A Payment Ecosystem Report by
Visa Payment Fraud Disruption

Biannual Threats Report

December 2022

VISA

Contents

Executive

Summary

Executive Summary

This report provides an overview of the top payment ecosystem threats within the past six-month period (June 2022 – November 2022) as identified by Visa Payment Fraud Disruption (PFD). Over the course of this period, threat actors continued to target payments ecosystem organizations with a variety of longstanding as well as novel methodologies. Threat actors innovated upon established methodologies to improve the effectiveness of fraud schemes and continued to develop new tactics for targeting the payments ecosystem.

The threats in this report are discussed within the context of the following threat types:

Technical Misconfigurations

Threat actors continued to exploit technical misconfigurations through various fraud schemes, including enumeration, ATM cashouts, automated fuel dispenser fraud, targeting banks failing to validate dynamic transaction data, and increased threat actor interest in one-time-password (OTP) bypass methods.

Malware Used to Facilitate Fraud

Over the last six-month period, Visa PFD identified an increase in several malware campaigns used by threat actors to conduct cyber-attacks against the payment ecosystem, including point-of-sale (POS) and ATM malware.

Cryptocurrency and Digital Payments

2022 was a record-breaking year for cryptocurrency thefts targeting blockchain-based entities, with over US$3B stolen in on-chain thefts. Over the past six-months, the payments ecosystem experienced an increasing trend in one-time-password (OTP) bypass schemes across nearly every global region.

Visa People, Technology, and Processes

Over the past 6 months, the **Visa eCommerce Threat Disruption (eTD)** capability increased identification of infected merchant websites by **4%** and was able to remediate **18%** more merchant compromises, resulting in a **6.25%** improvement from the average mean time to remediate a payment account related compromise.

The **Visa Account Attack Intelligence (VAAI)** capability monitors for enumeration attacks and takes action to notify affected acquiring banks and merchants and helps to block egregious attacks to mitigate and prevent the successful enumeration of payment accounts. Over the past six months, the US region was the most heavily targeted from both the acquiring side (**63.5%** of total acquiring enumeration) and issuing side (**38.8%** of total issuer enumeration).

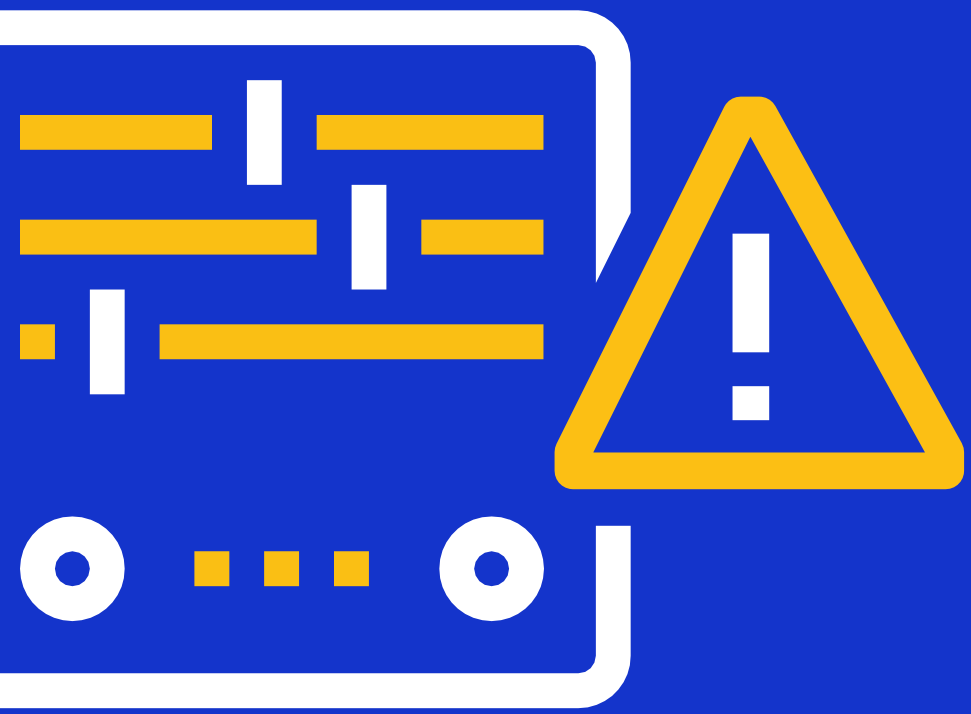
The 24x7 Visa **Risk Operations Center (ROC)** triages and analyzes fraud related incidents and transaction-level alerting globally and around the clock to ensure the threats are identified and mitigated. Over the past 6 months, the number of incidents the ROC responded to decreased by **1.4%**; however, the total number of transactions proactively blocked by the ROC during these incidents increased by **28%**, indicating that individual attacks have grown in size.

PFD's **Global Risk Investigations (GRI)** team conducts indepth investigations on a variety of different external data security incidents where cardholder payment data may be at risk.
PRA Cases – Increasing Trend: Fraudulent purchase return authorizations (PRAs) investigations increased **164%** in the June 2022-November 2022 period when compared to December 2021-May 2022.
Skimming Cases – Increasing Trend: Skimming cases increased **174%** in the June 2022-November 2022 period when compared to December 2021-May 2022.
Agent Cases – Fluctuating Trend: Third Party Agent breach investigations decreased by **75%** in the September 2022-November 2022 period when compared to December 2021-August 2022.
Ransomware Cases – Fluctuating Trend: Ransomware investigations decreased by **35%** in the July 2022-October 2022 period compared to December 2021-June 2022

This report includes a brief 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.

Technical

Misconfigurations



Technical Misconfigurations

Threat Actors Target Banks with Purchase Return Authorization (PRA) Fraud

Beginning in September 2022, Visa Payment Fraud Disruption (PFD) identified an increase in threat actors conducting purchase return authorization (PRA) fraud.

Threat actors conduct PRA fraud schemes to transact high amounts in purchase returns, either to a single card or distributed over various cards. Merchants often do not notice this activity until the funds are deducted from their bank account. If the activity is not detected or blocked by the merchant's bank, fraudsters cash out the funds from the purchase return transactions at ATMs.

In this current PRA fraud tactic, threat actors exploit insufficient risk controls in banks' open-to-buy (OTB) settings by conducting purchase return transactions. Threat actors are currently targeting banks in the Central Europe, Middle East and Africa (CEMEA) region using merchants acquired in the US. However, this scheme can impact any bank globally via a merchant acquired in any region if the bank's OTB settings are not configured properly.

In this PRA fraud scheme, a threat actor obtains unauthorized access to the merchant's gateway and/or terminal and initiates a PRA transaction for which there is no connected initial purchase of goods. The first PRA transaction is a pre-authorization request for a return-of-goods credit request, which is quickly followed by a reversal request. Due to the bank's misconfigured OTB settings, the bank releases the OTB prior to settlement. Additionally, to note, a pre-authorization should only occur for a purchase transaction and not for return-of-goods credit request transaction.

Beginning in September 2022, Visa Payment Fraud Disruption (PFD) identified an increase in threat actors conducting purchase return authorization (PRA) fraud

Fraud Scheme Continues to Target ARQC Validation

Beginning in December 2019 and continuing into the second half of 2022, Visa Payment Fraud Disruption (PFD) identified numerous point-of-sale (POS) fraud attacks. In these attacks, fraudsters use a physical POS device along with a mobile application loaded with compromised Primary Account Numbers (PAN) and expiration dates to emulate point-of-sale entry mode 05 (PEM 05) EMV® chip or 07 contactless (PEM 07) transactions.

Data validation is a primary defense against attacks this fraud scheme. The PEM 05 and 07 fraud activity detailed here is successful primarily due to the targeted banks not validating dynamic data, specifically EMV® Authorization Request Cryptograms (ARQC). Banks' validation of ARQC values on EMV® Chip and contactless transactions is essential in the prevention and mitigation of PEM 05 chip and PEM 07 contactless fraud activity. Visa client banks can also sign up for Visa Chip Authenticate, where Visa will validate the cryptogram values on behalf of the bank.

Continued AFD Fraud Activity

Between 01 June and 22 November 2022, Visa PFD sent numerous alerts to banks notifying of suspicious activity related to a specific automated fuel dispenser (AFD) fraud 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. Threat actors provision the accounts to mobile devices and carry out contactless transactions, or combine a mixture of point-of-sale entry mode 05 (PEM 05) EMV® chip, or 07 contactless (PEM 07) transactions at the AFD terminals. Visa PFD suspicious automated fuel dispenser (AFD) fraud alerting increased by **35%** compared to the same period in 2021. However, the total amount of AFD fraud decreased by **66%,** indicating PFD's proactive monitoring and alerting and clients alert actioning stopping the attacks quicker, saving issuers millions in potential fraud losses.

Correctly managing the Status Check authorization prevents fraudsters from performing multiple AFD transactions and surpassing the account balance associated with the card.

Enumeration Update and Trends

Again, as in years past, enumeration (i.e., the programmatic, automated testing of common payment data elements via eCommerce transactions to effectively guess the full payment account number, CVV2, and/or expiration date) remains among the top threats to the payment ecosystem.

Threat actors attack third-party merchant service providers susceptible to enumeration attacks due to insufficient security controls in the provided software and services. Acquiring banks are advised to conduct thorough due diligence during the merchant onboarding phase to ensure the validity of the merchant, as many fraudulently onboarded merchants are used for enumeration and the subsequent monetization of enumerated PANs.

An enumeration trend targeting Car and Truck Dealerships under MCC 5521 (CAR & TRUCK DEALERS/USED ONLY) was identified during this same period. Some Auto Dealerships under MCC 5999 (MISC SPECIALTY RETAIL) were also impacted. In August 2022 MCC 5811 (Caterers) experienced an increase in enumeration attacks.

PFD assesses that these merchants are targeted due to weak security controls on the respective checkout pages. Actors identify these vulnerabilities and then pivot to other merchants within the same industry vertical. Throughout 2022, PFD detected numerous attacks against merchants operating under specific merchant category codes (MCCs), which may indicate a vulnerability in a third-party service utilized by the merchants within each respective MCC.

In March 2022, PFD identified an enumeration trend involving the use of merchants in the Motion Picture Theaters merchant category code (MCC) 7832. The use of merchants in this MCC to conduct enumeration attacks continues.

Merchants under MCCs 8299 and 8211 (SCHOOLS) also experienced increased enumeration activity. The enumeration attacks against these merchants decreased significantly after initial detection of the attacks.

MCC 9399 (GOV'T SERV) experienced elevated enumeration attacks beginning in September 2022. However, there was a significant decrease in the number of merchants impacted in the past three months leading up to November 2022. Between June and November 2022, PFD continued to see a majority of the MCC's identified in this period impacted by ongoing enumeration.

Visa recommends the following to combat enumeration:

For **issuing banks**:

- Monitor transactions occurring on the MCCs listed in this report, especially in conjunction with attack transaction indicators such as repeated CVV2 failures, invalid expiration dates, and invalid PAN.
- Refer to Visa's Account Testing and Enumeration Procedures, and report enumeration events to Visa as directed within the procedures.

For **acquiring banks and merchants:**

- Use Visa Secure *(3DS) authentication and CAPTCHA controls to prevent automated transaction initiation by bots or scripts (e.g., high succession of authorization attempts on a single PAN from one IP address or device ID)
- Monitor network traffic for suspicious connections and host probing, and log system and network events.
- Use Point-to-Point Encryption (P2PE) and other Payment Card Industry (PCI)-validated encryption for all host connectivity and employ cryptographic keys for transaction sessions/packets.
- Monitor the velocity on various data elements such as IP address, device, and email used at checkout.
- Protect merchant credentials by issuing strong user IDs and passwords for payment gateway portals
- Be cognizant of phishing scams aimed to obtain payment gateway credentials as threat actors have been successful at gaining unauthorized access via credential obtained through phishing.

Card Present Fraud Schemes

Counterfeit Cards Used to Conduct Fallback Fraud

Between July and October 2022, retailers in the United States were targeted with a counterfeit payment account scheme. Within this scheme, threat actors presented a counterfeit card, most likely with a defective chip, forcing the transaction to be conducted via fallback magnetic stripe read (POS entry mode 90). The magstripe transactions generated an issuing bank response code of 19 (re-try transaction) due to the bank's rules on fallback transactions and the use of magstripe on these specific accounts. The merchant's acquiring bank and/or processor then improperly interpreted the response code 19 as an approval, despite the use of the non-authorized response code. Thus, as a result of the improper interpretation of the response code, the threat actors and cashier at the point-of-sale were provided with an approval, allowing the threat actor to walk away with the fraudulently purchased goods. While the transaction was not authorized by the issuing bank, the merchant completed the sale and subsequently force posted the transaction to the cardholder's account. As no authorization was obtained for the transaction, the transaction was eligible for chargeback, in accordance with Visa Rules.

The primary account numbers (PANs) used in this fraud scheme were likely purchased from the cybercrime underground as the accounts were noted to have transactions consistent with validation testing prior to the fraudulent counterfeit transactions.

This attack reaffirms the importance of presenting and handling proper response codes within a transaction to ensure this type of fraud does not occur. Visa provides extensive guidance and descriptions of the various response codes, available online. Banks should review this document to confirm response codes are handled appropriately.

Digital Skimming Update

In digital skimming attacks, threat actors deploy malicious code onto a merchant website targeting their checkout pages to scrape and harvest payment account data entered by consumers, such as primary account number (PAN), card verification value (CVV2), expiration date, and personally 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.

The past six-month period experienced numerous developments in the digital skimming threat landscape. The most notable developments within digital skimming as identified by PFD are as follows:

Outdated Payment Plugins

Various digital skimming campaigns within this six-month period continued to exploit unpatched and/or outdated eCommerce payment plugins used by merchant websites. Visa PFD identified three separate incidents in which different threat actors targeted the same eCommerce payment plugin used by eCommerce merchants.

In one of these attacks, threat actors targeted a North American (NA) eCommerce merchant and created a fake checkout webpage which was presented to customers as they purchased goods on the merchant's website. This fake checkout page harvested cardholder data including the PAN, expiration date, and the CVV2. After this malicious fake webpage was removed, the same threat actors compromised an administrator account, likely due to a weak or compromised password, and then appended malicious digital skimming code onto the merchant's actual checkout page.

A second attack saw threat actors first conducting an SQL injection attack against an outdated eCommerce payment plugin used by an eCommerce merchant, which was used to obtain administrator credentials. Once the compromised administrator credentials were obtained, the threat actors appended malicious digital skimming code to the legitimate code of the outdated payment plugin, which was used to then deploy this same malicious skimming code on the merchant's checkout page.

The third compromise, in which the outdated payment plugin was targeted by threat actors, involved threat actors using a web shell to access the eCommerce merchant's checkout page. Through this web shell, the actors appended digital skimming code to the payment processing plugin on the merchant's checkout page.

Reverse Shell

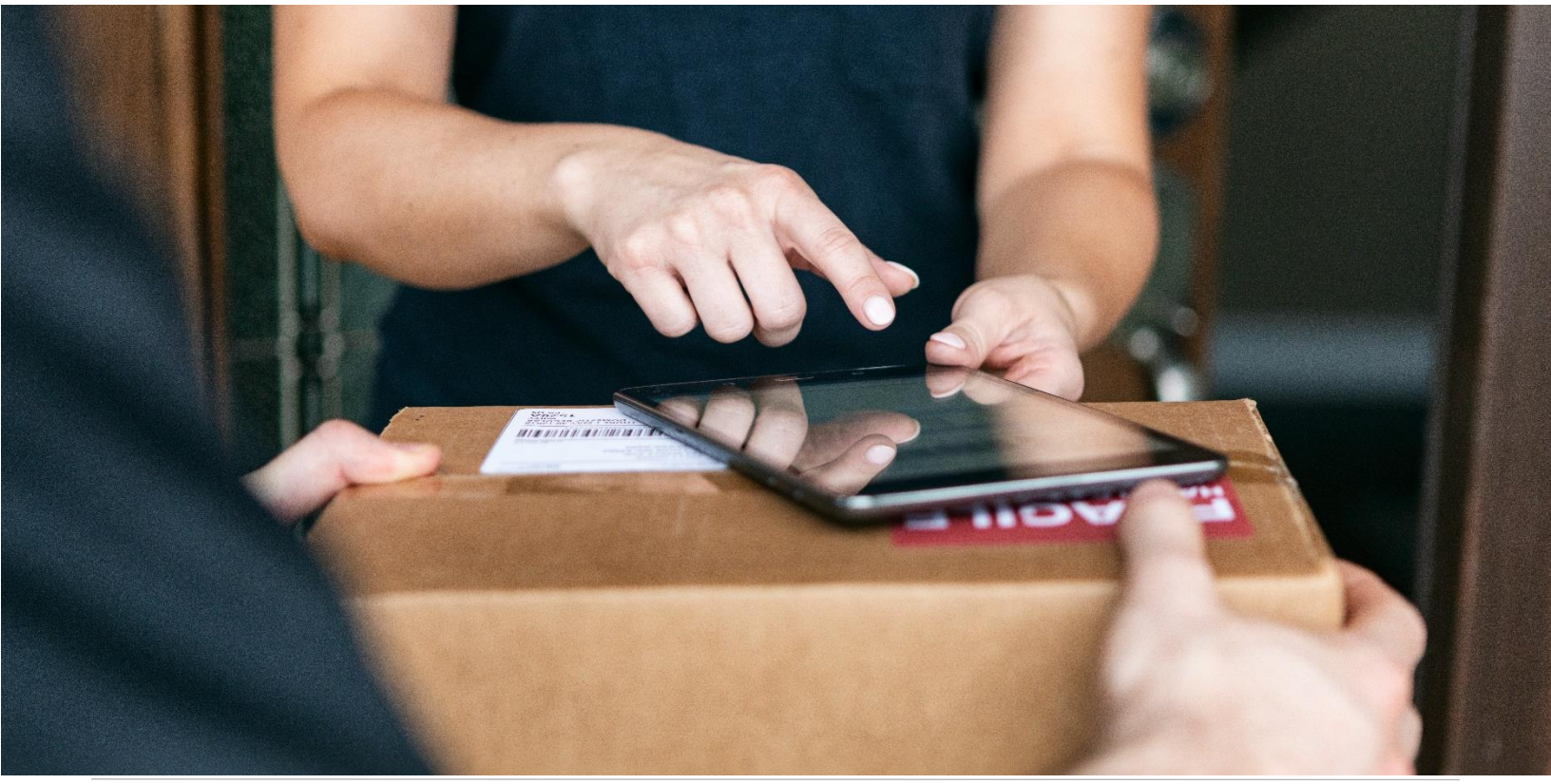
In September 2022, Visa PFD identified a digital skimming attack wherein the threat actors placed a reverse shell dropper on the targeted eCommerce merchant's file system. Once a shell session is initiated, the reverse shell (or 'connect-back shell') redirects the input and output connections of the victim's system allowing the attacker to have remote control over the system. Once the attacker gained control over the victim's system, they appended malicious digital skimming JavaScript code into the legitimate code of the victim's eCommerce platform's checkout webpage. This malicious digital skimming code harvested payment account data as victims entered the data into the site's checkout fields. The malware harvested the victims' full PAN, expiration date, and cardholder information.

Coupon or Promotion Integrations on Merchant Websites

Another campaign involved threat actors exploiting a promotion or coupon-code integrated into a NA eCommerce third-party payment service provider's webpage. The threat actors appended malicious code into five (5) legitimate files in the victim's environment, which was accessed remotely through webshells. This malicious code included two digital skimming malware variants which harvested payment account data from 45 eCommerce merchant environments using the victim's payment services. The first digital skimming malware infection consisted of malicious code to harvest and exfiltrate payment account data stolen during the checkout process. The malware sent the stolen payment data to an external domain controlled by the threat actors. The second digital skimming malware infection targeted merchant checkout processes and stored payment account data compromised during the checkout process in base64 format in a local .png file. The malware harvested full PAN, expiration date, CVV2, and cardholder information, such as the customer's physical address, when the customer entered this information into the customer input fields of the checkout page.

Targeting eCommerce Cigar Shops

Threat actors also used digital skimming malware to target a series of eCommerce cigar shops during a campaign in July 2022. In this campaign, the threat actors targeted nine (9) eCommerce cigar shops in a one-month span where they appended malicious digital skimming malware into the JavaScript of the cigar merchant's checkout pages. All of the victims used the same eCommerce platform to build their websites, were hosted on one or more of the same shared servers with the same IP address registered in the U.K., and the eCommerce websites were owned by or related to the same consumer brand management company based in Europe. Visa PFD assesses the threat actors were able to exploit a vulnerability within the parent company's network infrastructure or within the eCommerce platform used by all of the compromised cigar merchants. Of note, PFD previously published the malicious domain identified in each of these compromises in a previous report. This campaign highlights threat actors' ability to compromise several victims who use the same platform once a common vulnerability is found within the initial victim's environment.



eCommerce Platform Code Repository Publicly Exposed

In a recent campaign, threat actors modified the code of a health-related eCommerce merchant's platform by accessing its code repository. The threat actors were able to gain access to the code repository because it was publicly exposed, allowing the actors to obtain administrative credentials for the platform. Once the actors obtained administrative credentials, they were able to append digital skimming malware to the code of the merchant's checkout page, from which they harvested payment account data. Insufficient security measures on the merchant's checkout page may have also led to the compromise. Specifically, the checkout page did not have brute force prevention measures and multi-factor authentication (MFA) was not implemented on the admin portal.

Third Party Service Providers

In the last six-months, Visa PFD also identified a compromise wherein a technology-related eCommerce merchant was subjected to a digital skimming attack because the merchant's third-party hosting provider did not adequately update or patch the libraries for the merchant's website's Java-based logging utility identified as Log4j 2. This outdated version of the Log4j 2 logging utility contained a remote code execution (RCE) vulnerability, tracked as CVE-2021-44228, which allowed the threat actors to gain remote access to the merchant's eCommerce website environment. From there, the threat actors appended malicious digital skimming code into the legitimate code of the merchant's checkout page, enabling the threat actors to harvest payment account data, such as PAN, CVV2, and expiration date. This attack underscores the need for merchants to keep all software within an eCommerce environment patched and up-to-date, and merchants must ensure they are aware of and mitigate vulnerabilities impacting their supply chain and third-party services, providers, and platforms.

Malware

Used to Facilitate

Fraud

Malware Used to Facilitate Fraud

Increase in Point-of-Sale Malware

Over the last six-month period, Visa PFD identified an increase in several different malware families used by threat actors to conduct attacks against the payment ecosystem. One such general malware type is Point-of-Sale (POS) malware which is generally used by threat actors to compromise magstripe payment account data at brick-and-mortar merchants. Visa PFD saw threat actors increasingly resort to conducting fraudulent activities at brick-and-mortar merchants as COVID-19 restrictions were eliminated or reduced by government authorities around the world, and as a result, more consumers are conducting transactions in-person, especially as they travel.

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 October 2022, Visa PFD investigated a POS malware attack against a hospitality merchant in North America. In this attack, threat actors used the ModPipe POS malware to infect the victim and inject a scraper to extract payment account details. The ModPipe malware runs within legitimate system processes and installs and downloads modules for different functions, such as connecting to the command and control (C2) infrastructure, scanning for IP addresses, stealing database credentials, and listing running processes. Another module, the JHook module, is used to replace the POS terminal system's payment account decryption process with a malicious function. This malicious function obtains magnetic stripe data from the payment accounts used on the POS terminal. Once run, the module searches for decrypted payment account data, such as the primary account number (PAN), which the core module exfiltrates to the threat actor's C2 server.

New Prilex Variant

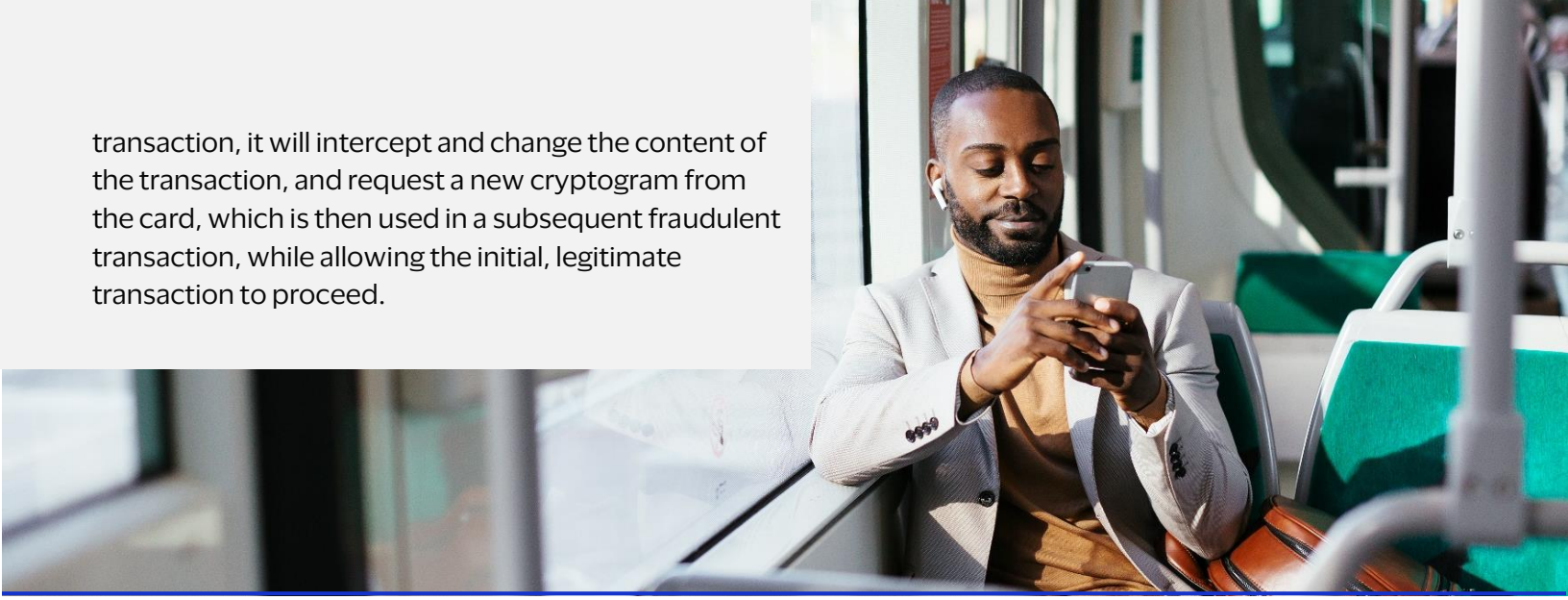
Additional POS malware identified by security researchers in recent months includes a new variant of the Prilex malware. Prilex, which was first seen in the ecosystem in 2014, began as an ATM-focused malware and evolved to target POS systems to conduct fraudulent transactions using intercepted data.

Prilex is attributed to the financially motivated cybercrime group Prilex Group (aka Prilex Gang). The group's primary objective is to target financial institutions to cash out via ATMs or POS systems.

Visa PFD previously reported on Prilex and the malware's update to include POS targeting. In this

new variant, which is spread through phishing emails impersonating a POS vendor, the malware is deployed into the POS environment either physically on-site or through remote access. The new Prilex variant performs what threat researchers refer to as a "ghost transaction" wherein the malware uses a stealer module to intercept all communications between the POS terminal and POS software during the transaction. Once the malware detects a legitimate

transaction, it will intercept and change the content of the transaction, and request a new cryptogram from the card, which is then used in a subsequent fraudulent transaction, while allowing the initial, legitimate transaction to proceed.



ATM Malware in CEMEA

Threat actors also increasingly resorted to using ATM malware in recent compromises against banks to conduct ATM cash-out attacks. This trend is likely to continue as COVID-19 protocols are removed around the world and consumers begin conducting more in-person transactions.

Visa PFD recently analyzed an ATM malware compromise of a bank in the Central Europe, Middle East and Africa (CEMEA) region. In this attack, the threat actors removed the front panels of a dozen targeted ATMs before inserting USB drives loaded with the ATM malware into the USB ports on the ATMs. This enabled the threat actors to override the ATMs' systems and fraudulently dispense cash, however they were only successful at six (6) of the ATMs. The threat actors targeted older ATM models running outdated and unpatched software and operating systems. The targeted ATMs were also not Payment Application Data Security Standard (PA-DSS) compliant. Additionally, the bank did not have real-time ATM monitoring capabilities implemented on its network. This attack underscores the importance of running up-to-date and patched ATM operating systems and employing sufficient monitoring of all ATMs within a network.

Cryptocurrency
and Digital Payments

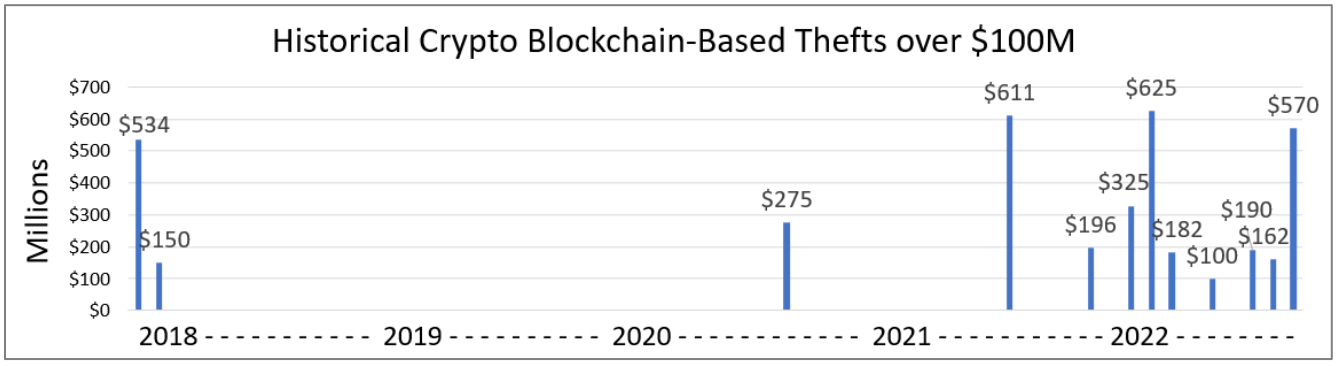
Cryptocurrency and Digital Payments

Cryptocurrency Thefts Hit All-time High in 2022

2022 was a record-breaking year for cryptocurrency thefts targeting blockchain-based entities, with over US$3B stolen in 2022 (as of November 2022). Cryptocurrency bridge services were a favored target for threat actors throughout 2022, with threat actors exploiting platform vulnerabilities to steal cryptocurrency as platforms transfer funds from one blockchain to another. Cryptocurrency bridge platforms operate cross-chain services by locking the original token in a smart contract and then minting a "wrapped" version of the locked token that can be transferred to a different blockchain. Over the past six months, PFD identified numerous incidents of crypto thefts involving blockchain bridge services. A common tactic used in bridge service attacks is the exploitation of vulnerabilities in a bridge service's smart contracts to either forge new transactions or allow for the approval of unauthorized transactions, which allows threat actors to either mint or steal funds and move into fraudster-controlled wallets.

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. From January through early October 2022, the cryptocurrency ecosystem experienced thirteen (13) separate bridge attacks totaling US$2B in thefts, with US$1.3B stolen between January and March 2022 alone. Figure 2 below shows some of the major cryptocurrency heists since 2014 where US$100M or more was stolen.

Figure 2 (Source: Investopedia: Largest Cryptocurrency Hacks So Far)



As cryptocurrency and DeFi 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 such as the ones mentioned above.

One-Time-Passcode Bypass Schemes Targeting Digital Payments

Over the past six-months, the payments ecosystem experienced an increasing trend in one-time-password (OTP) bypass schemes across nearly every global region. eCommerce security continues to improve through significant developments such as cardholder authentication, tokenization, secure checkout pages and merchant website implementations, and other technologies and fraud prevention tactics used by payments ecosystem participants. One highly effective mechanism for combatting eCommerce fraud is the use of multi-factor authentication (MFA), such as OTPs, of consumers at the point of login to websites or during the transaction process. The effectiveness of MFA in combatting fraud led to threat actor innovations to thwart such authentication measures.

In a recently identified crypto-focused phishing campaign, threat actors use emails impersonating a crypto exchange company in order to trick account holders into clicking on a malicious link embedded in the email which takes victims to a spoofed web page. Threat actors then harvest the victim's account login data in real time and use it to log into the victim's actual account on the real exchange website at the same time. The threat actor then uses a tactic known as "2FA relay" wherein once the real site prompts the threat actor for the two-factor authentication (2FA), the threat actor tells the spoofed site to prompt the victim to enter their 2FA information. The threat actor uses the real 2FA from the spoofed site to complete the login process to the victim's account on the legitimate crypto exchange site.

Once in control of the victim's cryptocurrency account, the threat actor initiates a high volume of transactions, sometimes hundreds or thousands of transactions, from the victim's account to fraudster-controlled accounts. Funds are then pushed to other services on the blockchain in an attempt to obfuscate the flow of funds, such as mixers, gambling services, and cybercrime marketplaces. In the meantime, the spoofed site denies the victim's login attempt – since it is not the actual exchange site – and informs the victim their account was locked. To keep the victim occupied and distracted from any potential notifications they may be receiving from the real exchange site while the threat actor drains the victim's account, the threat actor engages the victim on the spoofed site via a "customer service" chat box pretending to be a representative from the crypto exchange. Once the funds transfers are complete and the crypto account is drained, the threat actor abruptly closes the chat session and deactivates the phishing page.

MFA continues to be a critical component of a robust security posturing and should be implemented wherever possible. However, Visa PFD assesses threat actors will continue to find innovative ways to circumvent MFA of consumers at the point of login to websites or during the transaction process. Banks and merchants should remain vigilant in combatting MFA-related fraud. Visa published a best practice guide for consumers with tips on protecting themselves against phishing scams, and a Visa Business News containing best practices for mitigating risks of Account Take Over (ATO) fraud.

Threats

Landscape Forecast

Threats Landscape Forecast

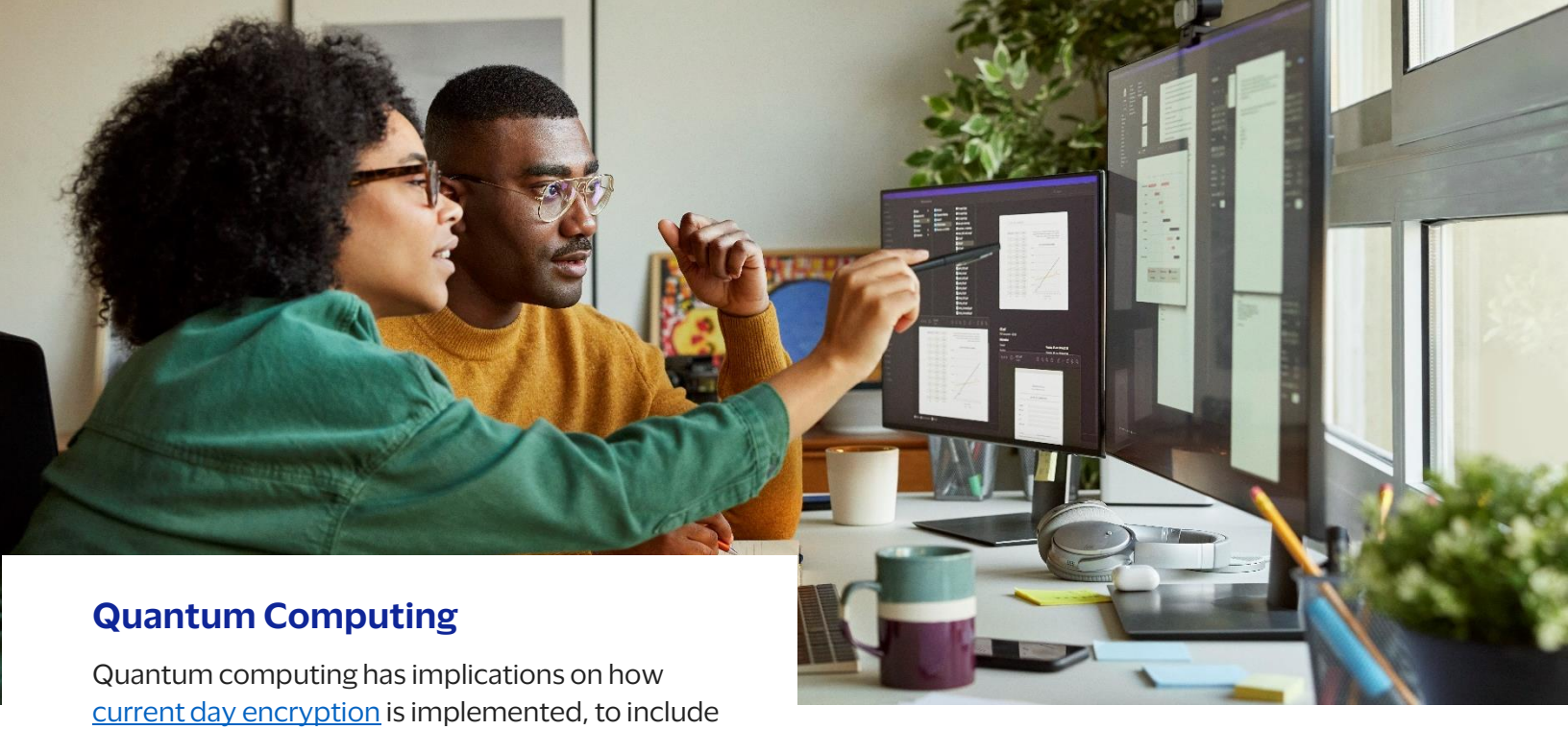
Unemployment Insurance and Government Disbursement Fraud

Visa expects the number of applications for Unemployment Insurance (UI) and Small Business Administration (SBA) loan programs, and other government disbursement programs, to increase over the next six to twelve months due to the current global economic environment. With the increase in UI and SBA applications, threat actors almost certainly will attempt to take advantage of states' government disbursement programs.

Generally, to commit UI fraud, threat actors will obtain stolen credentials, which include complete personal identifiable information (PII) records, known in the cybercrime underground as 'fullz', from other threat actors. The threat actors will then use these 'fullz' to fraudulently apply for UI programs. Once the applications are approved, threat actors quickly monetize the UI or SBA payment accounts in various ways, including ATM cash-outs, cryptocurrency purchases, or Person-to-Person (P2P) transfers. Visa PFD has developed numerous processes and capabilities to identify, mitigate and prevent government disbursement fraud within the payments ecosystem.

Visa PFD recommends issuing banks implement the following mitigants to help combat UI fraud:

- Review/Require a copy of applicant's driver's license and selfie and compare both the recent/real-time selfie to the applicant's driver's license photo
- Verify the state address of the account is the same as the state from where the funds are disbursed
- Identify accounts where multiple state/federal funds are disbursed to the same account
- Identify where multiple prepaid accounts sent to the same address
- Place velocity checks on dollar amounts and number of transactions on spend per day, especially on high-risk Merchant Category Codes (MCCs)



Quantum Computing

Quantum computing has implications on how current day encryption is implemented, to include sensitive payment account information and personally identifiable information. Visa PFD assesses threat actors will attempt to use quantum encryption to obtain sensitive consumer information to include payment data.

Researchers believe fault-tolerant quantum computing will be able to crack the many secure forms of cryptography, especially asymmetric algorithms, used today, including the Rivest-Shamir-Adleman (RSA) algorithm. As fault-tolerant quantum computing becomes more commonplace, encrypted data, such as passwords or credit card details, may be at risk of compromise by threat actors. Criminal activity conducted by threat actors via encrypted communications or money transfers are also at risk of being discovered with emerging quantum technology.

Threat actors are already harvesting encrypted data from companies and organizations as they await the breakdown of prominently used encryption methods via quantum computing. These attacks are known as "Harvest-Now, Decrypt-Later" or "HNDL" attacks, as the threat actors intend to hold onto encrypted data until it can be decrypted using quantum computers. Because of alleged risk to RSA and other cryptographic algorithms, researchers believe over 20 billion digital devices will face upgrades or replacement to use quantum-safe encryption algorithms. In May 2022, the White House released a memorandum citing security of eCommerce transactions as one of the at-risk areas in the world of quantum computing. The US National Institute of Standards and Technology (NIST) set the first quantum-safe cryptography protocol standards in 2022. President Biden expects public release of these standards in 2024 and is aiming to mitigate the majority of the risk of quantum information science (QIS) by 2035.

Visa PFD recommends staying current on news pertaining to quantum-safe encryption and be sure to transition to new encryption methods, once implemented. In doing so, payment information, cardholder personal identifiable information (PII), and business information will remain protected against compromise from threat actors.

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. Over the past 6 months, the number of incidents the ROC responded to decreased by **1.4%,** compared to the prior six-month period; however, the total number of transactions proactively blocked by the ROC during these incidents increased by **28%**, indicating that individual attacks against the ecosystem have grown in size.

Visa Risk 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 intelligence built by Visa Risk's personnel is then used to develop robust, innovative, and effective technologies and processes to combat these threats on behalf of the payments ecosystem.

Moreover, **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.

VCA is a global team composed of hundreds of payments consultants, data scientists and economists across six continents providing the cybersecurity expertise needed to navigate the changing commerce landscape and protect clients from emerging cybersecurity threats through analytics and Artificial Intelligence-enabled capabilities.

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.

The **eCommerce Threat Disruption (eTD)** capability protects the eCommerce channel by scanning eCommerce merchant infrastructure and identifying digital skimming attacks.

eTD increased identification of infected merchant websites by **4%** and was able to remediate **18%** more merchant compromises in the previous six-month period. The eTD capability resulted in a **6.25%** improvement from the average mean time to remediate a payment account related compromise.

PFD vigilantly monitors for enumeration attacks through the **Visa Account Attack Intelligence (VAAI)** capability and takes action to notify affected acquiring banks and merchants and helps to block egregious attacks to mitigate and prevent the successful enumeration of payment accounts.

Over the past six months, the US region was the most heavily targeted from both the acquiring side (**63.5%** of total acquiring enumeration) and issuing side (**38.8%** of total issuer enumeration).

Additional Visa Risk technologies are deployed that monitor for transaction anomalies in the card-not-present / eCommerce, ATM, and point-of-sale channels, and Visa is constantly developing new technologies to prevent attacks occurring from OTP intercepts and authentication bypass by pursuing the development of more robust authentication through biometrics and other combinations of authentication.

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.

In the event of material compromises, including those resulting from the threats discussed throughout this report, PFD conducts detailed investigation processes to ensure the compromise is mitigated and intelligence is obtained from the incident.

PFD's Global Risk Investigations (GRI) team conducts indepth 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 banks, third party agents including integrators/resellers, and all merchant levels to help ensure any at risk data is identified and impacted stakeholders are notified.

An incident is reported to Visa in one of the following channels:

- Common Point of Purchase (CPP) Report
- Self-reporting by entity
- Media reported
- Intelligence/Research Firm reported
- Law enforcement reported (e.g., United States Secret Service)

GRI noted the following investigation trends over the last six months:

- PRA Cases – Increasing Trend
  - Fraudulent purchase return authorizations (PRAs) investigations increased 164% in the June 2022-November 2022 period when compared to December 2021-May 2022.
- Skimming Cases – Increasing Trend
  - Skimming cases increased 174% in the June 2022-November 2022 period when compared to December 2021-May 2022.
- Agent Cases – Fluctuating Trend
  - Third Party Agent breach investigations decreased by 75% in the September 2022-November 2022 period when compared to December 2021-August 2022.
- Ransomware Cases – Fluctuating Trend
  - Ransomware investigations decreased by 35% in the July 2022-October 2022 period compared to December 2021-June 2022.

For any questions regarding how these assets can be deployed on behalf of your organization, please reach out to your Visa Risk Manager.

Additional Resources

- Visa's eCommerce Threat Disruption (eTD) capability
- Visa's 'Website Security for Ecommerce Merchants' document
- Visa Account Attack Intelligence (VAAI)

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