A Payment Ecosystem Report by
Visa Payment Fraud Disruption

Biannual Threats Report

June 2023

VISA

Contents

Executive

Summary

Executive Summary

This report provides an overview of the top payment ecosystem threats within the past six-month period (December 2022 – May 2023) as identified by Visa Payment Fraud Disruption (PFD). Over the course of this period, threat actors increasingly employed new and emerging technologies to facilitate advanced and technical fraud schemes. These include the use of malvertising and search engine optimization (SEO) techniques to cultivate compelling and effective phishing and social engineering campaigns, the utilization of emerging advanced language model (ALM) technologies, and the increased targeting of authentication processes. While new technologies and processes such as user authentication, dynamic data, and ALMs help in securing the payments ecosystem, these new technologies are also often exploited by threat actors or used maliciously to facilitate fraud, as seen over the past six-month period. Threat actors also remained consistent in conducting tried and tested fraud schemes such as ATM targeting, automated fuel dispenser fraud, point-of-sale malware attacks, and payment account enumeration. Such longstanding methodologies are consistently identified in both historic and more recent payments ecosystem threat activity. However, threat actors are continuing to innovate upon these traditional methodologies in novel ways.

While the global fraud rate has trended at or below normal levels for the past six closed months, threat actors were successful in conducting targeted and sophisticated fraud schemes impacting specific institutions, technology, and processes. Examples of this asymmetric fraud impact include insufficient internal security controls enabling actors to exploit weaknesses and move laterally within systems to facilitate cashout operations, misconfigurations in authentication processes leading to inaccurate authentication of threat actors during digital skimming campaigns, and auto-onboarding of merchants within eCommerce platforms that allow threat actors to effectively create fraudulent merchants for the purposes of enumeration and fraud. This impact on various payments ecosystem institutions highlights threat actors' increasing innovation, expertise, and efficiency. Actors are becoming more advanced and technical and are able to exploit an identified vulnerability with alarming efficiency and expediency, as discussed throughout this report. In response, the Visa Risk Operations Center (ROC), Visa's 24x7 team responsible for triaging and analyzing fraud-related incidents and transaction-level alerting globally, responded to 1,985 incidents with 33% of these incidents generating a pre-emptive, targeted block to mitigate/prevent fraud while ensuring legitimate transaction activity continued. These instituted blocks of presumed fraudulent transactions resulted in over 53.1M declined transactions for US$32B, helping prevent fraud in the ecosystem. Visa strives to determine the best surgical block methods to prevent further fraud while minimizing impact to legitimate transactions. This involves detailed analysis of attack transactions and authorization messages, as well as overall payment volume and impact.

Top Fraud Trends

Threat actors continued to exploit technical misconfigurations through various fraud schemes, including:

- exploiting lax merchant auto-onboarding processes by using synthetic or stolen identities to pose as legitimate merchants when applying for payment services with the intent to commit fraud once granted access to the payment system
- innovating card present fraud techniques, including the use of vulnerabilities in supply chain entities operating in specific merchant verticals, the use of recurring payment vectors, and the continuation of automated fuel dispenser fraud

- enumeration attacks continue to be a popular vector for threat actors to validate and breach payment credentials, resulting in significant follow-on fraud. Over the past six months, the US region was the most heavily targeted from both the acquiring side (54% of total acquiring enumeration) and issuing side (39% of total issuer enumeration)
- continued targeting of cardholders and financial institutions through social engineering in attempts to bypass authentication procedures
- bribing a financial institution employee to deploy malware on the issuer's network and subsequently facilitating fraudulent point-of-sale (POS) transactions using various payment accounts
- ransomware groups continue to be active and expand their activities, with ransomware incidents increasing significantly over the past six months; 62% higher compared to the same period in 2022. In fact, March 2023 surpassed prior ransomware attack records for the most attacks in one month
- compromising a merchant's network to deploy POS malware configured to identify and harvest payment account details within the merchant's POS environment
- data security incidents increased by 3.4% in the December 2022-May 2023 period when compared to June 2022-November 2022. The top two contributors of at-risk credentials during this period are Third-Party Agent (TPA) cases and accounts recovered by Visa's intelligence team from various sources
- eCommerce continues to be disproportionately targeted from a data security perspective; eCommerce merchants were responsible for 58% of total fraud and breach investigations, while brick and mortar merchants made up 20%, and ransomware/fraud scheme made up 7%

Over the next six month period PFD assesses threat actors will increase attacks and attention on the authentication stage as authentication technology becomes more ubiquitous across the payments ecosystem, further exploit and utilize ALMs to cultivate effective social engineering campaigns and facilitate fraud, continue ransomware attacks by exploiting vulnerabilities in technology, target identity data with increased frequency, and focus significant attention on supply chains and third parties.

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.

Ecosystem Fraud Overview

Ecosystem Fraud Overview

The Risk Management Information Systems (MIS) Team 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 the payments ecosystem. MIS observed the global fraud rate trending at or below normal levels for the past six closed months.

From Dec 22 – Feb 23, fraud rate improved slightly year-over-year (YoY), and the latest data is trending upward. This has the potential to change considerably as more fraud is reported to Visa. During Dec 22 – Feb 23, the improvement in Global Fraud Rate was driven by a decrease in card not present (CNP) fraud rate. The global fraud rate decrease is due to the further adoption of secure eCommerce technologies such as 3D Secure and tokenization. At the same time, card present (CP) fraud rate had a slight increase YoY, due to increased cross-border chip and contactless fraud activity in the Europe, Asia-Pacific, and Canada regions, driven primarily by Travel, Restaurants and Department & Apparel industry segments. This increase is largely the result of provisioning fraud as well as the elimination of the remaining COVID-19 restrictions globally. Payment volume in the card present channel has increased as a result, and the fraud rate increased in tandem with the increase in payment volume.

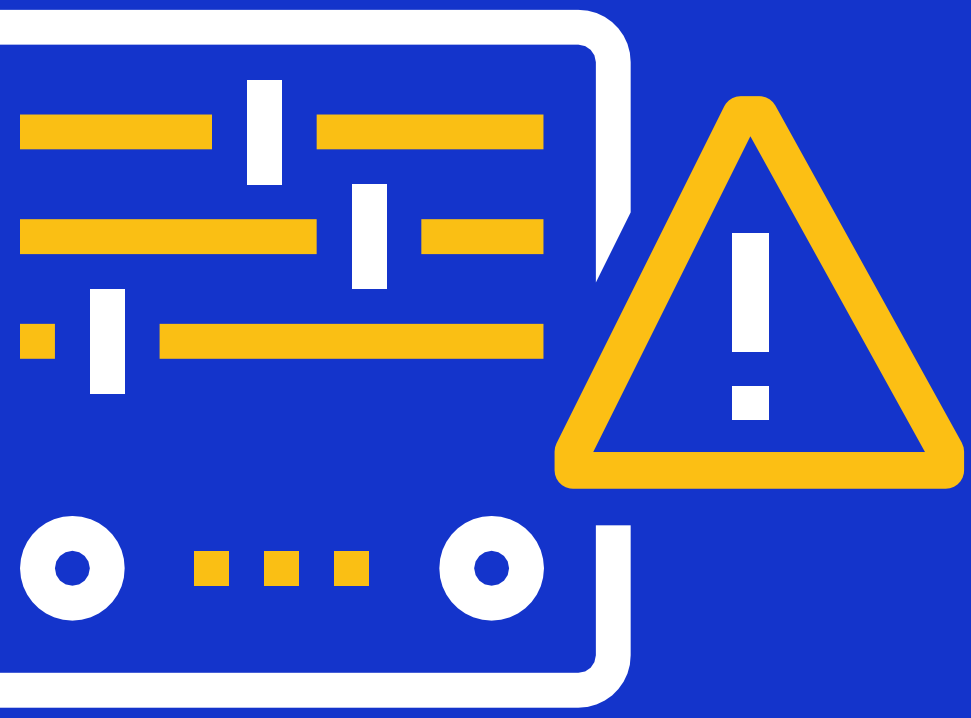
The global fraud statistics are representative of the threats and fraud trends discussed throughout this report. For example, the efficacy of secure eCommerce transactions, such as 3DS and tokenization, are reflected in the decreased CNP fraud rate. However, actors are increasingly focusing efforts on bypassing this technology through more advanced and technical fraud schemes and/or finding new and novel ways to conduct fraudulent activity. Moreover, the card present schemes discussed in this report, along with the continuation of one-time-passcode bypass and provisioning fraud discussed in previous reporting, significantly contributed to the global increase in the card present fraud rate.

Moreover, Visa PFD's **Hawkeye** team, which aims at mitigating fraud at an early stage via anomaly detection, monitoring and alerting noted the following investigation trends over the past six months:

- CAMS Fraud Identifications – Increasing Trend ▪ Potentially fraudulent identifications from the Compromised Account Management System (CAMS) Predictive Solution increased by **25%+** in the Dec 2022-May 2023 period when compared to May 2022-Nov 2022, meaning that fraudsters were more successful in the monetization of breached credentials during this period.
- Fallback Fraud Identifications – Increasing Trend ▪ Fraudulent identifications from the Risky Fallback tools increased by **97%+** in the Dec 2022-May 2023 period when compared to May 2022-Nov 2022, denoting a greater focus from threat actors on exploiting fallback transactions.
- Automated Fuel Dispenser (AFD) Cross-border (XB) Fraud Identifications – Decreasing Trend ▪ Fraudulent identifications from our AFD XB Predictive Solution has decreased by **17%** in the Dec 2022-May 2023 period when compared to May 2022-Nov 2022 as fraudster have shifted away from this fraud vector.

Technical

Misconfigurations



Technical Misconfigurations & Novel Fraud Schemes

Increase in Deep Insert ATM Skimmers

Automated teller machine (ATM) fraud schemes are a constant issue for the payments ecosystem. In the past six-month period Visa Payment Fraud Disruption (PFD) identified a continued increase in ATM schemes globally, both novel and revitalized.

In February 2023, an increase in reports of deep insert skimmers on North American ATMs was identified, which was corroborated by media reports of an increase in these skimmers identified in North America in March 2023. In skimming attacks, threat actors place a removable device on an in-store, fuel pump, or ATM point-of-sale (POS) terminal to harvest the magstripe track data from card present transactions at the targeted terminals. The data stolen from skimmers is then sold in cybercrime underground marketplaces, used for fraudulent transactions, or used in the creation of counterfeit cards. Recent improvements in skimmer technology have made skimming devices more challenging to detect, as some are only 0.68 millimeters wide and fit inside of the ATM card acceptance slots. Additionally, actors hide "pinhole" cameras on the ATM to capture the personal identification number (PIN) affiliated with the skimmed card.

Visa PFD anticipates that ATM-focused fraud schemes will continue to rise, due to simplicity and efficacy of attack methods and accessibility of ATMs. Additionally, Visa PFD recommends monitoring ATM transaction activity for excessive refund and reversal transactions, as well as for indicators of physical tampering of the machine.

Exploitation of Merchant Onboarding

An increase in fraud associated with threat actors exploiting weak or inadequate merchant onboarding practices to establish fraudulent merchants was identified in the past six-month period. Threat actors posing as legitimate merchants attempt to apply for payment services with the intent to commit fraud, once granted access to the payment system. The actors often use synthetic or stolen identities obtained through data breaches, social engineering, or in cybercrime underground marketplaces. A key factor compounding the risk of onboarding fraudulent merchants is the widespread adoption of automated onboarding or "auto-boarding" by payment facilitators and marketplaces. Auto-boarding, if not properly managed and controlled, could increase the risk of approving fraudulent merchant applications. Common fraudulent merchant schemes include:

- **False, spoofed, or counterfeit merchants:** established to take customer orders but do not actually fulfill the goods or services ordered, and instead steal customers' payment account information.
- **Triangulation schemes:** threat actors create illegitimate merchants and accompanying websites offering bargains on in-demand or luxury goods/services and fulfill orders made on their website through purchasing goods via legitimate websites using stolen payment accounts.

- **Cash-out merchants:** fake merchants established solely to cash-out stolen payment accounts obtained through enumeration or from cybercrime underground marketplaces. These merchants have no online or physical presence and are generally known only to the fraud ring conducting the cash-out activity.
- **Bust-out schemes (aka flash fraud merchants)**: threat actors establish a legitimate merchant and process a small number of legitimate payments to establish credibility. Once a satisfactory payment processing history is established, the seller suddenly submits a large number of fraudulent transactions—often using stolen payment account data – and quickly disappears after they obtain the funds from the stolen accounts.

In the past six months, Visa Payment Fraud Disruption (PFD) identified several schemes wherein threat actors used fraudulent merchants to cash out funds from compromised primary account numbers (PANs), in a similar manner to the "cash-out merchant" category noted above.

Visa PFD anticipates threat actors will continue to exploit weak or inadequate merchant onboarding practices. Acquirers should remain vigilant in combatting fraud related to fake and newly onboarded merchants.

Increase in Scams and Social Engineering

Over the past six months, Visa Payment Fraud Disruption (PFD) observed an increase in reports of the number and variety of scams impacting consumers, including investment/cryptocurrency scams, opportunistic/situational scams, and general financial and eCommerce scams propagated by malvertising, phishing, and illicit search engine optimization (SEO). Threat actors also continued favoring social engineering to commit scams and account take over (ATO).

Investment/Cryptocurrency Scams: In investment schemes victims are often prompted to use their credit or debit account to purchase the crypto, in addition to wire and bank transfers. Visa PFD previously reported on a fraud scheme involving 11K fake investment domains identified in Europe, and highlighted the continued interest from threat actors to conduct fraudulent investment schemes. The US Federal Trade Commission (FTC), which compiles data received from consumers as well as federal, state and local law enforcement agencies to track the top types of fraud, reported a similar significant increase in investment scams. Indeed, there were over 30 percent more consumer losses reported in 2022 than in 2021, with reported investment scam fraud losses more than doubling to US$3.8B in 2022. The FTC's findings reflect investment fraud as the top scam type in terms of total dollar losses in the US, and investment scams had the highest number of consumer generated fraud reports over this period.

Opportunistic Scams: Threat actors are often quick to innovate new fraud schemes in times of uncertainty or natural disaster, such as the numerous COVID-related scam merchants during the pandemic or fake donation sites that emerged to allegedly assist Ukrainians in 2022. In a similar fashion, during the March 2023 collapse of Silicon Valley Bank (SVB), researchers identified an increase in newly established suspicious domains using the SVB name and unstable situation in threat actors' attempts to phish victims. On the day the bank collapsed, nine (9) new domains were registered containing the character string "SVB"; over the following two days, 78 new suspicious domains using "SVB" were registered. In these types of scams, actors often try to obtain payment account information and other sensitive data from their victims which will then be used to commit financial fraud and theft.

Use of Malvertising and Illicit SEO: In January 2023, Visa PFD identified an increase in threat actors using illicit search engine optimization (SEO) and advertisements to promote phishing websites for purchase return authorization (PRA) fraud.

Given the steady increase in the types of scams noted above and the efficacy of such scams to perpetrate fraud in various forms, Visa PFD assesses scams will continue to be an attractive threat tactic employed by threat actors globally.

AFD Fraudsters Continue Targeting Issuers

In general, automated fuel dispenser (AFD) fraud rates trended favorably YoY. While the reporting period is still open as of June 2023, the current rates show significant improvement when compared to the same period in the previous year.

While general AFD fraud is trending in a favorable direction, Visa Payment Fraud Disruption (PFD) continued to identify significantly impactful AFD fraud schemes perpetrated against issuers with insufficient processing configurations in the AFD channel. This further underscores actor interest in circumventing new and emerging technologies by identifying vulnerabilities and conducting increasingly advanced fraud schemes. Indeed, between 01 December 2022 and 30 May 2023, AFD fraud alerts sent by PFD increased **64%** from the prior six-month period.

Visa PFD previously observed AFD fraud mainly targeting issuers in the North America (NA) and Latin American and Caribbean (LAC) regions. This trend continued in FY23, where approximately **70%** of identified AFD fraud totals involved LAC payment accounts in FYQ1 and FYQ3, and **85%** on NA payment accounts in FYQ2.

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.

General Data Breach and Ransomware Update

Visa Payment Fraud Disruption (PFD) tracks data breaches and ransomware attacks impacting Visa merchants, processors, third parties, acquirers, and issuers, as well as other payments ecosystem organizations around the globe. Such attacks are extensively researched to identify payment data exposure. When necessary, a formal investigation and case is created, and the impacted organization is contacted by Visa to determine if any payment data was exposed and to aid with mitigation and remediation.

March 2023 surpassed prior ransomware attack records for the most attacks in one month with nearly **460** attacks; a **91%** increase over February 2023 numbers and **62%** higher compared to the same period in 2022. A 2023 ransomware report identified that exploited vulnerabilities were the most common (36%) root cause of ransomware attacks, followed by compromised credentials (29%).

Ransomware and data breach attacks that involve exfiltration of data remain opportunistic. Ransomware attacks and related threat actors do not always target payment data specifically but will compromise any data accessible during their attacks including payment data or personal identifiable information (PII). PII can be valuable to threat actors for use as leverage with their victim and subsequently for monetization if the threat actor chooses to sell the PII in cybercrime underground marketplaces.

Clop Ransomware Group Targets Another File Transfer Service in 2023

Visa PFD recently reported a third-party breach impacting entities across the payments ecosystem. The incident, which occurred in February 2023, was the result of the Clop ransomware group, also known as "Cl0p," targeting two different file transfer services by employing similar tactics, techniques, and procedures (TTPs) as was used in another attack perpetrated by Clop in 2020. The 2020 attack resulted in the compromise of approximately 100 companies, and the recent 2023 attack allegedly involves stolen data from over 130 companies across multiple sectors including financial organizations, investment services, healthcare, retail, hospitality. In both attacks, the Russian-linked Clop group used zero-day vulnerabilities in file transfer services admin browsers, such as internet accessibility, publicly exposed ports (8000 and 8001), and lack of cross-site request forgery (CSRF) protection to compromise data from companies using the file transfer services. Clop then used the stolen data to extort the impacted companies. To address the 2023 vulnerability, the file transfer service added a "license request token" in the patch, acting as a CSRF token. The National Institute of Standards and Technology (NIST) released a common vulnerabilities and exposures (CVE) report for this vulnerability (CVE-2023-0669) in February 2023.

In February 2023, threat actor group BlackCat (aka ALPHV), reportedly also targeted victims using the same vulnerability (CVE-2023-0669). Visa PFD assesses that Clop, ALPHV and other threat actors will likely continue to target file transfer services with similar vulnerabilities, to include payments ecosystem organizations utilizing such vulnerable services. Visa PFD continues to closely monitor Clop attacks for impact to the payments ecosystem.

BidenCash Release Containing Millions of Compromised Payment Accounts

In March 2023, the cybercrime underground carding shop, "BidenCash" released another data set of over 2.1 million allegedly compromised payment accounts and affiliated personal identifiable information (PII) for free. The March 2023 release primarily affected issuers in the US and contained primary account numbers (PANs), expiration dates, CVV2, cardholder names, mailing and email addresses. Researchers suspect BidenCash obtains data from other underground carding shops and forums, in addition to sourcing compromised cardholder data from malware infections, such as the Redline Stealer or Racoon malware, which are offered as Malware-as-a-Service by cybercriminals.

As the ecosystem employs more secure acceptance technologies, such as tokenization and EMV Chip, the usefulness of such compromised payment account data has significantly decreased from a threat actor perspective as the monetization of such data is more difficult. Moreover, disruption efforts of large criminal operations and infrastructure, such as the takedown of Joker's Stash and the illicit Try2Check testing service, impacted threat actor ability to peddle compromised payment account data. Indeed, for the first three quarters of this year, **the overall fraud rate of at-risk accounts decreased significantly year-over-year**. This underscores threat actor focus shifting towards exploiting vulnerabilities, technical misconfigurations, and utilizing compromised or synthetic identity data rather than the more traditional model of obtaining compromised payment account data to conduct fraud.

Malformed JSON Web Token Used to Bypass Authentication Protocols

Threat actors recently conducted attacks wherein JSON Web Tokens (JWT) were modified to bypass authentication controls. In these attacks the threat actors targeted the JWTs presented to visitors during the user authentication process. The threat actors were able to present a malformed JWT to the system, and the victim's system erroneously authenticated the threat actors, giving them access to a legitimate customer account. Once inside the victim's system, a coding error in the victim's Application Programming Interface (API) allowed the threat actors to query stored payment account data in the compromised user's account. This enabled the threat actors to extract sensitive cardholder data, including the primary account numbers (PANs), expiration date, and CVV2. In a second reported example, a threat researcher discovered how to successfully modify the JWT presented to a visitor of a manufacturer's supply chain management web application. This allowed the researcher to create valid JWTs to authenticate a user by only using an employee's email account, as the application did not require a password for authentication. The researcher was then able to exploit API configurations to identify privileged roles, change login emails, and elevate privileges to gain access to the victim's entire supply chain network.

These examples highlight threat actors' interest in exploiting JWTs to bypass the user authentication process, as well as the importance for organizations to properly secure all APIs utilized within an organization and ensure the code of all APIs are routinely tested for any potential vulnerabilities, especially when using JWTs to authenticate users.

Potential Fraudulent Applications of Emerging AI Technologies

In the last six-month period, ChatGPT and other advanced language models (ALMs), such as Bard AI and Chat Sonic, rapidly became famous in nearly all facets of society. Visa Payment Fraud Disruption (PFD) assesses these ALMs can be exploited by threat actors to enhance phishing campaigns or assist in the modification of code to become malicious or obfuscate a malware's signature. Threat actors may be able to exploit ALMs to conduct fraud in the following ways:

Creating phishing lures:

- ALMs can produce any written request free of grammar or spelling errors which makes it especially difficult for security protocols using the detection of grammatical/spelling errors to identify and prevent phishing emails or other messages from reaching the threat actors' intended target. These emails can also contain language to evoke a sense of urgency, a common social engineering tactic used by threat actors.
- Other AI products are capable of generating realistic speech capable of mimicking human emotions and logic, which could be exploited by threat actors to impersonate financial institutions to obtain one-time passwords (OTPs) or execute vishing campaigns to steal payment account credentials.
- Enhanced programs such as Auto-GPT can automate the prompt delivery process used to make requests of ALMs, meaning threat actors can use Auto-GPT in conjunction with bots to automatically create and distribute phishing campaigns with minimal effort and human-interactions.

Creating malware:

- ALMs, such as ChatGPT, can be exploited by threat actors to create malware and assist in the development of malicious code, which could be deployed to execute digital skimming or other attacks to steal payment account credentials.
- ALMS are capable of creating malware acting as file stealers and threat actors have used ChatGPT to create a crypter capable of obfuscating malware to evade security programs. Other threat actors generated malware capable of encrypting an entire device in a ransomware attack.
- These AI programs can be used to create polymorphic malware which can automatically alter its digital signature to evade detection and create scripts, also known as SMS bots, to send numerous SMS notifications to a victim's device in an MFA Fatigue attack to bypass security controls and gain access to a victim's account.

Enumeration Remains Consistent Ecosystem Threat

Over the past six months, 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) remained among the top threats to the payments ecosystem. In this period, Visa Payment Fraud Disruption (PFD) noted a 40% increase in enumeration transaction volume as compared to the previous period.

In January 2023, Visa PFD alerted on an enumeration trend impacting Merchant Category Codes (MCCs) related to health, medical and dental service and providers: **MCC 8011 – Doctors & Physicians, MCC 8021 - Dentists/Orthodontists and MCC 8099 – Medical/Health Services.** The number of merchants targeted, as well as the number of enumerated transactions, spiked at the end of December 2022. As of June 14, 2023, activity on these MCCs is increasing and continued monitoring on these MCC's is advised.

In April 2023, Visa PFD alerted on enumeration attacks utilizing virtual terminals, virtual point-of-sale (VPOS) and mobile point-of-sale (MPOS) devices occurring between August 2022 and February 2023. Two notable attacks were identified, and the attacks share a similar modus operandi: using a compromised merchant email account to gain access to the merchant's gateway terminal to conduct enumeration attacks on the merchant's VPOS or MPOS. In both attacks, threat actors added new virtual devices to the merchant's VPOS configurations which enabled them to run the attack transactions within the VPOS environment. Visa has not identified any patterns nor commonalities across the merchants or the MPOS/VPOS providers impacted in these attacks. Additionally, Visa PFD identified a reduction in these types of attacks since mitigation and prevention measures were implemented in March 2023. Nonetheless, Visa PFD assesses the threat actors in these attacks, in addition to others with similar levels of capability, will likely continue to employ these tactics on VPOS and MPOS services to facilitate enumeration attacks.

In the period March to May 2023, two new tactics employed by threat actors conducting payment account enumeration attacks were identified. The newly identified tactics involve the use of recurring transactions, indicated by POS (Point-of-Sale) Environment Code = R, and the exploitation of lax onboarding policies within large merchant ecosystems to onboard fraudulent merchants and utilize these merchants for enumeration activity. Visa PFD assesses actors are likely employing recurring payments to circumvent fraud detection and anti-enumeration strategies that do not consider the POS environment code or treat recurring transactions as less risky. As such, issuers and acquirers should monitor for spikes on recurring payments with POS Environment Code = R to prevent such enumeration attacks. Threat actors are also targeting merchant ecosystems with auto-onboarding policies enabling actors to create new, fraudulent merchants quickly and efficiently, and subsequently use the merchants to conduct enumeration attacks. s.

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 block egregious attacks, pending extensive impact review, analysis and client/stakeholder review and analysis, to mitigate and prevent the successful enumeration of payment accounts. Global enumeration remained relatively stable when compared YoY.

The US region remained the most heavily targeted from both the acquiring side (**54%** of total acquiring enumeration) and issuing side (**39%** of total issuer enumeration)as shown in Figure 1, below.

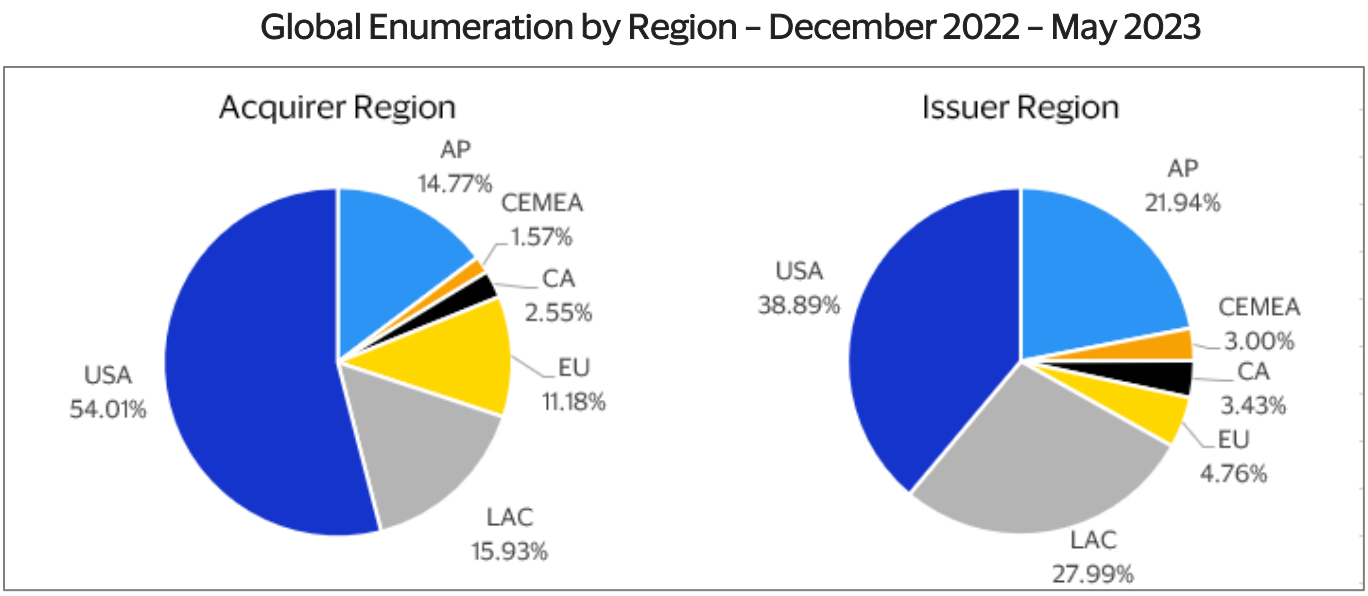


Figure 1: Source - Visa Payment Fraud Disruption

Digital Skimming Threat Actors Continue Targeting eCommerce Merchants

In digital skimming attacks, threat actors deploy malicious code onto a merchant website targeting their checkout pages to harvest payment account data entered by consumers, such as primary account number (PAN), card verification value (CVV2), expiration date, and personal identifiable information (PII). Digital skimming attacks are often the result of misconfigurations or lack of security controls within a merchant's environment, which threat actors exploit to deploy the malicious skimming code.

Numerous developments in the digital skimming threat landscape were identified over the past six-month period with threat actors increasingly targeting payment gateway and third-party supply chain or web infrastructure providers with malicious web shells or backdoor malware to compromise multiple entities at once. Threat actors have also used fake iFrames and modals to impersonate eCommerce merchants' legitimate checkout forms to steal payment account data. In many of these incidents, the victims did not employ proper controls to secure administrator credentials, such as multi-factor authentication (MFA) or one-time passwords (OTP).

The most notable developments within digital skimming as identified by Visa Payment Fraud Disruption (PFD) are as follows:

eCommerce Payment Gateway Providers Compromised through Web Shells

In the past six-month period, two incidents occurred in which eCommerce payment gateway providers were compromised through the deployment of malicious web shells and SQL queries were used to facilitate the compromise of payment account data.

In the first incident, an eCommerce payment gateway provider was compromised in an attack wherein threat actors likely gained initial access to the victim's environment by obtaining administrator credentials. Using these stolen credentials, the threat actors gained remote access to the victims' host server. Due to an unrestricted file upload vulnerability which existed within the server, threat actors were able to upload malicious ASP web shells onto the source code directory of the victim's payment application servers. The threat actors eventually extracted payment account data, including the cardholder's name, primary account number (PAN), expiration date, CVV2, and the name of the issuing bank, and stored the stolen data within the two text files, which were then exfiltrated to a threat actor command-and-control (C2) server.

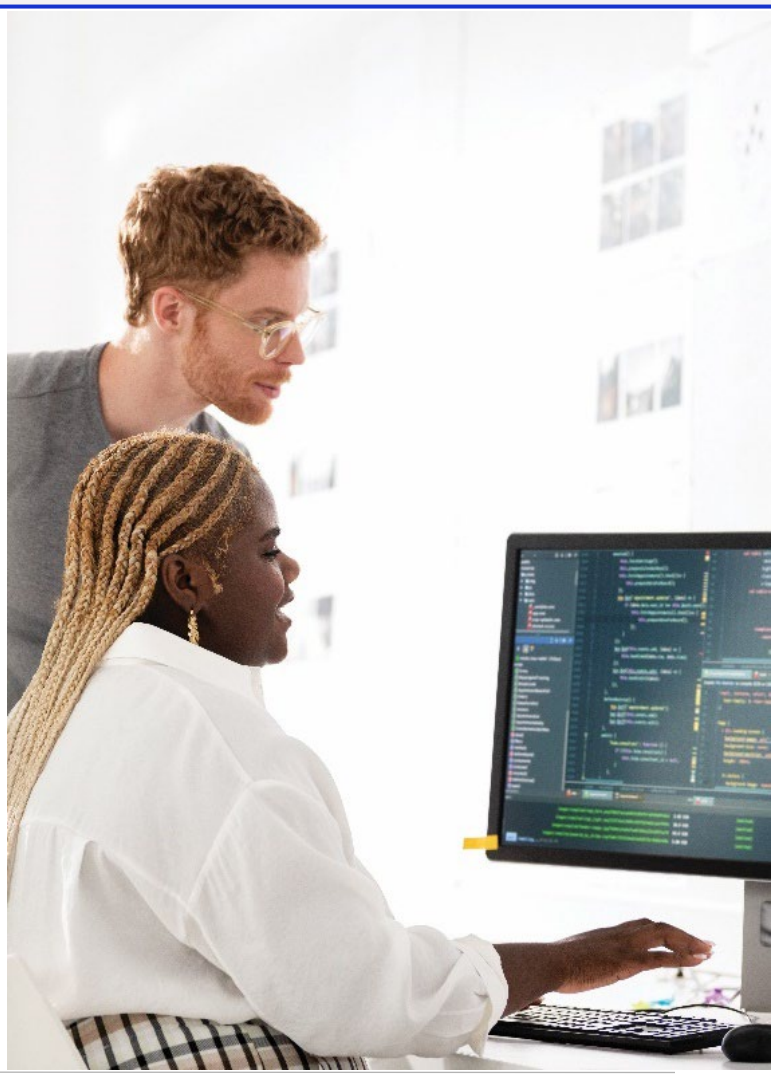
In the second payment gateway provider compromise, threat actors targeted a separate payment gateway provider through an SQL injection attack and deployed malicious web shells into the victim's environment. Once inside the victim's environment, the threat actors identified the payment processing servers and deployed malware to obtain payment account credentials, such as the primary account number (PAN), cardholder name, CVV2 and expiration date, and exfiltrated the data to a threat actor-controlled server from the victim's payment gateway server.

Of note, this second victim lacked several security protocols enabling the threat actors to conduct this attack. Notably, the victim's Endpoint Detection and Response system (EDR) did not function properly at the time of the incident. Also, the victim's File Integrity Monitoring (FIM) tool was not properly employed onto critical network infrastructure, which allowed modifications to be made to several additional files.

Web Infrastructure Provider Compromised

A threat actor group targeted several eCommerce retailers in a digital skimming campaign, whereby threat actors gained backdoor access to the victims' websites through the compromise of a shared domain hosting service provider's server. While the initial method of intrusion is unknown, the threat actors likely gained access either through the retailers' websites' publicly accessible administrator panel or the actors compromised the website developers' administrator credentials. After obtaining the domain hosting provider's administrative credentials, the threat actors used the Mumblehard malware to create a backdoor in each of the merchants' eCommerce website environments.

Once inside the victims' eCommerce platform, threat actors modified existing PHP files to act as digital skimmers within the victims' eCommerce payment plugin. Through OPcache poisoning, threat actors directed skimmed payment account data, such as the PAN, CVV2, and expiry, to their servers, inserted a HTTP callback code to alert the actors of changes to administrative credentials, and remained undetected during entity investigation, allowing reinfection to occur. Multiple impacted merchants suffered a subsequent compromise shortly after the identified malware was removed and administrator credentials were changed, due to the initial malware infection and configuration.



Threat Actors Use Customized iFrames to Target eCommerce Merchant

The creation of fake or malicious iFrames is a common technique used by threat actors to obtain compromised payment account data. In one such incident in the past six months, threat actors gained access to an eCommerce merchant's environment after administrator credentials were compromised through a phishing campaign. After acquiring the administrator credentials, threat actors modified the legitimate code of the merchant's eCommerce web application by appending a test URL, to the footer section of the merchant's web application. As the victim maintains subdomains for each country in which the retailer conducts business, the threat actors appended this test URL to validate if all subdomains were hosted on the same server environment as the parent domain. Once the threat actors verified the domains shared the same web infrastructure, the threat actors removed this test URL and appended malicious code which contained a digital skimmer malware to the checkout webpages on each of the merchant's country-specific subdomains. The malware, deployed through an iFrame, harvested customer payment account data, such as the PAN, CVV2, and expiration date, that was input into the malicious iFrame during the checkout process. The stolen payment account data was sent to an external domain controlled by the threat actors through a POST request." It was noted during the investigation of this incident that the victim did not have multi-factor authentication (MFA) implemented on administrator accounts for the eCommerce platform, which enabled threat actors to gain access to the administrator environment with relative ease. Further, the malware used in this compromise created merchant-specific variants for each merchant targeted by the threat actors and the malware can identify and disable iFrame checkout forms before displaying its own malicious iFrame checkout form, from which the payment account data was stolen. Malicious iFrames are a common tool used by fraudsters to spoof legitimate eCommerce payment infrastructure and dupe victims into providing their payment account information, which is typically exfiltrated to a threat actor's C2 server or domain.

Threat Actors Continue to Target eCommerce Third-Party and Supply Chain Providers

Visa PFD also observed threat actors continuously targeting popular eCommerce payment platforms and other third-party providers in various digital skimming attacks. Known vulnerabilities within these platforms often allow threat actors to create new customer accounts on an eCommerce merchant's website and inject the checkout data fields with malicious digital skimming code during the order placement process. Once the order is approved and the email confirmation is generated, the malicious code runs backdoor commands and executes remote access trojans (RATs). Through these RATs, the threat actors can append malicious digital skimming code onto the checkout webpages of the targeted eCommerce merchants and steal payment account data entered into the checkout pages by customers. Additionally, threat actors also targeted payment platforms with new variations of digital skimming malware. Visa PFD previously reported on one

such malware referred to threat researchers as 'Kritec'. To prevent digital skimming campaigns and eCommerce threats, Visa recommends merchants and acquirers implement the following:

- Regularly ensure the shopping cart, other eCommerce modules, and all related software are upgraded or patched to the latest versions.
- Require strong administrative passwords and enable two-factor authentication.
- Regularly scan and test eCommerce sites for vulnerabilities or malware.
- Ensure familiarity and vigilance with code integrated into eCommerce environments via service providers by reviewing and validating code and updates.
- Implement network segmentation to prevent threat actor movement and ensure the cardholder data environment (CDE) is sufficiently protected.

Malware Used to Facilitate Fraud

Over the past six months, threat actors used various malware variants and tactics, including colluding with insiders, to bypass user authentication protocols and gain access to victims' environments. These malware variants include remote access tool (RAT) malware, keylogger malware, and point-of-sale (POS) malware, as well as other methods to obtain access to victims' sensitive data or cardholder information.

POS Malware Identified in Hospitality Merchant Compromise

In an ongoing trend, threat actors use Point-of-Sale (POS) malware to compromise magstripe payment account data at brick-and-mortar merchants. In POS malware campaigns, threat actors compromise a merchant's network, generally through large phishing campaigns or compromised user credentials, and move laterally within the compromised merchant's systems. The ultimate target is the POS environment in which the POS malware is deployed, which often consists of a RAM scraper configured to identify and harvest payment account details. After the payment account details are harvested and exfiltrated from the merchant environment, they are often sold on the cybercrime underground.

In a recent attack threat actors targeted a hospitality merchant with POS malware. In this attack, the threat actors deployed various tools to gain remote access to the victim environment, obtained compromised admin user credentials, moved laterally in the network to the POS environment, and ultimately deployed a Random Access Memory (RAM) scraper onto the victim's POS environment. The RAM scraper harvested Track 1 and Track 2 payment account data that transacted at connected POS terminals, and the actors then exfiltrated this data from the victim environment.

Threat Actor Disruption

Threat Actor Disruption

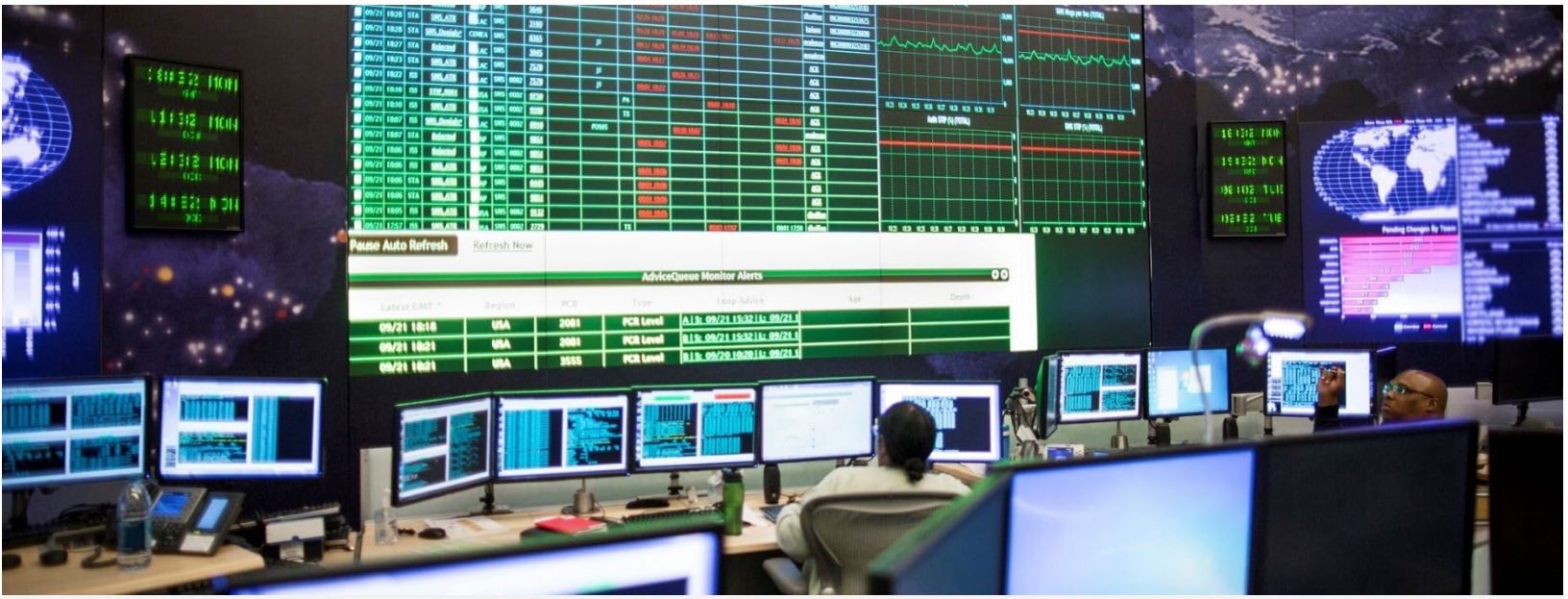
Visa Payment Fraud Disruption (PFD) supported global law enforcement and government entities throughout the past six-month period to disrupt criminals targeting the financial and payments ecosystem. Many of the law enforcement and disruption efforts focused on dismantling criminal operations that leveraged new and novel techniques and technologies, which further represents the shifting threat landscape. Some of the top actor disruption operations are included below:

Try2Check Takedown

In May 2023, the US Secret Service, with partners in Germany and Austria dismantled the largest and longest-running cybercrime underground illicit card-checking platform, Try2Check, and announced the indictment of the site administrator, Denis Gennadievich Kulkov (Russia). The Try2Check platform was commonly used among cybercriminals who bought and sold payment card data on underground forums and marketplaces to validate compromised payment account data through single low-dollar transactions. Upon arrest, Kulkov faces 20 years of imprisonment for access device fraud, computer intrusion, and money laundering.

Operation Urban Justice

In February, March and June 2023, the US Secret Service and local law enforcement made arrests to address the ongoing issue of electronic benefit transfer (EBT) fraud in California, as part of "Operation Urban Justice." The threat actors involved in this scheme conducted ATM withdrawals using counterfeit cards within the first few days of the month, in order to collect the money as soon as the funds are dispersed to the recipient accounts. The operation has resulted in the arrest of 20 suspects, to date. Based on previous arrests for EBT-related fraud, law enforcement believes there to be an Eastern European organized crime syndicate targeting EBT cards in California. California Department of Social Services believes theft of EBT funds totals over US$38.9M, with over US$2.9M stolen from Los Angeles County in January 2023 alone.



Genesis Market Shutdown

On 4 April 2023, an international coalition of law enforcement agencies from around the world, led by the US Department of Justice (DOJ) and the US Federal Bureau of Investigation (FBI) and Europol, seized the cybercrime marketplace known as "Genesis Market." This coordinated effort, dubbed 'Operation Cookie Monster' dismantled Genesis Market's leadership, resulting in the arrest of 119 individuals responsible for operating and maintaining the cybercrime underground marketplace. The market, which launched in 2018, started selling compromised credentials, before expanding to include the purchase, sale, and exchange of criminal services and products. The market sold data from over 1.5M compromised devices, impacting 80M unique account credentials. While this takedown is a significant cybercrime disruption development, Visa PFD assesses new marketplaces, such as the Styx Market, will attempt to fill the void left by Genesis Market.

Cryptocurrency
and Digital Payments

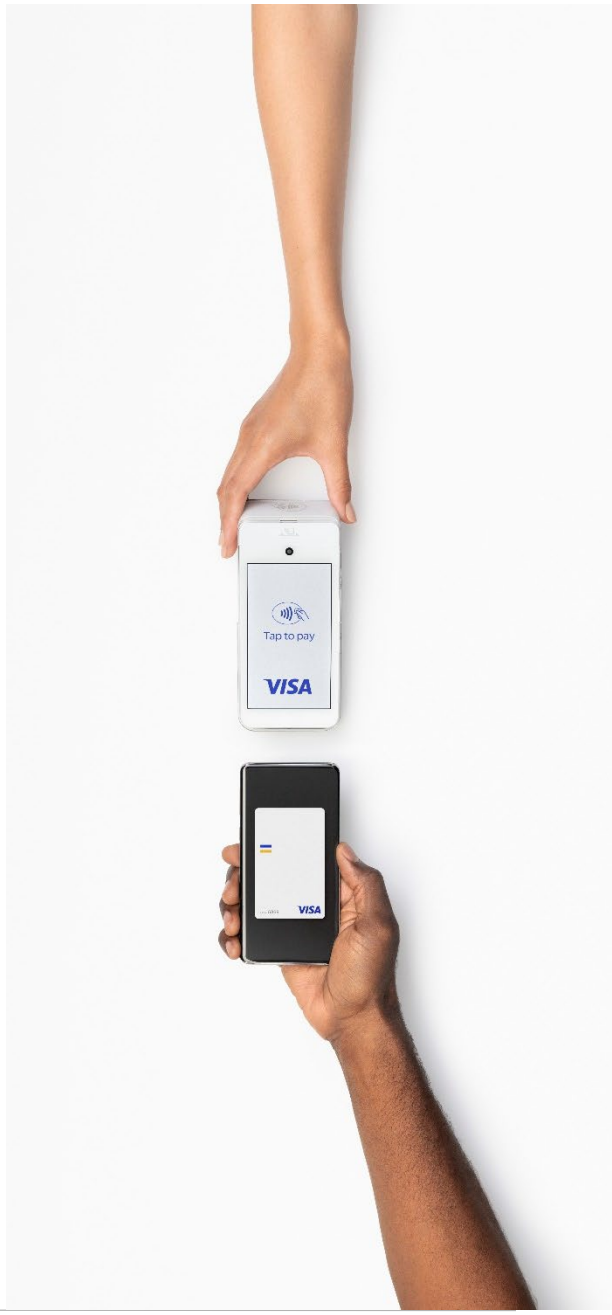
Cryptocurrency and Digital Payments

NFT and Digital Asset Thefts and Scams Continue

Consumers continued to be targeted with scams and thefts involving non-fungible tokens (NFTs) and other digital assets. Scams involving malicious free gift non-fungible token (NFT) campaigns continue to be a popular attack vector and are often spread through social media platforms. Attacks using vulnerabilities in platform code or smart contract processing are also used to steal digital assets and cryptocurrency wallet balances. Additionally, in the past six months, numerous "rug pull" schemes, which are often seen targeting cryptocurrency, targeted consumers in the NFT and digital asset space.

A non-fungible token (NFT), is a cryptographic digital token that is tied to, and represents ownership of a specific asset. Assets can be digital media or goods or tangible/physical goods that have been "tokenized" in order to be bought and sold in digital marketplaces. Non-fungible tokens, and the transactions involving the purchase and sale of NFTs, are written to a blockchain ledger, and the hash value representing the NFT is stored in a consumer's digital wallet. Unlike cryptocurrencies, however, NFTs are *not fungible,* meaning that the one NFT does not inherently hold the same value as another NFT.

- **Free gift scams**: there are a number of ways threat actors can perpetrate free gift scams. One common method involves fraudsters creating malicious art files containing executable JavaScript code. The malicious "free gift" is offered via a pop-up window asking the victim to confirm the transaction. By clicking the pop-up, the malicious payload is executed, which includes a file with an iframe that inserts an object onto the page offering the malicious NFT, allowing the fraudsters to communicate with the victim's wallet using the Ethereum JSON-PRC API. Once communication is opened, the fraudster can perform actions on behalf of the victim, such as authorizing cryptocurrency/digital asset transfers to send the balance of the victim's wallet to a fraudster-controlled wallet.
- **Vulnerability-based attacks**: threat actors exploiting vulnerabilities to steal cryptocurrency was a common theme throughout 2022. Visa Payment Fraud Disruption (PFD) reported on numerous incidents of crypto thefts involving blockchain bridge services, and the US Federal Bureau of Investigation (FBI) recently issued a warning to cryptocurrency investors about the increase in threat actors targeting Decentralized Finance (DeFi) crypto services. The FBI reports that through the targeting of vulnerabilities in the smart contracts governing DeFi platforms, between January and March 2022, threat actors stole US$1.3B in cryptocurrency. The same types of vulnerabilities exploited to steal cryptocurrency can also be used to steal victims' NFTs and other digital assets.
- **Rug pull scams**: a rug pull scam involves threat actors inflating the value and interest in a digital asset, NFT, coin, or cryptocurrency to attract investors, and after a significant amount of money has been invested, the threat actor exits the project, stealing all funds and assets that had been invested by victims. In the past six months, media highlighted multiple arrests, alleged embezzlement, and legal action taken involving individuals and scams associated with NFT platforms.



As cryptocurrency and digital asset/NFT platforms continue to develop and more virtual assets are held in consumers' digital wallets, threat actors will likely increase their attempts at stealing money and assets through exploiting vulnerabilities and perpetrating scams, such as the ones mentioned above.

Threats

Landscape Forecast

Threats Landscape Forecast

Increased Attacks and Attention on Authentication Stage of Transactions

Over the past year, Visa Payment Fraud Disruption (PFD) identified an increase in threat actors targeting step-up authentication within the transaction process to commit fraud. Authentication is the process of ensuring the Primary Account Number (PAN) is valid and that the proper authorized user of the PAN is attempting the transaction. This can be conducted through various means such as risk scoring based on behavioral patterns (e.g., device ID, location, IP address, etc.) or through step-up authentication such as one-time passwords sent to the cardholder.

The effectiveness of step-up authentication in combatting fraud has led to threat actor innovations to thwart such authentication measures. Over the past year, Visa PFD reported on multiple one-time passcode (OTP) bypass schemes, including phishing, social engineering schemes, and OTP relay schemes.

Authentication is an extra layer of security for payments to assist in the prevention of unauthorized transactions. However, the benefits of authentication require proper implementation, and issuers, acquirers and merchants should employ a multi-tiered approach to payment security.

Visa PFD reported in the previous Biannual Report an increase in targeting of authentication and as this trend has continued.

Exploitation of AI Technologies to Commit Fraud

Visa PFD assesses AI technologies will likely help facilitate fraud by lowering the barrier to entry in many threat types and enable actors to more efficiently scale their operations. Threat actors could use ALM technology in phishing campaigns to target victims around the world using easily created and effective phishing lures, regardless of the threat actors' or victims' locations or native languages, and deploy malware modified by ALMs capable of avoiding detection to obtain sensitive information, including payment account information.

Social engineering techniques will become more effective as threat actors can create spoofed written messages, speech, or images nearly indistinguishable from the legitimate entity or individual. Business Email Compromise (BEC) attacks will likely become more commonplace as threat actors can manipulate employees through voice and email messages impersonating a company's management or leadership executives, and threat actors can request ALMs generate messages using specific language to convince the victim the phishing messages were sent from the spoofed entity or person.

With the rise in the popularity of ALMs, it is imperative security protocols used to detect phishing attempts are enhanced to identify potential fraud or malicious emails beyond spelling and grammatical errors. Employees and consumers should be continuously educated on how ALMs can be exploited by fraudsters to socially engineer victims through phishing or vishing campaigns to gain access to their accounts or obtain payment account credentials.

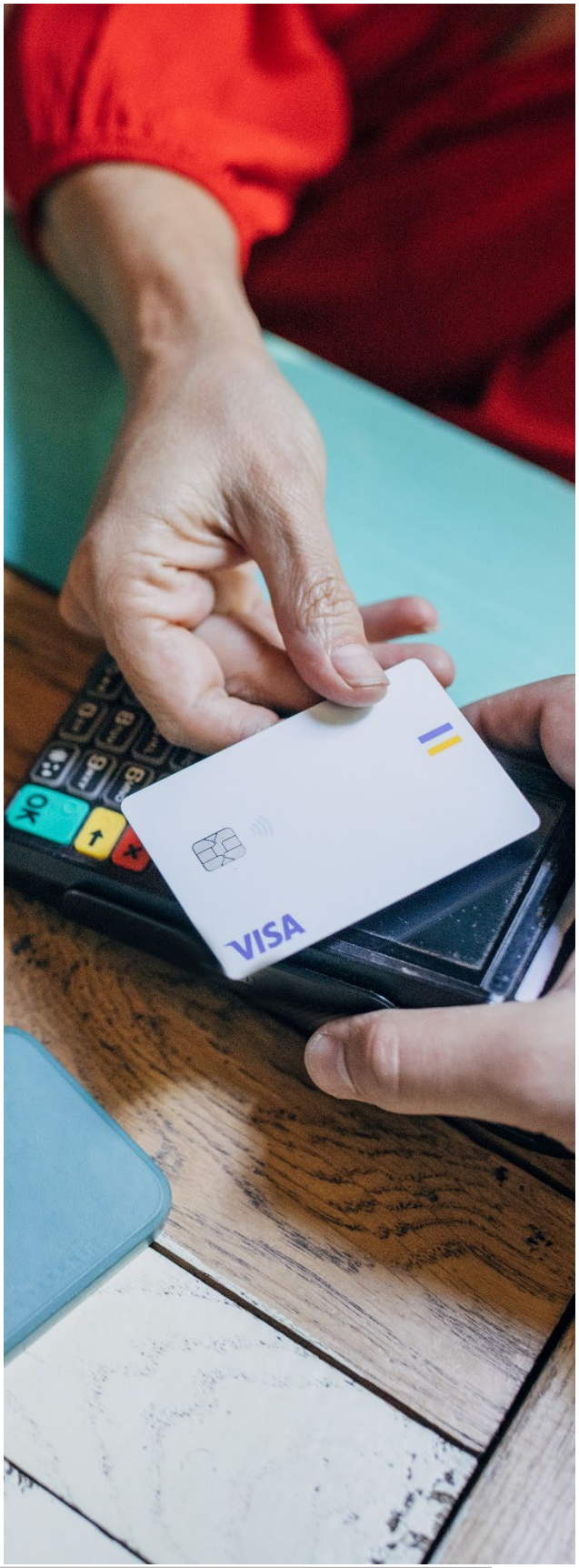
Ransomware

In addition to the unprecedented spike in ransomware attacks in March 2023, Visa PFD also identified continued ransomware and data breach attacks that were opportunistic in exfiltrating data. PFD Global Risk Investigations (GRI) ransomware cases identifications increase 66% from Mar 2023 – May 2023 when compared to the prior three-month period. GRI actively works with all entities who are impacted by ransomware to contain any payment data exposed and provided impacted accounts to

issuers in a timely manner. Over the next six-month period, ransomware threat actors will likely continue to target critical infrastructure to include financial organizations, among other critical entities. Additionally, Visa PFD forecasts threat actors will continue to utilize the same frequently used attack methods of phishing attacks and malicious email campaigns, and shift toward exploiting known vulnerabilities among file transfer services and remote access tools.

Targeting of Identity Data

Threat actors remain interested in using stolen or synthetic identities that can be created or purchased in cybercrime underground marketplaces and used to commit fraud. Synthetic identities are mixes of falsified credentials that do not belong to any individual, such as using a potentially legitimate social security number (SSN) in combination with fabricated personal identifiable information (PII). Visa PFD has observed suspected stolen or synthetic identities through the monitoring of prepaid card fraud and other payment channels.



Threat Actors Continue Trend of Targeting Supply Chain and Third-Party Providers

Threat actors continued the trend from the last 12-months in which third-party service providers and supply-chain infrastructure entities are targeted in various attacks. In the past six-month period, Visa Payment Fraud Disruption (PFD) published three security alerts wherein third-party providers, including payment gateway providers, were compromised by threat actors with the ultimate goal of obtaining payment account data.

Over the next six-month period, Visa PFD assesses third-party and supply chain providers will be a favored target for cybercriminals and threat actors across the global payments ecosystem. Threat actors will likely continue to target third-party providers, especially eCommerce payment gateway providers, in cybercriminal operations as the compromise of a shared service or provider enables threat actors to target a much larger population of potential payment account data for the same effort as a single eCommerce merchant. This threat potentially impacts merchants, processors, and acquirers around the globe and, particularly, those eCommerce entities lacking proper security controls or those not adhering to a strict vulnerability and patch management program.

Data Breach Forecast

PFD Global Risk Investigations (GRI) provided support in multiple Purchase Return Authorization (PRA) cases over the past six months. Visa Payment Fraud Disruption assess threat actors will continue to evolve tactics to target merchants and distribute fraudulent PRAs.

From Mar 2023 – May 2023, GRI identifications of point of sale (POS) skimming cases increased 58% when compared to the prior three-month period, which is the highest number of skimming cases for a three-month period. Visa PFD assesses targeted merchants will likely continue to include automated fuel dispensers (AFDs) and large brick-and-mortar retailers, and threat actors will likely continue to target unattended POS devices, necessitating the need for clients to implement monitoring and controls to detect skimming device.

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 prevents 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 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.

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 block egregious attacks to mitigate and prevent the successful enumeration of payment accounts.

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.

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), Risk Management Information Systems (MIS), and the entire Visa Risk organization.