A Payment Ecosystem Report by
Visa Payment Fraud Disruption

Biannual Threats Report

Fall 2024

VISA

Contents

Executive

Summary

Executive Summary

This report provides an overview of the top payments ecosystem threats within the past six-month period (January – June 2024) as identified by Visa Payment Fraud Disruption (PFD). In the December 2023 Biannual Report, Visa PFD noted an interesting shift in threat actors' organization, access to tools, and target choice, with threat actors increasing in their scope of abilities and sophistication given advances in technology. The past six-month period saw a continuation of these expanding trends in cross-sector collaboration and ingenuity, with a specific targeting two aspects of the ecosystem: 1) system misconfigurations and vulnerabilities and 2) cardholders.

Threat actors continue to probe the payments ecosystem for vulnerabilities and were successful in conducting fraud schemes affecting multiple financial institutions, technologies, and processes. An example of this impact is the erroneous approval of fraudulent transactions. These transactions are approved due to a mishandling of the authorization process and are used to initiate **Purchase Return Authorization** (PRA) attacks. Visa PFD opened a record number of PRA investigations over the past six months, an **81%** increase from the previous six-month period. Per successful attack, each of these fraud operations have resulted in potential losses of nearly **US$184K** for Visa's issuing partners.

Enumeration attacks remain a popular vector for threat actors to validate and compromise payment credentials, resulting in significant follow-on fraud. Over the past six months, the US region increased as the most heavily targeted region from the issuing side (**58%** of total issuer enumeration, increase of **16%** from the same period in 2023), but decreased from the acquiring side (**61%** of total acquiring enumeration, decrease of **3%** from the same period in 2023).

From January through June 2024, Visa PFD continued to identify **ransomware and data breach attacks** that were opportunistic in exfiltrating data. Overall, Visa PFD observed a **12.3%** decrease in the number of individual ransomware and data breach incidents tracked by the team as compared to the prior six-month period, within this figure, Visa PFD identified a continued trend of targeting of third-party service providers, as Visa PFD observed a **24%** increase from the previous six-month period in third-party service provider cases.

Digital skimming attacks remain prolific and consistent threats to the payments ecosystem. Over the past six months, the number of compromised websites detected by PFD remained relatively consistent.

The expansion and use of **Artificial intelligence** (AI) technology remains a top interest for threat actors. Visa PFD continues to track threat actors' interest in use of AI technologies to facilitate fraud and continues to note spikes in the volume of threat actor discussions in underground communities related to the release of new AI technology to public and underground marketplaces.

As threat actors are targeting identity data to perpetrate various fraud schemes, Visa PFD is identifying malicious enrollments and registrations of prepaid payment accounts. In addition to identifying individual instances of fraud, Visa PFD noted trends in registration information, which has resulted in the identification of larger fraud rings.

Equally, threat actors are also increasingly turning their focus to cardholders, using advanced **social engineering** techniques to facilitate elaborate and well-designed **scams**. Over the past six months, Visa PFD identified new scam tactics targeting retailers' digital wallet programs, evolved and increasingly complex impersonation scams, and a continuation of targeting authentication data, such as one-time passcodes (OTP). An interesting and seemingly contradictory tactic to the scams using innovating technology is the identified uptick in physical theft of cards and devices, with some threat actors turning back to the use of card-present transactions using physically stolen EMV® chip-enabled cards.

Overall, threat actors and groups continue to evolve into more organized and sophisticated operations, utilizing advanced tactics and cutting-edge technology to facilitate large-scale fraud operations that can exploit an identified vulnerability quickly and efficiently, as discussed throughout this report. In response, the **Visa Risk Operations Center** (ROC), Visa's 24x7 team responsible for working in conjunction with clients to triage and analyze large-scale fraud-related incidents globally, implemented pre-emptive, targeted blocks in coordination with impacted organizations on **68%** of these incidents to mitigate fraud without impacting legitimate transactions. These instituted blocks of presumed fraudulent transactions from January through June 2024 resulted in over **51.8M** declined transactions for **US$11.8B**.

This report includes an overview of notable payment ecosystem threats, best practices to mitigate, prevent and disrupt these threats, and how Visa Risk is combatting these threats to better protect the entire payments ecosystem.

Payments Threat Landscape

Payments Threat Landscape: Overview and Trending Tactics

Ecosystem Fraud Overview

Visa PFD identified trending tactics used by threat actors repeatedly throughout the course of the past six months. These tactics include:

- Sustained strengthening of threat actors' organization and sophistication to increase the efficacy of well-used techniques, as evidenced in enumeration and purchase return authorization attacks,
- The use of widely available tools and the latest advances in technology to exploit system misconfigurations and vulnerabilities, as seen in ever-evolving malware campaigns, and a
- Consistent interest in targeting cardholders to facilitate complex and costly consumer-focused scams.

The Visa Risk Management Information Systems (MIS) Team delivers insights to monitor fraud rate, proactively identify opportunities to reduce fraud within the payments ecosystems. Visa Risk MIS continued to observe the global fraud rate trending at or below normal levels for the past six closed months. While the overall global fraud rate has remained relatively stable over the past year, threat actors are shifting their focus and tactics to various areas within payments based on innovative technology, the global financial climate, and newly identified vulnerabilities. As noted in the December 2023 Biannual Threats Report, and continuing into 2024, threat actors are increasingly focusing efforts on bypassing fraud and security controls and newly implemented technology through more advanced and technical fraud schemes and/or finding new and novel ways to conduct fraudulent activity. The past six-month period experienced the continued trend of a general decrease in high-volume, low-level fraud and an increase in advanced, targeted, and more impactful fraud, which is reflected in the data below.

Enumeration Remains a Top Threat to the Payments Ecosystem

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, resulting in significant follow-on fraud.

Visa PFD tracks which Merchant Category Codes (MCCs) are targeted in attacks and, over the past six-months, identified MCC 5999 - *Miscellaneous and Specialty Retail Stores* as having the most enumerated transactions, followed by MCC 5812 – *Eating Places and Restaurants*, which is reflected in Figure 1. MCC 5999 was also the top enumerated MCC in the prior six-month period, making it the top overall MCC targeted consistently over the past year.

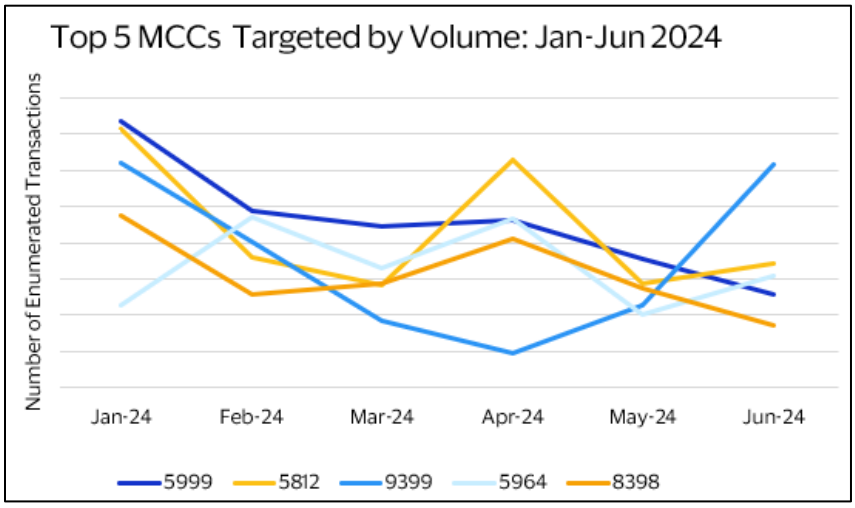
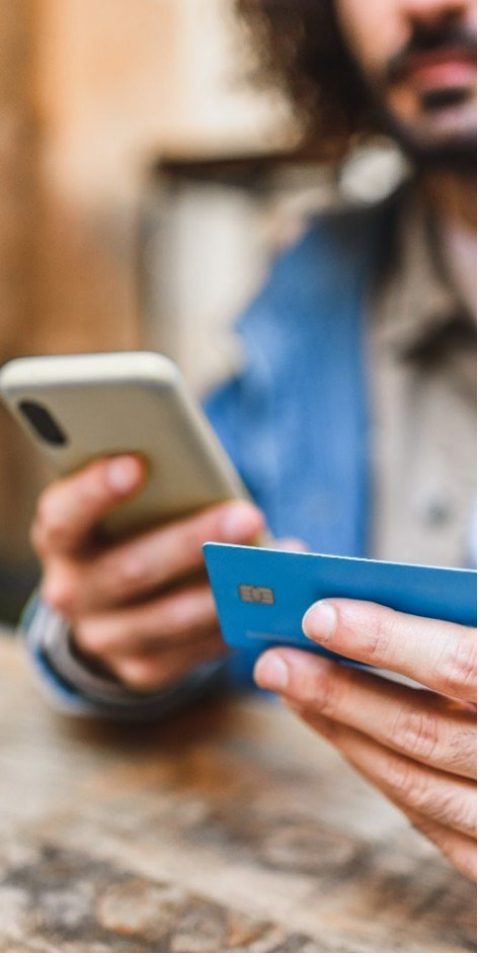


Figure 1 – Source: Visa PFD

Visa PFD vigilantly monitors for enumeration attacks through the Visa Account Attack Intelligence (VAAI) capability using machine learning 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 action implementation, Visa PFD undertakes an extensive impact review and analysis including client/stakeholder analysis in order to mitigate and prevent the successful enumeration of payment accounts while maintaining minimum impact on any legitimate activity.

MCC 5999	*Miscellaneous and Specialty Retail Stores*
MCC 5812	*Eating Places and Restaurants*
MCC 9399	*Government Services – Not Elsewhere Classified*
MCC 5964	*Direct Marketing – Catalog Merchant*
MCC 8398	*Charitable and Social Service Organizations*



The US region remained the most heavily targeted from both the acquiring side (61% of total acquiring enumeration) and issuing side (58% of total issuer enumeration), as shown in Figure 2. Compared to the same six-month period in 2023, this represents an increase in targeting of the US region for issuers (+16%) and a decrease in targeting of US acquires (-3%). Targeting of the Latin America and Caribbean (LAC) region decreased for both acquirers (-10%) and issuers (-8%) relative to the prior six-month period (Jul-Dec 2023).

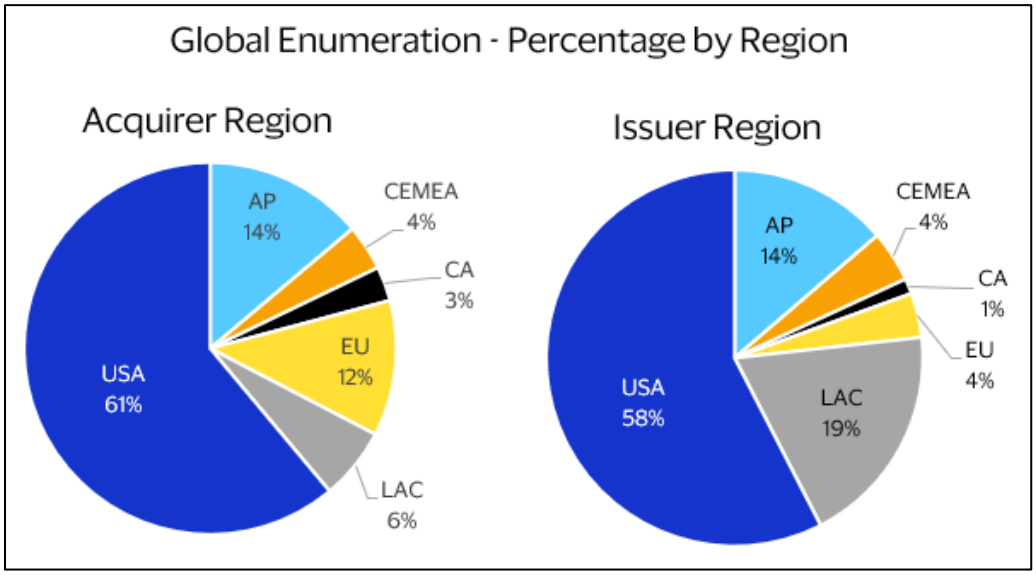


Figure 2 - Source: Visa PFD

The overall general trend of a decrease in global enumeration over the past eighteen months can be seen in Figure 3, with most regions showing a decrease in enumeration on both the acquiring and issuing sides, except for issuers in the US region, which saw a slight increase in the past six months.

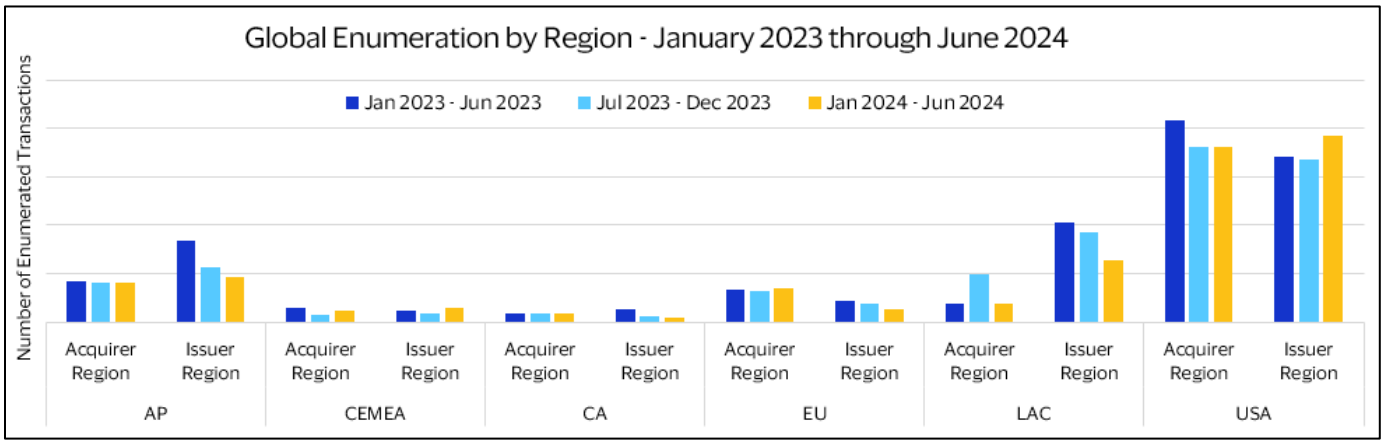


Figure 3 - Source: Visa PFD

The **Visa Account Attack Intelligence Score** is a new value-added real-time service grounded in artificial intelligence (AI) that aims to help issuers detect suspected enumeration activity. The Visa Account Attack Intelligence Score uses historical and near real-time data for transactions processed by VisaNet to generate a score with values in the 01-99 range for issuers to use when processing card-not-present transactions. Further details can be found on the Visa website.

In addition, in early 2024, enumeration attacks evolved to include distributed activity. The activity targeted merchants that belonged to various chains or a certain merchant category code. The activity was distributed across hundreds of merchants to give the appearance of minimal impact, however, when combining the merchants the activity had a significant impact. This type of distributed attack has been observed on merchants globally as well as impacted issuers globally. For more information on enumeration, visit Visa's website or contact your Visa account representative.

Trends in Digital Payments

The Visa Digital Payments space has also seen the consistent use of well-known tactics commonly used in direct money movement, including the tactics noted above, along with a persistence of various account takeover (ATO) scams used to obtain access to a victim's account then subsequently drain the account through direct money transfers. Another fraud technique noted over the past six months is the process of adding enumerated PANs to newly established (threat actor-controlled) accounts at money movement originators for the purpose of debiting funds from the enumerated PANs and adding those funds to an account already controlled by the threat actor or their network of mules or accomplices.

Increase in Account-Based Fraud

Account registration can be a significant fraud vector. Threat actors often use synthetic identities (i.e., an identity built by an actor using a combination of falsified personally identifiable information (PII) along with fake data), to conduct illicit activity, making threat actor identification more challenging. Synthetic identities can also contain pieces of legitimate PII belonging to someone else, likely stolen or purchased from the cybercrime underground. In the payments space, threat actors use synthetic identities to fraudulently register for primary account numbers (PANs), thus simultaneously committing identity theft *and* financial fraud.

In addition to identifying individual instances of fraud, Visa PFD noted trends in registration information, which has helped identify several large fraud rings. Although these trends were observed in the prepaid channel, Visa PFD assesses a high likelihood of similar trends in the credit and debit channels.

To combat threat actors conducting account-based fraud, Visa PFD developed the Automated Payment Fraud Disruption (APFD) capability to identify payment account fraud and notify impacted Visa issuers.

APFD enables Visa PFD to detect prepaid fraud by identifying fraud indicators from the personally identifiable information (PII) used to register for prepaid primary account numbers (PAN), as well as intelligence derived from research and transaction analysis. APFD generates holistic pictures of potential fraud at the prepaid account-level, meaning all corresponding PII and related PANs associated with the same prepaid account registration (herein referred to as 'prepaid accounts'), rather than at the transaction level. APFD uses registration data (PII and PANs) provided by issuers to identify potential fraud on prepaid accounts. Through APFD, Visa PFD can alert issuers via email notifications of prepaid accounts potentially involved in prepaid fraud, which allows issuers to implement controls on those prepaid accounts to prevent fraud. APFD can further customize its capabilities on a client-by-client basis through Visa PFD's Risk-as-a-Service (RaaS).

Automated Fuel Dispenser Fraud (AFD) Attacks Decrease in Frequency but Increase in Impact

Visa PFD continued to identify significantly impactful automated fuel dispenser (AFD) fraud schemes perpetrated against issuers with insufficient processing configurations in the AFD channel. This highlights threat actors continued interest in circumventing new and emerging technologies, such as payment account provisioning to mobile devices, by identifying vulnerabilities and conducting increasingly advanced fraud schemes.

From 1 January 2024 to 30 June 2024, Visa PFD sent numerous alerts to dozens of issuers notifying of suspicious activity related to this specific, previously reported AFD fraud scheme, which represents a **19%** decrease in the number of alerts sent as compared to the prior six-month period (Jun-Dec 2023). However, the alerts from this timeframe total significantly more (USD) in assessed AFD fraud, which is a **373%** increase from the assessed fraud total for the prior six-month period (Jun-Dec 2023), as shown in Figure 4, below.

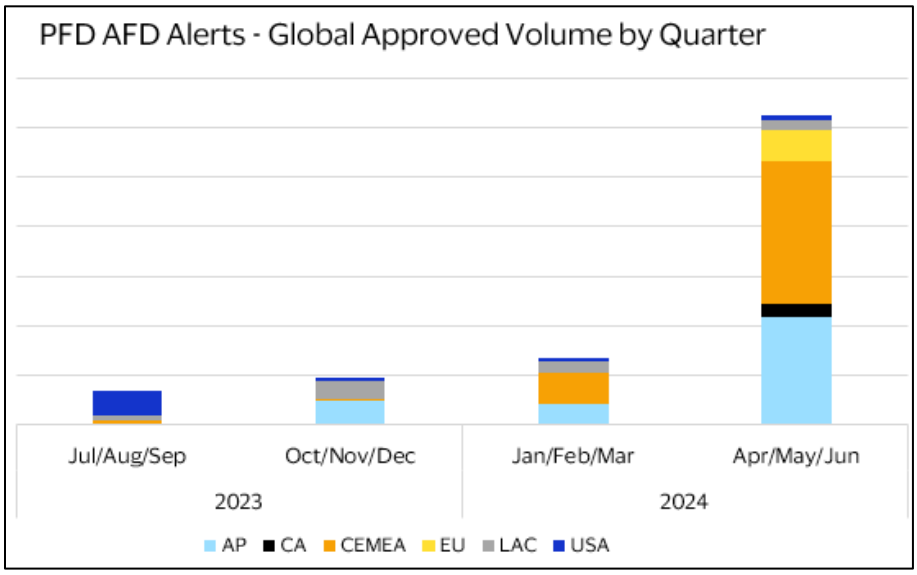


Figure 4 – Source: Visa PFD

This signifies a new trend in which threat actors are conducting a lower overall volume of attacks, but attacks that do occur are significantly more profitable *per incident* for the threat actors, as shown in Figure 5, below. Additionally, threat actors have shifted from targeting the same issuers in multiple attacks, to typically moving on to a new issuer after each individual incident, which is particularly evident in the US region.

In this specific scheme, typically, AFD threat actors purchase fuel from AFDs located in multiple US locations using EMV® debit accounts issued by financial institutions across the globe. The accounts are often legitimately issued accounts reportedly with little to no funds in the account.

The fraudulent transactions are sent as a US$1 status check authorization to ensure the payment account is valid. The full amount for the fuel dispensed is subsequently sent as an advice matching the value of fuel dispensed from the pump. However, in this scheme, the affected issuers receive the US$1 status check authorization but do not hold funds to the maximum allowable AFD transaction limit and/or do not receive the subsequent AFD confirmation advice for the transaction amount of dispensed fuel. As a result, the US$1 Status Check authorizations are approved, but later settle for much higher dollar amounts, which reflect the full amount of dispensed fuel.

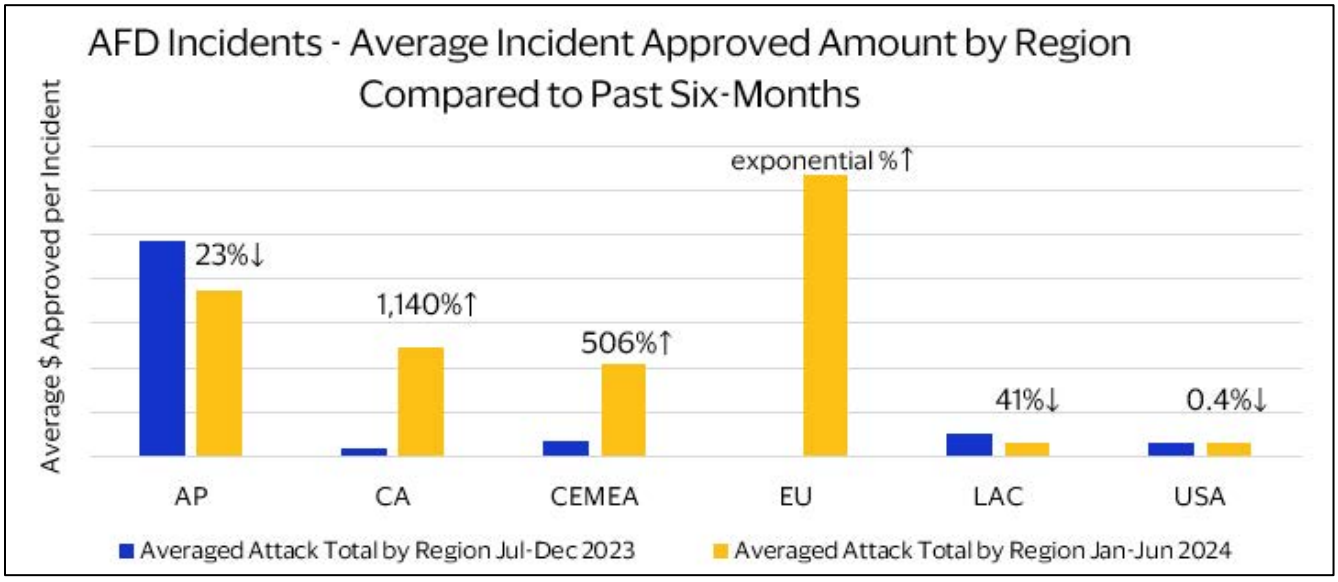


Figure 5 – Source: Visa PFD

In the past six-month period, activity has significantly shifted from the targeting of issuers in the US and Latin America and Caribbean (LAC) regions to the targeting of issuers in the Central Europe, Middle East, and Africa (CEMEA) region, as shown in Figures 6. Canada (CA) and the European Union (EU) regions each experienced a single attack, though the approved totals for these singular incidents represented a significant increase in AFD fraud activity for these regions. Targeting of the Asia Pacific (AP) region remained relatively stable in the number of incidents as compared to the prior six-month period. However, the incidents impacting AP issuers were significantly more costly in the past six-months as compared to July to December 2023.

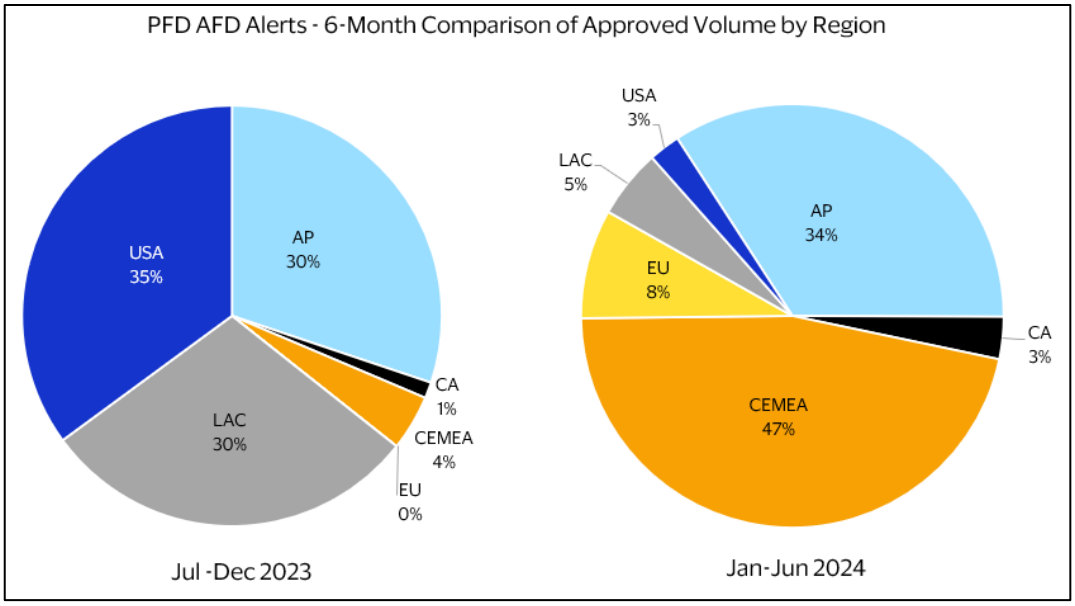


Figure 6 – Source: Visa PFD

Continued Increase in Purchase Return Authorization Attacks

In the past six months, Visa PFD observed threat actors compromising merchants to conduct Purchase Return Authorization (PRA) attacks. When conducting a PRA attack, threat actors compromise legitimate merchant gateways and initiate purchase return authorizations for which there was no initial purchase. The PRA is requested for threat actor-controlled primary account numbers (PANs). Upon approval, threat actors immediately cash out these funds through ATM withdrawals or send them into wallets via peer-to-peer (P2P) payments.

From January through June 2024 Visa PFD opened a record number of PRA investigations accounting to an **81%** increase from the previous six-month period. A successful PRA attack resulted in potential fraud losses to financial institutions of approximately US**$184K** on average. This reflects an increase in the average cost of **58%** compared to the previous six-month period. These figures indicate that PRA attacks are not only becoming more prevalent, but also causing issuers to incur higher costs.

In PRA attacks, threat actors continue to exploit issuers' open to buy (OTB) policies to circumvent fraud monitoring processes. Visa PFD assess threat actors will continue to innovate upon their fraud strategies to effectively conduct additional PRA fraud.

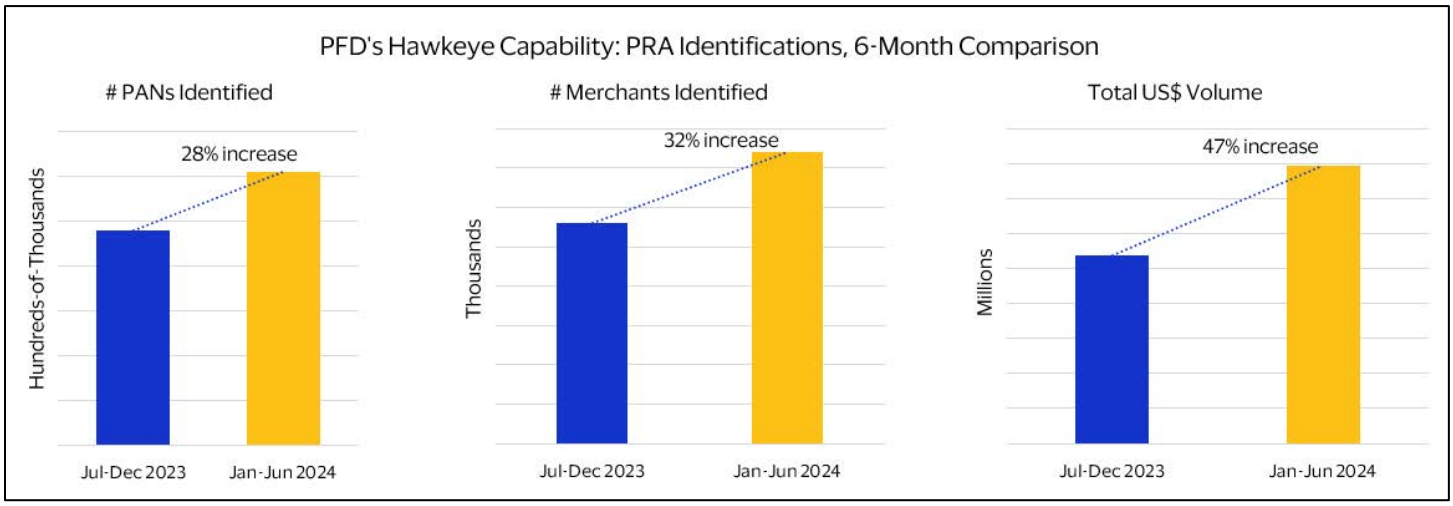


Figure 7 – Source: Visa PFD

Threat Actors

Use of Tools & Technology

Threat Actors Utilize Widely Available Tools and Technology

Threat actors continue to innovate in their use of technology to perpetrate fraud. With the expansion, evolution, and availability of generative Artificial Intelligence tools, and the associated increase in underground forum discussions of how to use AI tools to facilitate crime, threat actors have an ever-increasing array of tools and technologies at their disposal. The threat actor toolbox has evolved to include an expanding collection of cybercrime-as-a-service offerings, such as proxy networks, ransomware-as-a-service variants, and fraud tutorials, enabling them to scale their campaigns more effectively. The articles in this section illustrate this evolution, emphasizing how threat actors are using new and emerging technology and cybercrime services to facilitate attacks.

Fraud Schemes Targeting Contactless Technology

Visa PFD continues to observe sophisticated and unique fraud schemes seeking to exploit the prevalence of contactless payments. Contactless payments significantly contribute to the security of the payments ecosystem by facilitating authentication, devaluing payment data, and utilizing dynamically generated data points. However, as with any new and emerging technology, threat actors are finding new ways to exploit the technology and have employed sophisticated social engineering tactics, malicious mobile applications, compromised point-of-sale (POS) terminals, and token provisioning to defraud consumers, issuers, and merchants.

Malicious App Used to Conduct Fraudulent Contactless ATM Transactions

While some threat actors are using mobile device applications to emulate contactless card-present transactions, others are combining the use of malicious mobile applications with social engineering tactics to fraudulently conduct *valid* contactless transactions. In March 2024, threat actors in the Europe region combined these two tactics to conduct Near Field Communication (NFC) relay attacks on unsuspecting individuals. Using a malicious mobile application and sophisticated social engineering schemes, threat actors convince victims to unknowingly participate in this scheme and provide payment information.

To conduct this attack, threat actors pose as bank representatives to initiate a sophisticated social engineering process wherein the threat actors convince the victim there is a fraud issue with the victim's financial account. Once a sense of trust is established with the victim, threat actors direct the victim to download an application to the victim's mobile device. The victim is unaware that the application is malicious and is spoofing the official banking app. Threat actors then instruct the victim to place their payment card on a table and place their mobile phone on top of the card, or to tap their card against their phone "for verification." The victim is also prompted to enter their personal identification number (PIN) into the fraudulent application. The payment card information along with information for a contactless transaction and the victim's PIN is then relayed from the fraudulent application on the victim's mobile device to a threat actor-controlled mobile device. Threat actors use the harvested contactless transaction information to conduct fraudulent automated teller machine (ATM) withdrawals in real time.

Digital Pickpocketing: The Latest in "Physical" Theft

Beginning in March 2023, Visa PFD identified a new fraud scheme Visa PFD is calling "digital pickpocketing" where threat actors use mobile point-of-sale (MPOS) devices to conduct fraudulent card present contactless transactions. To conduct this scheme, threat actors create a fraudulent merchant using merchant ecosystems that have less robust merchant onboarding procedures. From there, threat actors register a mobile device as MPOS terminal for the fake merchant. Threat actors then attempt to tap the MPOS against a victim's purse, wallet, or pocket to initiate a card present transaction on the MPOS. Another variation of this scheme sees the threat actor use previously stolen cards to conduct the fraudulent transactions using the MPOS registered to the created fake merchant. Since

these fraudulent transactions are actual physical tap transactions, the dynamic data from the transactions are correct. Despite the dynamic data being correct, Visa PFD identified a pattern of elevated Visa Advanced Authorization (VAA) scores for this scheme. The fraudulent merchants are typically registered to a cross-border location, outside of the country of the targeted digital pickpocket fraud activity. Visa PFD assesses threat actors will continue to exploit less robust merchant onboarding practice to perpetrate the creation of fraudulent merchants to conduct digital pickpocketing attacks.

Consumers should be aware of their surroundings and keep wallets and purses secure and in sight. Always physically secure wallets, purses, devices, etc., and immediately report to your bank any theft of payment accounts.

Threat Actors Increasingly Interested in Using Artificial Intelligence Technology

The expansion and use of Artificial intelligence (AI) technology remains a top interest for threat actors. AI has been beneficial in many ways for both business and consumer use, and threat actors have also found ways to use the same tools for illicit activity. In February 2024, a Hong Kong finance employee made headlines when he wired US$25.6M to several bank accounts at the request of his "chief financial officer" (CFO) during a videoconference with the CFO and other executives. However, the individual the targeted employee responded to was not, in fact, the CFO, instead scammers using AI generated voice and video created a deepfake impersonation of the CFO in order to deceive the employee into transferring funds.

It takes only three seconds of audio to clone a voice using AI voice cloning technology, which can be obtained by threat actors from victim's videos on social media or voicemailbox message. The use of cloned voices enhances imposter scams by creating a façade of legitimacy as victims believe they are speaking to the actual person, rather than an AI-generated voice or video. Aside from audio, AI tools can mimic human movement, writing style, and has predictive functionalities, which enables threat actors to perpetuate more believable scams. For these reasons, consumers are advised to be cautious in trusting caller ID, links from unknown sources, and advertisements, and to be guarded in over-sharing of personal information online. The creation of a "safe word" for family and friends can also help to identify an AI-assisted scam.

In addition to the use of AI for voice cloning, AI is also being used to conduct reconnaissance on individual victims or victim organizations by scraping publicly available information and open social media. This information can be used by threat actors to create more convincing phishing emails or other forms of engagement between threat actors and victims.

Researchers predict AI will cause an increase in global volume and severity of cyberattacks over the next two years.

Visa PFD continues to track threat actors' interest in use of AI technologies to facilitate fraud. Over the past two years, Visa PFD noted spikes in the volume of threat actor discussions in underground communities related to the release of new AI technology to public, including malicious versions of AI chat bot programs such as "Fraud GPT" and "Worm GPT" in cybercrime underground marketplaces.

Visa PFD assesses threat actors will continue to use advancements in AI technology to enhance financial scams, making scams more challenging for victims to identify, likely resulting in an uptick in financial losses due to scams. Visa PFD will continue to closely monitor threat actor strategies for new and novel scam tactics as threat actors continue to innovate and will provide updates on the Visa Merchant Resource Library.

Data Breach & Ransomware: Activity Slows After Record Levels in 2023

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 data on the cybercrime underground. From January through June 2024, Visa PFD identified a **12.3%** decrease in the number of ransomware and data breach attacks that were opportunistic in exfiltrating data as compared to the prior six-month period.

A likely cause for this overall decrease in the total number of cases tracked from January through June as compared to the last six months of 2023 is the major breach event in the summer of 2023 impacting a popular file transfer service. The ransomware threat group known as CL0P claimed responsibility for the attack, which was effectively a single breach effort that affected an estimated 2,620 organizations along with 77.2 million individuals whose PII was breached across the compromised organizations.

Of note, is a trend identified wherein the number of overall incidents slightly decreased, but the breaches that are occurring are becoming more impactful, both to the organization breached and to the payments ecosystem as a whole, due to an increasing amount of data obtained by threat actors during breach and ransomware incidents, which threat actors the use for extortion and resale.

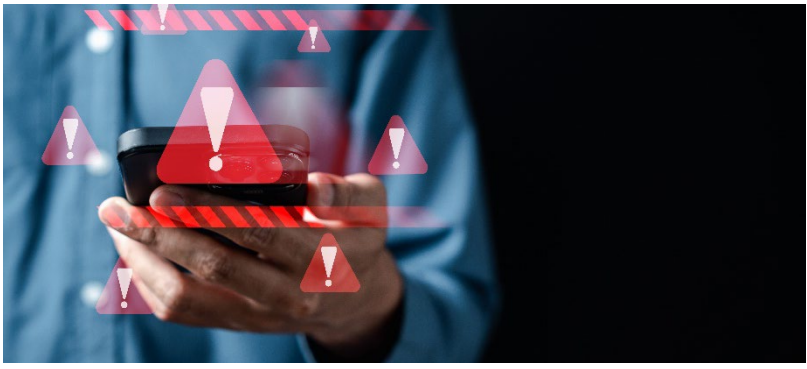
Additionally, although the total number of incidents tracked and cases opened have both decreased slightly from the prior six-month period, threat actors show a continued interest in targeting third-party service providers. Visa PFD observed threat actors continuing to leverage known vulnerabilities among third-party service providers such as cloud storage providers, file transfer services, and remote software providers, which threat actors can then leverage to access their victims' customer accounts to impact as many down-stream organizations as possible. Indeed, Visa PFD identified a significant trend within the Third-Party Agent sub-category, having assessed a **24%** increase from the previous six-month period.

Threat Actors Continue Innovating in Ransomware Tactics

Ransomware and data breaches have evolved in the past few years to include threat actors extracting and exposing sensitive personally identifiable information (PII) which some actors then use as leverage by threatening to leak, sell on the dark web, and/or use to launch additional attacks. Additionally, some victim organizations reported double and triple-extortion wherein actors extract sensitive data and then threaten the victims with distributed denial-of-service (DDoS) attacks releasing stolen data, threats of direct contact with victim organizations' customers, and even reporting to regulatory organizations. Organizations also reported that data compromised during a ransomware attack was posted data for sale on the dark web even after a ransom was paid.

Threat actors are expanding the tools used in ransomware attacks. For example, Ransomware-as-a-Service (RaaS) offerings are increasing across the underground. RaaS is a cybercrime business model wherein ransomware developers create services and tools, such as malware and infrastructure that are then sold in cybercrime marketplaces to other cybercriminals to launch attacks. These underground posts often advertise kits that can include information on how to create a ransomware variant, payment or chat portals to communicate with victims, "customer" support, and other features. Recent research concluded threat actors engaging in the post-compromise deployment of ransomware continue to primarily rely on commercially available and legitimate tools to facilitate intrusion. Notably, one group of researchers observed a decline in the use of Cobalt Strike BEACON, and a corresponding increase in the use of legitimate remote access tools.

One prolific ransomware threat group, Lockbit, used the triple-extortion tactic to include DDoS attacks for nearly two years, beginning in August 2022. Lockbit, a ransomware-as-a-service threat group, along with their subsequent Lockbit 2.0 and 3.0 evolutions, consistently remain one of the most prolific malware threat groups targeting the payments ecosystem since the second half of 2021.



The North America region continued to be the most impacted region in terms of ransomware/data breach incidents impacting the payments ecosystem, shown in Figure 8.

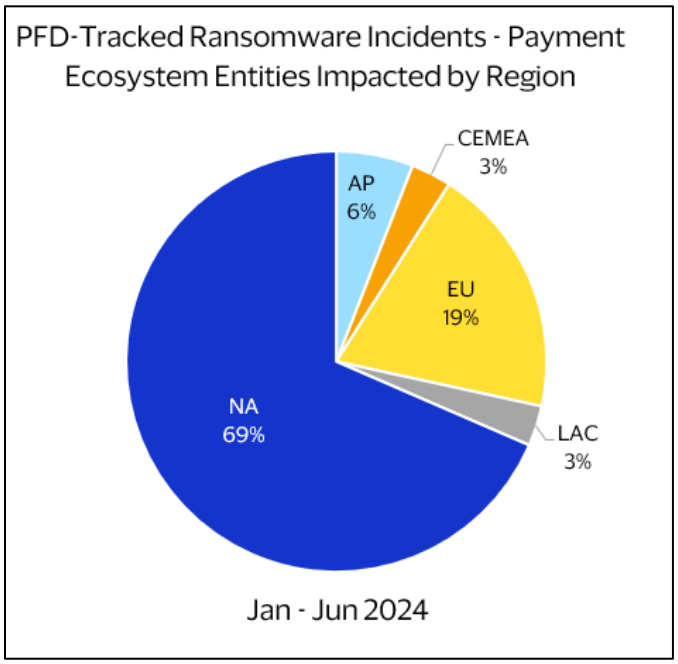


Figure 8 – Source: Visa PFD

Threat actors are also evolving in how they share data in cybercrime underground marketplaces, including stolen PII, payment account numbers and login credentials. Visa PFD observed threat actors increasingly sharing data for free across various underground forums and shops over the past six months. Some threat actors will give data away free of charge to promote themselves or their shop on underground forums.

In April 2024, a new carding shop known as "b1ack's Stash" emerged touting the alleged sale of 1M payment account details. The threat actors behind "b1ack's Stash" promptly posted large data sets of payment account information for free on the shop's website. Researchers analyzed a subset of the leaked cards from six issuers and found that 42,310 of the 45,195 stolen cards reviewed were unique and had not been observed in previous data leaks. This tactic is growing in popularity and follows the trend of free data releases conducted by other carding shops such as Biden Cash. Generally, the majority of the data included in such "free" releases is often found to be outdated, invalid, or fake. Visa PFD assesses cybercrime underground carding shops will continue to release compromised payment account data to increase their brand reputation with other threat actors.

While ransomware attacks remain a prolific threat to the payments ecosystem, data leaks are also on the rise and the number of impacted individuals having personally identifiable information (PII) breached continues to grow year over year. In January 2024, cybersecurity researchers discovered a database containing 26B exposed records consisting of stolen user credentials, comprised of usernames and passwords, along with PII which allegedly was obtained from thousands of previous leaks, data breaches and privately sold databases. Researches named the database "the mother of all breaches (MOAB)" as it represents one of the largest consolidated data leaks in history. The large repository of data potentially creates risk to individuals and organizations globally, as threat actors could use the sensitive data for criminal activity including identity theft, targeted cyberattacks and phishing schemes. Visa PFD actively monitors and tracks data breaches across the payments ecosystem and anticipates threat actors will continue to fraudulently obtain user credentials and PII as well as continue to leak or sell the data that they obtain for the purposes of financial gain or for increased credibility across the cybercrime underground. As fraud and cybercrime continuously moves upstream to target authentication processes, identity data, and other sensitive data and payment flows, Visa PFD is developing cutting edge technology and processes to combat such cybercrime activity, such as the APFD service, and remains committed to bolstering the security of the payments ecosystem.

The increase in ransomware, data breaches, digital skimming, and underground carding shops demonstrates an ever-increasing threat actor interest in payments and payment accounts. Threat actors continue to employ sophisticated methods to compromise vulnerable companies and consumers alike. Despite the increasing sophistication of threat actor attack vectors, Visa PFD cooperates with global law enforcement to secure the payments ecosystem and hold threat actors responsible for their actions.

Trends and Evolution of Malware Threats to the Payments Ecosystem

Threat actors continue their development and use of malware campaigns to victimize payment entities and steal data from consumers. Visa PFD tracks and reports on a number of malware and digital skimming campaigns and variants. Notable evolutions and updates in this space are included below.

North Korean-backed Lazarus Group Shifts Focus

Visa Payment Fraud Disruption observed numerous malware variants and families targeting the payments ecosystem over the last several years with one of the most notorious being the malware variants operated and deployed by the North Korean state-sponsored group, Lazarus. Lazarus malware variants are used to target the payments ecosystem in order to gain access to victim organizations' fiat or cryptocurrency funds. While the Lazarus/APT38 CageyChameleon malware campaign was one of the most prolific threats tracked by Payment Fraud Disruption in 2021 and 2022, over the past six-month period, Visa PFD observed a rapid decline in the frequency of the CageyChameleon and other Lazarus malware variants targeting the payments ecosystem.

According to published reports, the North Korea-backed threat group is now laundering stolen cryptocurrency funds outside of the payments ecosystem, such as through cryptocurrency mixers. Visa PFD assesses Lazarus/APT38 will continue to expand their targeting beyond financial institutions over the next six-month period.

Threat Actors Continue to Develop New and Evolved Point-of-Sale Malware

Threat actors continued to exploit vulnerabilities within payments ecosystem organizations' point-of-sale (POS) networks and devices to gain access to sensitive payment account data.

Digital Skimming Remains a Popular Tool for Threat Actors

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 personally identifiable information (PII), such as primary account number (PAN), card verification value (CVV2), and expiration date, entered into checkout forms by the merchant's customers.

Visa PFD combats digital skimming attacks with the eCommerce Threat Disruption (eTD) capability. 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 six months, the number of compromised websites detected by eTD remained consistent. However, eTD noted a decreasing trend in the overall number of skimmers identified monthly over the past 12 months. If a skimmer is identified, eTD also works with web infrastructure providers to takedown the infected malware from the compromised eCommerce merchant's webpage before payment account data can be stolen. At-risk PANs identified in these attacks are distributed to impacted issuers through the Compromised Account Management System (CAMS) alerts.

Visa PFD's Global Risk Investigations (GRI) team also identified a slight decreasing trend in digital skimming, with formally-opened skimming cases representing a **3%** decrease from the previous six-month period (Jul – Dec 2023), but a **5%** increase from last year's same period (Jan – Jun 2023).

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 9. The Europe region experienced the second-highest number of compromised merchant websites identified.

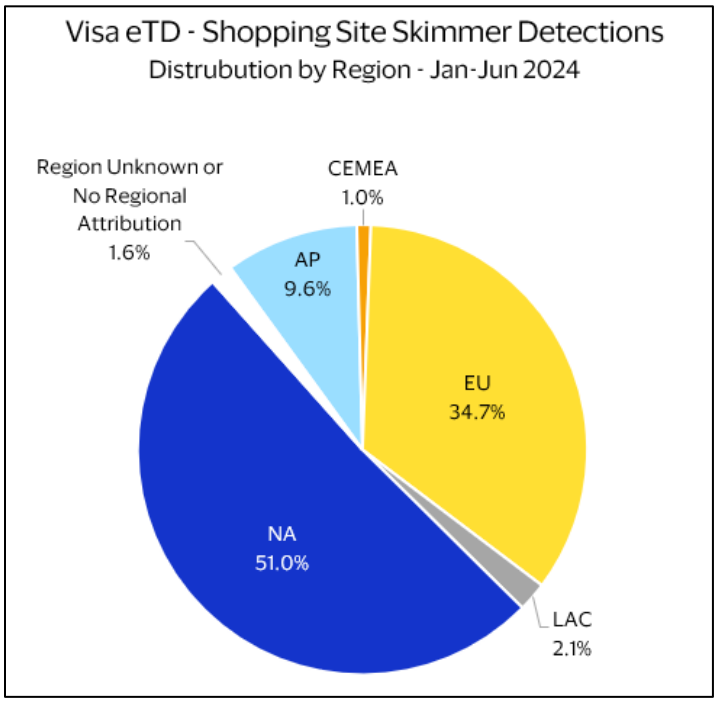
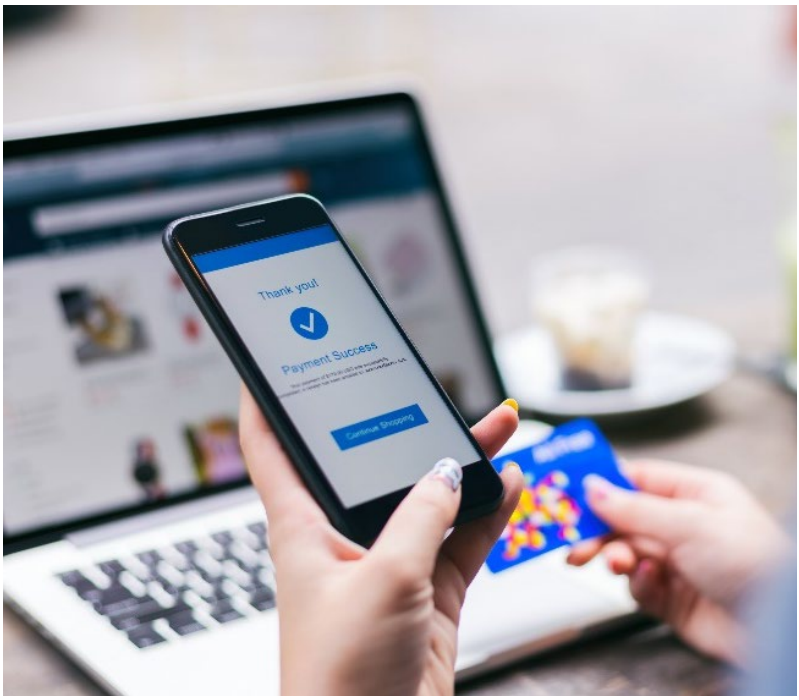


Figure 9 – Source: Visa PFD



Digital Skimming Levels Remain Consistent While Victimology Shifts

Over this past six-month period, Visa PFD's Global Risk Investigations (GRI) team observed a 6% decrease in digital skimming incidents targeting either eCommerce merchants or third-party providers, compared with the prior reporting period of July – December 2023, revealing threat actors are still utilizing digital skimming as a popular method to compromise eCommerce victim environments and obtain payment account data.

Visa PFD noted a significant decline of 83% in digital skimming third-party provider targeting over the past six-months (January – June 2024), compared with the prior reporting period, July - December 2023. This change in victimology in the digital skimming space may be related to more highly targeted attacks against singular eCommerce merchants. As threat actors have increasingly become more sophisticated and tend to conduct more robust reconnaissance on their victims prior to launching an attack, this enhanced sophistication may have led to more threat actor groups focusing their efforts on eCommerce merchants as they are more likely to have direct access to sensitive payment account data stored within cardholder data environments (CDEs) or provided via the victims' checkout webpages.

Public-Facing Webpages Offer Easier Entry for Digital Skimmers

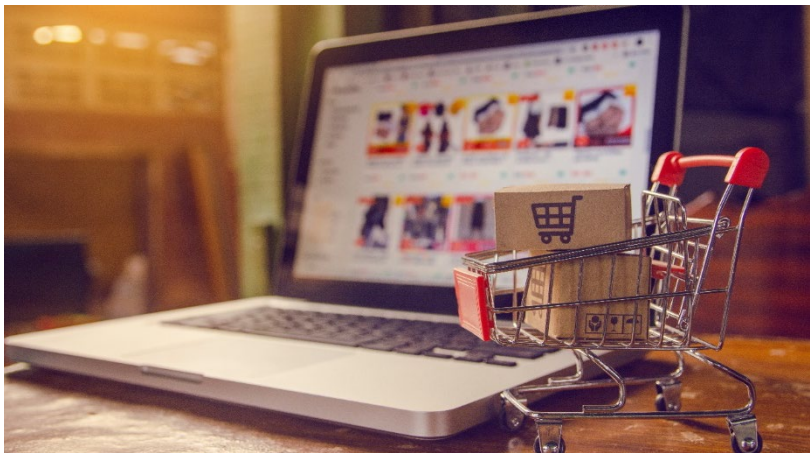
Threat actors continue to innovate in their digital skimming tactics, techniques, and procedures (TTPS), opting for a mixture of various "tried-and-true" techniques, along with some new evolved tactics. The most common attack vector seen within Visa PFD's past 12 months of alerts was through the use of compromised administrator credentials to gain initial access to the victims' networks and exploit vulnerabilities within the victims' publicly facing web infrastructure, enabling threat actors to conduct SQL injection or XSS attacks to gain access into the victims' eCommerce environments. The threat actors would then typically exploit file upload vulnerabilities to deploy web shells, and from there, append malicious digital skimming malware onto the eCommerce merchants' checkout webpages.

Additionally, Visa PFD identified a trend indicating third-party provider victims tended to lack strong password and user authentication controls, such as multi-factor authentication (MFA) or one-time passwords (OTPs) enabled on user and administrative accounts, which contributed to the compromises.

Other notable digital skimming trends involve the targeting of non-payments infrastructure by threat actors to gain initial access to victims' environment, and from there, pivot to the payments environment. In both this reporting period and the previous reporting period, Visa PFD observed multiple digital skimming attacks wherein threat actors exploited vulnerabilities in non-payments infrastructure, such as a blog webpage, a chatbot application, and an internally developed customer inquiry form, to compromise the victims' environments. As non-payments infrastructure may lack stringent security controls, threat actors can more easily gain initial access into the victim's environment, and from there, deploy digital skimming malware into the checkout environment to obtain payment data. This trend in the targeting of non-payments infrastructure by threat actors reinforces the importance of ensuring all code deployed onto web environments is routinely reviewed and a file integrity monitoring (FIM) system is implemented to monitor for unauthorized activities.

Consumer Redirection, Fake Checkouts, and Compromised Credentials Used to Steal Payment Data

Over the past six-months, Visa PFD identified several new tactics used by threat actors to perpetrate digital skimming attacks and extract compromised payment account data from compromised webpages. One of these tactics, involves threat actors successfully redirecting legitimate consumer DNS web traffic from the victim eCommerce merchant's checkout webpage to a phishing landing page in order to steal payment account data. In this incident, which impacted a travel industry merchant, threat actors compromised multiple victims' user credentials and used those credentials to upload JavaScript (JS) files onto the victim's checkout webpage. These JS files enabled threat actors to replace the victim's payment processor URL with a phishing URL that presented a fake checkout form to consumers and exfiltrated their payment account data to a threat actor-controlled domain. Visa PFD assesses this novel tactic reveals how threat actors are continuously experimenting with and developing new methods to attack the payments ecosystem and compromise payment account data. While this novel tactic was used against a travel eCommerce merchant, the same TTP may also be used against other types of eCommerce merchants and third-party providers. This incident further represents the importance of ensuring all user credentials are secured with MFA and FIM systems are deployed onto payment environments.



Visa PFD also observed threat actors who exploited victims lacking PCI DSS requirements which would have otherwise thwarted threat actor attempts to obtain payment account data. In another novel digital skimming tactic identified, threat actors compromised the victim's third-party payment provider's user credentials and with those credentials, created a "super user" account with escalated privileges. These enhanced privileges allowed threat actors to query the victim's cardholder data environment (CDE) for payment account data. However, as the victim only stored encrypted payment account data, the threat actors were forced to conduct reconnaissance to identify the decryption key for the encrypted payment account data. The victim insufficiently stored the decryption key within a publicly accessible file that was not secured or encrypted, thus providing threat actors with the means to decrypt any encrypted payment account data exfiltrated out of the victim's environment. This incident is another example of is the importance for all payments organizations to ensure they are PCI DSS compliant and conduct regular reviews of their systems to ensure all the PCI DSS requirements are properly implemented.

Threat Actors Increasingly Target Consumers

Threat Actors Increasingly Target Consumers

Given the significant increase over the past two years in criminal profits gained from various types of scams, scams directly targeting consumers continued to be an attractive threat tactic employed by actors globally over the past six months. Threat actors will often solicit payment via payment accounts or other digital channels during scam activity, which significantly impacts the global payments ecosystem. Over the past six months, threat actors continued to target process vulnerabilities and gaps in systems in order to facilitate fraud. This includes One-time Passcode (OTP) processes, merchant onboarding systems, and the consistently weakest link in any system: people.

Cashout Times Increase as Threat Actors Continue Provisioning Fraud

Threat actors continue their efforts in fraudulently provisioning payment accounts to threat actor-controlled mobile devices, typically through OTP bypass schemes like the one mentioned above. Over the past six months, Visa PFD 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 cash out funds. Correspondingly, Visa Risk MIS also identified that, in general, provisioning fraud rates in the first seven days after token activation continue to trend downwards, though fraud rates have been steady or slightly increased on transactions taking place in the 8- to 30-day and 30- to 90-day periods.

This shift in provisioned PAN cash-out tactic is likely due to more sophisticated fraudsters attempting to circumvent issuer-based controls that may be in place on days 1-7 after provisioning, thus waiting to attempt a cash out after, they perceive, fraud controls may be less stringent (days 8 to 90). 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). Figure 10 shows this change in fraud volume from 40% on day 1 as reported in the December 2023 Biannual Threats Report, to a decrease to 29% on day one in the latest available data.

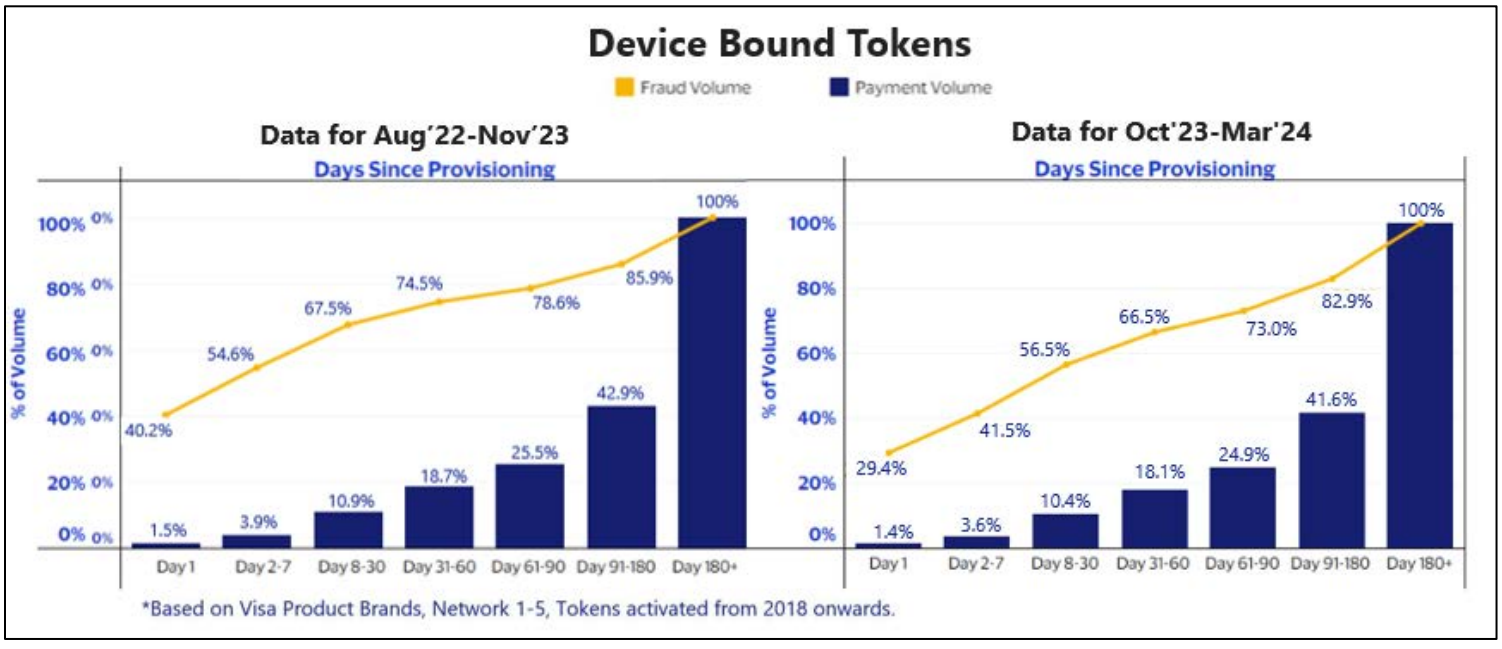


Figure 10 – Source: Visa Risk MIS

At present, fraud trends indicate issuers are successfully distinguishing potentially fraudulent Device Bound tokens, sending them through a step-up method for additional authentication such as one-time-passcode (OTP), but that step-up methods are being successfully circumvented by fraudsters. Post-Provisioning, Key-Entered Device Bound OTP tokens stand out as the most material vector at present. The effectiveness of MFA in combatting fraud has led to threat actor innovations to thwart such authentication measures. Over the past year, Visa PFD reported on multiple MFA and OTP bypass schemes, including phishing, social engineering schemes, and OTP relay schemes.

Compared to Device Bound tokens, Card on File tokens still have a very similar distribution of fraud by time, as compared to the prior reporting period, as fraudsters have less control over the provisioning request and time the transaction takes place, as shown in Figure 24.

Visa is looking to the latest in AI technology to assist clients in the fight against various forms of OTP bypass related fraud with the launch of the Visa Provisioning Intelligence score in December 2023 aiming to help strengthen and secure this portion of the provisioning process. Visa Provisioning Intelligence (VPI), an AI-based product designed to combat token fraud at its source. Available as a value-added service for clients, VPI uses machine learning to rate the likelihood of fraud for token provisioning requests, helping financial institutions prevent fraud in a targeted way and enable more seamless and secure transactions for Visa cardholders.

Some Scammers Show Preference for Cash

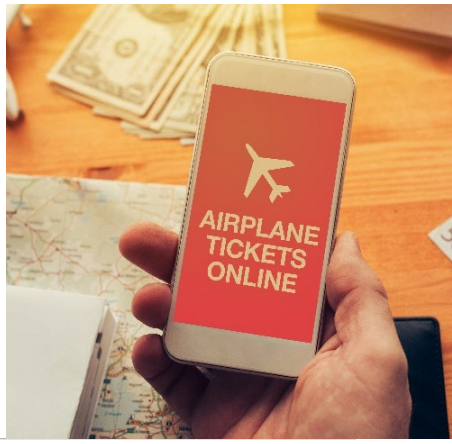
A June 2024 press release from the US Federal Trade Commission (FTC) revealed that government impersonation scammers are now opting for cash payments over other payment methods. Government impersonation scams typically involve threat actors posing as a government or law enforcement entity, reaching out to victims via phone calls, emails, text messages, or other social media platform messaging, regarding an "urgent matter" where immediate payment is the only resolution. The scammers tell the victim to make the payment using a specific payment method, such as specific money transfer applications, cryptocurrency, wiring funds, or purchasing gift cards and providing the card information to the scammer. However, scammers are now looking for cash payments to be sent via mail or to be picked up by a courier working for the scammer.

Per the FTC statement, in the first three months of 2024, the average government impersonation scam victim lost US$14K in cash, totaling US$20M across victims in the first quarter of 2024, representing a significantly higher total sum lost than with other payment methods. Additionally, between 2022 and 2023, the FTC reports a 90% increase in losses from cash payments from government impersonation scams.

As government impersonation scams move toward cash payments, Visa PFD assesses that issuers will see an increase in large cash withdrawals by customers at automated teller machines (ATMs) and bank branches. Additionally, as government impersonation scams are seeing success in scamming victims using cash payments, it is likely other scam methods will also begin requesting cash payments, as threat actors are constantly looking for the most lucrative method to make money. Issuers should be vigilant for customers making unusually large cash withdrawals and remain aware of current scam methods impacting cardholders in the payments ecosystem.

Threat Actors Look to Travel Season to Attract Victims

With travel season in full swing, threat actors are finding ways to exploit consumers' travel plans. With popular events such as music concerts, festivals, and significant regional sporting events all taking place over the coming months, the number of scams advertising fake and fraudulent tickets is on the rise. According to a recent report from a UK financial institution, UK-based music fans of a popular American singer have lost over US$1M in fraudulent ticket purchases for summer concert dates, with 90% of those losses stemming from malicious advertisements on social media. Officials advise fans to only purchase tickets from official retailer's or reputable ticket exchange sites, and to be cautious of ticket advertisements on social media, tickets that must be purchased through bank transfer, and ticket deals that look too good to be true.



Travel Sector a Popular Target for Scams During the Holiday Travel Season

During the busy holiday travel season, consumers should also be on the lookout for scams targeting the airline industry. A common scam targeting consumers involves threat actors setting up fraudulent websites that "spoof" or imitate major airlines. These fraudulent websites entice consumers with low-ticket prices and deals. Unfortunately, once the consumer purchases the airfare the scammer attempts to upcharge them for additional in-flight amenities. The threat actor then cuts off communication with the victim. Scammers are also impersonating airline officials and sending out fake flight cancellation emails. The threat actor notifies an individual that their flight has been canceled and request the individual's payment account information to book a new flight. When consumers follow up with a legitimate airline representative, they realize their flight was not actually canceled and they were socially engineered to give their credit card information to a scammer.

A third use for these spoofed airline websites is for use in call center scams. Threat actors create a spoofed website and use malvertising (malicious advertising) or illicit search engine optimization (SEO) to promote the spoofed site or to ensure the fake site appears at or near the top of browser search engine results. A victim looking to contact or call a major airline but who stumbles across a spoofed site instead will find themselves in a chat or on a call with a fake customer service representative, purporting to be from the airline. The scammer will "assist" the cardholder in booking or changing a flight, only to charge the victim's account high dollar booking or change fees, with funds being directed to a fake or misrepresented merchant, and the victim's actual flight never booked or changed. Additionally, the victim's payment account details are often stolen alongside the erroneous charge and later sold in cybercrime underground marketplaces or used in triangulation fraud schemes. Consumers are encouraged to ensure the URL is valid for the airline, travel, or hospitality booking provider they are intending to contact and be wary of navigating to travel sites seen in social media advertisements or in sponsored search results.

Increase in Physical Thefts of Payment Cards and Phones

Another tactic consumers should be on the lookout for during the busy holiday and travel season is the physical theft of payment cards and phones. Although threat actors are evolving to be able to perpetrate fraud using sophisticated social engineering and impersonation scams, actors continue stealing physical cards to conduct fraud. Over the past six-month period, Visa PFD identified an increase in threat actors targeting physical payment cards to perpetrate fraud. Threat actors use physical theft to conduct fraud in a variety of ways including purchasing physical goods to resell, purchasing gifts cards, using the card number for online/eCommerce transactions and money transfers (typically those that do not require step-up authentication), and conducting fraudulent transactions at malicious MPOS terminals.

Although the level of physical card theft and targeting fluctuates over time, criminals targeting consumers directly or placing card capture devices in unattended terminals (UATs), such as ATMs, for the purpose of stealing payment cards, potentially including PIN numbers, remains a persistent threat within the payments ecosystem. In recent attacks, actors are using a variety of methods to obtain physical payment cards, such as devices placed over payment card readers on UATs that prevent the payment card from being returned to the cardholder. The victim will eventually vacate the premise of the UAT, and the threat actor will subsequently remove the device from the UAT and obtain the captured payment card. While this method has been used by actors for decades, Visa PFD identified a notable recent increase in such attacks globally beginning in late 2023.

Additionally, actors are resorting to other tried and true methods to obtain physical payment cards such as vehicle break-ins, mail theft, and pickpocketing. The recent increase in physical theft reflects a broader trend wherein actors are encountering more friction in conducting fraud due to increased secure acceptance and fraud controls across the ecosystem which is driving them to the targeting of consumers. Visa PFD assesses this trend will persist as threat actors continue to find success targeting cardholders directly.

Given the significant increase over the past two years in criminal profits gained from various types of scams, Visa PFD assesses such scams directly targeting consumers will continue to be an attractive threat tactic employed by actors globally as threat actors will often solicit payment via payment accounts or other digital channels during scam activity, which significantly impacts the global payments ecosystem. Visa PFD monitors for and regularly reports new scam tactics and variants via the Visa Merchant Resource Library.

Threat Actor

Disruption

Threat Actor Disruption

Visa PFD supported global law enforcement and government entities throughout the past seven-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. Some of the top actor disruption operations are included below.

Arrests Made in Gift Card and Social Engineering Scams

In March 2024, three individuals were sentenced for laundering an estimated US$2.5M in stolen gift cards for a large retail store between June 2019 and November 2020. The individuals, a California resident and two Chinese nationals, worked as "runners" in association with a Chinese-based scam group, self-named "Magic Lamp." Magic Lamp actors would conduct social engineering scams targeting senior citizens by posing as law enforcement, government employees, retail workers, or technical support operators. The scammers would claim there was a warrant out for the victim's arrest, the victim's identity had been stolen, or there was an issue with the victim's account or device that needed to be addressed. To remediate the perceived issue, the scammers enticed the victims into purchasing gift cards, often in increments of US$500, and provide the gift card number and access code to the scammer over the phone. Magic Lamp is estimated to have provided the runners over 5,000 gift card credentials obtained through these methods. Using a popular Chinese messaging application, the scammers would then provide the gift card information to the runners, who would go to retail stores in California and quickly purchase high-dollar electronics and other items to liquidate the gift card balances. The retailer was unable to recoup the funds for the fraudulent purchases because of the speed at which the gift cards were used.

Visa PFD has supported the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) investigative efforts since 2020.

Operation April Fools Arrests 10 Individuals for Benefit Fraud

Visa PFD supported to the US Secret Service in their pursuit of Electronic Benefit Transfer (EBT) fraud. As highlighted in the June 2023 edition of Visa PFD's Biannual Threats Report, US Secret Service and local law enforcement made arrests for EBT fraud as part of Operation Urban Justice in March and June 2023. In April 2024, the law enforcement efforts around Electronic Benefit Transfer (EBT) fraud continued with the multi-day operation, "Operation April Fools," and the arrest of 33 individuals in California, alleged to be associated with transnational crime organizations targeting EBT payments.

EBT fraud typically occurs at point-of-sales (POS) terminals or automated teller machines (ATMs), where threat actors installed skimming devices to steal payment card numbers upon use. EBT cards are targeted, in part, because many utilize magnetic stripe transactions (POS entry mode 90), which are easier to skim than the unique cryptogram generated by an EMV® chip card for transactions. The US Secret Service recommends cardholders thoroughly inspect card readers, particularly in tourist areas, for skimming devices. Additionally, US Secret Service advises cardholders to cover ATM keypads when entering a PIN, as threat actors sometimes place pinhole cameras above the keypad to collect PIN entry.

Law Enforcement Disrupt Malware Campaigns with Operation Endgame Arrests

Visa PFD supported the US Secret Service, Federal Bureau of Investigation (FBI) and Europol in a global effort known as "Operation Endgame," which aimed to disrupt "dropper" services used to gain access and deploy malware or ransomware to victim devices. Once the desired malware has been dropped, cybercriminals are able to collect sensitive data, such as financial login information, which can then be used or sold for illicit purposes. By pursuing actors involved in dropper services, such as those contributing to dropper development and maintenance, law enforcement can simultaneously disrupt numerous cybercriminal organizations that have operational dependencies on the droppers.

Operation Endgame was underway between 27 and 29 May 2024, targeting malware campaigns including IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee, and Trickbot droppers and their associated infrastructures. The operation resulted in the arrest of 4 individuals, search of 16 locations, disruption of over 100 servers, and law enforcement seizure of over 2,000 web domains, making Operation Endgame the largest ever operation against botnets.

20 Convicted and Sentenced for Major Retail Chain Data Breach

Visa PFD supported US Federal Bureau of Investigation (FBI) efforts to investigate 22 suspects involved in a criminal case related to the purchase and use of stolen payment cards. In February 2024, twenty (20) of the defendants were convicted and sentenced for their involvement in a sizeable breach of a North American retailer first detected by Visa PFD and US Law Enforcement in 2016 and 2017. These large-scale brick-and-mortar retailer network intrusions resulted in the theft of over 9M Visa accounts from over 400 retailer locations. The 20 defendants, originally arrested and arraigned in May 2021, were charged and convicted in US District Court in Northern Illinois for the theft and sale of the stolen account data and associated fraud totaling US$25M. Prison terms ordered in sentencing range from 3.5 years to 7 years, and all were remanded to the custody of US Bureau of Prisons. Two indicted co-conspirators charged in the malware installation and account data theft remain at-large in Eastern Europe.

Payments Fraud Scheme Defendants Plead Guilty

Visa PFD assisted US Federal Law Enforcement agencies in a multi-year investigation involving the establishment of over 100 fake merchant accounts used to perpetrate over US$150M in high-risk and fraudulent transactions. Of the five individuals involved in the case, two pleaded guilty in 2020 and 2021 to wire and bank fraud conspiracy, and two are set to plead guilty at upcoming sentencing hearings in November 2024. The fifth defendant is a fugitive on these charges along with an additional indictment from December 2021.

According to court documents, the defendants ran a payment processing company that fraudulently processed prohibited or high-risk transactions for merchant that had been terminated for fraud or compliance issues, defrauding acquirers, payment networks, and issuers out of over US$150M. The defendants established shell companies and fake websites pretending to sell low-risk retail and consumer goods in order to be able to process the high-risk transactions fraudulently using merchant category codes related to lower-risk sectors. The US$150M in transactions were processed using over 100 fake merchant accounts set up through the scheme. The defendants face sentences of up to 30 years in prison and a fine over US$1M.

Threats

Landscape Forecast

Threats Landscape Forecast

Visa PFD noted an interesting shift throughout 2023 in threat actors' organization, sophistication, and targets. While there continues to be threat actors and groups using basic, rudimentary, often "smash-and-grab"-type tactics, over the past six months, Visa PFD continued to identify movements in threat actors and groups evolving into more organized and sophisticated operations, utilizing advanced tactics and cutting-edge technology to facilitate large-scale fraud operations. Threat actors continue to probe organizations and networks for vulnerabilities in systems and processes to conduct extensive and complicated operations with expansive downstream ecosystem impacts. With this increase in sophistication, threat groups are aiming at cardholders directly, using advanced social engineering techniques and AI technology to make scams even more believable for victims and to circumvent financial network security and fraud prevention protocols. Visa PFD assesses the next year will see threat actors continue to develop innovative tactics in probing vulnerabilities and targeting cardholders.

Threat Actors Will Continue Targeting Vulnerabilities

Visa PFD assesses threat actors will remain opportunistic in targeting vulnerabilities in processes and systems in the coming months given increases in activity seen over the past six months. Visa PFD anticipates the following trends will likely continue in the coming months:

- Continued probing of vulnerable merchants within MCC verticals to conduct **enumeration and card testing** attacks.
- Expanded geographic targeting of financial institutions in conducting **AFD fraud** with likely a continuation of lower overall attack volume with higher individual attack size.
- Threat actors persistent use of fake data for account creation in conducting **prepaid fraud.**
- Continued targeting of financial institutions increasing open-to-buy prior to settlement to perpetrate **PRA fraud**.

Cardholders Will Remain Attractive Targets for Scams and Theft

Given the significant increase over the past two years in criminal profits gained from various types of scams, Visa PFD assesses such **scams directly targeting consumers** will continue to be an attractive threat tactic employed by actors globally and will likely continue to increase in both complexity and volume. Many of these scams will solicit payments from victims using payment accounts, and a key component of such scams is the victim is willingly making a payment. Customer service and **bank impersonation schemes** will likely continue to evolve in sophistication and quantity in threat actors' further attempts to socially engineer cardholders into providing sensitive information, account access, or fraudulent payments. Scams will also continue to be global in scale, with threat actors in one region targeting cardholders in another region. Moreover, through the proliferation and use of AI tools, scamming victims in different locations and those who speak different languages will become easier for threat actors. Visa PFD will continue to closely monitor threat actor strategies for new and novel scam tactics as threat actors continue to innovate.

Ransomware and Data Breach Forecast

Visa PFD assess threat actors will continue to leverage known vulnerabilities among third-party service providers such as cloud storage providers, file transfer services, and remote software providers with respect to **ransomware attacks**. Visa PFD additionally assesses that phishing emails will be crafted to be increasingly more realistic and misleading, and that compromised PII will remain a top target and threat to organizations globally. This threat potentially impacts merchants, processors, and acquirers around the globe and, particularly, entities lacking proper security controls or those not adhering to a strict vulnerability and patch management program.

While the number of **digital skimming** cases slightly decreased over the past six months, Visa PFD assesses this trend will likely reverse and begin to increase as we approach the end-of-year holiday shopping season. Threat actors will likely look to this increase in online transaction volume to obtain larger quantities of sensitive and payment account data by placing new and novel digital skimmers on merchant websites.

Visa PFD assess that threat actors will continue to target merchants with unattended POS devices such as automated fuel dispensers (AFDs) and large brick-and-mortar retailers. The increase in instances of skimming highlights the need for clients to implement monitoring of their devices to detect skimming devices.

How Visa Helps

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

These individuals 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 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.

The Risk **Management Information Systems** (MIS) team maintains the mission of driving value for Visa by transforming data into actionable insights that drive secure commerce experiences in both the physical and digital world, and delivers data-based solutions, analysis and deep, risk-focused insights targeted at maintaining security, proactively reducing fraud rates and preserving the integrity of transactions within our ecosystem. The Visa Risk MIS Team is organized and aligned to support the global Risk organization and serve both internal Visa stakeholders and clients via various areas, such as risk reporting and insights, and build, develop and foster partnerships across the ecosystem.

Visa Consulting & Analytics (VCA) is uniquely positioned to work with clients to help formulate a cybersecurity strategy, risk governance and compliance assessment and provide cyber training, awareness, and education.

People are the most important component in combating the threats described throughout this report, and Visa remains committed to working closely with its partners to ensure the threats to the ecosystem are effectively identified and mitigated.

Technology

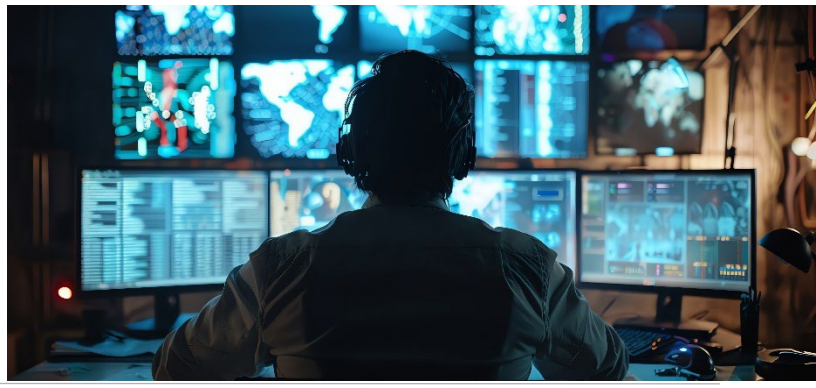
Visa has invested heavily in security technology to prevent, detect, and eradicate threats to payment data and infrastructure.

eCommerce Threat Disruption (eTD), a Visa developed solution, protects the eCommerce channel by scanning eCommerce merchant infrastructure and identifying digital skimming attacks.

Visa PFD vigilantly monitors for enumeration attacks through the **Visa Account Attack Intelligence** (VAAI) capability uses machine learning to identify enumeration attacks, analyzes the details of the attack, and enables Visa to take appropriate action in near real time to notify affected acquirers/merchants and to help block egregious attacks to mitigate and prevent the successful enumeration of payment accounts.

Visa PFD's **Hawkeye** team aims at mitigating fraud at an early stage via anomaly detection, monitoring, and alerting. Hawkeye leverages various Machine Learning models, decision trees and historical data trends to unearth insights that flag potentially fraudulent activity in their nascent stages, and tracks various ecosystem trends, technologies, and participants.

To provide a test environment that more accurately reflects an issuer's authorization decisioning logic when it is experiencing a fraud attack, Visa PFD's **Visa Payments Threats Lab** (VPTL) enables Visa and the issuer or its processor to proactively probe for vulnerabilities in processing logic, fraud controls, and consequent exposure to real-world fraud attacks. Ethical identification of logic gaps enables clients to defend against attacks while maintaining brand integrity before threat actors exploit such gaps. VPTL conducts proactive tests with fraud scenarios and payment card transaction configuration vulnerabilities within an issuers authorization platform and provides actionable recommendations.



Processes

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 PFD's **Global Risk Investigations** (GRI) team conducts in-depth investigations on a variety of different external data security incidents where cardholder payment data may be at risk. Global Risk Investigations engages with all payment ecosystem participants, ranging from financial institutions such as issuers and acquirers, third party agents including integrators/resellers, and all merchant levels to ensure any at risk data is identified and impacted stakeholders are notified.

Acknowledgements

The authors would like to thank the numerous contributors across Visa Payment Fraud Disruption (PFD), Visa Risk Management Information Systems (MIS), and the entire Visa Risk organization.