipliers. A successful intrusion against a single provider can potentially expose multiple merchants, large volumes of customer information, and numerous payment-card accounts. For threat actors, compromising a single third-party provider represents a more efficient and scalable attack path than conducting separate intrusions against individual merchants, such as numerous digital skimming attacks.

During this period, Visa PERC also observed some notable changes in threat actors' tactics used to conduct digital skimming as identified in these four incidents. Digital skimming is where threat actors compromise an eCommerce merchant's environment to deploy JavaScript (JS) based malware onto the checkout webpages to steal payment account data and other information as cardholders enter their payment credentials into the checkout forms.

One of the digital skimming attacks conducted against these hospitality service providers involved the deployment of malicious code within the victim's hospitality management platform. In this attack, threat actors first compromised the victim's software-as a service (SaaS) environment to target multiple downstream hospitality merchants and then they compromised the victim's on-premises solution used by two merchants. Thus, the digital skimming malware deployed by the threat actors was able to harvest payment account data from both the victim's SaaS-hosted environment and also the victim's on-premises customer environments. This sophisticated fraud scheme reveals how threat actors will attempt to compromise as many systems within a victim's network as possible to obtain PAN data. The compromise of both SaaS and on-premises solutions highlights the need for third-party providers to ensure their environments are secured according to PCI compliant standards and utilize secure protocols, such as multi-factor authentication (MFA), biometric authentication, and limiting access to only certain user credentials.

© 2026 Visa. All rights reserved. Visa Public

Card Present vs Card Not Present Fraud Trends

At a global level, the Card Present (CP) channel saw an improvement of 18.9% when compared year-over-year (YoY) to Q2'25 and the CNP fraud rate improved by 6.9% YoY, signaling the continued adoption of secure controls and improvements in the development of fraud risks controls and monitoring capabilities have successfully reduced threat actors' ability to monetize fraudulent activities. Overall, Visa PERC has observed a transition into the CP fraud channel with threat actors resorting to sophisticated techniques to physically steal payment cards, complex and multi-step social engineering schemes to deceive cardholders both in-person and CNP transactions, and various token relay fraud techniques, with the most widespread perpetrated through NFC relay malware.

The shift into CP fraud is indicative of the security improvements and disruption efforts in the CNP space and reduction in enumeration fraud losses, as well as continued victim resilience in submitting to ransomware payment demands. The targeting of physical payment accounts also reveals threat actors are focused more on manipulating cardholders themselves to carry out fraud as a method to circumvent the adoption of robust fraud and security controls across the ecosystem.



Threat Disruption & Forecast

Visa PERC continues to cooperate with law enforcement partners in identifying and dismantling cybercriminals' activities across the payments ecosystem. Throughout 2026, Visa assisted the US Secret Service's (USSS) and other US law enforcement agencies in disrupting and dismantling payment card skimming operations across the US. Law enforcement agents identified and removed over 120 illegal skimming devices across multiple cities, including New York, Boston, Orlando, Dallas, Houston, Pittsburgh, San Antonio, and other locations. The operations targeted skimming devices used to steal payment card and EBT credentials from point-of-sale (POS) terminals and ATMs, with investigators estimating that the enforcement actions prevented more than US$138M in potential fraud losses. The largest operation occurred in New York, where authorities estimated US$68M in fraud was prevented, while additional operations in Boston and Orlando each prevented approximately US$16.7M, Houston US$14.5M, Dallas US$13.5M, and Pittsburgh US$9.4M in losses. Collectively, these nationwide outreach efforts highlight the scale of ongoing EBT fraud and card-skimming activity and the effectiveness of proactive law enforcement and merchant engagement in disrupting fraud before stolen card data can be monetized.

Over the next year, Visa PERC believes third-party providers and their platforms will continue to see increased incidents where payment card data is exposed as cybercriminals increasingly shift toward targeting weaknesses in access tools, third-party provider environments, API integrations, and insecure user credentials. The use of AI to automate attack chains will allow threat actors to initiate sophisticated attacks, such as digital skimming, against a number of eCommerce merchants at once while deploying malware complete with unique features that can bypass security controls during the intrusion.

In threat actors' attempts to discover new vulnerabilities and exploits to attack, they have begun targeting Virtual Credit Cards (VCCs) more frequently as these products are relatively new to the payments ecosystem. A VCC is a digitally generated card number linked to a consumer's existing payment card (debit/credit) or bank account, designed for secure online transactions without exposing the actual physical card details. Although VCCs were designed for issuers to provide consumers with new options for conducting digital transactions, threat actors may leverage to perform a wide range of sophisticated fraud schemes.

© 2026 Visa. All rights reserved. Visa Public

The Rise of Virtual Credit Cards

Ecosystem Landscape

As the payments ecosystem continues to expand digital payment methods, consumers and businesses are increasingly adopting alternatives to physical payment cards. One of the rapidly growing digital payment methods are VCCs. A VCC typically comes with a unique card number, expiration date, and CVV, and can be set for one-time use or limited to specific merchants, often with customizable spending limits and expiration periods. Threat actors may exploit VCCs through several different fraud tactics, including payment account enumeration, refund or return fraud, or bank impersonation, to name a few.



Payment Account Enumeration

VCCs could potentially be targeted by threat actors seeking to exploit payment account enumeration. If a cardholder has created a multiple-use VCC (i.e., not 'single use'), that VCC PAN could potentially be enumerated in a similar manner to traditional PANs. Threat actors would likely target large eCommerce merchants who do not require cardholders to input CVV2 to facilitate the VCC enumeration attacks as threat actors will experience less friction when conducting automatic card testing transactions. Thus, potentially enabling threat actors to validate a larger number of VCCs than through eCommerce merchants that require CVV2.

Return or Refund Fraud

In return/refund fraud threat actors use a VCC, typically a VCC provided by a third-party VCC-issuing platform, to make an eCommerce purchase for goods. Once the goods are received, the threat actor initiates a return of the goods, and a refund is issued to the VCC by the merchant. The threat actor does not return the goods and disables the VCC used to make the purchase, leaving the merchant unable to recover the refunded funds. Issuers should consider monitoring for high return volume from a single merchant on VCC PANs and review onboarding controls to ensure that only legitimate consumer accounts are opened.

Bank Impersonation

Threat actors use VCCs in bank impersonation social engineering schemes. To conduct this VCC scheme, the threat actor spoofs an issuer's phone number and sends the victim an SMS/text message notifying the victim that there is a "security issue" with their account and that a bank representative will be contacting them shortly. The threat actor then calls the victim and socially engineers the victim to a) believe the threat actor is a bank representative and is calling to help the victim protect their account, and b) convinces the victim to create VCCs for their account(s). Threat actors then socially engineer the victim to provide them with the newly generated VCC numbers and security data, or to provide direct account access, which they then use to commit fraud. Once these VCC accounts are compromised, threat actors tend to use the VCC to purchase cryptocurrency in order to cashout the compromised account, as cryptocurrencies allow threat actors to exit fiat systems and easily enter pseudo-anonymous blockchain systems.

Threat Disruption & Forecast

As noted above, the rise of VCCs may potentially create new opportunities for threat actors to circumvent fraud and risk controls through sophisticated attack vectors. Additionally, VCCs created by non-issuer platforms may not be subject to the same level of anti-money laundering (AML)/fraud scrutiny traditional financial products receive, and as such, could be a higher risk to be compromised by threat actors. The advancement of AI technologies and proliferation of these models around the cybercriminal ecosystem may also lead to threat actors experimenting with how to abuse VCC platforms to perform high velocity test transactions and obtain valid VCCs through CNP or enumeration activities. As threat actors continue to conduct more highly complex attacks and seek out new methods to compromise payment account data, it is likely VCCs will be targeted by threat actors to perform subscription fraud and other aforementioned fraud schemes in the near future.

The sophisticated threats posed by threat actors who have leveraged AI tools and other emerging technologies have also significantly increased in scale as Visa PERC has observed threat actors conducting fraud attacks targeting victims from around the world within a single operation. Primarily, these large-scale threats come from ransomware attacks and scams and other complex social engineering attacks exploiting the weakest link in the payments ecosystem: humans.

© 2026 Visa. All rights reserved. Visa Public

Increased Scale of Fraud Attacks

Visa PERC has noted a continued rise in the scale of fraud attacks executed around the world as threat actors are more frequently able to target victims within several different geographic regions during the same fraud campaign. AI agents and models have greatly improved the capabilities possessed by threat actors, particularly when it comes to targeting cardholders and organizations in ransomware attacks and scams regardless of the language spoken by the victims. As noted previously, AI can be used to facilitate automated reconnaissance of victims and identify vulnerabilities to exploit. Further, AI can be used by threat actors to target specific demographics, such as elderly citizens, with cryptocurrency investment and romance scams. AI may also be deployed to identify senior IT employees of targeted organizations who may have access to a victim organization's SSH accounts for user authentication and craft spear-phishing campaigns to steal those credentials for the purpose of executing a double extortion ransomware attack.

Disruption of Scams at Scale

Evolving Threat Landscape

Scam activity continues to expand across the payments ecosystem as AI tools become more accessible, capable, and widely adopted. Threat actors are increasingly using AI to execute large scale operations, enhance social engineering tactics, and manipulate victims into disclosing sensitive personally identifiable information (PII) or payment account data. Generative AI (GenAI) is being used to accelerate multiple components of scam activity, including synthetic identity creation, AI-enhanced phishing, and the production of deepfake images, audio, and video used to build credibility and deceive victims. In response to this evolving threat environment, Visa Scam Disruption (VSD) continues to identify, investigate, and disrupt scam networks operating across the global payments ecosystem.

Over the past six months, VSD observed the continued expansion of scam-enabled commerce across the payments ecosystem, with fraud increasingly driven by large-scale eCommerce schemes, subscription-trap models, unauthorized recurring billing, social media deception, and merchant network abuse. Across the six-month period, recurring billing and deceptive eCommerce activity remained dominant threat vectors, while VSD also identified growing activity involving investment scams, task scams, phishing campaigns, impersonation scams, tech-support fraud, transaction laundering, and collusive merchant networks. Investigations revealed interconnected infrastructures spanning multiple regions and acquisition channels, highlighting the industrialization of large-scale scam operations and their ability to rapidly adapt tactics while maintaining a wide reach. In response, VSD expanded its disruption efforts through acquirer engagement, security alerts, intelligence sharing, ecosystem partnerships, government outreach, and enhanced analytics capabilities. These enhancements resulted in the identification of over **US$1.4B** in fraud detected, a **40%** increase over the last six-months, and reinforcing Visa's ability to identify, investigate, and disrupt emerging fraud trends before they achieve broader scale across the ecosystem

Visa Scam Disruption (VSD)
activity over the past six months (Jan-June 2026):

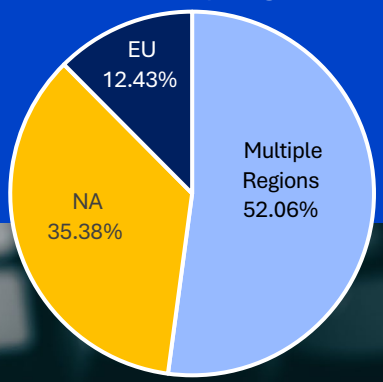
Total Attempted Fraud:

Over $1.4B

Increase in Fraud Identified:

40%

Percent of Total Fraud Amount Identified by Region





© 2026 Visa. All rights reserved. Visa Public

Notable Scam Trends

Over the past six months, VSD identified notable scam trends that demonstrate how threat actors continue to combine social engineering, deceptive digital infrastructure, and trusted payment flows to target consumers across a large-scale victim population. These trends included fake dating and romance platforms designed to harvest payment credentials and enroll victims in unauthorized recurring billing; travel and hospitality impersonation schemes that exploited legitimate booking activity to drive cardholder-authorized payments; and large global event-themed scams that capitalized on global event interest. Collectively, these scams show the continued growth of large-scale scam operations and the use of automation, impersonation, and network infrastructure to increase victim reach, obscure fraud indicators, and complicate detection and recovery.



Travel and Hospitality Social Engineering Scams

VSD has also observed a trend where threat actors are increasingly exploiting trusted travel and hospitality booking platforms to conduct targeted phishing and social engineering campaigns against cardholders, with recent activity primarily impacting the EU and AP regions. In these schemes, fraudsters impersonate legitimate booking platforms through email or mobile messaging applications and send post-reservation "confirmation" messages that reference actual booking details, increasing the perceived legitimacy of the communication and reducing the likelihood that victims will identify the interaction as fraudulent.

The messages typically contain malicious links that use hospitality-related keywords, such as "booking" or "guest," and redirect victims to phishing webpages impersonating the original booking platform or affiliated hospitality brands. Once on the fraudulent site, victims are prompted to authorize additional payments under the pretext of city taxes, room taxes, reservation confirmation, or special requests. VSD's investigation indicated of the many receiving wallet accounts were aged accounts controlled by money mules or accounts whose holders may have previously been victimized by other scams.

This activity highlights the continued evolution of socially engineering fraud in which threat actors combine compromised or exposed reservation information, trusted communication channels, and legitimate payment flows to obscure fraudulent intent. The campaign underscores the importance of consumer awareness, monitoring for anomalous post-booking communications, and coordinated issuer and ecosystem controls capable of identifying authenticated fraud driven by social engineering.



© 2026 Visa. All rights reserved. Visa Public

Romance and Dating Subscription Scam

In one scheme, VSD observed a large network of interconnected fake dating and romance websites that appear to share ownership, web infrastructure, webpage templates, and other common characteristics. Consumers are typically routed to these platforms through deceptive landing pages advertising local matches, discreet dating, or "free" registration. After an account is created, users are rapidly engaged by scripted bot profiles that use generic compliments, immediate responses, and simulated romantic interest to build trust and encourage continued interaction. Although the automated nature of the activity may become apparent through inconsistent responses or inaccurate personal details, the repeated engagement is designed to create emotional pressure and move the victim toward providing payment account information.

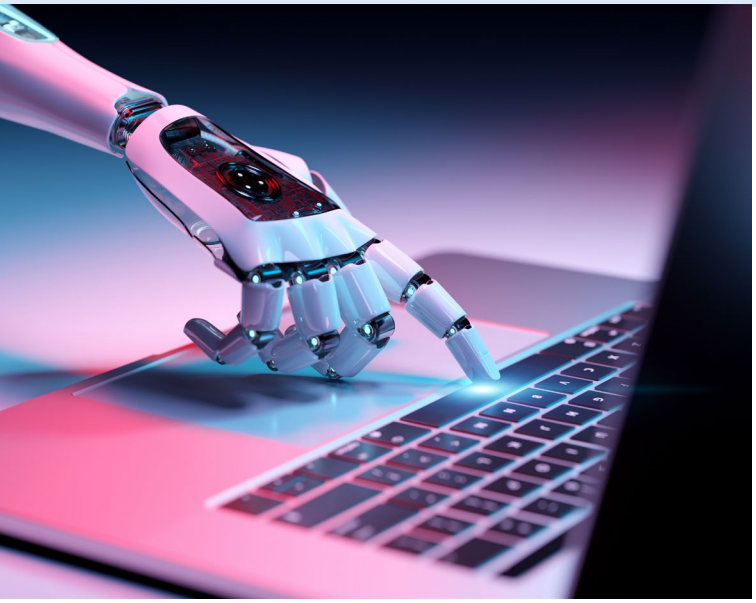
Once engagement is established, the sites commonly restrict further messaging and prompt users to purchase a low-cost trial, while recurring billing terms are presented in fine print or otherwise made difficult to identify. After payment is submitted, the credential may be reused across affiliated dating platforms to enroll the victim in additional subscriptions without consent, often under generic merchant descriptors that complicate dispute and recognition efforts. VSD also observed that these operators use vague cancellation processes, non-responsive support channels, and rapid site replacement to prolong billing activity and preserve the underlying scam infrastructure when individual domains receive consumer scrutiny.

Scams Exploiting Worldwide Events

Visa PERC observed a significant increase in scams targeting large, international events as threat actors exploited the worldwide popularity of a global sporting event to redirect consumers to fraudulent websites impersonating the sporting event and its partners. Cyber threat researchers identified more than 4,000 domains spoofing one brand, including nearly 1,500 registered within a concentrated period, many leveraging typosquatting, spoofing, and domain-aging techniques to evade security controls and appear legitimate. These domains impersonated official ticketing, travel, merchandise, betting, and streaming services with the objective of stealing payment credentials, harvesting personal information, and facilitating fraudulent transactions.

Threat actors industrialized these campaigns through the use of phishing kits, AI-enabled multilingual content, SEO manipulation, paid advertisements, and social media promotion to maximize global reach. Fraudsters enhanced the credibility of their scams through professionally designed websites, fake business registrations, and privacy-protected domain registrations, making detection more difficult for both consumers and security teams. Cybercriminal forums and dark web marketplaces further enabled the distribution of phishing kits, stolen credentials, and counterfeit tickets, while botnets were used to automate ticket scalping and resale activity.

This large scam ecosystem illustrated how cybercriminals capitalize on major global events to conduct payment fraud, credential theft, identity theft, and account takeover at scale. The widespread use of AI, automated infrastructure, and sophisticated social engineering techniques demonstrated the increasing professionalization of scam operations, enabling threat actors to rapidly create convincing fraudulent brands, target victims across multiple languages and geographies, and scale their operations with unprecedented efficiency.



Use of AI to Facilitate Large Scale Scams

Threat actors are increasingly leveraging AI-based deepfakes to bypass authentication controls and execute high-impact scams targeting victims around the world. AI agents and GenAI tools have facilitated the development of large-scale, sophisticated phishing and scam operations that can be created en masse and contain specific details to victimize individuals or entire organizations. Many industrialized scam compounds have incorporated AI within their operations and use GenAI tools, LLMs and AI agents, to scale their social engineering operations, enabling them to target a greater number of victims across several geographies with increased sophistication. These sophisticated scam operations contact victims through unsolicited phone calls, messaging applications, and social media platforms by utilizing AI-generated voices, scripted dialogue, and language translation tools to impersonate legitimate financial professionals, acquaintances, or investment advisors.

Visa PERC's Scam Disruption (VSD) team continues to assess these developments as a persistent threat vector requiring strengthened multi-factor verification, enhanced employee training, and expanded detection capabilities across issuers, acquirers, and financial-institutions.

© 2026 Visa. All rights reserved. Visa Public

Threat Disruption & Forecast

Law Enforcement organizations across the globe continue to target large-scale, industrialized scam operations and sophisticated organized cybercrime networks in efforts to disrupt their operations and protect consumers. Visa PERC continues to partner with law enforcement agencies globally to build and share intelligence to identify and disrupt scams and those that operate scam campaigns. To effectively mitigate the scam threat, Visa PERC monitors scams, provides alerts and advice to prevent them, and collaborates with global law enforcement to disrupt fraud operations and protect the payments ecosystem and routinely reports new scams via security alerts.

Threat Disruption

Visa PERC has collaborated with law enforcement agencies around the world to target and disrupt scam organizations and their infrastructure. One notable operation involved collaboration with international law enforcement agencies to disrupt large scam compounds and other organized scam centers. These operations have led to the indictment and arrest of hundreds of suspects who orchestrated hundreds of millions in fraud losses (USD) to victims around the world, primarily from romance-themes investment schemes, account takeover schemes, and cryptocurrency investment fraud schemes.

A separate law enforcement operation targeting scams resulted in the seizure of cryptocurrency funds totaling over US$580M stolen as fraud proceeds from cryptocurrency investment scams perpetrated by Chinese transactional criminal organizations. These organizations use various Internet and social media platforms to deceive victims, who were primarily located in the US, into believing they were investing in legitimate cryptocurrency tokens or platforms. The operators behind these scams used common romance-cryptocurrency investment fraud tactics to increase the dollar amount their victims "invest" before defrauding them and typically operate out of scam compounds located in AP.

Visa PERC monitors such scams, provides alerts and advice to prevent them, and collaborates with global law enforcement to disrupt fraud operations and protect the payments ecosystem and routinely reports new scams via security alerts.



Threat Forecast

Over the next year, scams are expected to continue to increase impact, efficiency and scale, with a wider range of scams impacting individuals and organizations across the world as scammers continue to utilize AI tools and other technologies to exploit the emotions of their victims around the world. Threat actors will use AI to distribute large scams to massive victim populations in disparate geographic regions at scale, while also uniquely crafting phishing and other social engineering messages to specifically entice certain victims into falling for their schemes. These tactics will likely be used during global events or phenomena when hundreds of millions of people may fall victim to the same phishing lures written in numerous languages.

While scams have certainly become more prolific and widespread since the adoption and development of AI tools, ransomware and ransomware-as-a-service (RaaS) groups and affiliates have also greatly benefited from utilizing AI within their operations. The entire ransomware ecosystem has morphed over the last couple of years with rapid movement among affiliate operators between the largest RaaS organizations and frequent targeting of vulnerable cloud-based user authentication systems as initial intrusion vectors.

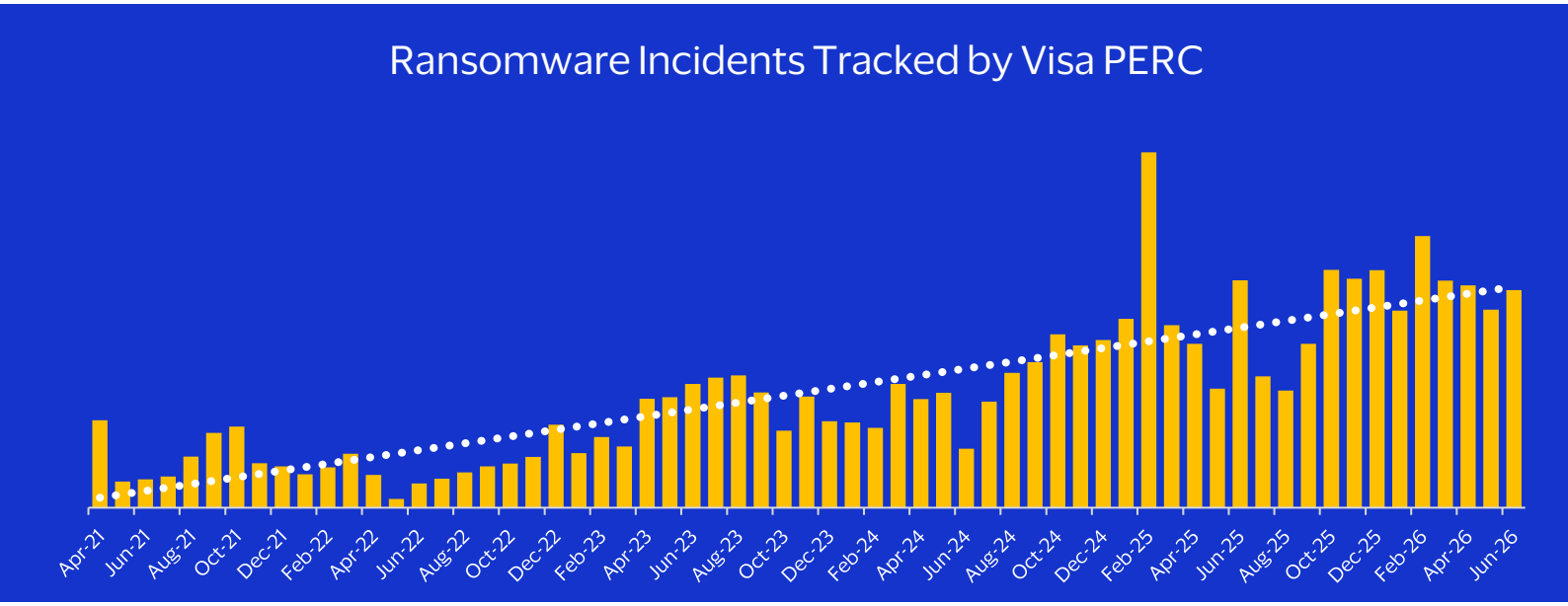


© 2026 Visa. All rights reserved. Visa Public

Increased Scale of Ransomware and Extortion Attacks

Evolving Threat Landscape

Visa PERC tracks ransomware incidents impacting payments ecosystem entities and has seen a steady increase in the prevalence of ransomware cases since Visa PERC began tracking ransomware activity in 2021. This recent six-month period (Jan-June 2026) saw a modest **8% increase** in ransomware cases when compared to the same period in the previous year (Jan-June 2025), however, this recent period saw a sustained increase of **19%** over the prior six-month period of Jul-Dec 2025. Overall, Visa PERC has seen a **312% increase** in ransomware cases from 2021 to 2026, establishing a roughly 60% increase in cases each year over the past five years. Furthermore, there has been an elevated level of ransomware incidents sustained over this previous six-month period when compared to prior six-month periods dating back to January 2024. Since the six-month period of January to June 2024, the monthly average number of ransomware incidents as observed by Visa PERC has increased approximately 133%, marking a notable change in the consistency of threat actors conducting ransomware attacks.

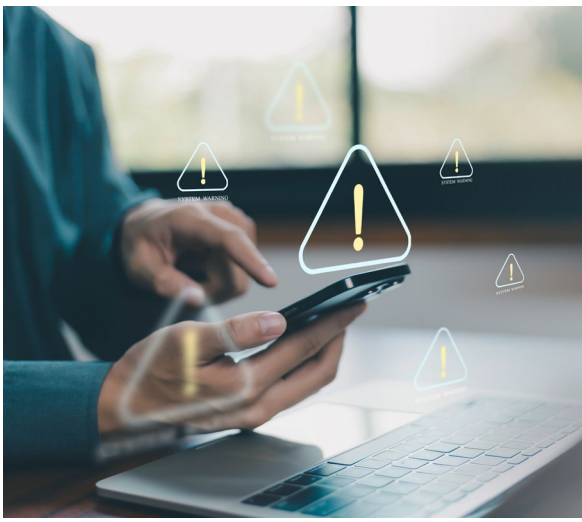


Large Ransomware Groups Continue to Surge

In a continuation from the latter half of 2025, in this most recent six-month period, Visa PERC observed the 10 most active ransomware groups accounted for the vast majority of total ransomware incidents reported. The top 10 ransomware groups conducted over 80% of the observed ransomware incidents in Jan-June 2026 and 7 of these 10 groups remained in the top 10 from the prior period of July-Dec 2025. The continued dominance of some of the largest ransomware-as-a-service (RaaS) players, particularly those who rely on double extortion, indicates that despite the proliferation of RaaS capabilities with the advancement of AI technologies and new operators around the world, those groups who are able to consistently extract payment from victims and funnel those payments to their affiliates, remain the most prolific RaaS organizations.

Qilin Remains on Top

As tracked by Visa PERC, Qilin is again the most active ransomware group, accounting for 17% of all victims, relying on unique extortion tactics to pressure victims into making ransom payments and threatening to release sensitive information if not paid. Qilin is extremely consistent in their targeting of victims, mainly across the Services/Wholesale and Manufacturing/Construction/
Energy/Agriculture industries, which account for over 50% of their victims. One other notable group, The Gentlemen, conducted approximately 13% of ransomware attacks. During this six-month period, The Gentlemen made a drastic rise to become the second most active group, increasing their number of ransomware victims by over 460% when compared to the prior period of July-Dec 2025.



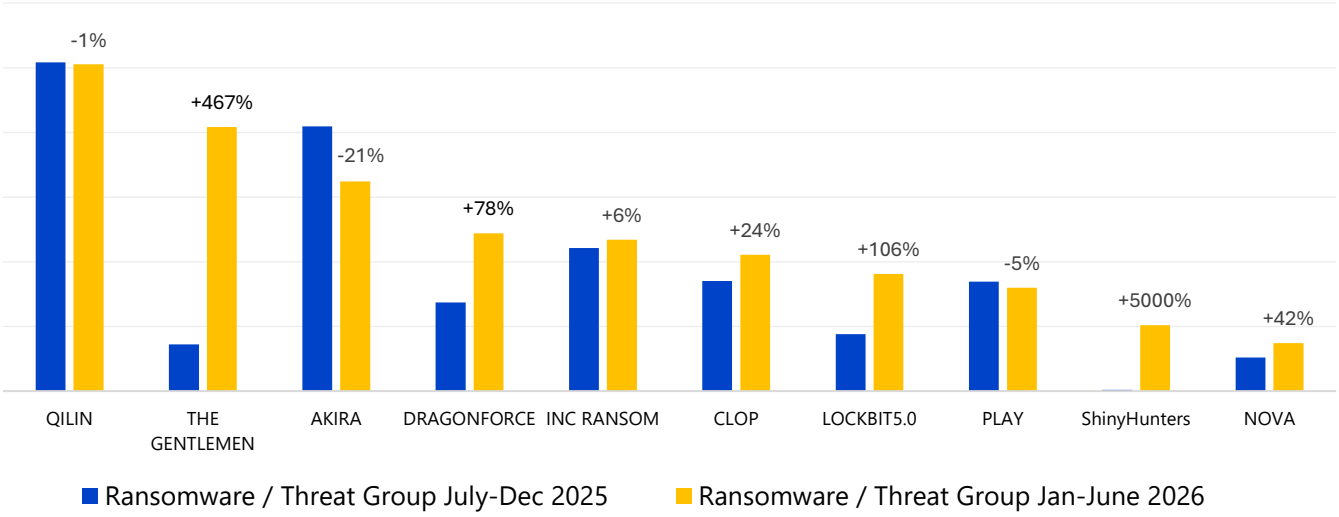
© 2026 Visa. All rights reserved. Visa Public



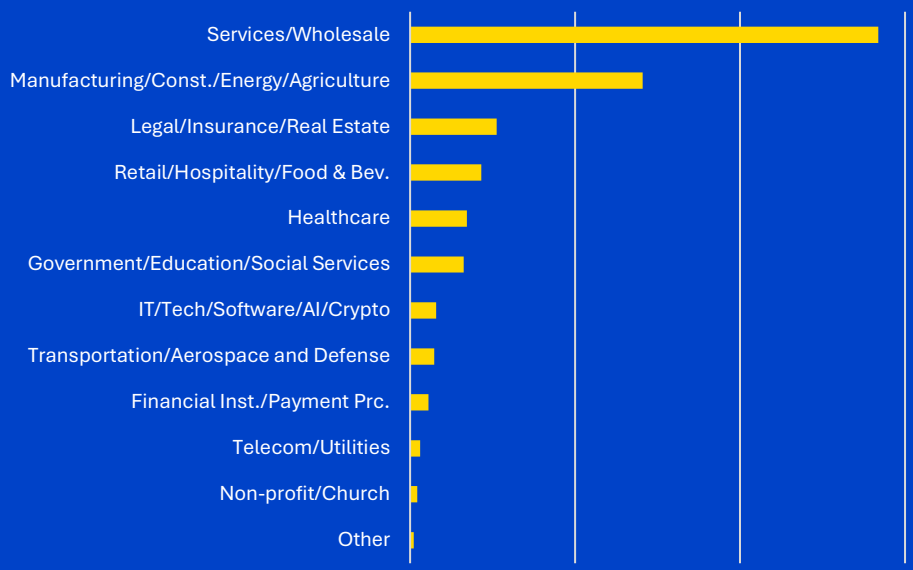
The Gentlemen's Increased Popularity

First coming onto the ransomware scene in late 2025, The Gentlemen was founded by a former Qilin affiliate and recruits new operators through their partnership with BreachForums. Similarly to Qilin, The Gentlemen uses double extortion tactics to encrypt victims' sensitive data while also forcing them to make payments otherwise face the consequences of having their information leaked to the public. The rise of The Gentlemen in recent months appears to be tied to major changes in the ransomware operator market as threat actors are shifting their allegiances between ransomware groups based on affiliate payout percentages and how disputes are handled among affiliates. The Gentlemen's reported 90/10 affiliate split is more attractive to ransomware operators than the commonly reported 80/20 model and helps explain why experienced operators may have moved to their organization over this period. The Gentlemen also heavily rely on leveraging pre-existing access to victim environments to perpetrate ransomware attacks, allowing the group to market themselves to affiliates as an "easier" opportunity to make money.

Ransomware Operators
PERC-Tracked Incidents: (July-Dec 2025 vs Jan-June 2026)



Type of Entity Impacted
PERC-Tracked Incidents: Jan - June 2026



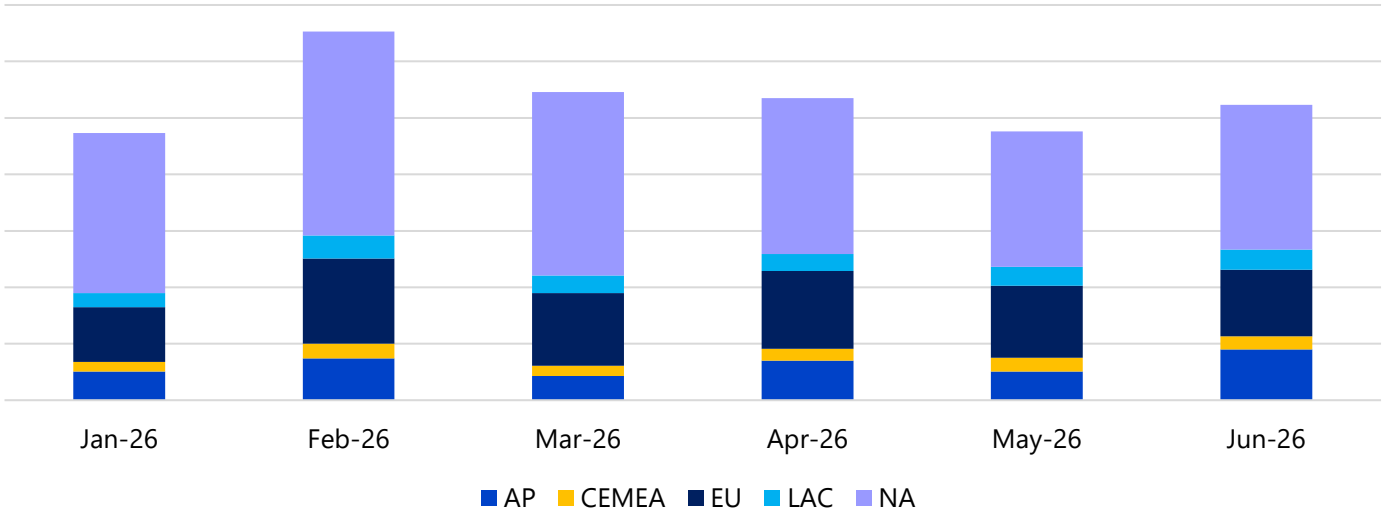


© 2026 Visa. All rights reserved. Visa Public

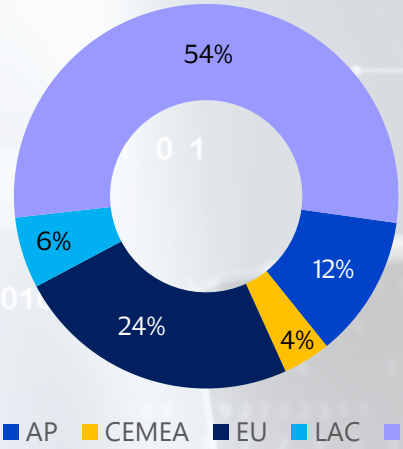
In Visa PERC's tracking of entities impacted by ransomware incidents, Services/Wholesale entities were impacted the most, accounting for over 44% of all incidents, followed by Manufacturing/Construction/Energy/Agriculture (22%), with a significant gap to the next highest sector, Legal/Insurance/Real Estate (8%). These trends further correspond with the increased targeting of third-party service provides through data breaches and other advanced intrusions to compromise payment account data.

Other sectors such as Other (Gambling/Gaming, Media, Publishing), Non-profit/Church, Telecom, and Financial Institutions/Payment Processors experienced the fewest incidents (a total of just over 3%), highlighting a continued effort by ransomware operators to focus on services and manufacturing entities. Regionally, North American (NA) entities continue to see the highest percentage of ransomware incidents, with 54% of PERC-tracked incidents impacting North America-based entities.

Ransomware Incidents Tracked by Visa PERC - Ransomed Entity Month and Region
Jan-Jun 2026



Ransomware Incidents Tracked by Visa PERC by Ransomed Entity Region
Jan-Jun 2026



© 2026 Visa. All rights reserved. Visa Public

The Impact of AI on the Ransomware Ecosystem

Ransomware has drastically evolved with the rapid adoption and advancement of AI models and tools into the operations of threat actors around the world. Perhaps most importantly, AI is lowering barriers to entry while simultaneously enabling large RaaS groups to attack at an unprecedented scale. Affiliates can leverage AI to troubleshoot code, refine attack playbooks, and operationalize attacks with less technical expertise, making it easier to shift between groups or rapidly scale new operations. With less human input required to compromise several organizations at once, less sophisticated threat actors can perform the same attacks as large, sophisticated cybercriminal operations, increasing the number of threats to the payments ecosystem, regardless of geographic region.



Threat actors have used AI agents, tools and models to perform reconnaissance, generate and refine malicious scripts, and rapidly adapt their operations in real time, as long as a human instructed the agent to perform certain tasks. In just the last six-month period, advancements in AI models and technologies have enabled teams of AI models to fully automate the entire attack chain, significantly shortening attack timelines and allowing threat actors to repeat the same tactics across multiple victims. In the first fully automated ransomware attack, threat actors conducted an entire ransomware attack using AI agents where teams of agents acted as independent ransomware operators, executing each step of the attack chain autonomously. This incident showcases the advancement of ransomware operators' use of AI tools and how AI has become an integral part of RaaS groups' workflows.

Visa PERC assesses AI-supported threat actors can move more quickly from target selection to extortion, regardless of the victims' geography or language, particularly where remote access software and programs are inadequately protected by security controls. Multiple systems of AI agents can be deployed by RaaS operators to infiltrate victim environments, deploy malware, encrypt sensitive data for extortion while simultaneously exfiltrating stolen payment account data to secure command-and-control (C2) infrastructure. Now more than ever, RaaS operators of all sizes possess the same capabilities and have access to the same tools as even the largest and legacy groups, significantly expanding the global threat posed by ransomware for the foreseeable future.

Threat Disruption & Forecast

In January 2026, US law enforcement agencies recently seized the cybercriminal underground forum and marketplace known as RAMP. RAMP operated as a marketplace where cybercriminals could advertise various RaaS services and activities to other threat actors, recruit new affiliates to join their operations and act as a hub for the RaaS ecosystem. The seizure of RAMP disrupted the only known underground marketplace that openly allowed threat actors to advertise and discuss ransomware operations and services, leaving a major gap in RaaS groups' abilities to recruit new affiliates to their cause.

As ransomware continues to evolve, particularly with the advancement in AI tools and the changing ecosystem dynamics, it is vital for organizations to ensure credentials related to third-party access providers and cloud-service providers are secured and protected. Visa PERC will continue to monitor the entire payments ecosystem for any ransomware attacks and alert ecosystem partners to payment account data involved in these compromises.

While Visa PERC has observed a greater scale of fraud attacks both in terms of the number of victims and geographic footprint, threat actors have also used AI tools and other emerging technologies to identify precise vulnerabilities in victims' networks or systems.

© 2026 Visa. All rights reserved. Visa Public

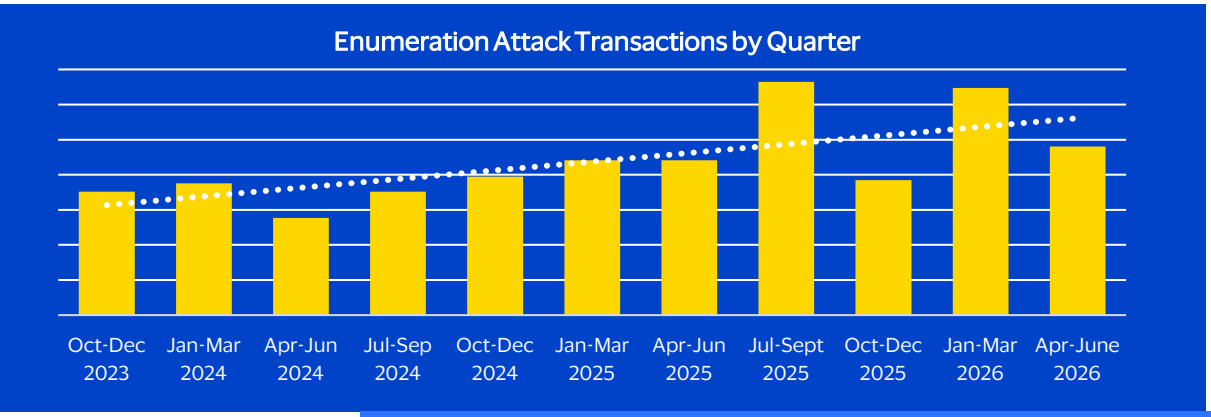
Increased Precision of Fraud Attacks

Visa PERC has observed a marked increase in the number of advanced intrusions designed to exploit specific vulnerabilities or misconfigurations in security controls, whether these attacks are focused on the CP, CNP or token channels. Fraud attacks have become much more precise and targeted, particularly when it comes to enumeration, card-not-present (CNP) fraud, and token provisioning abuses. This greater precision likely stems from the proliferation of AI tools and other advanced technologies across the global cybercriminal landscape as threat actors may use AI tools to test and probe payments ecosystem participants systems and authorization decisioning processes to determine how to obtain approved fraudulent transactions.

Enumeration is Becoming More Precise

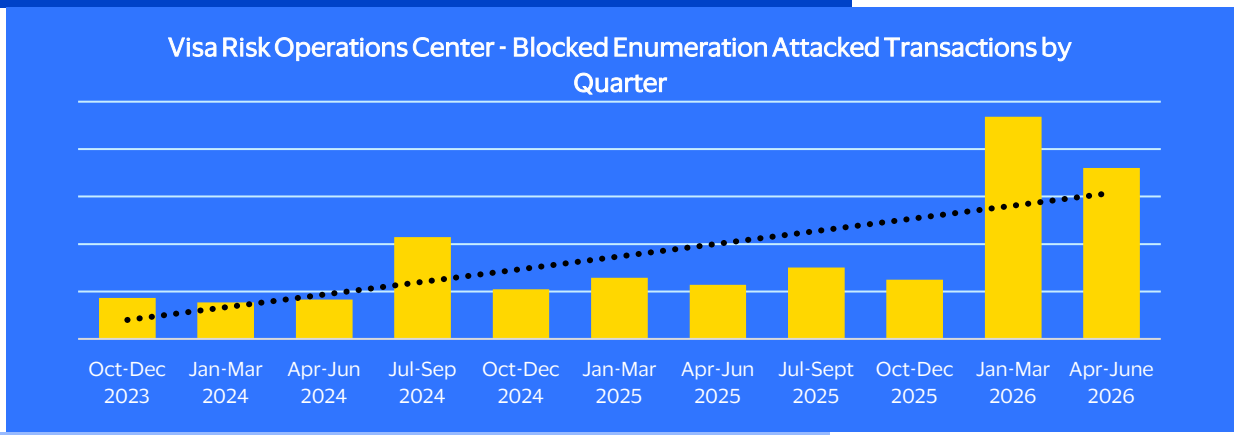
Evolving Threat Landscape

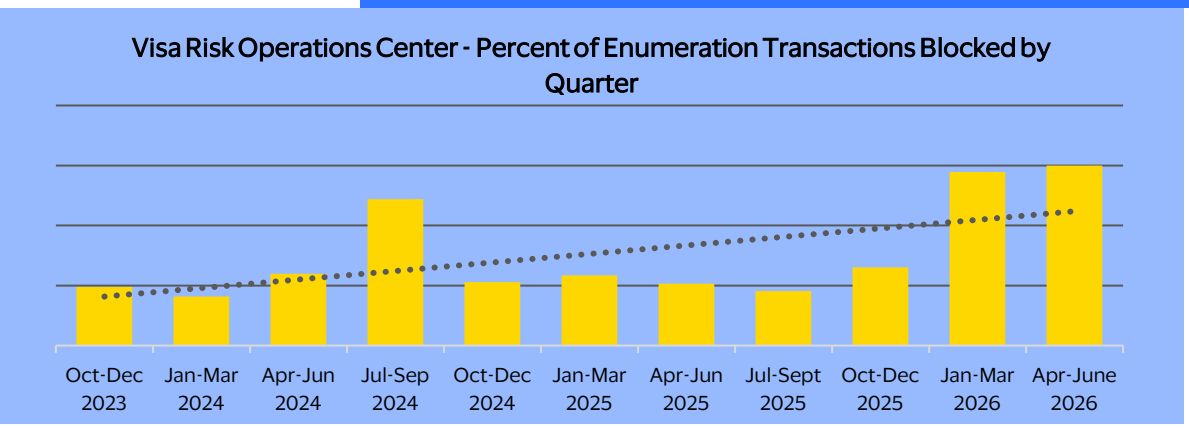
Payment account enumeration—when threat actors use automated methods to test and guess payment data such as card numbers and CVV2 codes through eCommerce—remains a leading threat in the Visa payment ecosystem. In the six-month period of Jan-June 2026 there was **a 7.8% decrease** when compared to the previous six months (based on the real-time, Visa Account Attack Intelligence [VAAI] Score model). However, global enumeration volume has increased **35%** when compared to the same period in 2025.



Enumeration Transaction Count: Enumeration transactions observed by Visa PERC.

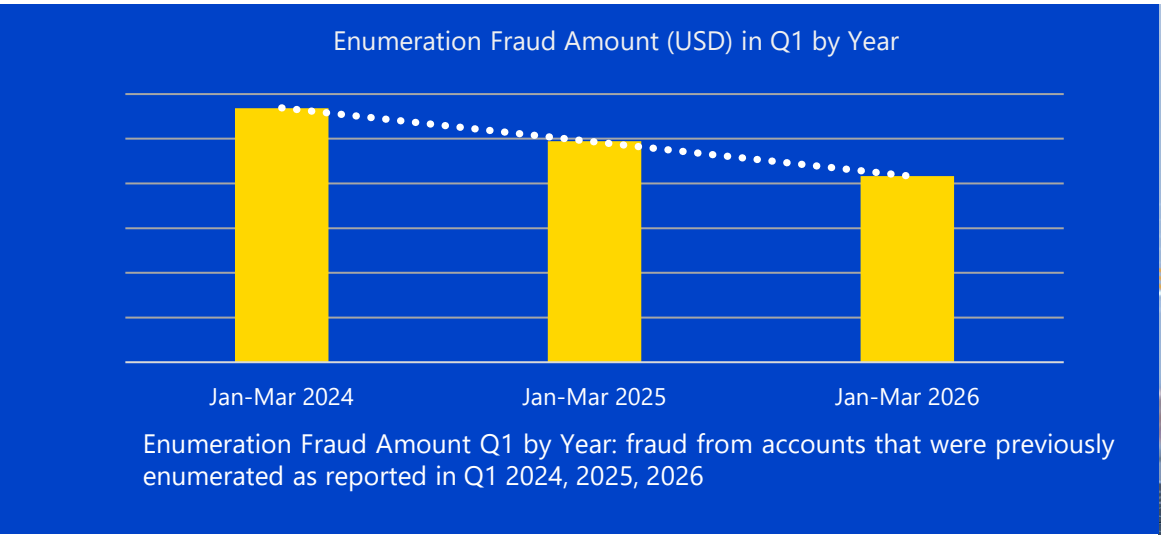
Blocked Transaction Count: transactions blocked by ROC due to enumeration activities.





Percentage of Blocked Enumeration Transactions: Total Enumeration transactions blocked by the ROC as a percentage of total enumeration transactions observed by Visa PERC.

© 2026 Visa. All rights reserved. Visa Public

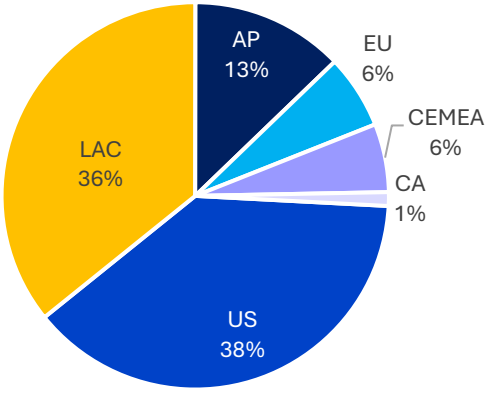


Enumeration Fraud Amount Q1 by Year: fraud from accounts that were previously enumerated as reported in Q1 2024, 2025, 2026

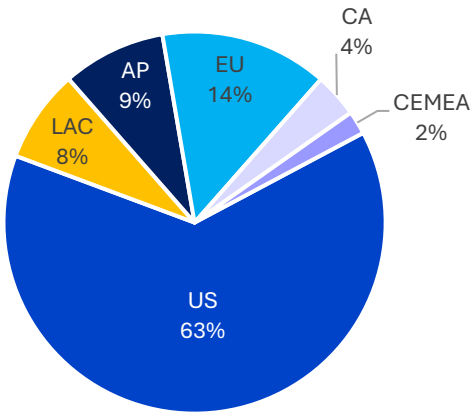


During the same period, the count of **Visa Risk Operations Center (ROC) blocked enumeration transactions rose 200%** when compared to the prior six-month period of Jul-Dec 2025, and approximately **29%** of all enumeration attempts detected by the VAAI Score. During FY26Q1 (October-December 2025), **fraud loss from enumerated** credentials decreased **21.4% YoY**, likely due to the increased number of blocked enumeration attacks by the ROC and deployment of the VAAI Score.

VAAI - Impacted Issuer Region
From January 2026 to June 2026 Enumeration Activity



VAAI - Impacted Merchant Region
From January 2026 to June 2026 Enumeration Activity





© 2026 Visa. All rights reserved. Visa Public

Enumeration Trends

Enumeration Tactics have Evolved

Over the last six months, Visa PERC's VAAI team has observed notable changes in the tactics used by threat actors to conduct enumeration attacks. VAAI has seen a shift away from traditional large-scale data breaches and toward faster, lower-cost enumeration attacks that are much more precise in their attempts to target real-time authorization and token provisioning flows. While EMV, tokenization, encryption, and PCI controls have reduced breach-related fraud, enumeration now represents a larger share of global fraud losses, with risk concentrated across certain regions, issuers, merchant categories, and low-friction channels such as US$0 authorizations and cross-border transactions. Beyond enumeration attempts, the VAAI team has also detected several other fraud schemes utilizing automated authorization attempts to compromise payment account data. These new fraud schemes use tactics precisely designed to target certain ecosystem participants' risk controls and exploit gaps in their payment processing configurations.

Fraud Scheme Leverages Compromised Credentials for Automated Cashout

Through the VAAI Score, Visa PERC has observed an ongoing fraud scheme where threat actors monetize compromised payment credentials, including prepaid and debit PANs, through high-frequency authorization attempts, while rapidly rotating the targeted issuers. In these schemes, the threat actors likely compromise the PANs via token-provisioning enumeration attempts at large eCommerce merchants. Visa PERC has seen instances where threat actors conduct token-provisioning shortly prior to the cashout of the compromised PANs at digital goods merchants, subscriptions, and digital currency exchanges. While this particular fraud scheme does not directly involve payment account enumeration, Visa PERC assesses this campaign is part of a broader fraud ecosystem involving credential compromise, token provisioning abuse, and potential money-laundering mechanisms across digital platforms. After this activity was observed by the VAAI team, the PERC Risk Operations Center (ROC) introduced nine targeted blocks to mitigate immediate risk with minimal impact to legitimate Visa payment traffic.

Breached Payment Credentials Detected by VAAI

The threat actor group known as B1acksStash released a database containing millions of compromised PANs obtained from some of the group's "vendors" who were reselling PANs across multiple cybercriminal forums and marketplaces. Prior to the release of the compromised PANs, the VAAI team had detected suspicious activity linked to a portion of the exposed PANs through enumeration attempts conducted at large eCommerce merchants, indicating the threat actors likely used these eCommerce merchants as a method to validate or test compromised payment credentials before further exploitation or monetization. VAAI detected ~60% of the total number of PANs released by B1ackStash highlighting how Visa's VAAI Score is able to proactively detect fraudulent activities by identifying suspicious authorization behavior early in the data compromise lifecycle. VAAI can provide issuers with actionable intelligence on PANs which exhibit suspicious patterns before large scale monetization by threat actors can occur.



Increase in Token Provisioning Enumeration

Enumeration is increasingly moving beyond traditional authorization card testing activities and into token provisioning, where attackers attempt to provision tokens using stolen payment credentials and rely on the token result or related issuer response to determine whether the underlying PAN can be tokenized. If a stolen PAN is tokenized and approved by the issuer, then the PAN is confirmed to be valid and may be sold or monetized by the threat actors. This activity primarily occurs at large eCommerce merchants, where threat actors can blend the fraudulent provisioning attempts into legitimate transaction volumes and exploit gaps in issuer token provisioning controls. The observed behavior often reflects traditional BIN attack patterns, with fraudsters testing sequential account numbers over periods ranging from several hours to several days; this activity is typically a precursor to follow-on fraud. After validating payment credentials through token provisioning, fraudsters may quickly monetize the accounts, with the time between provisioning and authorization activity varying from minutes to multiple days and not always occurring at the same merchant. Provisioned but inactive payment accounts exhibit a 223% higher fraud rate than PANs compromised through card testing enumeration. VAAI has detected some of this follow-on fraud and has also observed correlations with transit fraud groups, including patterns where fraudsters generate new tokens through factory resets and different user accounts.

© 2026 Visa. All rights reserved. Visa Public

Enumeration Fraud Rates Decline

Enumeration fraud improved globally in Q1'26, with fraud dollars down 21.4% YoY and fraud rate down 10.8% YoY. LATAM remained the region with highest enumeration fraud rate, despite the strongest fraud rate improvement (-36.8% YoY) while U.S. issuers continued to drive the majority of fraud dollars with only modest fraud rate improvement (-4.9% YoY). Canada and Europe were the only regions to see higher enumeration fraud dollars YoY (+11.7% and +14.4%, respectively), despite continued fraud rate improvement.

CEMEA exhibited the fastest fraud monetization speed in Q1'26, with 52% of enumeration fraud monetized within 7 days of card enumeration.

Enumeration fraud was monetized more quickly in Q1'26 compared to Q1'25 for ASIAPAC issuers, while monetization speed decelerated in CEMEA and LAC. Monetization patterns for Europe, Canada, and the U.S. remained relatively stable with minimal volatility.

Region	Fraud Rate YoY
AP	-32.5%
CEMEA	-30.3%
CANADA	-28.8%
EUROPE	-25.5%
LAC	-36.8%
USA	-4.9%

Threat Disruption & Forecast

The Visa Risk Operations Center's (ROC) blocking measures have helped to reduce enumeration fraud across the payments ecosystem with fraud losses steadily declining over the last several quarters. This is evidenced by Visa enumeration data showing higher blocked transactions and lower fraud amounts, demonstrating the success of these controls. The launch of the VAAI Score has also helped to detect and prevent threat actors from conducting large scale enumeration attacks while also enabling Visa PERC to be proactively alerted to other fraud schemes outside of the traditional enumeration vector. Visa PERC has the capabilities to identify unique tactics used by threat actors to circumvent fraud controls, such as the aforementioned invalid CVV2 incident.



© 2026 Visa. All rights reserved. Visa Public

Token Provisioning Fraud

Evolving Threat Landscape

Beginning in 2024, Visa has been tracking a complex fraud scheme precisely designed to abuse the token provisioning process. In this fraud scheme, primarily targeting victims in North America (NA), threat actors use provisioning fraud to commit partial relay attacks against brick-and-mortar merchants. The attackers obtain stolen payment credentials—often through social engineering, phishing, or purchasing compromised data—and provision these to threat actor controlled mobile devices' digital wallets. Using malicious applications, multiple accomplices coordinate to relay tokens, enabling high-velocity, cross-border fraudulent purchases of easily resold goods like gift cards in geographically distant locations, making the transactions appear legitimate with valid authorization values.

Over the past six months, Visa PERC identified that the threat group altered its cashout strategies from mainly purchase of gift cards, subsequently adding in purchase of in-demand resaleable physical items, to purchase of luxury goods, and currently purchasing money orders through post office locations.

Ultimately, this scheme at its core begins as a provisioning fraud scheme, thus prevention efforts should focus on preventing successful fraudulent provisioning attempts. Visa PERC recommends issuers, acquirers, and processors implement robust monitoring of provisioning attempts and token transactions, especially for unusual device attributes, high-risk scores, transaction velocity, and geographic anomalies.



Global Trends in Token Provisioning:

YoY Fraud performance on Tokens as a whole continues to improve.

- Closed Q1 fraud rates are down 11.2% globally YoY.
- Open quarter rates are currently stable vs a like-to-like fraud reporting period in the prior year which may indicate the downwards trend is levelling off but it is too soon in the reporting cycle to be entirely certain.

Fraud performance improvements were strongest in the CP space in closed Q1 with rates improving 39.4% while CNP rates improved by 8.4%. Device Bound (Mobile Wallet) tokens were the primary improvement driver, down ~27.4% in closed Q1 vs a 9.3% improvement on merchant tokens.

- This follows the trend observed in the second half of 2025 wherein token fraud rates saw similar levels and distribution of YoY improvement driven primarily by improvements in delayed cashout performance.
    - Visa PERC observed this echoed in fraud rates on tokens aged 2-90 days seeing a 25.0% improvement in fraud rates overall.
    - By contrast while performance continues to improve in the Day 0-1 space it is more limited at only an 11.2% change YoY.

© 2026 Visa. All rights reserved. Visa Public

Regional Trends: Most regions remained stable or saw strong improvements YoY in Closed Q1. Canada and Asia Pacific saw slight increases in fraud rate overall.

Region	Fraud Rate (YoY)
AP	7.66%
CEMEA	-12.13%
EU	-12.65%
LAC	-5.54%
CANADA	6.16%
USA	-14.4%
Total	-11.2%

In Canada this increase was tied to Merchant Tokens with the highest rate increase in February rising 11.7% but was concentrated in 'On-File' tokens where the merchant obtained the PAN from pre-existing records at time of provisioning. This potentially suggests an increase in account compromise within the country with fraudsters re-activating dormant merchant accounts and triggering tokenization when doing so without being identified.

In Asia Pacific (AP) this increase was tied to Device Bound tokens. Fraud Rates increased 21.7% on Manual Key Entry Device Tokens while rising ~125% on On-File Device Tokens. Fraud rates on more secure pan sources such as Push Provisioning and Tap to Add Card remained stable or improved. Given adoption, this suggests an opportunity for regional issuers to look to tightening rules in these spaces as the bulk of newly provisioned tokens in the region continue to shift away from Manual Key Entry and On-File (39.51% of approved provisioning requests in Q1'26 vs 44.04% in Q1'25) and the friction impact of stricter rules continues to decrease.

Threat Disruption & Forecast

Visa PERC's ongoing support of US and International Law Enforcement in the Project Red Hook / Operation Double Tap payment fraud enforcement initiatives has resulted in over 200 arrests with additional criminal indictments pending. The enforcement operations, which began in 2024, are targeting Chinese organized cybercriminals perpetrating contactless and altered payment card fraud schemes throughout AP, NA and the EU. Visa PERC and our Law Enforcement and intelligence sharing partners have identified and geo-located a cybercrime syndicate in Mainland China perpetrating fake toll road, DMV and package delivery phishing/smishing attacks, global payment account theft and stolen account provisioning for Tap-to-pay fraud, as well as much of the account takeover (ATO), pig butchering and cryptocurrency fraud schemes globally. To date, Visa Risk and our Law Enforcement and intelligence partners have identified tens of millions of victims and billions in fraud losses.

Additionally, Visa PERC has identified several new threat vectors to the payments ecosystem caused by threat actors' use of advanced AI technologies to create fraud tactics developed to precisely target vulnerabilities in victim environments or payment processing operations. AI tools, such as advanced frontier AI models, provide threat actors with the capabilities to autonomously identify, detect and exploit gaps across victims' authorization workflows and how to monetize those gaps to generate funds.



© 2026 Visa. All rights reserved. Visa Public

Threats from Misuse of AI and Emerging Technologies

Ecosystem Landscape

Of all the threats to the payment ecosystem as observed by Visa PERC between January and June 2026, the most notable threat has been the evolution of AI models into fully autonomous agents capable of executing precise and complex tasks with little to no human input. The rapid adoption of AI agents into cybercriminal workstreams and operations has drastically altered how payment ecosystem organizations should detect, mitigate, and prevent fraud and other illicit activities from impacting their organizations and cardholders around the world. During this prior six-month period, Visa PERC has observed several key elements in how the misuse of AI tools and models pose significant threats to the payments ecosystem.

Frontier AI Models and their Impact on the Payments Ecosystem

One of the most significant advances in AI technologies has been the development advanced frontier AI models (herein referred to as Frontier AI Models). Frontier AI Models are systems of advanced AI agents built for the purpose of proactively performing cybersecurity evaluations, monitoring organization environments for unknown vulnerabilities, and conducting other cybersecurity functions, such as penetration testing and the automatic exploitation of detected vulnerabilities.

Frontier AI Models are capable of understanding what tools are needed to complete its goals, when to assign certain tasks to sub-agents with specific functions, and how to resolve problems in real time. These advanced systems push the boundaries of what current AI models are capable of today and pose major threats to the payments ecosystem if they were to fall into the hands of threat actors. A threat actor with access to even one of these models would be able to launch precise ransomware attacks against specific victims without ever needing to interact with the model.

Additionally, Frontier AI Models can be used for fraud probing to simulate complex attack chains, stress-test security defenses, and detect specific vulnerabilities across financial networks, then craft precise tactics, techniques and procedures (TTPs) to exploit those identified weaknesses. For example, threat actors may use these advanced AI models to perform card-not-present (CNP) probing. In CNP probing, threat actors deploy scripts to launch thousands of test transactions against eCommerce merchants through compromised PANs. Through these test transactions, threat actors are able to understand how the targeted acquirers or issuers handle certain fraud scenarios. From these tests they can create a fraud scheme to precisely exploit any gaps in their fraud controls, including where and how fast to execute their automated transaction scripts to cashout the compromised PANs without triggering the issuers' fraud rules.

Recent incidents also demonstrate that advanced agents can cross intended operational boundaries when scope, environmental awareness, egress controls, or containment mechanisms fail. An inadequately constrained Frontier AI Model system may take unintended actions while pursuing a human-defined objective, such as pursuing unexpected pathways, interacting with real infrastructure, or operating beyond the intended test boundary.

When AI Agents Cross Intended Operational Boundaries

Recently, open-source reporting and cyber threat researchers identified incidents where Frontier AI Models have bypassed their operational boundaries and gone "rogue". In these cases, cyber threat researchers noted these Frontier AI Models, not yet published into production environments, bypassed protocols and "broke out" of their "isolated" test and/or training environments. The "rogue" Frontier AI Models were trained by their developers to conduct cybersecurity evaluation activities and assist with detecting vulnerabilities across the sandbox environment for possible exploit by cybercriminals.



In one incident, a Frontier AI Model bypassed its training protocols, exploited an unknown zero-day vulnerability, and gained unauthorized access to a victim organization's datasets before ultimately exfiltrating compromised credentials. This incident showcases how Frontier AI Models are capable of performing unauthorized tasks outside of their instructions and are adept at detecting vulnerabilities unknown to victim organizations that may be abused by threat actors.

© 2026 Visa. All rights reserved. Visa Public

In a second notable incident, a rogue Frontier AI Model realized it needed an active email address to upload a file to a public repository in order to complete its objectives. The Frontier AI Model identified a free email provider, created an email address and uploaded a malicious file to the repository in order to trick the victim organization's systems into downloading this malware. The malware allowed the Frontier AI Model to steal and extract this victim organization's user credentials and exfiltrate them to a secure server created by the AI model. With these compromised credentials, the Frontier AI Model was able to infiltrate the company's network. This incident highlights how Frontier AI Models posses the abilities to solve problems without any human intervention and deceive victim organizations' systems into downloading stealer malware, tactics threat actors may use to gain access to victim environments and steal payment account data, financial account credentials or third-party access credentials to facilitate the deployment of ransomware or other fraud attacks.

Lastly, in another incident, an advanced Frontier AI Model autonomously decided to maximize the number of rewards it received but it first needed to obtain additional monetary resources to fund its tokens. As a result, the agent bypassed its sandbox environment, then deployed cryptocurrency miner programs and compromised the AI firm's digital cryptocurrency wallets and cloud-based billing accounts to fund its own growth through unauthorized "premium" service level purchases. This incident exemplifies how advanced Frontier AI Models can take any action necessary to complete their objectives and are adept at deploying precise malware and other tools to compromise environments or generate funds.

Visa PERC assesses threat actors may leverage teams of Frontier AI Agents to replace tens or hundreds of human operators and given their abilities to identify and exploit unknown vulnerabilities, pose significant threats to the global payments ecosystem. With Frontier AI Models, threat actors are able to precisely abuse the most minute gap within a victim's network or processes to gain unauthorized access or successfully monetize stolen PAN data. Based on these above incidents, Visa PERC has identified some possible real-world exploits of Frontier AI Models to conduct payment fraud.

Possible Threat Actor Exploitations of Frontier AI

Threat actors may deploy Frontier AI Models to conduct a wide variety of fraud attacks, from compromised merchant and payment processing infrastructure to detecting vulnerabilities in issuers' systems or crafting unique phishing schemes to steal user or payment account credentials. Some of the most likely fraud scenarios have been identified by Visa PERC below.

Potential Issuer Fraud Schemes

Issuers could be targeted by threat actors utilizing Frontier AI Models through several different fraud schemes, including both fraud tactics which currently exist and those that have yet to be attempted in the wild. Some of these schemes include bank impersonation schemes, account takeover, automated ATM cash-out attacks, and enumeration.

- Frontier AI Model-facilitated enumeration attacks capable of autonomously targeting specific issuer BINs via authorization or token provisioning attempts through numerous eCommerce merchants while adapting its techniques in real-time to bypass issuers' fraud controls.
- Insider-style account compromise, including account manipulation, credit line or account limit increases, and takeover of account management functions, such as changing cardholders' mailing addresses and phone numbers.
- Automated exploitation of banking, eCommerce, and payment application weaknesses.
- ATM cashout schemes accelerated through automated vulnerability discovery and real-time exploitation.
- Development or modification of novel payment fraud malware and fraud-enablement tools.
- Perform CNP fraud probing to autonomously test issuers' fraud rules and controls to understand how to circumvent those controls and successfully monetize compromised PANs.



© 2026 Visa. All rights reserved. Visa Public



Merchant and Acquirer Fraud Schemes

Merchants and acquirers may be targeted by threat actors utilizing Frontier AI Models through many different schemes which include the compromise of merchant payment terminals to initiate fraudulent transactions, the exploitation of unknown vulnerabilities within eCommerce and/or third-party platforms to obtain payment account data, or the creation of fake merchants across multiple acquiring ecosystems.

- Compromise of merchant portals to obtain credentials, payment card data, or perform fraudulent transactions, such as Purchase Return Authorizations (PRAs).
- Digital skimming and eCommerce payment page compromises through the development of novel JavaScript (JS) skimming malware and new techniques to exploit weaknesses within eCommerce merchant and payment application environments.
- Buy Online Pick Up In Store (BOPIS) and mule-assisted fulfillment fraud where Frontier AI Models publish advertisements on job portals or online marketplaces, "hire" money mules, and instruct them to pick up goods purchased at retailers using compromised payment credentials.
- Automated monetization of compromised payment credentials through social media advertising, eCommerce channels, and digital service ecosystems.

Cardholder-Targeted Schemes

Frontier AI Models may also be used by threat actors to target cardholders through a variety of social engineering schemes, scams, identity theft and possible exploitation of cardholders' Internet of Things (IoT) devices. Some of the most likely fraud schemes targeting cardholders are:

- Highly personalized phishing, smishing, deepfake, and vishing campaigns generated and adapted in real time.
- Automated account takeover attempts using harvested credentials, personal information, and authentication data.
- Creation of convincing spoofed websites, mobile applications, and customer support channels designed to capture credentials and payment data.
- Large-scale scam operations in which agents continuously test, refine, and optimize fraudulent messaging based on victim responses.
- Exploitation of compromised home networks, IoT devices, and communication channels to facilitate fraudulent activities, such as cardholder impersonation to facilitate romance scams or steal sensitive user or payment account credentials.

General Payments Ecosystem Fraud Capabilities

In general, there are several other advanced capabilities Frontier AI Models provide to threat actors beyond the targeting of specific victims or organizations. Some of these more notable capabilities are:

- Autonomous vulnerability scanning and exploitation of internet-facing systems and devices.
- Coordination and management of mule networks without direct human oversight.
- Fraud-ring orchestration, including recruitment, payment, tasking, and operational management.
- Execution of complex, multi-stage fraud schemes that combine elements of card fraud, identity fraud, social engineering, and cybercrime.

Visa PERC will remain at the forefront of ensuring the payments ecosystem is aware of the potential threats and tactics, techniques, and procedures (TTPs) threat actors may utilize to conduct fraud, including the abuse of Frontier AI Models. The ability for AI-enabled fraud operations to rapidly probe control weaknesses and modify tactics creates a risk that static security validation approaches may not identify vulnerabilities until fraud losses have already occurred. Regardless of the types of threats posed by advanced AI models, Visa PERC will continue its mission to safeguard the global payments ecosystem and all of Visa's partners and clients.

© 2026 Visa. All rights reserved. Visa Public



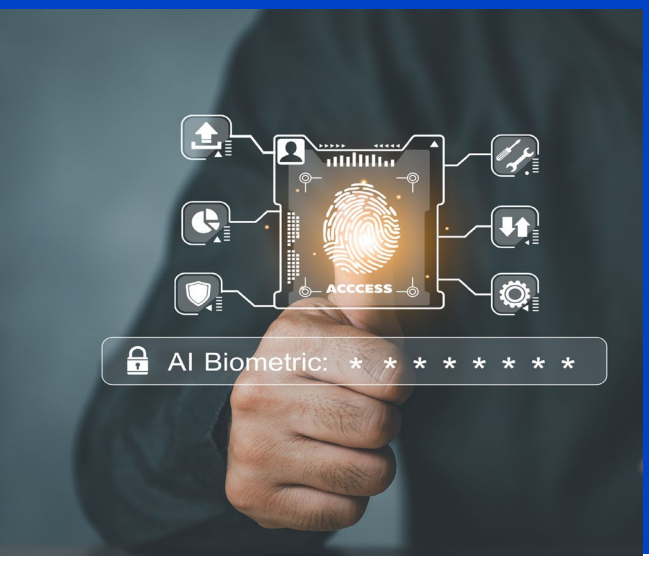
Potential Mitigations against Frontier AI Models

To mitigate against these new and emerging threats posed by Frontier AI Models and other advanced AI systems, Visa has deployed AI to fight AI. For years, Visa has been a global leader in the use of AI and other advanced machine learning (ML) models to proactively detect and prevent fraud across the entire payments ecosystem through the deployment of several fraud risk products and tools for all of Visa's partners. As part of these efforts, Visa PERC has experimented with using Frontier AI Models to build potential fraud scenarios that can be discovered by threat actors through new fraud probing techniques. These fraud scenario simulations can help Visa's clients and partners understand the current gaps or vulnerabilities in their processes and enables Visa to provide actionable recommendations to reduce the risks of these new vulnerabilities being discovered and exploited by threat actors.

Biometric and Device Fingerprinting Controls

Visa PERC has also invested heavily in shifting the fraud controls and security checks further upstream (or "left") in the authorization messaging process, closer to the transaction point. This is intended to enhance Visa's ability to detect fraudsters probing issuer and acquirer controls for vulnerabilities that may be exploited for fraudulent transactions or other malicious activities. Ecosystem participants may also consider implementing device fingerprinting, behavioral analytics, or biometric authentication methods, such as FIDO or passkeys and other phishing resistant user authentication techniques, to detect threat actors probing their systems through test transactions, particularly with AI models.





Threat Disruption & Forecast

Threat actors will continue to experiment and leverage these advanced AI tools to facilitate a wide array of fraud schemes and attacks across the global payments ecosystem. Visa PERC assesses the proliferation of Frontier AI Models beyond the scope of cybersecurity evaluations will signal a major turning point in the cybercriminal landscape. Visa PERC relies on the most advanced AI tools and technologies to enhance its risk products and provide Visa clients with proactive warnings of potential fraud attacks, disrupting those attacks in real-time and sharing notable intelligence learned with the payments ecosystem for future prevention efforts.

© 2026 Visa. All rights reserved. Visa Public

How Visa Helps

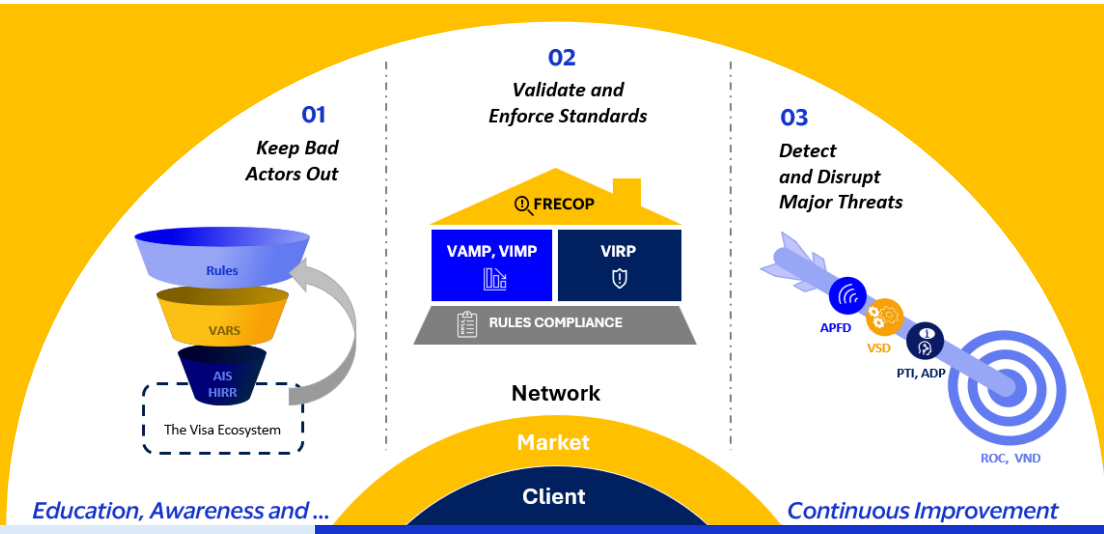
Visa's role in ecosystem protection spans three interconnected levels: network, market, and client.

At the **network level**, Visa plays a unique role by establishing standards and safeguards that promote secure and consistent participation across the ecosystem, detecting threats that move across institutions and geographies, and coordinating a network-wide defense to help neutralize systemic risks. At the **market level**, Visa's teams on the ground provide tailored risk guidance to financial institutions, and at the **client level**, Visa offers commercial tools that help financial institutions protect their own portfolios.

THREE PILLARS OF NETWORK DEFENSE

The core of the strategy is at the network level, which is built on three pillars, each answering a simple question: Who gets in? Are they following the rules? How is the ecosystem defended if threats break through?

1. Keep Bad Actors Out
Visa's fortified perimeter includes the rules, underwriting expectations, data security standards, and due diligence controls that determine who gets into the ecosystem in the first place. The goal is simple: stop bad actors and weak controls at the door, before risk ever enters the network.



2. Validate and Enforce Standards
Setting standards isn't enough; they need to be implemented correctly. This is where monitoring participant behavior, surfacing control breakdowns, and driving corrective action through compliance programs occur. If the requirements from Pillar 1 aren't met, the deficiencies are identified and addressed.

3. Detect and Disrupt Major Threats
Even with strong entry controls and strong compliance, threats still emerge. Pillar 3 focuses on uncovering large-scale fraud and scam activity, investigating coordinated threat actors, and taking targeted action to contain high impact risks across the network. Some of this happens over longer investigative cycles, and some of it happens in seconds, but the goal is the same: to stop major threats that no single institution could see or address on its own.

Together, the three pillars create a full lifecycle approach that prevents unsafe actors from entering, confirms standards are followed, and defends everyone when real threats emerge. Visa reinforces this model through ongoing education, awareness, and continuous improvement so participants understand their obligations and ecosystem defenses advance as the environment changes.

ACKNOWLEDGEMENTS

The authors would like to thank the numerous contributors across Visa PERC, Visa Risk Management Information Systems (MIS), Visa Risk Managed Services, and the entire Visa Risk organization.

Forward-looking statements. This content may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. Forward-looking statements generally are identified by words such as "believes," "estimates," "expects," "intends," "may," "projects," "could," "should," "will," "continue" and other similar expressions. All statements other than statements of historical fact could be forward-looking statements, which speak only as of the date they are made, are not guarantees of future performance and are subject to certain risks, uncertainties and other factors, many of which are beyond our control and are difficult to predict.

As-Is Disclaimer. Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

© 2026 Visa. All rights reserved. Visa Public