A Payment Ecosystem Report by
Visa Payment Ecosystem Risk and Control

Biannual Threats Report

Spring 2025

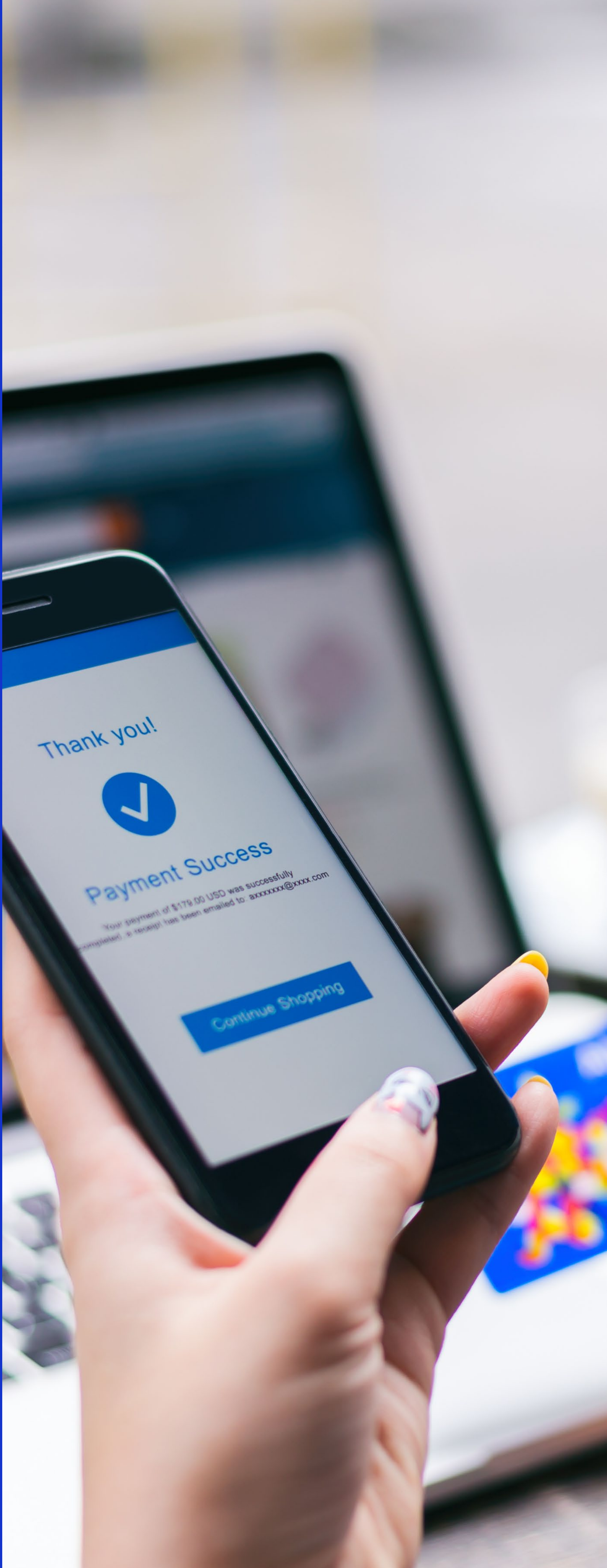

Thank you!
Payment Success
Your payment of $179.00 USD was successfully completed, a receipt has been emailed to: axxxxxxx@xxxx.com
Continue Shopping

Table of Contents

Executive Summary 2
Payments Threat Landscape: Overview and Trending Tactics 3
Exploitation of System Misconfigurations 6
Scams Continue to Proliferate Across the Payments Landscape 7
Threat Actor Disruption 9
How Visa Helps 10

Executive Summary

This report provides an overview of the top payments ecosystem threats within the past six-month period (July – December 2024) as identified by Visa Payment Ecosystem Risk and Control (PERC). Over the past six months, Visa PERC noted a marked increase in threat actors combining the targeting of cardholders with exploiting advances in technology to facilitate scaled and impactful fraud schemes. Scammers continued to use tried-and-true social engineering tactics to obtain sensitive information from cardholders, and the past six-months saw scams grow in scope and volume. Threat actors also used technology to their advantage to facilitate and scale their fraud schemes, including creating malicious mobile applications and the use of near field communication and data relay technology. Threat trends highlighted in this report include:

- **Enumeration** attacks remain a popular vector for threat actors to validate and compromise payment credentials, resulting in around **US$1.1B** in follow-on fraud in a one-year period. Over the past six months, there were hundreds-of-millions of suspected attack transactions representing **22%** increase from the prior six-month period.
- In the latter half of 2024, Visa PERC identified multiple sophisticated fraud schemes leveraging **provisioning fraud, malicious mobile applications, vulnerabilities in point-of-sale (POS) environments, and social engineering tactics**. Overall, these emerging threats increased in volume and present significant risks to payments organizations globally. Visa PERC analysis identified a continued interest from threat actors in innovating fraud tactics, particularly in the use of social engineering, one-time passcode (OTP) bypass scams, and provisioning fraud.
- Visa PERC continues to detect, investigate, and disrupt **scam activity** impacting the ecosystem. In the last twelve months, Visa PERC detected US**$357M** in fraud associated with scams and over **20K** merchants involved in scams.
- Visa PERC's eCommerce Threat Disruption (eTD) capability, which scans webpages of eCommerce merchants for any known **digital skimming** malware or malicious code and alerts the impacted merchant or their acquirer of the potential compromise, identified a **7%** increase in websites identified as infected.
- From July through December 2024, Visa PERC identified **ransomware and data breach** attacks that were opportunistic in exfiltrating data, with several thousand ransomware and data breach incidents tracked by Visa PERC over the past six months, a **51%** increase from the prior six-month period.

In response to many of the threats detailed in this report, Visa PERC implemented pre-emptive, targeted blocks in coordination with impacted organizations on **76%** of these incidents to mitigate fraud. These instituted blocks of presumed fraudulent transactions from July through December 2024 resulted in over **134.3M** declined transactions.

Over the past five years, Visa has invested US**$12B** in cutting-edge technology to combat fraud. During the 2024 holiday season, as shoppers flocked to both physical and digital stores, fraudsters were also on the move. However, Visa's advanced **Artificial Intelligence** (AI) and machine learning blocked nearly **85% more** suspected fraud globally during this period compared to last year.

Payments Threat Landscape: Overview and Trending Tactics

Enumeration Remains a Top Ecosystem Threat

Enumeration (i.e., the programmatic, automated testing of common payment data elements via eCommerce transactions to effectively guess the full payment account number, CVV2, and/or expiration date) remains among the top threats to the payment ecosystem. Global enumeration rose overall over the past six months, peaking in November 2024.

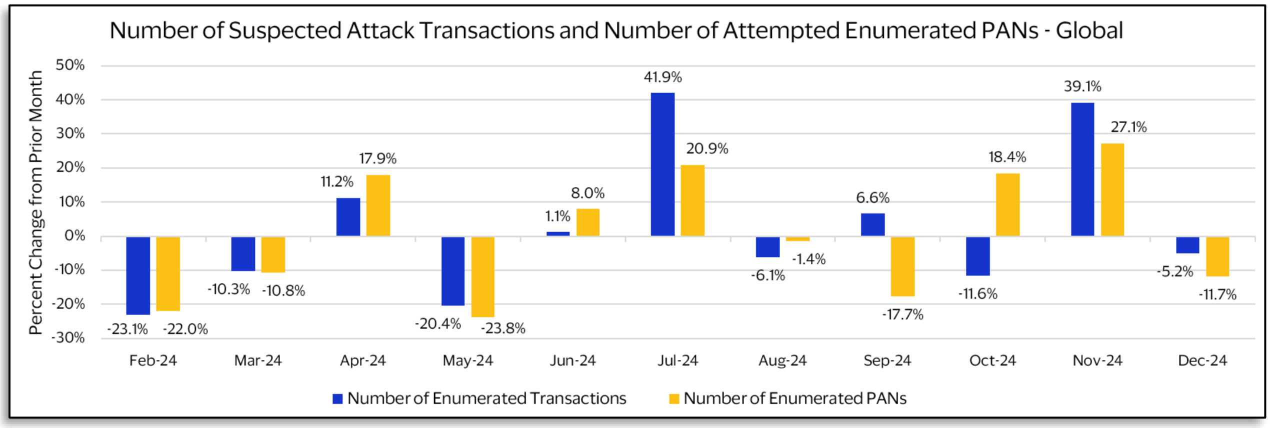
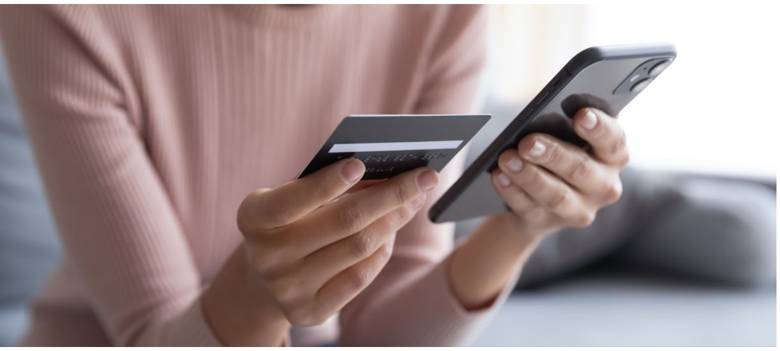


Figure #1 - Source: Visa PERC

The number of enumerated transactions increased **22%** and the number of enumerated PANs increased **8%** compared to the total global volume over the prior six-month period.



Visa PERC vigilantly monitors for enumeration attacks through the Visa Account Attack Intelligence (VAAI) capability using generative AI to identify enumeration attacks. VAAI then analyzes the details of the attack and enables Visa to notify affected acquirers/merchants and help affected acquirers/merchants block egregious attacks. Prior to any blocking, Visa PERC undertakes an extensive impact review and analysis, including client/stakeholder analysis, to mitigate and prevent the successful enumeration of payment accounts while maintaining minimum impact on any legitimate activity.

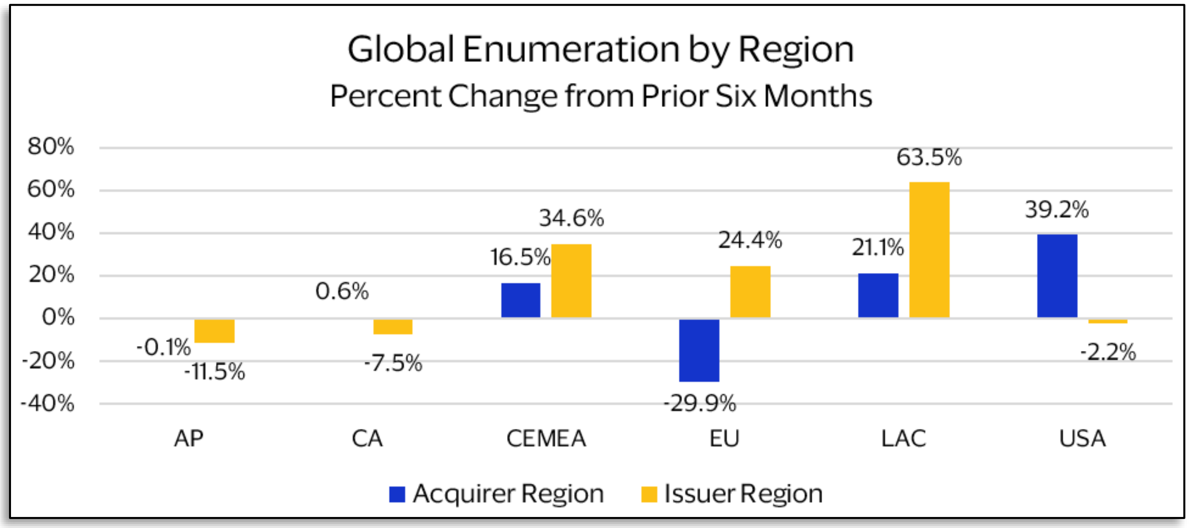


Figure #2 - Source: Visa PERC

Visa Increases Identifications of Website Skimmers

One of the most prolific and consistent threats to the payments ecosystem are digital skimming attacks. In digital skimming attacks, threat actors deploy malicious code onto the checkout page of a merchant website in an attempt to harvest payment account data and other PII, such as PAN, card verification value (CVV2), and expiration date, entered into checkout forms by the merchant's customers. Visa PERC combats digital skimming attacks with the eCommerce Threat Disruption (eTD) capability. Visa eTD scans webpages of eCommerce merchants for any known digital signature, footprint of digital skimming malware, or malicious code and alerts the impacted merchants' acquirer, webmaster, or merchant of the potential compromise. Over the past year, the number of digital skimmers detected on websites has remained generally consistent, as shown in the graph below.

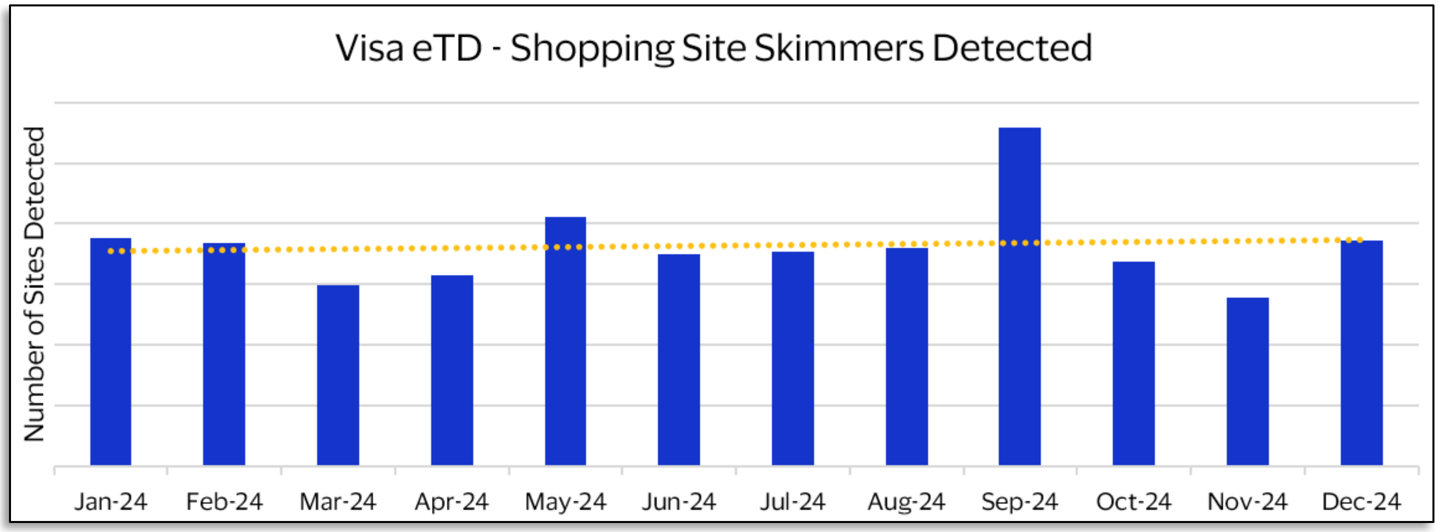


Figure #3 - Source: Visa PERC

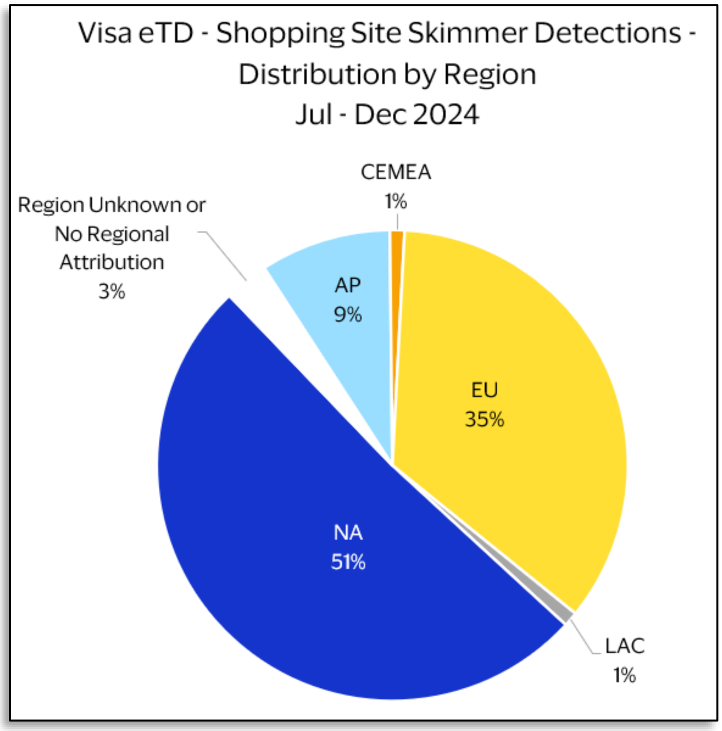
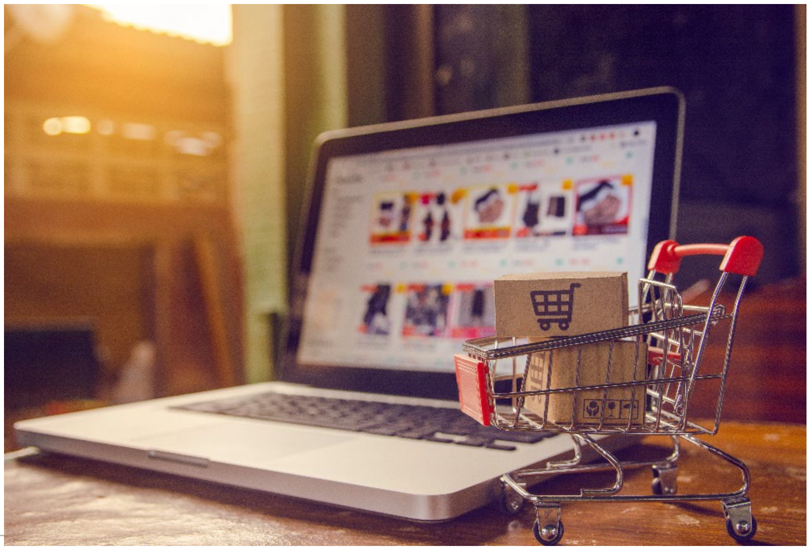


Figure #4 - Source: Visa PERC

Over the past six months, Visa eTD identified the North American region as the most targeted global region, with **51%** of the detections occurring on North American merchants, as shown in Figure #4. The Europe region experienced the second-highest number of compromised merchant websites identified. The regional percentages remained steady when compared to the prior six-month period.



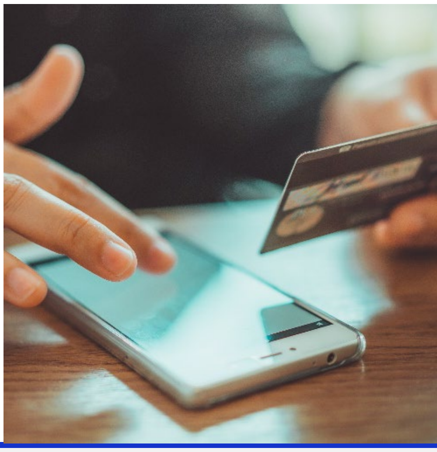
Fraud Schemes Employ Malicious Apps and NFC Technology

In the latter half of 2024, Visa PERC identified multiple sophisticated fraud schemes leveraging provisioning fraud, malicious mobile applications, vulnerabilities in point-of-sale (POS) environments, and social engineering tactics.

Malicious Mobile Application and POS Vulnerability

In September 2024, Visa PERC identified a fraud scheme involving threat actors completing a fraudulent provisioning request or loading compromised or invalid payment account data into a malicious mobile application. Using the malicious application, the threat actors conduct card present (CP) transactions at brick-and-mortar retailers. The malicious application triggers an offline authorization response from the terminal, allowing the threat actors to receive in-store offline approvals for purchases with compromised or invalid account data.

Visa PERC observed a variation of this fraud attack in the Europe region where threat actors used automated teller machines (ATMs) as the cashout vector as opposed to brick-and-mortar retailers.



Near Field Communication (NFC) Code Used in Relay Fraud

Visa PERC identified a continuation of the use of Near Field Communication (NFC) relay attacks in which threat actors use a malicious mobile application and sophisticated social engineering schemes to convince victims to unknowingly participate in this scheme and provide payment information.

Since Visa PERC first reported on this fraud scheme, threat actors continue to use the open-source project NFCGate to conduct relay attacks. NFCGate enables a malicious application to capture, analyze, and modify NFC data. This data can then be sent from the victim's device to multiple threat actor devices anywhere in the world. Threat actors then monetize the victim's payment information at a different physical location.

It is important for individuals to be vigilant and remain wary of downloading applications from potential threat actors. Lastly, Visa PERC assesses that threat actors will continue to attempt to exploit misconfigurations in POS environments and settings, and issuers, acquirers, and merchants should remain vigilant in combatting fraud related to offline transaction fraud schemes.

Enhanced monitoring, strict controls around token provisioning, employee training, and industry collaboration are essential to combat these sophisticated fraud schemes. Visa PERC will continue to monitor and report on emerging threats to support clients in maintaining secure and trusted payment environments.

Provisioning Fraud Continued to Shift to Delayed Cashout Times

Provisioning related fraud – defined as fraudulent transactions occurring within seven days of a token's activation primarily impacting device bound tokens – continues to be a favored tactic for threat actors.

Threat actors continue their efforts in fraudulently provisioning payment accounts to threat actor-controlled mobile devices, typically through OTP bypass phishing schemes such as "package delivery" or bank impersonation schemes. In the July 2024 Biannual Threats Report, Visa PERC noted a shift in threat actors' choice in cashout timing after fraudulently provisioning a payment account, with an increasing preference to lengthen the lag time after provisioning before attempting to monetize. Visa PERC continued to see that trend expanding over the July to December 2024 period. Correspondingly, Visa Risk identified that, in general, provisioning fraud rates in the first seven days after token activation trended downwards in 2024, with a **29%** decrease globally in the first seven days post provisioning when compared to prior year data. This supports the identification of the threat trend to delay the monetization of the account for a week or more after the fraudulent provisioning.

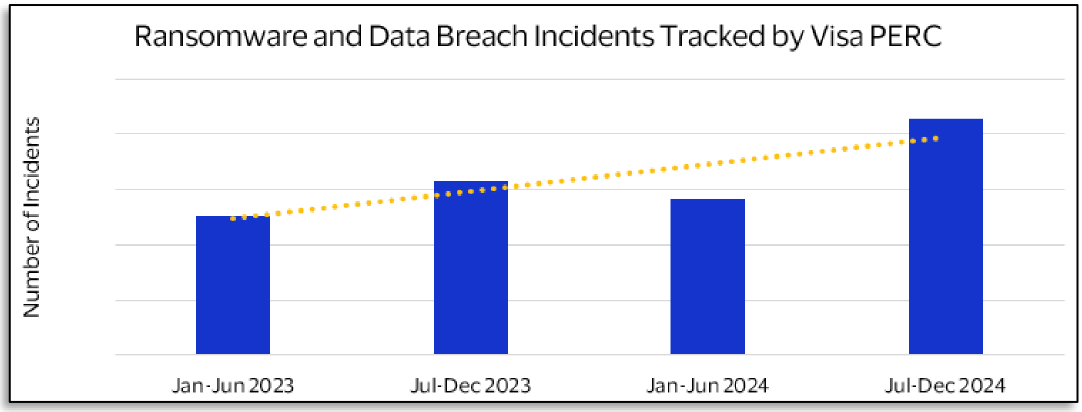
Mitigations against this change in fraud tactic could include issuers considering token age, in terms of time since activation, as well as time since first transaction with the credential (i.e. treating a token that is transacting for the first time to the same rules implemented for a token transacting immediately after provisioning).

Exploitation of System Misconfigurations

Threat actors continued to probe the payments ecosystem for vulnerabilities and were successful in conducting targeted and sophisticated fraud schemes impacting specific institutions, technology, and processes.

Ransomware Continues to Strike Payments Ecosystem Entities

Ransomware and data breaches continue to threaten the payments ecosystem. Threat actors exfiltrate payment data and personal identifiable information (PII) from their victims, which aids in their profit-making goal by extorting victims and selling / releasing data on the cybercrime underground. From July through December 2024, Visa PERC identified ransomware and data breach attacks that were opportunistic in exfiltrating data, with thousands of ransomware and data breach incidents tracked by Visa PERC over the past six months, a **51%** increase from the prior six-month period.



Although ransomware and data breach attacks remain a global concern, the North America region remains the most targeted region.

Figure #5 - Source: Visa PERC

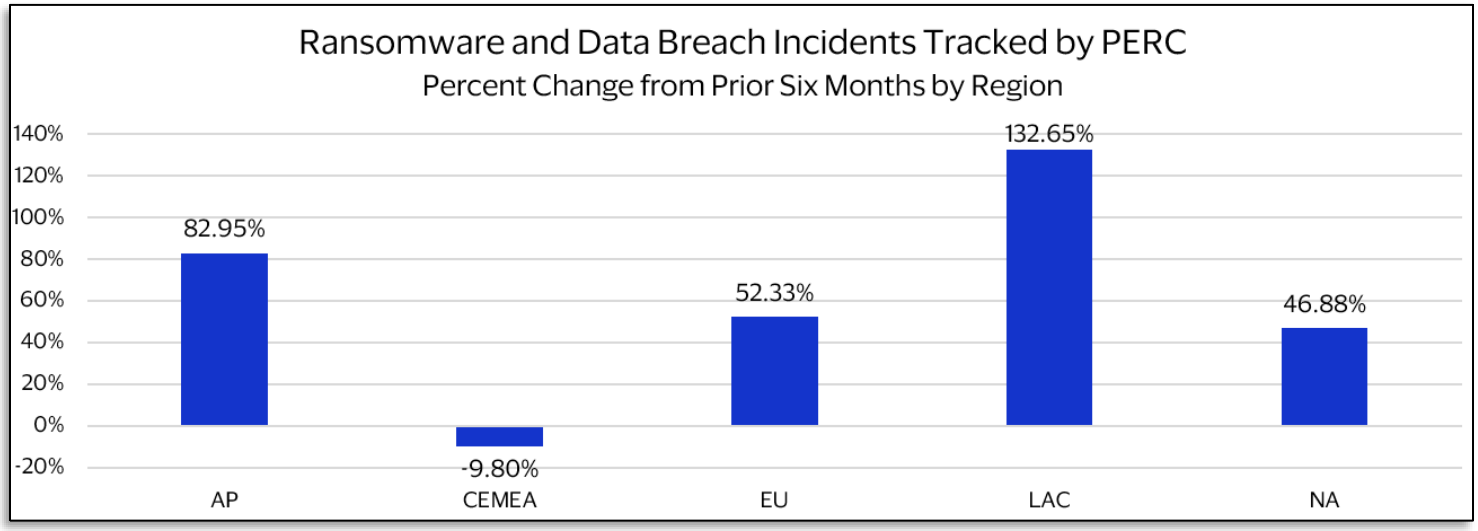


Figure #6 - Source: Visa PERC

The presence of ransomware and data breach attacks across sectors should serve as an indication that threat actors will attempt to target any vulnerable entity. Visa PERC and global law enforcement are partnering closely to disrupt threat actors carrying out ransomware campaigns.

Scams Continue to Proliferate Across the Payments Landscape

Threat actors are increasingly turning their focus to cardholders, using advanced social engineering techniques to facilitate elaborate and well-designed scams. To combat the increase in consumer-focused scams, Visa PERC established a Scam Disruption capability that proactively and reactively addresses scams targeting consumers and the payments ecosystem. Through this capability, Visa Scam Disruption has dismantled numerous fraud rings responsible for hundreds-of-millions of US dollars in fraud losses. Additionally, Visa works closely with ecosystem partners to identify, mitigate and disrupt scam activity at a global scale. By identifying the tactics, tools, and infrastructure the threat actors are using to conduct scam activity, Visa Scam Disruption dismantles scam campaigns at the source. Visa is committed to maintaining and bolstering the security of the payments ecosystem, and Visa Scam disruption continues to ensure Visa is the safest and most secure way to pay and be paid.

Visa Scam Disruption

Visa PERC continues to detect, investigate, and disrupt scam activity impacting the ecosystem. Visa PERC defines scam activity as an authorized payment that a cardholder was deceived into making. Scam activity disrupted by Visa PERC includes multimillion dollar marketing scams, fraudulent debt consolidation scams, and widespread scam rings using fake eCommerce sites to commit fraud. Visa PERC has made significant steps to expand Visa's scam disruption capabilities and further secure the payments ecosystem. Through partnerships with clients, law enforcement, technology providers, and internal partners, Visa PERC's scam disruption efforts have had an immediate impact. In the last twelve months, Visa PERC has detected US**$357M** in fraud and over **20K** merchants involved in scams.

In November 2024, Visa PERC investigated a marketing scam operated out of North America wherein fraudsters targeted individuals looking to create and market online businesses. The scammers charged high fees, often amounting to thousands of dollars, for assisting the victim in setting up a business and website. If the victim lacked sufficient funds, scammers persuaded or coerced victims into opening new credit accounts or the scammers opened new credit accounts using the victim's personal identifiable information (PII). The investigation preceding the alert identified tens-of-millions of USD in fraud exposure as well as several million in reported fraud loses between September 2023 and August 2024.

While some scammers capitalize on individuals' entrepreneurial ambitions, others take to preying on individuals looking to streamline their personal finances. In late 2024, Visa PERC identified a debt consolidation scam operating in North America. Threat actors impersonated customers and spoofed customer account numbers to bypass fraud detection, misleading victims into believing their debts would be consolidated at lower interest rates. These scams led to compromised PII at other financial institutions, exacerbating the threat landscape. Through this investigation Visa PERC uncovered US**$10M** in fraud exposure and US**$1M** in confirmed fraud. This new scam trend demonstrates threat actors' continued creativity and persistence in developing new scam vectors and targeting vulnerable communities.

As well as investigating sophisticated social engineering scams, Visa PERC also investigated and disrupted widespread eCommerce scams impacting the global ecosystem. Throughout the last six months, Visa PERC investigated and continues to disrupt a global scam ring focused on using fake eCommerce shops to steal individual payment card information or entice victims to make purchases wherein no goods or services are subsequently received. These fake eCommerce shops are known to impersonate well known luxury brands as well as take the form of fraudulent store fronts selling an assortment of goods. By abusing legitimate eCommerce platforms and website template building services, threat actors easily create thousands of fraudulent eCommerce shops. This tactic allows threat actors to overwhelm the ecosystem with fake shops, not only increasing their chances of successfully stealing from victims but also making it more difficult to dismantle all of their malicious infrastructure. To date, Visa PERC identified over **20,000** domains associated with this fraudulent eCommerce activity / campaign. Throughout this investigation, Visa PERC identified common infrastructure among fraudulent merchants, originating out of the EU and AP regions, and promptly engaged with the merchants' acquirers to disrupt the activity and secure the ecosystem. Visa PERC continues to identify shared infrastructure among these scam merchants and is actively working to dismantle this infrastructure.

Despite scams becoming more sophisticated, threat actors continue to use low cost and effective methods, such as phishing, to compromise victims' information. Threat actors are also taking advantage of people looking for jobs or extra income through what the United States Federal Trade Commission (FTC) is calling "task-based scams." These task-based scams originate with the threat actors sending text messages to victims, advertising online work related to app optimization. The victim is asked to complete small tasks within an app and may even receive a small sum of money from the threat actors to make the job seem more legitimate. After the victim completes multiple tasks, they are asked to pay to unlock more tasks with the promise of this leading to additional monetary compensation. The victims are most often asked to pay using cryptocurrency. Unsurprisingly, once the victim pays for a new task, their money is lost. The FTC reports a 300% increase in task-based scams over the past year, with over 20,000 victims and US$41M in losses. The FTC recommends individuals ignore generic texts about jobs from unknown senders and advises that individuals should not participate in any job that requires them to "pay to get paid." Visa PERC advises individuals to stay vigilant for phishing attacks, protect their PII, and report phishing attempts to the necessary parties.

Threat Actors Continue to Enhance Fraud Campaigns through the use of AI

As Visa PERC reported over the past year, threat actors are increasingly leveraging artificial intelligence (AI) to commit various types of fraud, exploiting the technology's capabilities to enhance their schemes. Trends in the use of AI-driven fraud include:

- Voice Cloning and Deepfakes: AI-powered voice cloning is used to mimic the voice of a known individual, such as a company executive, to authorize fraudulent transactions or gain access to sensitive information over the phone. Additionally, AI-generated deepfake videos and audio can convincingly impersonate individuals, often used to deceive targets into transferring money or revealing sensitive information. For example, a deepfake of a CEO might be used to instruct an employee to fraudulently wire funds to a new account.
- Phishing and Social Engineering: AI is used to craft highly convincing phishing emails that are personalized to the recipient. By analyzing social media profiles and other publicly available data, AI algorithms can create messages that appear to be from trusted sources, increasing the likelihood the recipient might fall for the scam.
- Automated Attacks: AI can automate and scale up cyber-attacks, such as credential stuffing or brute force attacks, by rapidly testing numerous combinations of usernames and passwords to gain unauthorized access to accounts.
- Synthetic Identities: AI can generate realistic synthetic identities by combining real and fake information. These identities can then be used to open bank accounts, apply for credit, or commit other financial fraud.
- Ransomware: AI can enhance ransomware attacks by making them more sophisticated. For instance, AI can be used to evade detection by traditional security measures, identify high-value targets within a network, and optimize the timing of attacks for maximum impact.
- Fake Stores, Reviews, and Promotions: AI can be used to scale the creation and execution of fake eCommerce website stores in attempts to steal customers' payment information. Additionally, AI can generate fake reviews for products and services to manipulate consumer opinions and boost the reputation of fraudulent businesses. Similarly, AI can create fake social media profiles and posts to promote scams.

Threat Actor Disruption

Visa PERC supported global law enforcement and government entities throughout the past six-month period to disrupt criminals targeting the financial and payments ecosystem. Many of the law enforcement and disruption efforts focused on dismantling criminal operations that leveraged new and novel techniques and technologies, which further represents the shifting threat landscape toward more advanced use of technology.

Accounts Recovered from Third Party Service Provider Breach of Ticketing Merchant

Visa PERC distributed 250 million at-risk accounts recovered in the ticketing merchant third party service provider breach investigation that recently resulted in the arrest of the perpetrators behind the May 2024 cyberattack on the third party service provider that impacted 165 companies. Two suspects were apprehended by law enforcement in 2024 for their alleged involvement in breaching dozens of networks by using stolen credentials from previous compromises to gain access to victim environments, steal the accounts at scale, and then demand ransoms from victims, ranging from US$300K to US$5M.

Suspects Arrested for Conducting US$150M in Fraud Transactions

Visa PERC's multi-year support of the international criminal investigation into a payment processor Allied Wallet, dating back to 2017, resulted in the indictment and arrest of the perpetrators behind the processing of US$150M in fraud transactions via over 100 fake merchant accounts. The five defendants in this case conspired to process thousands of high-risk fraudulent transactions via dozens of fake merchant accounts created to facilitate the fraud scheme. Four of the five defendants have pleaded guilty and face a potential of 30 years in Federal prison and a US$1M fine and restitution.

Joker's Stash Administrators Indicted

Visa PERC's multi-year support of the international investigation and 2021 takedown of the Jokers Stash carding forum by coordinated law enforcement efforts resulted in the Federal indictment of the top Jokers Stash administrators and money launderers. Jokers Stash, which was the world's largest and longest running illicit carding marketplace, was the illegal online shop where 100s of millions of stolen accounts from dozens of brick-and-mortar and online merchant network compromises were sold, dating to back to 2014. In addition to these criminal indictments, law enforcement also seized Cryptex, an illicit crypto exchange where US$1.15B in criminal proceeds stemming from Jokers Stash sales and fraud were laundered.

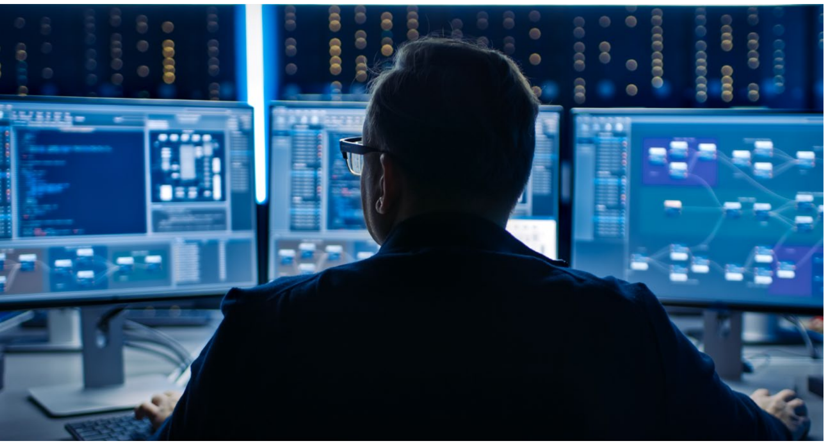
How Visa Helps

Visa Risk employs best in class individuals whose mission it is to combat the multitude of threats to the payments ecosystem.

People • Processes • Technology

People are the most important component in combating the threats described throughout this report, and Visa's experts work across various teams within Visa Risk, such as the 24x7 Risk Operations Center (ROC) which triages and analyzes fraud related incidents and transaction-level alerting globally and around the clock to ensure the threats are identified and mitigated. Through this always-on monitoring, Visa proactively identifies and mitigates catastrophic losses from fraud attacks. The Visa Payment Threat Intelligence (PTI) team compiles robust intelligence on the threats targeting the payments ecosystem and communicates these threats, alongside best practices and recommendations, to mitigate and prevent the threats. The intelligence, which is developed through transaction data analysis, source monitoring, and technical analysis of malware, tools, and infrastructure used to facilitate cyber and fraud attacks against the payments ecosystem, is available to Visa clients through the VPTI service. Through the close integration of people and technologies, Visa Risk developed processes to mitigate and prevent payments ecosystem attacks. For example, upon the identification of egregious fraud attacks Visa conducts extensive processes to determine the best surgical block methods to prevent further fraud but minimize impact to legitimate transactions. This involves detailed analysis of attack transactions and authorization messages, as well as overall payment volume and impact.

Visa has invested heavily in security technologies to prevent, detect, and eradicate threats to payment data and infrastructure. Capabilities such as eCommerce Threat Disruption (eTD), Visa Account Attack Intelligence (VAAI) and Visa Payments Threats Lab (VPTL) enable Visa to proactively identify eCommerce threats, enumeration attacks, and clients' systems vulnerabilities to increase security and protection of clients and cardholders across the payments ecosystem. Over the past five years, Visa has invested US**$12B** in cutting-edge technology to combat fraud. During the 2024 holiday season, as shoppers flocked to both physical and digital stores, fraudsters were also on the move. Throughout the Black Friday / Cyber Monday holiday weekend, suspected fraudulent transactions rose **200%** around the world, due in part by the adoption of AI by fraudsters. However, Visa's advanced AI and machine learning capabilities blocked nearly **85% more** suspected fraud globally compared to last year.



Recommendations

There are many resources available for banks and cardholders on Visa's website providing methods, strategies and best practices for preventing and mitigating many of the threats identified in this report.

Visa recommend **banks, merchants, and other payment ecosystem entities** consider implementing the following best practices:

1. Ensure all utilized software, including point-of-sale (POS) terminals and payment acceptance devices, are updated to the latest software version, including deployed security patches. Regularly conduct security audits and vulnerability assessments.
2. Regularly train employees on recognizing phishing attempts, social engineering tactics, and other common fraud schemes. Communicate the importance of safeguarding customer information and data and establish clear protocols for reporting and responding to suspected fraud incidents.
3. Enhance Customer Authentication Processes by requiring multi-factor authentication (MFA) and biometric verification during payment processes and to prevent unauthorized access to customer accounts.

4. Work closely with industry partners such as payment networks, law enforcement, and other key payment ecosystem stakeholders to share threat intelligence and collaborate on disrupting fraud schemes.
5. Proactively educate customers on current scam trends and how to effectively recognize and protect themselves against the threat activity.

Visa recommends **cardholders** consider the following best practices to help prevent fraud:

6. Do not click on unsolicited hyperlinks found in emails or text messages from unknown or suspicious sources.
7. Use cybersecurity best practices, including enabling anti-phishing protection on your web browser and ensuring multi-factor authentication (MFA) and unique, strong passwords are implemented on all sensitive log in environments.
8. Contact your bank directly by using the phone number or website listed on the back of your card, rather than following guidance from an email, phone call, or text message you received.
9. Watch for scam indicators in the method of payment being requested: scammers often ask for payment in the form of wire transfers or other money transfers, reloadable or prepaid gift cards, cryptocurrency, or sending cash, since these formats are more difficult to trace. Monitor financial statements for any suspicious or unexpected transaction activity.
10. If you suspect a scam, stop and talk to someone you trust about the situation and seek guidance from the organization’s official website before acting on the suspected scammers request

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.

Disclaimer: This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it. All Visa Payment Fraud Disruption Situational Intelligence Assessment content is provided for the intended recipient only, and on a need-to-know basis. PERC reporting and intelligence are intended solely for the internal use of the individual and organization to which they are addressed. Dissemination or redistribution of PERC products without express permission is strictly prohibited.