A Payment Ecosystem Report by
Visa Payment Fraud Disruption

Biannual Threats Report

December 2023

VISA

Contents

Executive

Summary

Executive Summary

This report provides an overview of the top payment ecosystem threats within the past seven-month period (June 2023 – December 2023) as identified by Visa Payment Fraud Disruption (PFD). Over the course of this period, Visa PFD noted an interesting shift in threat actors' organization, sophistication, and target choice. Threat actors and groups are evolving into more organized and sophisticated operations, utilizing advanced tactics and cutting-edge technology to facilitate large-scale fraud operations. At the same time, threat actors have turned their focus more directly on cardholders, using advanced social engineering techniques to facilitate elaborate and well-designed scams. They are increasingly targeting the weakest link in the financial security chain: humans.

Throughout 2022, threat groups displayed an increased interest in targeting supply chains and third-party services aiming to compromise as many organizations as possible with a single breach. This trend has increased significantly in 2023. Ransomware groups continue to be active and expanded their activities over the past seven months, with ransomware incidents targeting the payments ecosystem increasing 37% June through December compared to the prior seven-month period (tracked by Visa Payment Threat Intelligence) and increasing **92%** when compared to the same June-December period in 2022. PFD Global Risk Investigations (GRI) also identified a significant trend in ransomware, with ransomware cases representing a **64%** increase from the previous seven-month period and **300%** increase from last year same period (June – Dec 2022).

Threat actors continued to probe the payments ecosystem for vulnerabilities and were successful in conducting targeted and sophisticated fraud schemes impacting specific institutions, technology, and processes. An example of this asymmetric fraud impact includes misconfigurations in authentication processes leading to erroneous approvals of fraudulent transactions. Threat actors are becoming more advanced, more 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 working in conjunction with clients to triage and analyze large-scale fraud-related incidents globally, experienced **62%** of these incidents generating a pre-emptive targeted block to mitigate fraud without impacting legitimate transactions. In its efforts to assist clients in preventing fraud, the ROC instituted blocks of presumed fraudulent transactions from June through December 2023 resulted in over **49.8M** declined transactions for **US$5.6B**.

While enumeration attacks contribute to less than 1% of global Card-Not-Present (CNP) payment volume, enumeration attacks continue to be a popular vector for threat actors to validate and compromise payment credentials, resulting in significant follow-on fraud. Over the past seven months, the US region increased as the most heavily targeted region from both the acquiring bank side (**60%** of total acquiring bank enumeration, increase of **6%**) and issuing bank side (**48%** of total issuing bank enumeration, increase of **10%**).

Purchase Return Authorization (PRA) fraud attacks continued to be a chosen tactic for threat actors over the past seven months. Visa PFD's GRI team opened a record number of PRA investigations from June 2023 to December 2023, an **83%** increase from the previous five-month period. These attacks resulted in potential fraud losses to banks approximating **US$115K** per successful attack.

Visa PFD assesses the next six months will likely see threat actors continue to develop innovative tactics along these two diametric routes: targeting large service provider vulnerabilities with network breaches and ransomware activity, while honing their craft at tactical and sophisticated individual cardholder social engineering with the goal of compromising payment data for fraudulent financial gain.

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.

To note: Visa PFD is adjusting the reporting period for the Biannual Threats Report to align more closely to calendar year; thus, this version represents a seven-month period, but future versions will revert to six months to ensure a full calendar year is captured.

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 6 closed months. While the overall global fraud rate has remained relatively stable over the past year, threat actors are moving and shifting their focus and tactics to various areas within payments based on innovative technology, the global financial climate, and newly identified vulnerabilities. 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. In 2021, threat actors were keenly focused on the cryptocurrency space, driving up fraud rates in that payments category. In 2022, PFD noted a shift in threat actor focus veering away from cryptocurrency and towards authentication bypass; a focus that intensified in 2023. Over the past year, PFD noted a general decrease in high-volume, low-level fraud and an increase in advanced, targeted fraud, which aligns with the data below.

From June 23 – August 23 (closed period), fraud remained consistent with prior months and the MIS team projects fraud rates will continue to remain consistent through December 2023, once fraud reporting is complete. While the Card Present (CP) payment volume increased by 4.8% in the June – August period compared to March – May 2023, the fraud rate decreased slightly. Comparatively, the Card-Not-Present (CNP) payment volume increased slightly along with a slight increase in the overall fraud rate. Fraud rates for both CP and CNP track relatively in-line with bps rates for the same periods in 2022. The global fraud statistics are representative of the threats and fraud trends discussed throughout this report.

Key Fraud Trends

Key Fraud Trends

General Data Breach and Ransomware Update

Ransomware and data breach incidents involving exfiltration of data remain prevalent and are an increasing threat across the payments ecosystem. 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 leverage for threat actors when negotiating with victims and subsequently for monetization if sold in cybercrime underground marketplaces if the actors ransom/extortion demands are not met.

Throughout 2023, Visa PFD continued to identify ransomware and data breach attacks that were opportunistic in exfiltrating data and noted threat actors' continued interest in exploiting known vulnerabilities among file transfer services and remote access tools. The most impactful ransomware attack of 2023, associated with a popular file transfer service, affected an estimated 2,620 organizations along with 77.2 million individuals whose PII was breached across the infiltrated organizations. The ransomware threat group known as CL0P claimed responsibility for the attack on 6 June 2023, but researchers suspect that CL0P began leveraging a zero-day vulnerability (CVE-2023-34362) as early as July 2021. This followed CL0P's deployment of ransomware on 31 January 2023 exploiting a vulnerability (CVE-2023-0669) in a different file transfer software, enabling the actors to obtain data from 130 organizations. The targeted file transfer service was a common vendor across numerous merchants including financial services and institutions, retail, education, healthcare as well as other merchant sectors and industries.

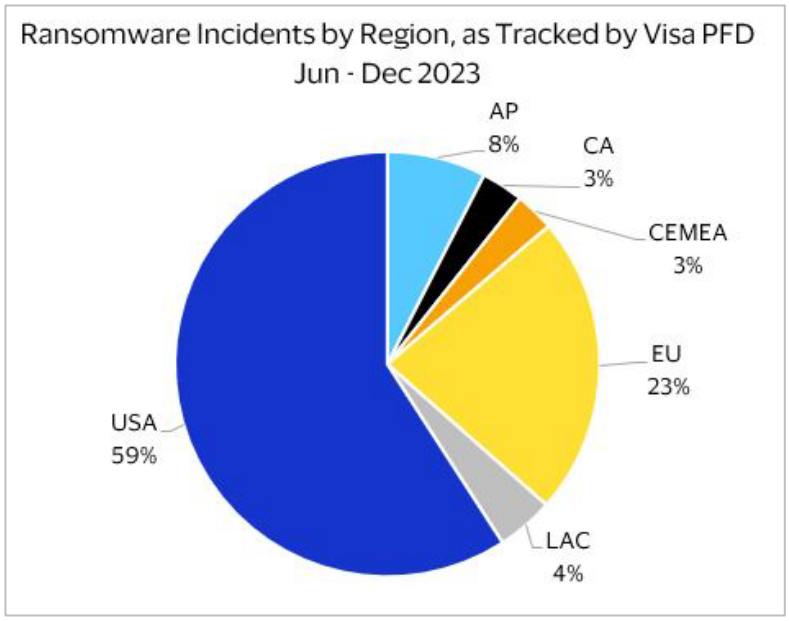


Figure 1: Source – Visa PFD

Additionally, Visa PFD identified North America as the most impacted region in terms of ransomware/data breach incidents impacting the payments ecosystem. The North America region experienced nearly three times the number of ransomware attacks compared to the Europe region, which experienced the second-highest level of incidents based on Visa PFD ransomware incident tracking, as seen in Figure 1, at left.

Figure 2, below, illustrates the number of ransomware and data breach incidents by region over the past seven months (1 June 2023 to 31 December 2023), which reflects a 37% increase in cases opened over the previous seven-month period, and a 131% increase in total incidents tracked in 2023 when compared to 2022 (as shown in Figure 5, below).

PFD Global Risk Investigations (GRI) assesses intelligence and opens formal investigation cases for Visa clients and merchants potentially impacted. From June through December 2023, PFD's GRI team identified a significant trend within the ransomware sub-category, noting a **64%** increase in ransomware cases opened from the previous seven-month period and **300%** increase from last year same period. Recently impacted entities included Level 1 and/or 2 merchants, financial institutions, agents, and span every region globally. PFD actively works with all entities who are impacted by ransomware to contain any payment data exposed and to provide impacted payment accounts to banks in a timely manner.

Figure 2, below, highlights the number of PFD Global Investigations Management Tool (GIMT) cases opened for ransomware/data breach cases by region over the past seven months (1 June 2023 – 31 December 2023), showing the US as the most targeted region by ransomware cases, with 59% of cases opened in the past seven months.

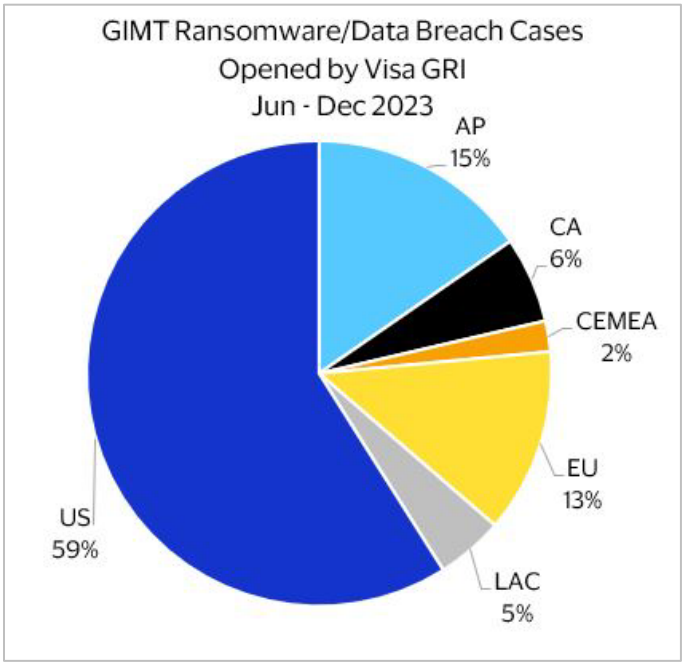


Figure 2: Source - Visa Payment Fraud Disruption

Additionally, Visa PFD observed a new tactic whereby threat actors began to leverage the United States Securities and Exchange Commission (SEC) to extort a ransomware victim. The ransomware threat actor group known as ALPHV, (AKA: BlackCat) was the first to employ a new approach to collecting a ransom from victims who disregard ransom demands and timelines. In an unprecedented move in mid-November 2023, the threat actors filed a complaint with the SEC, reporting that their victim did not disclose a material breach impacting "customer data and operational information." The threat actors' claim was based on new rules adopted by the SEC which were not set to take effect until 15 December 2023. While various ransomware actors previously threatened to notify the SEC of data thefts and breaches in the past, there is no evidence to suggest any of the groups took this action in prior ransom events.

Law enforcement continues to work aggressively to bring ransomware threat actors to justice. On 19 December 2023, the US Federal Bureau of Investigation (FBI) announced the takedown of the website belonging to ALPHV ransomware group, also targeted by the US Department of Justice (DOJ) due to the high ransoms paid by victims globally which is estimated to be in the hundreds-of-millions of dollars (USD). ALPHV's website went down on 7 December 2023 and the US FBI and DOJ confirmed involvement in the disruption on 19 December, advising several websites belonging to the group were seized. Additionally, federal investigators were able to create a decryption tool to mitigate the group's ransomware infections, which was shared with over 500 APLHV victims.

Hospitality Sector Widely Targeted by Threat Actors in 2023

The hospitality sector was increasingly impacted by ransomware and data breach incidents in 2023, along with the retail and travel sectors, which also reported being most affected by ransomware threat actor groups CL0P, Lockbit, and ALPHV/Blackcat, which is consistent with the top three threat actors identified in Visa PFD's analysis, as previously noted in the ransomware section of this report, over the payments ecosystem in the past seven months. In a scheme targeting the hospitality sector in the 2023, threat actors breached systems belonging to hotels, booking websites, and other travel and hospitality related merchants, that redirected guests to fake reservation websites in order to steal payment account data. Hotels and casinos impacted by ransomware in 2023 received extensive media coverage for causing problems for travelers and gamblers who were unable to use hotel keycards, slot machines, ATMs, and credit card machines when they stopped working due to ransomware attacks in September 2023 which were later claimed by APLV/Blackcat threat actors. Several of the hospitality merchants impacted exposed the PII of hundreds-of-thousands of people after being infiltrated by threat actors. Researchers conducted a study in 2023 related to security threats for the hospitality industry and found 31% of hospitality, retail and restaurant related companies experienced data breaches at least once in their company's history. Moreover, 89% reported being impacted by data breaches more than once within a year.

Another new campaign from QakBot, which began 11 December 2023, is targeting the hospitality industry. The campaign involves phishing messages wherein threat actors pose as a US Internal Revenue Service (IRS) employee and includes a PDF attachment with a malicious URL that, when opened, downloads malware. QakBot, initially designed as a banking trojan for harvesting bank credentials and suspected to be in use since 2008, developed into a multi-purpose botnet and malware variant enabling threat actors to deliver malicious payloads, including ransomware. In August 2023, Operation Duck Hunt conducted by the US FBI and international law enforcement agencies globally resulted in the successful takedown of the botnet and severed connections between victims' computers and QakBot's command and control (C2) servers. The new malicious payload and phishing campaign identified in December 2023 suggests the threat actors reassemble, as no threat actors were arrested in the FBI operation.

Visa PFD assesses the tactics described above will continue to be employed by threat actors attempting to obtain payment account data through targeting eCommerce merchants and environments, including hospitality merchants. It is recommended that all hospitality sector merchants remain vigilant to vulnerability exploits and new phishing schemes targeting the industry. Visa provides a digital Website Security for eCommerce Merchants guide, which provides useful mitigation recommendations for eCommerce merchants to prevent fraud attacks and unauthorized access to their eCommerce site.

Enumeration Trends Update

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) continues to remain among the top threats to the payment ecosystem. PFD vigilantly monitors for enumeration attacks through the Visa Account Attack Intelligence (VAAI) capability using machine learning to help identify enumeration attacks. VAAI then analyzes the details of the attack and enables Visa to notify affected acquiring banks/merchants and help block egregious attacks. Prior to any blocking action implementation, PFD undertakes an extensive impact review and analysis based on client guidelines and client/stakeholder review and analysis in order to mitigate and prevent the successful enumeration of payment accounts while maintain minimum impact on any legitimate activity.

Visa PFD tracks which Merchant Category Codes (MCCs) may have been targeted in attacks and, over the past seven-months, identified MCC 5999 - Miscellaneous and Specialty Retail Stores as having the most enumerated transactions, followed by MCC 5311 – Department Stores, which is reflected in Figure 3, below.

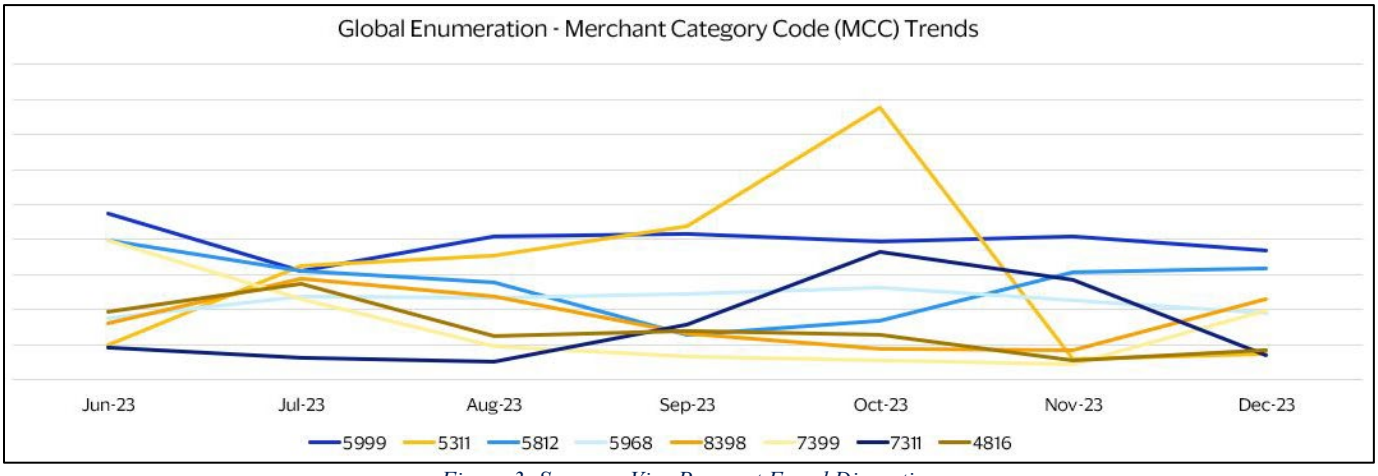


Figure 3: Source – Visa Payment Fraud Disruption

The US region remained the most heavily targeted from both the acquiring bank side (60% of total acquiring bank enumeration) and issuing bank side (48% of total issuing bank enumeration), as shown in Figure 4, below. This represents an increase in targeting of the US region for both issuers (+9.53%) and acquires (+5.75%).

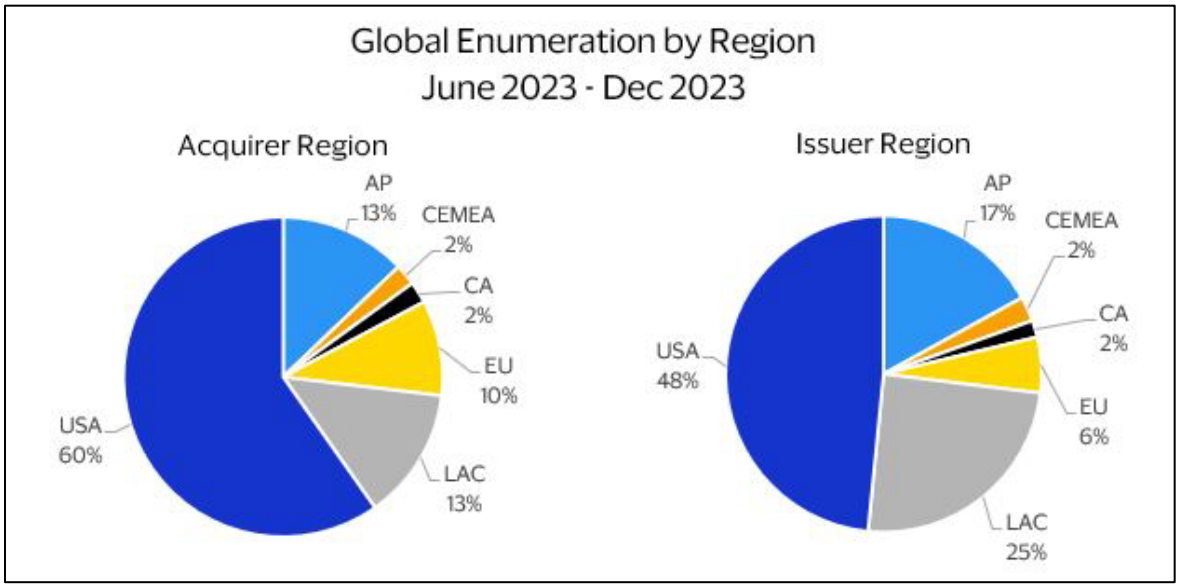


Figure 4: Source – Visa Payment Fraud Disruption

For more information related to Enumeration Fraud Best Practices and Visa Account Attack Intelligence, visit the Visa's Resources Website.

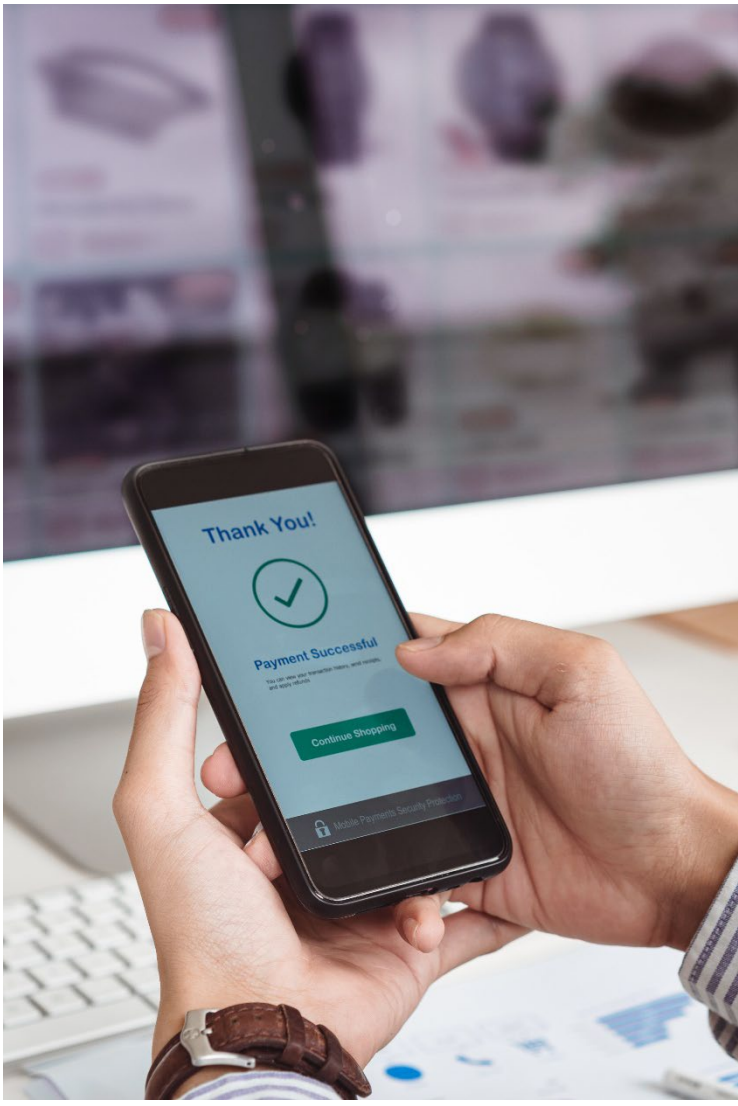
Digital Skimming Update

Digital Skimming Threat Actors Continue Targeting eCommerce Merchants

In digital skimming attacks, threat actors deploy malicious code onto merchant websites targeting checkout pages in attempts 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 seven-month period with threat actors increasingly targeting payment gateways and third-party supply chains or web infrastructure providers with web shells to compromise multiple entities at once. Threat actors have also targeted vulnerabilities within eCommerce merchants' blogs or content management systems (CMS) hosted on third-party platforms to create backdoor access into the victims' eCommerce environments. 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 passcodes (OTP).

The most notable developments within digital skimming as identified by Visa PFD are as follows:



eCommerce Third-Party Service Provider Compromised in Digital Skimming Attack

Visa PFD recently investigated a digital skimming attack against a third-party service provider in which the threat actors obtained payment account data from several downstream eCommerce merchants who utilized a script provided by the targeted service-provider. In this attack, the threat actors gained initial access to the victim's systems through a public-facing management PHP file with a misconfiguration vulnerability allowing the threat actors to conduct SQL injection attacks against this file. The SQL injection attacks enabled the threat actors to modify several legitimate files with malicious web shell code and deployed the web shells into the victim's environment. The web shells were then used to deploy customized digital skimming malware, which was uniquely created for each of the downstream merchants who use the targeted organization's services. This digital skimming malware obtained payment account credentials, such as the primary account number (PAN), expiry, CVV2, and cardholder name, from these downstream merchants and then exfiltrated the stolen payment account data to a threat-actor controlled domain.

These threat actors also targeted a second environment at the same victim organization through another public-facing PHP management file that also had a misconfiguration vulnerability. Through this vulnerability, the threat actors inserted malicious web shell files onto the web server and then appended malicious code into a legitimate JavaScript file used by the targeted merchant service provider. This malicious code communicated with a threat actor-controlled command-and-control (C2) domain and downloaded digital skimming code onto the eCommerce merchants' websites, which extracted payment account data and exfiltrated the stolen data to the same threat actor-controlled domain.

Notably, there were other vulnerabilities exploited by the threat actors in this incident, such as a lack of an Intrusion Detection and Prevention System (IPS/IDS) and web application firewall (WAF) on the victim's networks, the victim did not retain network logs of any connected devices to the network, and as such, the logs were not monitored on a routine basis. Visa PFD assesses the security configuration enabled the threat actors to compromise the victim's environments and obtain payment account data. Threat actors will continue to target third-party service providers in digital skimming attacks and exploit vulnerabilities to gain access to victims' sensitive information.

eCommerce Retailers' Non-Payment Related Website Targeted to Facilitate Digital Skimming

Over the past seven months, Visa PFD observed two separate incidents wherein threat actors targeted vulnerabilities within two eCommerce merchants' blog sites or CMS webpages hosted on third-party platforms to create backdoor access into the victims' eCommerce environments and compromise payment account data by deploying digital skimming malware. The first incident involved threat actors initially compromising the victims' CMS environment by deploying a PAS Web Shell onto the CMS infrastructure to facilitate persistent access. Although the victim segregated the CMS environment from the eCommerce web infrastructure, the threat actors discovered the victim had legacy SSH keys in use which connected the CMS servers and the payment infrastructure. Through these legacy SSH keys, the threat actors were able to move laterally between the compromised CMS infrastructure to the eCommerce infrastructure and deploy malicious PHP files embedded with digital skimming code. This code used regular expressions to search for terms associated with card payments, and when identified, exfiltrated the payment account data to a threat actor-controlled domain.

In the second attack, the threat actors gained access to a retailer's eCommerce environment and compromised payment account data. The investigation into this second attack was unable to determine the initial cause of intrusion, however, it is likely the threat actors were able to gain access to the eCommerce merchant's environment by obtaining and using compromised administrator credentials, providing the actors with privileged access to the network. With the privileged access, threat actors installed a malicious web shell onto the victim's payment infrastructure, enabling the threat actors to append digital skimming malware onto a legitimate PHP file on the victim's eCommerce checkout webpage. This digital skimming malware then exfiltrated payment account data to a threat-actor controlled domain. After the victim removed the malicious web shell mentioned above, the threat actors attempted to target the victim's non-payment related infrastructure with the goal of moving laterally from the non-payment environment to regain access to the eCommerce environment. While the threat actors successfully installed a backdoor file onto the non-payment infrastructure, they were unable to move laterally to the payment infrastructure due to controls placed around the malicious IP address used by the threat actors.

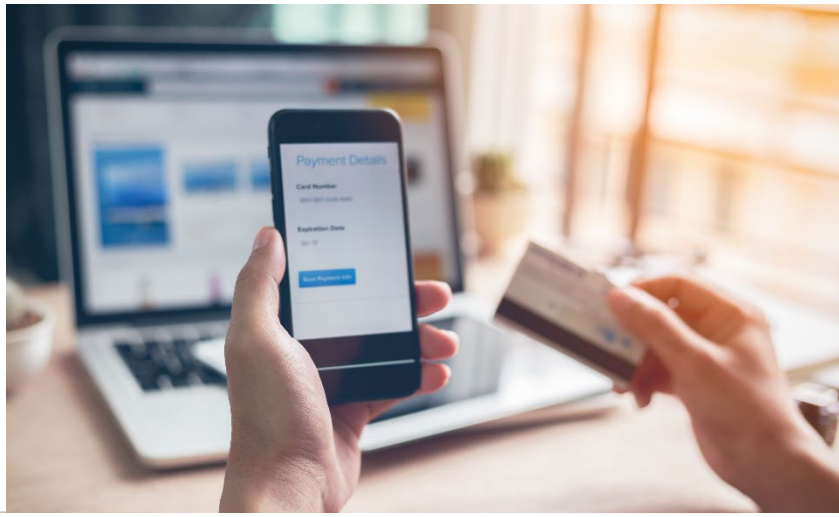
Both of these incidents highlight threat actors' interest in targeting non-payment infrastructure to facilitate digital skimming and underscore the importance of implementing proper security controls, such as network segmentation, enabling multi-factor authentication (MFA) on eCommerce environments, and utilizing file integrity monitoring programs and an internal/external network scanning capability to mitigate against these types of attacks.

Threat Actors Exploit Pixel Code Integrations

Visa PFD recently investigated two digital skimming attacks whereby the threat actors exploited pixel tracking code integrated onto two third-party eCommerce merchant service providers' platforms to obtain payment account data. Pixel tracking code are small pieces of code that track the behaviors of users who visit websites. In both attacks, it is suspected the threat actors compromised administrator credentials, likely obtained through phishing campaigns or credential stuffing attacks, and used those credentials to gain access to the victims' environments. In the first attack, threat actors targeted a merchant service provider for the entertainment industry by appending malicious JavaScript skimming code into legitimate pixel tracking code deployed on the merchant service provider's platform, and, consequently, the malicious digital skimming code was also deployed into the victim's downstream customers' checkout page environments. The malicious code enabled threat actors to obtain payment account information entered into the checkout page fields by consumers.

In the second incident, threat actors targeted a third-party service provider in the restaurant industry and likely used compromised administrator credentials to gain administrator access to the victim's web environment, including the victim's eCommerce POS platform. After accessing the victim's POS platform, the threat actors deployed malicious digital skimming code onto the customer database for many of the merchants who used this victim's platform. Through the eCommerce POS platform, unauthorized pixel code, which contained the JavaScript skimming malware, was integrated on the impacted downstream merchants' checkout pages, and enabled the malicious digital skimming code to harvest user data entered into the checkout page fields by the merchants' customers, including the PAN, expiration date, CVV2, physical address and other PII. The actors then sent the stolen payment account data to numerous threat actor-controlled C2 servers.

Visa PFD assesses threat actors will continue to target vulnerable eCommerce merchants, third-party service providers, and other supply chain entities with digital skimming attacks in efforts to obtain payment account information. Moreover, these attacks underscore threat actors' continued interest in targeting supply chains and third-party providers to obtain compromised payment account data, as well as their attempts to find new and novel methods by which to compromise sensitive cardholder information.



Novel Digital Skimming Technique Hides Code in "404 Error" Page

In a recent digital skimming campaign, threat actors use standard "404 Error" pages to hide digital skimming code as these pages may be overlooked in security checks, enabling the malware to persist in the victim's web environment. Threat actors deploy a malware loader onto the victim merchant's website that attempts a connection request to an invalid path, which results in a "404 Not Found" error. Within the loader is an encoded Base-64 string housing the JavaScript skimming code. The loader is instructed to perform a regular expression match on the 404 error page which actually embeds the malicious skimming code into the 404 error page code, and is then loaded and deployed onto the victim merchant's checkout page.

The attack then uses a fake payment form overlayed on top of the legitimate third-party checkout form. When consumers visit the merchant's checkout page and input payment account information into the fake checkout form, the JavaScript skimming code harvests any sensitive information and payment data entered into the overlayed form and exfiltrates it to an attacker-controlled command and control (C2) server via an image network request. Once the fake form is submitted, the form disappears from the page and the victim is presented with the legitimate third-party checkout form and asked to re-enter their information, thus the legitimate order is processed, and the victim is unaware data was stolen.

This novel campaign illustrates threat actors continued innovation in creating new techniques to obtain payment account data with digital skimmers. Visa PFD continues to monitor the evolving digital skimming threat landscape, as well as threat actors' continued interests in obtaining CNP payment account data.

Digital Payments Fraud Update

Token Provisioning Fraud

Provisioning related fraud is defined as fraudulent transactions occurring within seven days of a token's activation primarily impacting device bound tokens. At present, provisioning fraud manifests as the rapid monetization of tokens by threat actors in a use-and-lose pattern with little attempt to incubate the fraudulent credential.

This creates a sharp contrast to more familiar card fraud with over 40.2% of fraud volume for device-bound tokens concentrated in the first week of the credential's existence - during which time only 1.5% of token payment volume is generated, as shown in Figure 5, below. A similar, though lower, fraud volume-to-payment volume disparity exists for the first day of Card-on-File tokens, with 19.1% of fraud volume for only 3.7% of payment volume, as shown in Figure 6, below.

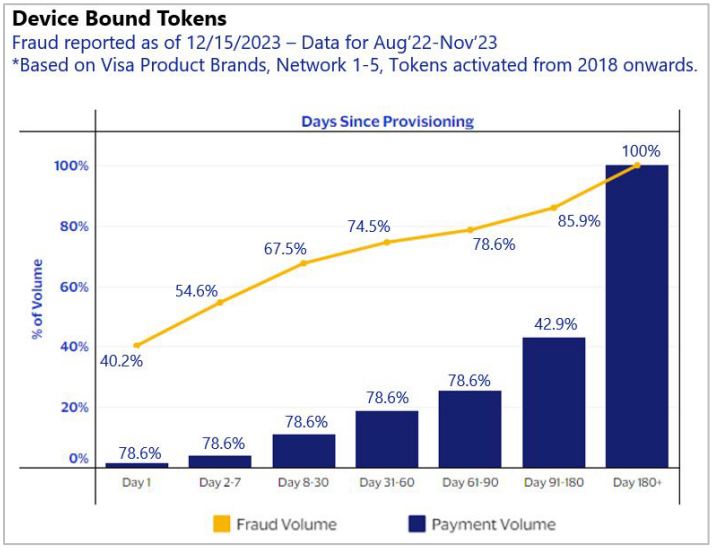


Figure 5, Source – Visa MIS

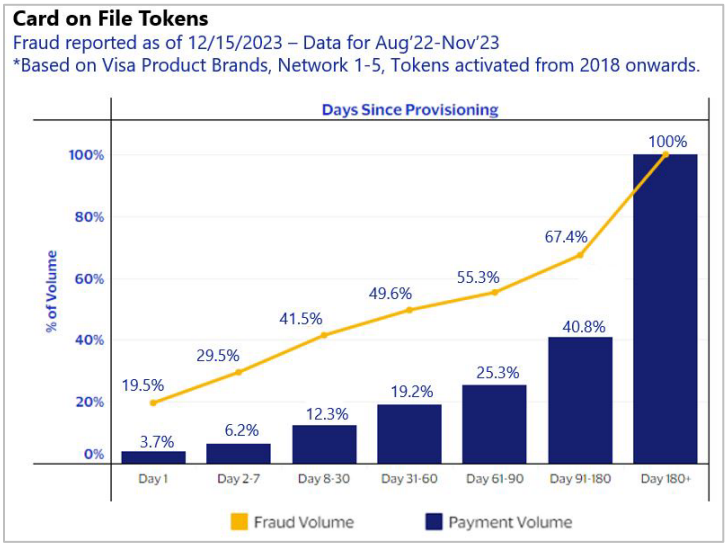


Figure 6, Source – Visa MIS

Provisioning Fraud Vectors

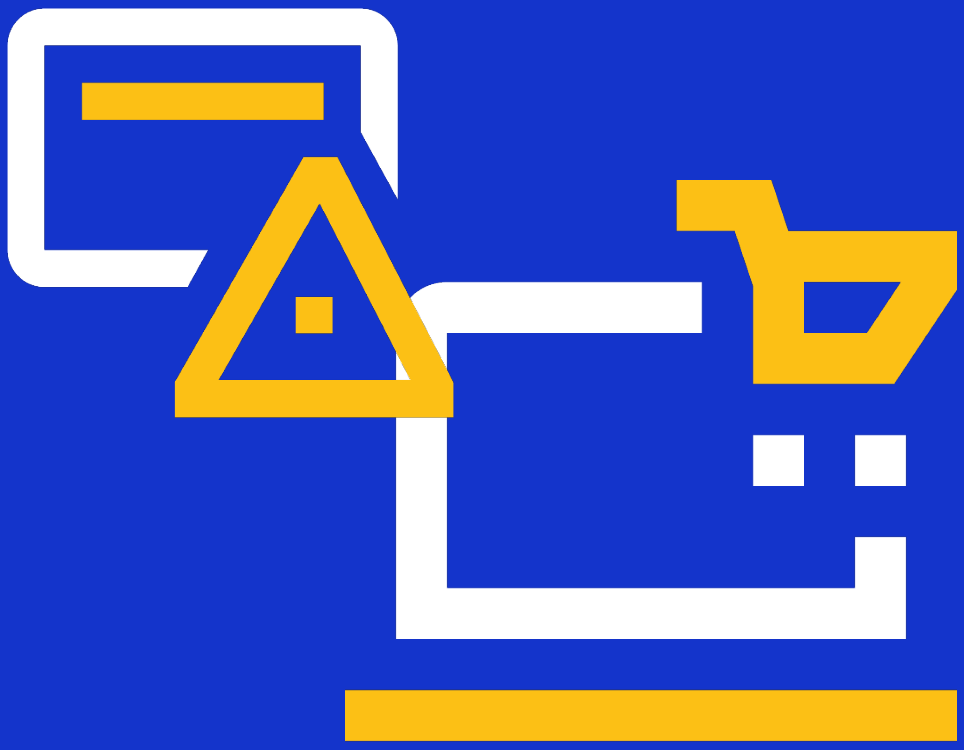
At present, fraud trends indicate banks are successfully distinguishing potentially fraudulent Device Bound tokens, sending them through a step-up method for additional authentication such as one-time-passcode (OTP), but that step-up methods are being successfully circumvented by fraudsters. Post-Provisioning, Key-Entered Device Bound OTP tokens stand out as the most material vector at present but there are additional hotspots such as tokens where the PAN is sourced from a mobile app (push provisioning) while leveraging the same channel for step-up, as shown in Figure 17, below. 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.

The recently launched Visa Provisioning Intelligence score is intended 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.

Digital Payments Fraud Trends

Digital payments continue to grow in popularity and Visa digital payment volume (PV) steadily increased over the past 12 months, from 6.1% of overall PV to 6.7% from December 2022 to November 2023. Additionally, the Visa Direct overall Card-Not-Present (CNP) fraud rate declined from last year's averages, and now falls relatively in-line with general (non-Visa Direct) CNP fraud rates.

Evolution of Payments Threats



Evolution of Payments Threats

Threat Actors Continue to Conduct ATM Jackpotting Attacks

Over the last seven-month period, Visa PFD observed a continuation in a trend of notable ATM jackpotting incidents from the first half of the year. ATM jackpotting refers to the use of a physical device or malware, launched via an executable file, used against an ATM allowing the attacker to empty the ATM cash cassettes via direct or remote manipulation. Although not a new or novel technique, threat actors have targeted ATMs with ATM jackpotting and other methods of physical tampering of ATMs to steal cash on a more frequent basis than in prior years.

In one notable ATM jackpotting attack, three actors in Texas were arrested for allegedly using a "Raspberry Pi" device to steal funds from multiple ATMs' cash drawers. A Raspberry Pi is a credit card-sized computer, as powerful as a typical desktop computer, which can be connected to an external screen. The three individuals connected the Raspberry Pi device to a targeted ATM, deactivated the ATM's security features, and removed the ATM's cash drawer to retrieve the cash. Although this was a recent incident, threat actors have been using Raspberry Pi computers to compromise ATMs and steal cash for years. To perpetrate these attacks, the threat actors obtain ATM maintenance keys along with malware appropriate for the targeted ATMs. They then download the malware onto the Raspberry Pi device, which when deployed onto the ATM, forces the ATM to treat the Raspberry Pi as a keyboard, thereby allowing the threat actors to input commands into the Raspberry Pi instructing the ATM to dispense cash or open the cash drawer.

Other ATM jackpotting schemes involve inserting a USB device loaded with malware into the ATM's USB port which is then installed onto the ATM's computer. The malware instructs the ATM to open the cash drawer or dispense cash until the ATM's cash cassette is empty. Threat actors typically acquire the malware used in ATM jackpotting attacks in cybercrime underground marketplaces. One recently identified ATM jackpotting malware known as "Cutlet Maker" has been used by various threat actors to target ATMs across the Latin America and the Caribbean (LAC), Asia Pacific (AP) and North America (NA) regions. Threat actors' conversations in underground communities often mention Cutlet Maker when discussing effective ATM jackpotting malware variants. These underground communities and marketplaces allow threat actors to quickly share ATM malware between regions and enable ATM jackpotting malware to expand rapidly once word of its success spreads in underground channels.

Visa PFD assesses threat actors will continue to explore new ways to compromise ATMs to steal cash, by either gaining access to the cash vault or forcing the ATM to dispense cash, as more consumers travel and shop at brick-and-mortar stores in similar frequencies to pre-COVID periods. As technological advances allow threat actors to use various devices to load ATM jackpotting malware onto ATMs, it is important for banks to be vigilant in physically securing their ATMs and monitoring ATMs in less populated locations.

Fraudulent Merchants Used for Purchase Return Authorization (PRA) Fraud

Visa PFD has observed a continuation in threat actors using fraudulent merchants to conduct purchase return authorization (PRA) attacks. In PRA attacks, threat actors either compromise legitimate merchant gateways or onboard fake merchants to large eCommerce merchant ecosystems, and initiate purchase return authorizations for which there was no initial purchase. The PRA is requested for threat actor-controlled primary account numbers (PANs) and is immediately cashed-out upon approval, typically through ATM cash-withdrawals or peer-to-peer (P2P) payments.

In the past seven months, PFD's Hawkeye capability identified 327K PANs and 4.9K merchants associated with high-risk PRAs that accounted for US$58.6M.

Visa PFD's Global Risk Investigations (GRI) team opened a record number of PRA investigations from June 2023 to December 2023, which is the highest number of PRA cases opened for a seven-month, period and an 83% increase from the previous five-month period. A successful PRA attack resulted in potential fraud losses to banks of US$115K on average.

Visa PFD assesses threat actors will continue to innovate upon PRA fraud attacks and will utilize the described tactics, techniques, and procedures to effectively conduct PRA fraud.

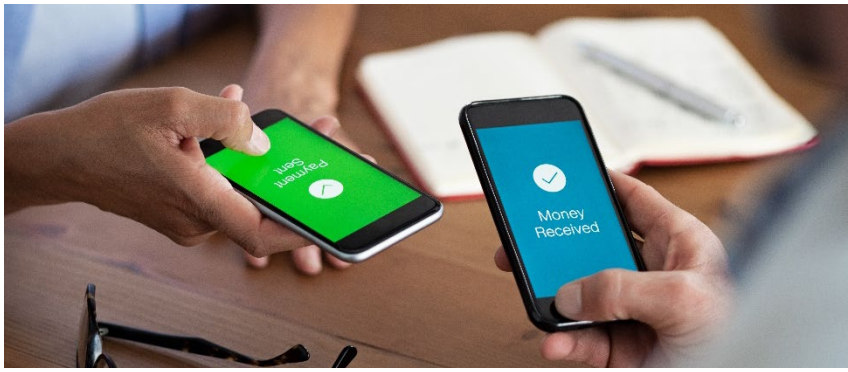
Underground Marketplace "BidenCash" Releases 1.9M Compromised Cards

On 21 December 2023, the BidenCash marketplace released its fourth free set of stolen credit and debit cards on the cybercrime underground, containing details for 1.9 million cards. BidenCash, which appeared in early 2022, is known to release vast amounts of free payment account data to gain recognition in the cybercrime community, and in turn, bring in paying customers for their shop of verified stolen payment account information. Visa PFD found the majority of payment accounts in the previous free releases were recycled from other stolen data sets, so it is probable the December 2023 release contains mostly recycled data as well. The December 2023 release contained card numbers, expiration dates, and CVVs.

Visa PFD identified 556K at-risk Visa accounts from the December 2023 BidenCash release. PFD did not observe any significant correlation from the BidenCash accounts to previous Compromised Account Management System (CAMs) alerts. Additionally, review of the at-risk Visa accounts revealed that Visa Account Attack Intelligence (VAAI) analysis identified 50% of the Visa accounts involved in the BidenCash release, as they were flagged for 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) in the three months prior to the December 2023 release. Through the VAAI capability, and working closely with impacted clients, these enumeration attacks were promptly identified and surgical block were implemented to prevent the attack transactions on the targeted merchants, while enabling the legitimate transactions to proceed, effectively mitigating the attack activity.

> VAAI 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 banks/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.

Visa PFD provided the at-risk payment account information from the BidenCash release to banks through an established process. Visa PFD also operates the eCommerce Threat Disruption (eTD) capability which proactively identifies digital skimming malware deployed on eCommerce merchant environments and often catches the malware and compromise before the actors obtain payment account details.



Threat Actors Use AI Tools for Nefarious Voice and Image Cloning

With the recent expansion and evolution of Artificial Intelligence (AI), AI's potential for both positive and negative use has become evident. As with any new technology, threat actors have quickly identified ways to exploit new AI tools for fraudulent purposes, including to enhance fraud campaigns against consumers and financial institutions. A number of recent examples reported in media highlight the rapid development and expansion of these tools within the threat actor realm, including an employee tricked into transferring US$25.6M to threat actors using deepfake technology to impersonate the company's executive leadership, and the targeting of celebrities, politicians, and prominent figures with explicit, inflammatory, or controversial audio recordings or videos made using deepfakes. A recently released report predicts that in just two years' time (by 2026), 30% of organizations will no longer trust the reliability of current identity verification and authentication solutions.

As AI tools continue to advance and gain acceptance across sectors, the use cases for this type of technology have become increasingly intricate. In July 2023, two new nefarious services called WormGPT and FraudGPT began being offered in cybercrime underground marketplaces, the latter being described as "an unmoderated chat bot trained for criminal purposes." These nefarious services offer users the ability to create phishing emails, develop cracking tools, conduct carding operations, scan for and test vulnerabilities in critical systems, identify victim networks with those vulnerabilities, and develop malicious scripts, apps, and programs, among other capabilities. The latest news in the AI space highlight the issues with the illicit simulation of real people to create misinformation, steal funds, and hijack identities. These rapid developments in the nefarious AI sector have the potential to make committing fraud easier while lowering the barrier of entry for would-be criminals to develop sophisticated, malicious campaigns. Underground chatter relating to posts asking about these services and where to find them have been observed in multiple languages, demonstrating that threat actors in all regions globally are interested in using this new technology.

In January 2023, developments in AI voice cloning technology claimed to be able to clone a voice from only 3 seconds of audio. Less than one month later, in February, security researchers published an article demonstrating the use of AI voice cloning to fraudulently access a consumer's bank account via a "voice-as-password" system. AI Voice Cloning is a deepfake technique that can analyze and replicate a human's voice. Essentially, it can clone anyone's voice and read any script provided to it, requiring only a short voice sample of the human voice intended to be replicated. Beginning in March 2023, media began reporting on ways fraudsters had already used AI to mimic the voice of loved-ones to perpetrate financial scams. The FTC even issued an alert on a specific "family emergency" scheme, and reports of those types of schemes have increased over the past few months. To perpetrate these types of schemes, fraudsters are employing these widely available voice cloning tools to dupe victims into believing their loved one is in trouble and needs money sent quickly. All it requires is a short clip of a person's voice, which may be obtained from internet or social media, a voicemailbox recording, or can be collected by recording a victim responding to a spam call. The clip can be as short as 3 seconds, and the AI only needs 10 minutes to process and learn and clone the voice.

Similarly, as noted in the recent news headlines, fraudsters can use AI tools to create visual clones of individuals and use those images and videos for nefarious purposes. AI tools also allow threat actors to create 3D avatars that mimic a real face from multiple perspectives to create what is known as a deepfake "puppet": an artificial video simulation of an individual created by filming an actor or using an animated model, then superimposing the targeted individual's face over the original footage. This realistic-looking "puppet" can be manipulated digitally in real-time to appear - to the unknowing - as if it is the actual, live person. In May 2022, media began reporting on the automated "liveness tests" specifically used by banks and other institutions which help verify users' identities as being easily fooled by deepfakes. With the advancements in AI technology, this type of visual biometrics bypass fraud targeting the payments ecosystem is on the rise. A May 2023 North America Fraud Statistics report published by an identity verification company that provides KYC and transaction monitoring solutions, noted that "Liveness bypass" - which is a method of fraud where

criminals swap in or edit biometric data - was the top verification fraud type they experienced in 2022. Liveness bypass fraud accounted for 34% of fraud this company identified that year in the U.S, which was followed by the more traditional fraud methods like Edited or Forged ID cards. More recently, a new report published by another identity authentication company noted they experienced a 704% increase in deepfake attacks on remote identity verification systems in 2023 compared to the previous year.

As with any new technology, threat actors have quickly identified several different ways to exploit AI voice and image cloning tools for fraudulent purposes. Visa PFD assesses threat actors will likely continue to use AI to enhance various attacks to perpetrate fraud campaigns against financial institutions and other entities involved in payments. Visa PFD will continue to monitor the use of nefarious AI tools by threat actors to target the payments ecosystem and will continue to report on any notable developments through PFD intelligence reporting.

Visa recommends issuers, acquirers and processors take the following actions to mitigate the risks of these threats:

- **Constantly monitor for new and emerging technology** and ensure a strategy to mitigate any fraudulent uses of such technology**.**
- **Employ strict cardholder authentication controls** to ensure the customer is the legitimate cardholder, especially under transactions occurring on advertising merchants.
- **Educate cardholders and employees on the dangers of phishing** and how to identify phishing or BEC attacks.
- **Implement Multi-Factor Authentication (MFA)** on all administrator and employee accounts, especially accounts with access to sensitive environments such as the card management system.
- **Implement behavioral biometrics to create digital fingerprints** for each user to authenticate a user's identity.
- **Provide each Admin user with their own user credentials**. User accounts should also only be provided with the permissions vital to job responsibilities. Merchants should perform audits on Admin accounts, to remove any non-essential users and add other security hardening practices, such as enabling multi-factor authentication (MFA) and IP Restricting access to the Admin panel.
- **Turn on heuristics (behavioral analysis) on anti-malware** to search for suspicious behavior and update anti-malware applications.
- **Secure remote access** with strong passwords, ensure only the necessary individuals have permission for remote access, disable remote access when not in use, and use two-factor authentication for remote sessions.

AI Chat Bots Manipulated to Distribute Malware

Throughout 2023, Visa PFD monitored the continued development of artificial intelligence (AI) technologies, including the advancement of advanced language learning models (ALM) and other AI chat bots, and the technology's increasing popularity among threat actors. Visa PFD recently became aware of a novel malware distribution technique whereby threat actors abuse the process by which a popular AI chat bot develops responses to users' prompts.

To execute this scheme, the threat actors successfully manipulate what are known as ALM hallucinations, which are incorrect or entirely fabricated answers generated by ALMs in responses to user prompts for which the ALM does not have sufficient knowledge. The threat actors initially ask the ALM how to solve a common code programming problem to which the ALM responds with various code packages, including some packages generated as 'hallucinations' which are not published in legitimate code package repositories. After identifying one of these unpublished code packages, the threat actors publish a malicious code package into that same unpublished code package repository. When a user prompts the ALM with the same code programming question as the threat actors, the ALM may include the now malicious code package in their recommendations to the user. If a victim installs the malicious code package onto their device, it executes the threat actors' malware, which can be used to install file and information stealers, remote access Trojans (RATs) keyboard loggers, and other malware to steal victims' sensitive information, such as payment account data stored on the victims' device or browser, login credentials, passwords, email addresses and additional personal identifiable information (PII).

Visa PFD previously reported on various methods by which threat actors could exploit AI chat bots and other ALM techniques in the June 2023 PFD Biannual Threats Report, including the creation of phishing lures or the development of malicious code. Visa PFD assesses threat actors will continue to exploit the popularity of AI chat bots and other popular novel technologies to execute malicious campaigns and steal sensitive information.

JsOutProx Malware Deployed Against Financial Institutions

As a continuation of Visa PFD's ongoing monitoring of payments ecosystem threat campaigns, new JSOutProx remote access trojan (RAT) malware samples, attributed to a known eCrime threat group, were identified. Over the last seven-month period, Visa PFD observed and reported on nine different JSOutProx campaigns.

The eCrime threat group behind JSOutProx is associated with phishing campaigns delivering the JsOutProx malware to financial institutions across the Central Europe, Middle East and Africa (CEMEA), and Asia Pacific (AP) regions.

JsOutProx is a highly obfuscated JavaScript backdoor, which has modular plugin capabilities, can run shell commands, download, upload, and execute files, manipulate the file system, establish persistence, take screenshots, and manipulate keyboard and mouse events. These unique features allow the malware to evade detection by security systems and obtain a variety of sensitive payment and financial information from targeted financial institutions.

From June 2023 through December 2023, Visa PFD observed and reported on nine different JSOutProx campaigns.

In one such identified campaign executed against several banks of an AP-region country, the JSOutProx infection began with spear phishing emails sent to employees of the victims. These malicious emails contain email attachments which mimic

financial documents to increase the likelihood the recipient opens the attachment and downloads the malware embedded within the file. In another campaign, the threat actors spoofed the central bank of a country in the AP region to socially engineer the employees of the targeted financial institution to open the malicious attachments which spoofed training materials. Once inside a victim's network, the JSOutProx malware enables the threat actors to steal user account credentials, gather sensitive financial documents, obtain payment account data and conduct a variety of other malicious activities against the victim.

These threat actors can either use the stolen payment account data to conduct fraudulent transactions or resell the PANs on the underground. They may also use the illicit access to execute business email compromise (BEC) campaigns in order to steal funds from unsuspecting clients of the targeted financial institutions. The JSOutProx malware poses a serious threat to financial institutions around the world, and especially those in the AP region as those entities have been more frequently targeted with this malware.

Visa PFD assesses the eCrime actors behind JSOutProx will continue to deploy the malware to primarily target financial institutions with the goal of obtaining sensitive financial and/or payment information through the execution of spear phishing campaigns. To help mitigate against this malware, educate employees about phishing emails and best practices when receiving unsolicited, suspicious correspondence. If malware is identified, it is imperative to ensure proper and full eradication of the malware to avoid further impact and/or reinfection.

Proliferation of Scams

Proliferation of Scams

Scams directly targeting consumers continue to increase in both complexity and volume. The US Federal Trade Commission (FTC) reported the total amount consumers lost to scams in 2022 increased to US$8.8B for the year, up from US$6.1B in 2021. While the number of individual reports of scams decreased, the total lost by individuals *increased*, indicating scammers are targeting individual victims with larger and more costly scams. The top categories for types of scams included 1) Imposter Scams, 2) Online Shopping Scams, and 3) Prize, Sweepstakes, and Lottery Scams. Additionally, the FTC reported social media platforms as a well-used channel for fraudsters to perpetrate online shopping and fake merchant scams through paid advertisements promoting the fraud merchant or domain, a fraud tactic Visa PFD reported on a number of times over the past several years. A recent survey of 2,000 US residents noted 70% of those surveyed reported an increase in 2023 in phone call or text message-based scams, many related to debt relief, package delivery, or other business imposter-related topics.

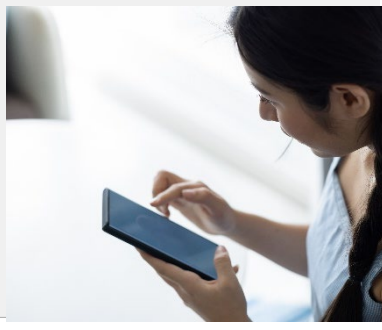
The UK experienced a slight reduction in 2022 in the overall financial fraud losses due to criminal scams, at over £1.2B, eight percent lower than reported in 2021, and 2023 appears to be on track for continued significant losses from financial scams, with £580M reported in losses for UK residents in the first half of 2023. The Singapore Police Force reported an increase of 69% in total number of scam reports in the first half of 2023 when compared to the first half of 2022. Law Enforcement agency, Interpol, reported the success of a six-month investigation into financial scam rings, arresting over 3,500 individuals and seizing over US$300M in assets and stolen funds across 34 countries. In Australia, consumers reported AUS$3.1B in financial scam losses in 2022, an increase from the AUS$2B reported losses in 2021. A recent survey of over 800 individuals across eight disperse African countries noted over 40% of survey respondents reported being victim of a financial scam and the favored tactics of scammers vary based on region; with Nigeria respondents reporting scammers mainly targeting victims through social media, and South African respondents reporting receiving scam message mainly via email.

Given the significant increase over the past two years in criminal profits gained from various types of scams, 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 provides reports on the Merchant Resource Library website.

Romance Scams Advance to "Pig Butchering"

Romance scams continue to target victims across the globe. Threat actors also use holiday times, such as Valentine's Day and New Year's, as themes to target victims. Actors have started to use AI and other technologies in combination with holiday lures to cultivate more convincing phishing campaigns, such as dating profiles using AI and deepfakes to create the most compelling profiles. They have also begun outsourcing stages of the attack to AI technology, such as initial correspondence with victims. The US Financial Crimes Enforcement Network (FinCEN) recently warned a particular evolution of the combination of general romance and investment scams called "pig butchering" is on the rise, noting victims' losses to pig butchering scams are in the billions (US$). In a pig butchering scam, threat actors use social media, dating websites and various apps to lure victims into online relationships and subsequently convince victims to invest in specified cryptocurrency trading platforms. As the specified trading platforms are fake, victims are instead unknowingly transferring money directly into threat actor-controlled wallets. Law enforcement organizations worldwide are continually working on combatting pig butchering scams not only due to the financial losses from victims, but also because many of the scams rely on victims of human trafficking to initiate and conduct the targeting of scam victims. On 21 November, the US Department of Justice announced the seizure of US$9M in cryptocurrency from scam profits gained by a criminal organization perpetrating pig butchering scams. The recovered funds are linked to over 70 individual victims targeted with a "fake crypto dashboard" pig butchering scheme executed by an organized fraud network.



Inheritance Scams: A Variation of the Lottery Scam

Threat actors are capitalizing on victims' excitement for financial gain with several versions of inheritance schemes, which fall into the same broad scam category as lottery scams, offering a financial payout for the lucky recipient. These inheritance schemes involve a victim being notified, typically via physical mail or email, with an "official-looking" letter or notification communicating an inheritance or unclaimed property left by a deceased or long-lost relative. Some variations of the scam claim the victim is likely the heir to millions of dollars. The letter or email usually appears to come from a law firm, inheritance or estate locator company, or another seemingly legitimate professional entity, and typically contains variations of the common themes below:

- The inheritance should be kept secret until the money arrives - this is the threat actors' attempt to keep the victim from speaking to others who may inform the victim of the scam.
- The inheritance / money is time-bound, and the recipient must act fast to secure the funds.
- The sender asks the recipient for sensitive personal identifiable information (PII) and/or payment account information.
- To claim the inheritance, the recipient must pay fees or taxes in order to begin the money acceptance process; payment is requested by money transfer, gift cards, or cryptocurrency, or for the recipient to provide their credit/debit card or bank account details.

Consumers should be aware of these types of financial windfall phishing lures and report scams to their local or federal law enforcement agency or governmental organization. Visa clients should also report any fraud schemes to PFD regularly reports on phishing scams and account take over fraud, available on the Merchant Resource Library website.

Threat Actors Exploit the Israel-Hamas Conflict to Scam Victims

As a result of the ongoing Israel-Hamas conflict, threat actors exploit the call for donations across social media to defraud unsuspecting donors with fake charities, fundraisers and other scams. Threat researchers identified over 500 different scam emails currently in circulation related to the Israel-Hamas conflict with phishing links to illegitimate charity websites written with adequate variation to evade email spam filters. These phishing emails, written in English, target donors who are "affected on both sides" of the current conflict and contain various images and language to evoke emotion within the readers to hopefully draw more fake donations. Some of the fake websites even resemble the layout of legitimate charities to make the scam emails more legitimate.

Threat actors also launched social media campaigns requesting fake donations through social media posts with links to cryptocurrency wallets, which are likely under the control of the threat actors. These social media campaigns also involve the use of social media posts from various individuals, likely from either fraudulent/fake accounts or from associates of the threat actor group, claiming they donated to the fraudulent charity. This further leads victims to believe the scam is legitimate.

Current events often spark an influx in fraudulent charities, due to an increase in charitable giving during natural disasters or other global crises. The US Federal Bureau of Investigation (FBI) warns the public that criminals use funds from fraudulent donation sites to fund criminal activity and advises individuals interested in making donations to research the charity prior to donating any money.

Beyond fake charities, threat actors initiated several phishing campaigns via email messages exploiting the Israel-Hamas conflict with the goal of obtaining victims' login credentials for their email accounts, leading to the compromise of victim's personal identifiable information (PII) and other

sensitive information, including bank account credentials or payment account information. Threat researchers noted the majority of these phishing emails contain malicious attachments, typically hidden as Microsoft Excel files, which prompt the victim to enter their username and password to access the file, thus allowing the threat actors to steal the victim's credentials.

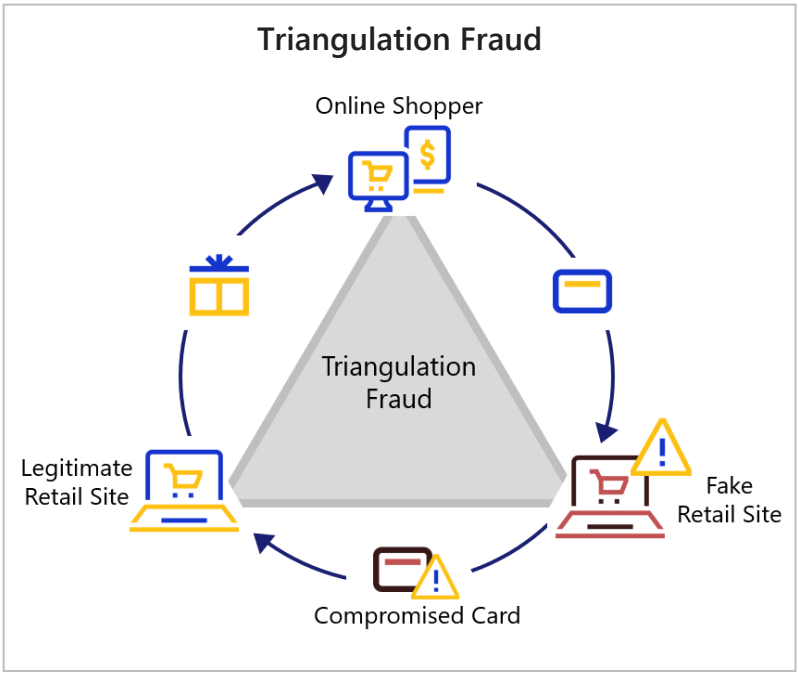
The threat actors behind these phishing campaigns send emails claiming to be from a news organization sharing important updates on the ongoing conflict and use the fake news headlines to lure victims into downloading malware. The malware could be used to compromise sensitive information, including cardholder payment account data, such as the primary account number (PAN) and PII. Visa PFD regularly tracks global conflicts and crises, such as the continuing conflict in Ukraine, to identify tactics threat actors devise to target victims.

Triangulation Fraud

Triangulation fraud continues to impact banks and merchants and is increasingly emphasized by law enforcement for the role triangulation fraud plays in human trafficking. Payments industry estimates on the financial losses to merchants stemming from Triangulation Fraud range from US$660M to over US$1B for the month of November 2022 alone. In triangulation fraud, threat actors create illegitimate merchants and accompanying websites offering bargains on in-demand or luxury goods/services. The illegitimate merchant takes a customer's order and charges the customer's payment account for the order, receiving payment for the goods. The illegitimate merchant then uses an unassociated, *legitimate* merchant to fulfill the customer's order and pays for the goods/service using stolen payment account information, often obtained via cybercrime underground marketplaces. This enables the threat actor to monetize the stolen payment account through a seemingly legitimate transaction. The illegitimate merchant then requests a positive rating from the customer, which increases the illegitimate merchant's relevance in search engine results and boosts its credibility.

During last year's holiday shopping season, Europol conducted a targeted and coordinated effort against eCommerce-related fraud scammers, including triangulation fraud, using compromised account data to purchase goods online, including those participating in triangulation fraud, and arrested 59 individuals across multiple countries. Similar efforts continued throughout 2023 globally, with Interpol announcing the success of an operation targeting online scam centers with ties to human trafficking. The five-month operation involved law enforcement agencies across the world and included the arrest of 281 individuals and freed 149 victims of human trafficking. Trafficking victims are often lured to foreign countries with the promise of new or better-paying jobs, only to find themselves working in online scam centers, forced to perpetrate a variety of fraud and scams, including lottery, romance, and cryptocurrency scams and operation of triangulation fraud sites.

In March 2023, Visa Payment Fraud Disruption (PFD) identified an increase in fraud associated with threat actors exploiting weak merchant onboarding practices to establish fraudulent merchants, which is a common tactic used by threat actors perpetrating triangulation fraud schemes. PFD assesses threat actors will continue to exploit such merchant onboarding practices. Banks should remain vigilant in combatting fraud related to fake and newly onboarded merchants. Additionally, the Visa Merchant Screening Service (VMSS) allows banks to identify potentially high-risk, unreliable or fraudulent merchants and third-party agents prior to making an onboarding decision and therefore helps reduce risk exposure to fraudulent and illegal transactions and helps protect against brand damage.



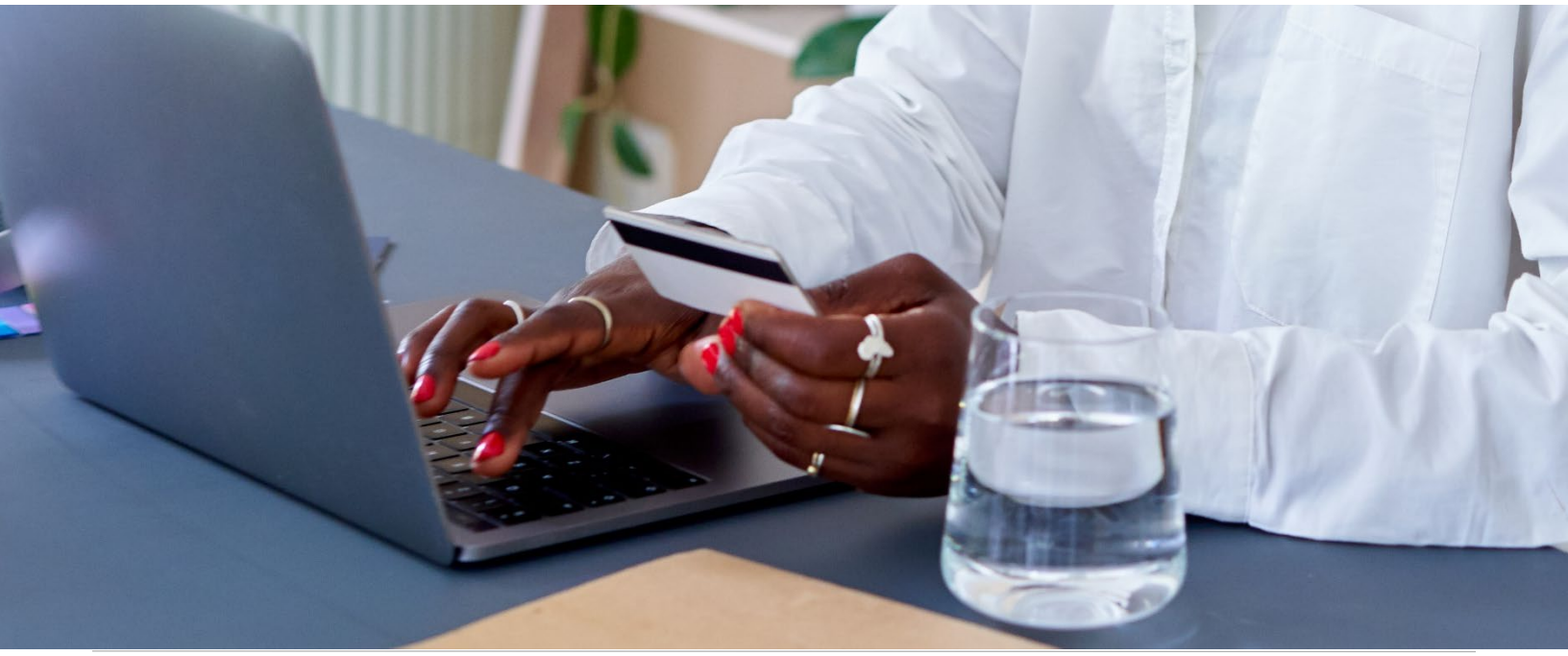
Surge in Threat Actors Targeting Gift Cards

Over the past seven months, PFD identified an increase in threat actors targeting gift cards to commit fraud. While there are various tactical versions of gift card-related fraud, the predominant tactic involves threat actors visiting brick-and-mortar retail merchants to obtain physical gift cards directly from store racks. Threat actors leave the store with numerous, unloaded gift cards, which they then physically manipulate by removing the card from the exterior packaging and altering the barcode. Variations of barcode altering include:

- Cutting the barcode portion off the gift card entirely.
- Copying the barcode or skimming the magstripe data located on the back of the gift card.
- Placing a new barcode associated with a threat actor-controlled gift card on top of the legitimate barcode via a printed barcode sticker.

After altering the barcode portion of the gift card, threat actors place the gift card back into the original packaging and replace the unloaded card back onto the store rack. When a customer purchases the gift card and loads funds at the register, the customer is unaware the barcode associated with the gift card is actually in the possession of a threat actor. Threat actors use various methods to routinely check the balance of any illicitly obtained gift cards, including online websites, call-in numbers, and adding the card number to a digital wallet. Once the threat actors see a card loaded with funds, they immediately proceed to cash out the full balance of the gift card. Cashout tactics include typical compromised card cashout methods, such as peer-to-peer (P2P) money transfers, purchase of in-demand goods and electronics, purchase of cryptocurrency, and other eCommerce transactions.

Visa recommends banks and merchants consider increasing the security of the physical gift card exterior packaging and/or location. Security tactics can include adding additional enclosures to the gift card packaging, using a tamper-evident packaging or barcode protection, and/or adjusting the physical location of gift cards within retail stores to protect from theft prior to being purchased.



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:

Key Suspect in OPERA1ER Ransomware Group Arrested

In July 2023, Interpol announced the arrest of a key actor in the cybercrime group OPERA1ER (aka NX$MS, DESKTOP Group, Common Raven) as part of *Operation Nevrone*, an intelligence sharing operation which enabled law enforcement to identify the location of OPERA1ER activities. Over the past four years, OPERA1ER gained a reputation for targeting financial institutions, attacking over 30 organizations across 15 countries in Africa, Asia, and Latin America. In the highlighted September 2022 attack, which displayed similar tactics, techniques, and procedures (TTPs) to previous attacks, OPERA1ER actors bribed an employee of a financial institution to upload malware, likely containing a remote access tool (RAT), onto the institution's servers. The malware enabled the threat actors to gain direct access to the victim servers and move laterally through the network to the victim's card management system (CMS) and core banking system (CBS). The actors then deployed keyloggers through a second RAT, which compromised user account credentials for a few of the victim institution's employees, which provided access to the victim CMS and CBS. Using the compromised account credentials, the actors increased withdrawal actor-controlled prepaid cards and load limits for previously acquired complicit customer primary account numbers (PANs). OPERA1ER then used the customer accounts to load funds onto the prepaid PANs, before cashing-out with the debit and prepaid PANs through fraudulent card present (CP) transactions at brick-and-mortar merchants or actor-controlled hand-held point-of-sale (POS) devices). OPERA1ER is estimated to have made up to US$30M in profits from their attacks involving malware, phishing, and fake wire order scams.

Five 5 Key Ransomware Group Players Arrested in Ukraine

On 21 November 2023, law enforcement from seven countries worked alongside Europol and Eurojust to search 30 properties in Ukraine, resulting in the arrest of five major players of a ransomware group responsible for attacking high-profile targets and obtaining hundreds-of-millions of dollars (USD) in ransom payments. The group was linked to the ransomware attacks that halted businesses across 71 countries, the group having encrypted over 250 servers during the attacks. The recent arrests were connected to arrests from 2021, where seized electronic devices led to the identification of the 2023 suspects. To conduct the ransomware attacks, the group used brute force, SQL injections, or phishing emails with credential-stealing malicious attachments to gain access to the targeted system. Once in the system, the group used tools like TrickBot malware, Cobalt Strike, or PowerShell Empire to gain additional access to as many systems as possible before using LockerGoga, MegaCortex, HIVE, or Dharma ransomware to execute the attacks. Once ransomware payments were made, the group laundered the cryptocurrency payments, likely through cryptocurrency mixers, peer-to-peer (P2P) exchange platforms, and other high-risk blockchain services.

Teen Lapsus$ Hackers Convicted

In August 2023, 18-year-old Arion Kurtaj has been sentenced for hacking activity in connection with the Lapsus$ data extortion group. Kurtaj's arrest is among law enforcement efforts to disrupt the Lapsu$ group's illicit activities. The Lapsus$ group, which is thought to be primarily comprised of teenagers, was known to use social engineering to initially breach a company's infrastructure. Once the actors gained access to a network, they would grant themselves administrative privileges, enabling access to sensitive company data, including customer financial information. The group would then extort their victims with the obtained sensitive data. The group is also known for conducting SIM swapping operations. Lapsus$ was active between 2021 and 2022, involving individuals in both the UK and Brazil. Kurtaj is believed to be one of the leaders of the Lapsus$ group and allegedly made over 300 bitcoin (BTC) in profits from his hacking endeavors, which targeted high-profile companies across a variety of sectors, to include financial services.

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, PFD noted threat actors and groups are evolving into more organized and sophisticated operations, utilizing advanced tactics and cutting-edge technology to facilitate large-scale fraud operations. Threat actors are continually probing organizations and networks for complex weaknesses and finding and exploiting zero-day vulnerabilities to conduct extensive and complicated operations with far-reaching impacts. Throughout 2023, threat groups displayed an increased interest in targeting supply chains and third-party services with the aim of compromising as many organizations as possible with a single breach. Additionally, and seemingly counter to that strategy, PFD also identified these increasingly sophisticated threat actors homing in on cardholders directly, turning their attention to the weakest link in the network – the human – to use social engineering at the most minute level in order to circumvent financial network security and fraud prevention protocols. Visa PFD assesses the next year will see threat actors continue to develop innovative tactics along these two diametric routes: 1) targeting large organizational service provider vulnerabilities, and 2) tactical and sophisticated individual cardholder social engineering, all with the goal of compromising payment data for fraudulent financial gain.

Threat Actors Will Continue to Exploit AI Technologies to Commit Fraud

Visa PFD assesses threat actors will continue to experiment and innovate with new and emerging AI technologies to facilitate cybercriminal activities and commit fraud. In the last seven-month period, threat actors created various malicious versions of AI chat bot programs, including some examples known as "WormGPT" and "FraudGPT". These fraudulent AI programs were designed without any security controls and are capable of generating responses to users' prompts free of grammatical or spelling errors and can mimic human language patterns based on the inputs it receives from users. The creators behind these malicious AI programs marketed the applications for the criminal community as they can create malicious code or scripts to be used as malware without needing to have a technical background in computer programming.

Beyond the creation of fraudulent AI programs, threat researchers discovered a method to bypass the security controls implemented by the developers of popular ALMs. These researchers trained an internally developed ALM, named 'Masterkey', on how to circumvent the controls restricting popular ALMs' responses. To circumvent the controls, the researchers instructed Masterkey to create malicious prompts which contained spaces at the end of each character and requested the legitimate ALM respond in a similar manner to a nefarious actor. When each prompt either succeeded in generating malicious responses or failed, the researchers trained their Masterkey model on what not to do when drafting new prompts. This enabled Masterkey to "jailbreak" the ALMs and generate malicious responses. Visa PFD assesses threat actors can use these same techniques to "jailbreak" ALMs for their own benefit, rather than using the less reliable, fraudulently created AI programs, WormGPT or FraudGPT, which may either be ploys by their creators to scam other cybercriminals or not nearly as effective as legitimate ALMs. Other threat researchers noted there is little evidence to prove these fraudulent AI programs are any more powerful or proficient as the legitimate ALMs.

As previously assessed by Visa PFD, fraudsters rapidly adapted to the new AI chat bot technologies and launched carefully crafted phishing and business email compromise (BEC) campaigns against a variety of financial institutions, social media sites and other popular brands using such AI technology. In one phishing attack, the threat actors impersonated a popular streaming service through fake email messages closely mimicking the legitimate service's subscription confirmation messages. These messages provided victims with the details of their recent subscription purchase and provided a customer service number to call if the customer wished to cancel. As these are entirely fake subscriptions, when victims call the phone number to cancel, the threat actors request the victim confirm their

payment account credentials or financial account information to cancel, which the victim often provides to the threat actors.

This phishing attack is just one example of how threat actors utilize AI technology for malicious social engineering and other phishing campaigns that are nearly indistinguishable from the legitimate entities being spoofed. Visa PFD assesses threat actors will continue to develop and experiment with new technologies, especially deep fake technologies, to exploit the trustworthiness of executives, managers, and other prominent individuals through a variety of schemes to compromise victims' credentials or payment account information.

Threat actors may also use AI technologies and ALMs to develop novel malware capable of identifying vulnerabilities within transaction messaging or fraud controls implemented by banks and processors. These tools can also assist threat actors in the creation of digital skimming code which can be embedded on an eCommerce merchant's checkout webpage and steal sensitive payment account data, such as the PAN and CVV2, from consumers checking out on these webpages.

Due to the sophistication of these programs, threat actors will be able to develop customized malware strains, including those used in digital skimming attacks, for each unique victim targeted by the threat actors. These tools enable threat actors to tailor the malware to their victims and allow the malware to exploit any vulnerability identified by the threat actors. Moreover, as these AI technologies continue to advance, it is imperative for employees and consumers to be continuously vigilant 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 & Data Breach Forecast

Visa PFD assesses threat actors will remain opportunistic in exfiltrating data during ransomware attacks in the coming months given the large spike in ransomware cases. Visa PFD anticipates the following in the ransomware and data breach space in the coming months:

- Ransomware threat actors will likely continue to target critical infrastructure, including financial organizations among other critical entities.
- Threat actors will utilize the same frequently used attack methods of social engineering, phishing, and malicious email campaigns. As payment data is highly sensitive and heavily sought after by threat actors, it is probable that social engineering approaches and scams will continue to be used by threat actors to obtain payment data in the future. For example, in September 2023, threat actor group Scattered Spider used social engineering to breach two large North American hospitality companies. Although payment data was not impacted in either incident, the attacks proved the power of social engineering in targeting large organizations.
- Actors will likely shift more toward exploiting known vulnerabilities among file transfer services, remote access tools, and other third-party applications, especially considering the success actors, such as CL0P ransomware group, had with this methodology in the past seven months. For example, CL0P was identified as targeting three file transfer services between 2020 and 2023 using similar tactics, techniques, and procedures (TTPs) for each attack through the exploitation of zero-day vulnerabilities in file transfer services File transfer services are a lucrative target for threat actors to attack numerous institutions simultaneously. While previous CL0P attacks had not specifically targeted the payments ecosystem, the 2023 attack resulted in the breach of multiple financial institution's data. For these reasons, Visa PFD assesses CL0P and other threat groups will likely target file transfer services with large user bases, enabling the groups to attack multiple downstream organizations in a single effort.
- Threat actors will likely continue to exploit the tactic of reporting victims to the SEC after a data breach, especially given that the new rules went into effective as of 15 December 2023. Organizations should stay vigilant in their cybersecurity monitoring and ensure compliance with the new SEC rules if any indication of a material cybersecurity event occurs.
- Despite numerous successes with disrupting threat actor infrastructure and operations, threat actors will likely continue to regroup and develop new means and tactics to commit additional fraud, especially in instances where no arrests are made in connection with criminal infrastructure being disrupted by authorities.

Evolution of Scams

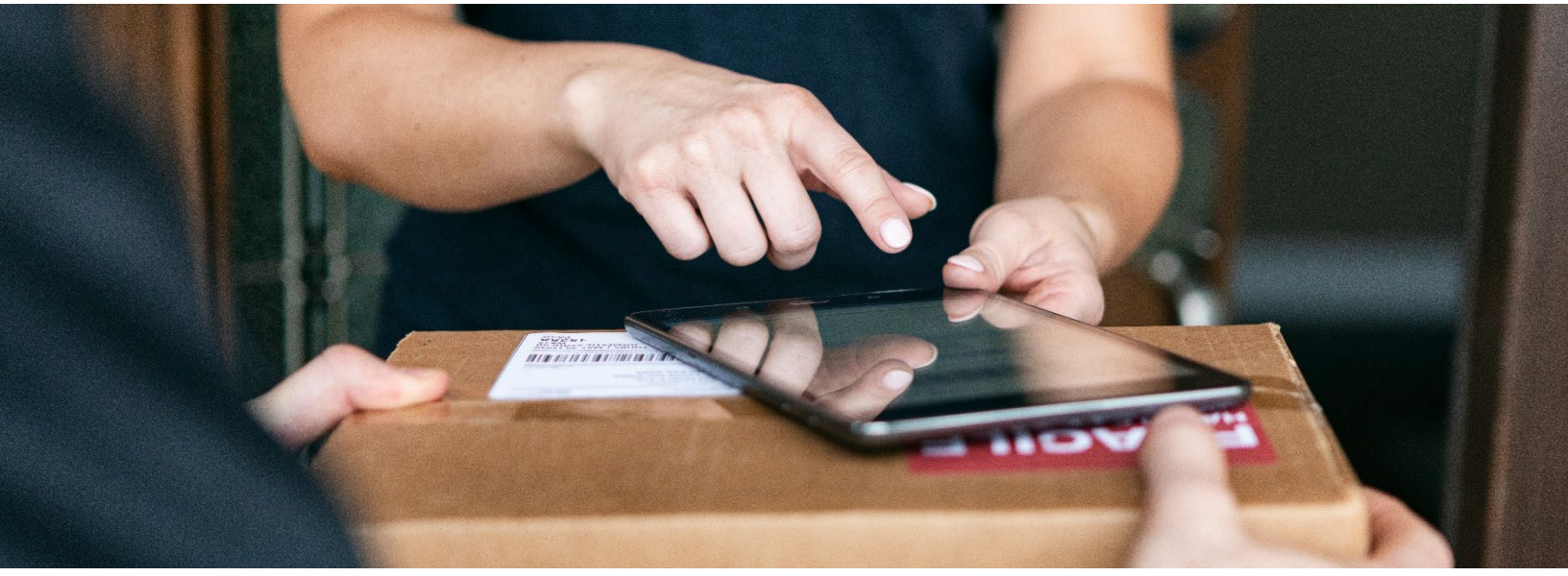
Given the increase over the past two years in criminal profits gained from various types of scams, Visa PFD assesses such scams directly targeting consumers will continue to be an attractive threat tactic employed by actors globally and will likely continue to increase in both complexity and volume. 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 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.

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

Threat actors continued the trend from the last 12-months of targeting third-party service providers and supply-chain infrastructure in various attacks. In the past seven-month period, threat actors targeted third-party providers, including payment gateway providers, 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 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 compromising a single organization. This threat potentially impacts payments ecosystem organizations around the globe and, particularly, entities lacking proper security controls or those not adhering to a strict vulnerability and patch management program.



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 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 banks/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 a bank's authorization decisioning logic when it is experiencing a fraud attack, PFD's **Visa Payments Threats Lab** (VPTL) enables Visa and the bank 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 banks 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.

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 and 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.

Disclaimer: This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it.