A Payment Ecosystem Report by
Visa Payment Fraud Disruption

Biannual Threats Report

June 2022

VISA

VISA PUBLIC

Table of Contents

Executive Summary **2**

Technical Misconfigurations **4**

AFD Threat Actors Add CEMEA to List of Regions Targeted 5

Enumeration Remains Prolific 6

Digital Skimming 6

The Return of Card Present Schemes 7

Token Fraud and OTP Bypass 8

Nation States and The Political Environment **10**

Ongoing Security Situation in Eastern Europe 11

Cryptocurrency and Digital Payments **12**

General Update 13

Threats Landscape Forecast **14**

How Visa can Help **16**

People 17

Technology 17

Processes 18

Additional Resources **18**

Executive Summary

This report provides an overview of the top payment ecosystem threats within the past six-month period (December 2021 – May 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 tried-and-true methodologies, such as payment account enumeration, digital and physical skimming, and malware related campaigns. Threat actors also innovated upon these methodologies to improve the effectiveness of fraud schemes and continued to develop new tactics for targeting cryptocurrency and digital payments.

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 automated fuel dispenser fraud, targeting issuers failing to validate dynamic transaction data, merchant terminal enumeration and takeover, and increased threat actor interest in OTP bypass methods.

The targeting of eCommerce platforms and third-party code integrations are among the most common tactics utilized by threat actors conducting digital skimming attacks. These eCommerce attack tactics are further affirmation that threat actors are targeting supply chains and third-party service providers with high frequency and exhibiting continued interest in payment account data and personally identifiable information (PII).

The trend of card present-related fraud schemes persisted into the past six-month period and also included the addition of new fraud schemes, including one targeting magstripe data and another using a new spin on purchase return fraud.

Nation States and the Political Environment

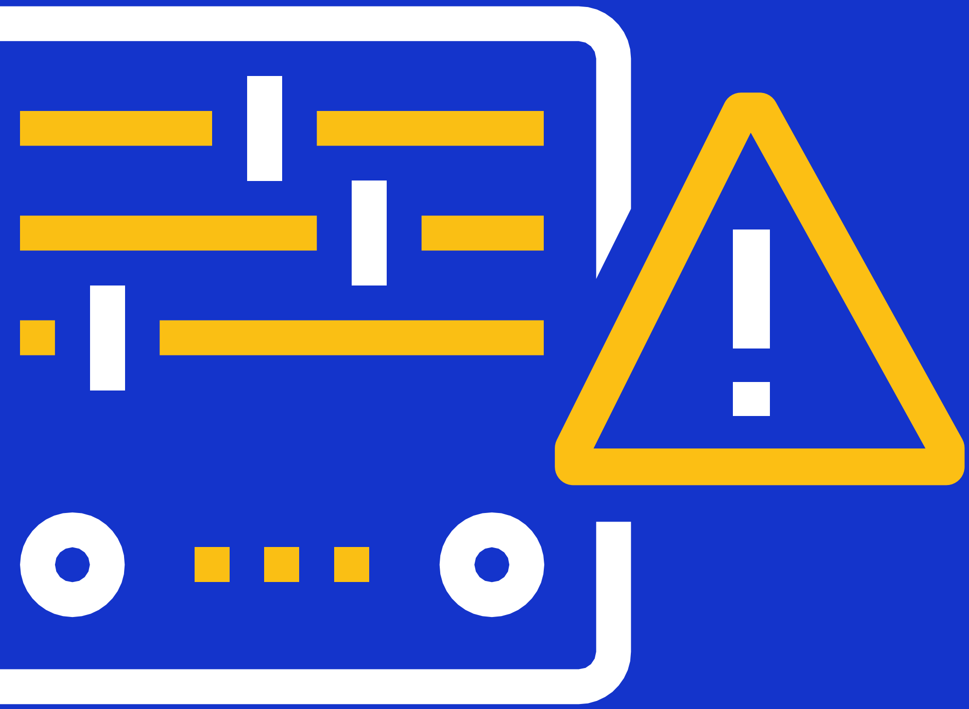
The payments ecosystem threat landscape in the past six-month period was significantly influenced by the ongoing conflict in Eastern Europe. Ransomware attacks have again returned to the prolific levels witnessed throughout 2021, and many of the most active actors have a nexus to Eastern Europe.

Cryptocurrency and Digital Payments

2021 saw a surge in global interest in cryptocurrency, and threat actors consequently capitalized on the increased interest and payment volume. Phishing campaigns and the use of social engineering tactics to compromise victims' data and steal funds remained a top threat targeting the cryptocurrency ecosystem over the past six months.

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



AFD Threat Actors Add CEMEA to List of Regions Targeted

Over the past six-month period, threat actors continued targeting issuers in North America and Latin America and the Caribbean (LAC) with automated fuel dispenser (AFD) fraud schemes and initiated fraud activity targeting issuers in the CEMEA region.

In this scheme, threat actors purchase fuel from AFDs located in multiple US locations using EMV® debit accounts issued by financial institutions in Latin America, the US, or CEMEA. The misconfiguration in this case was the handling of authorization advices subsequent to the US $1 authorization check (0100 Authorization Request), as per the mandated and standard process during AFD transactions. The actors were able to use this exploit to conduct fraudulent AFD transactions far beyond the account balance on the payment account that was being used. The activity represents continued threat actor interest in conducting AFD fraud, and the consistent innovation by threat actors.

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

Over the past six-month period, threat actors continued targeting issuers in North America and Latin America and the Caribbean (LAC) with automated fuel dispenser (AFD) fraud schemes and initiated fraud activity targeting issuers in the Central Europe, Middle East, and Africa (CEMEA) EMEA region.

Enumeration Remains Prolific

Payment account 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 current threats to the payment ecosystem. Over the past six months, PFD identified two notable enumeration trends involving targeted MCCs and/or merchant groups, as well as malicious infrastructure used to facilitate enumeration attacks. Issuers should use this information, which is published in Visa Security Alerts on a regular basis, to identify and prevent enumeration attacks from these trending MCCs.

Payment Account Enumeration Trends

Payment account enumeration threat actors continued targeting third party merchant service providers over this period, and PFD alerted on several such attacks through Visa Security Alerts. Specifically, threat actors targeted merchants under merchant category code (MCC) **7832 (Motion Picture Theaters) and 5521 (CAR & TRUCK DEALERS/USED ONLY).** The targeted merchants were running specific third-party services on their respective websites that had lacking security controls which enabled the actors to target the service and, in turn, the merchants utilizing the service.

Digital Skimming

In digital skimming attacks, threat actors deploy malicious code onto a merchant website that targets the checkout pages of these merchants and harvests the payment account data, such as PAN, CVV2, and expiration date, and often the personally identifiable information (PII), that the merchant's customers enter into checkout forms. Digital skimming attacks are often the result of misconfigurations or lack of security controls within a merchant's environment, which enables threat actors to exploit such misconfigurations and successfully deploy the malicious skimming code.

The past six-month period experienced numerous developments in the digital skimming threat landscape. The threat methodologies continued to exploit misconfigurations within eCommerce platforms and environments. The most notable developments within digital skimming as identified by PFD are as follows:

Threat Actors Target Code Integrations on Merchant Websites

In May 2022, a digital skimming campaign was discovered in which the threat actors exploit code integrations utilized by the targeted merchants, such as marketing tools and tracking, that are enabled on the merchant checkout pages. In the incidents investigated by PFD, the third-party marketing tools and scripts were compromised by threat actors and malicious JavaScript code was embedded into the otherwise legitimate code owned by the third-party. The third-party code, which contained a malicious JavaScript skimmer, was then integrated onto the merchant checkout page, enabling the threat actors to harvest payment account data entered into the forms on the checkout page.

The targeting of eCommerce platforms and third-party code integrations is among the most common tactics utilized by threat actors conducting digital skimming attacks. These eCommerce attack tactics are further affirmation that threat actors are targeting supply chains and third-party service providers with high frequency and exhibiting continued interest in payment account data and personally identifiable information (PII). These campaigns reflect the need for stringent security controls on merchant websites and checkout pages, and merchants must also ensure that external code is not enabled on sensitive cardholder environments, such as the checkout page on eCommerce merchant websites.

eCommerce Merchants Utilize Unpatched and/or Outdated Platforms

Various digital skimming campaigns within this six-month period continued to exploit unpatched and/or outdated eCommerce platforms utilized by merchant websites. In one notable campaign, threat actors targeted multiple Japanese merchants that were running an outdated version of a popular eCommerce platform. The vulnerabilities in the outdated platform enabled actors to place an online order that contained a cross site scripting (XSS) payload, along with a malicious JavaScript URL within the customer information section in the order form. The malicious URL was accessed by an employee at the merchant and the associated malicious payload was executed as a result. Subsequently, the actors deployed further malicious payloads, including webshells, PHP file uploader scripts, JavaScript files, and database management tools, onto the compromised merchant environment.

Additionally, in early 2022, security researchers identified another digital skimming campaign in which more than 500 eCommerce merchants running Magento v1 were targeted with digital skimming malware. The actors reportedly utilized a single command and control (C2) domain to deploy the malware on the targeted merchant websites and harvest payment account details from the merchant's customers.

The Return of Card Present Schemes

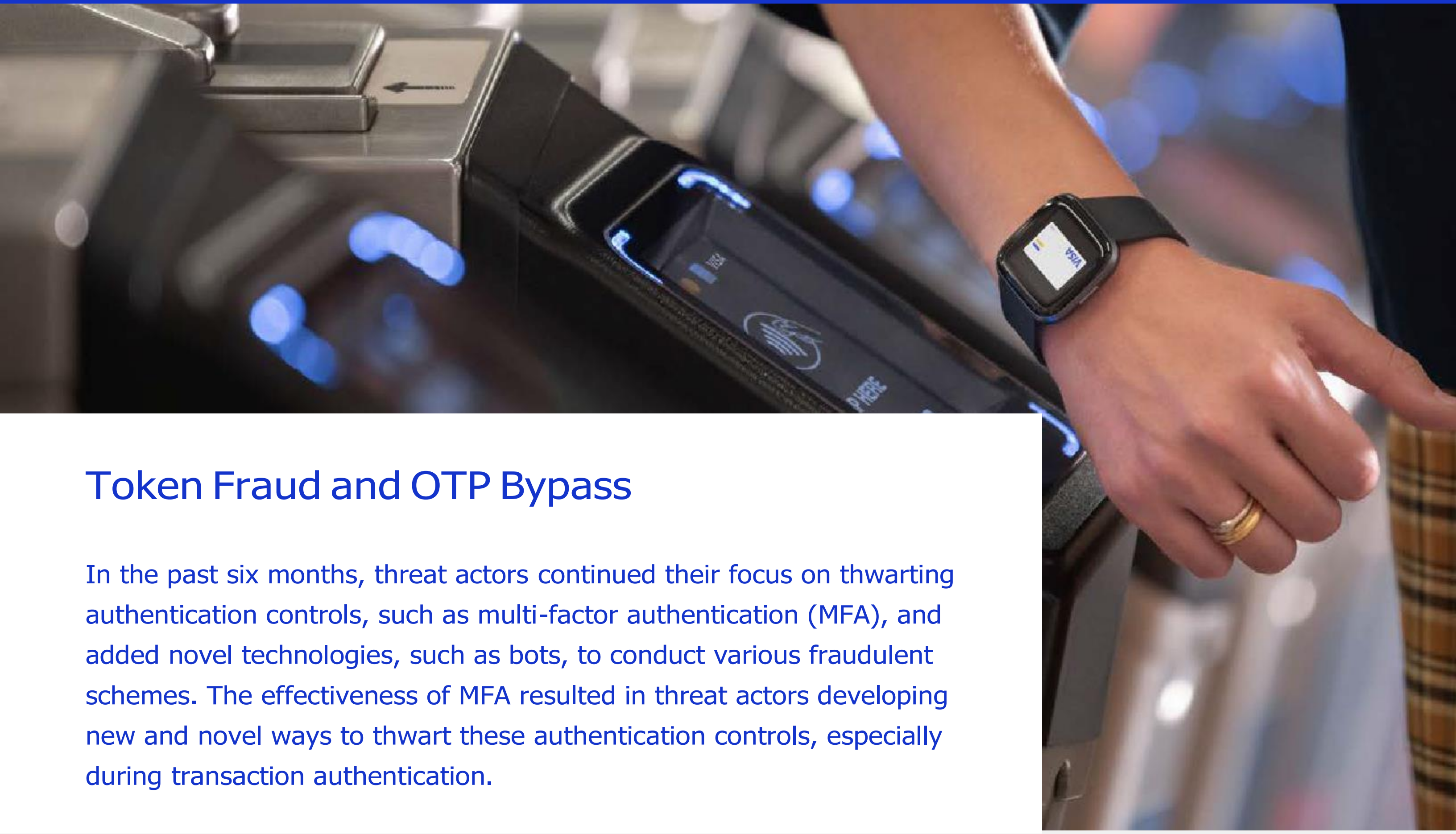
The December 2021 edition of PFD's Biannual report included an analysis on the increase of physical skimming targeting brick-and-mortar point-of-sale (POS) and automated fuel dispenser (AFD) terminals, due largely to the lifting of COVID-19 related restrictions on in-person commerce and the subsequent increase in card present payment volume. The trend of card present related fraud schemes persisted into the past six-month period and included the addition of new fraud schemes:

Fraud Schemes Utilizing Magstripe Data

From December 2021 to February 2022, threat actors conducted three separate fraud attacks with magstripe data. The first attack began in mid-December 2021 and persisted until early February 2022. In this attack, threat actors obtained magstripe data, provisioned the data on mobile devices, and conducted payment entry mode 91 (contactless, using magnetic-stripe data rules) transactions at various grocery stores. The fraudulent transactions occurred in the European region, reflecting the need for strict controls around cross-border transactions, especially within less secure entry modes such as 91.

In the second attack, which occurred in February 2022, threat actors obtained compromised magstripe data and targeted large North American retail merchants with in-store fraudulent purchases. However, the actors did not have valid cardholder verification values (CVV) for the compromised PANs and the authorization requests using these accounts were initially declined for CVV validation failures. Despite these declines, threat actors found a processing misconfiguration which resulted in the acquirer or merchant mishandling the authorization response code declines as approvals, thereby allowing the actors to fraudulently purchase goods.

In a third attack, which also occurred in February 2022, an issuer was targeted with a fraud attack in which threat actors conducted cross-border ATM transactions in a Latin American country. The actors were again using card present magstripe data with invalid CVV that was ultimately approved despite the invalid CVV submitted during the fraudulent ATM withdrawals.



Token Fraud and OTP Bypass

In the past six months, threat actors continued their focus on thwarting authentication controls, such as multi-factor authentication (MFA), and added novel technologies, such as bots, to conduct various fraudulent schemes. The effectiveness of MFA resulted in threat actors developing new and novel ways to thwart these authentication controls, especially during transaction authentication.

Visa Payment Fraud Disruption (PFD) identified techniques such as social engineering, advertising fraud, bots, and phishing kits used to obtain one-time passwords (OTPs) from cardholders, issuer-targeted malware to access and change customer contact details, and the use of social engineering to conduct token fraud.

Social Engineering, Phishing Kits, Bots Used to Obtain OTPs

The use of social engineering to obtain card data or to take over an account continues to be a top threat in the consumer space. Threat actors often contact cardholders and claim to be an employee from the cardholder's bank. In these schemes the actors generally call the cardholders, or send an SMS text, alleging that the cardholder's account was involved in fraud and prompts the cardholder to either call back a provided number or provide sensitive information to the threat actors. The result is the compromise of one-time-passwords (OTPs), tokenized/one-time use PANs, or sensitive user account data such as bank login credentials (username/password).

Threat actors also use relatively inexpensive, easy to use, and readily available custom phishing kits that facilitate the bypassing of MFA. These phishing kits employ the use of reverse proxies in which the actors can create a situation whereby the fraudster acts as man-in-the-middle (MiTM) between the legitimate consumer and the legitimate website. In these schemes, and with the use of the phishing kits, the actors present the legitimate website to the consumer and operate as an invisible intermediary. This greatly decreases suspicions from the consumer as the legitimate website is presented, rather than a spoofed phishing website as is often the case in phishing schemes. The actor is then able to harvest any information that is entered into the website by the consumer, which often includes OTPs as well as username, password, and even session cookies which can be further used to thwart MFA as the cookie could represent a session in which the consumer already authenticated.

Malware Targeting Organizations to Access and Change Customer Details

In late March 2022, Visa Payment Fraud Disruption (PFD) received intelligence regarding an attack against an organization in which threat actors utilized an unidentified malware variant to infect user endpoints. The actors eventually moved laterally in the victim's environment and compromised the credentials for an administrative user of a mobile banking application portal. This access was then used to edit the contact information of specific customers, as well as increase the limits on the customer accounts. The information changed included mobile device numbers, which enabled the threat actors to bypass one-time-password (OTP) authentication as the OTPs were sent to the new mobile devices. The actors used the increased account limits and changed customer information to monetize their illicit access through fraudulent funds transfers in a short amount of time.

While this specific incident involved the fraudulent transfer of funds, similar tactics, techniques, and procedures (TTPs) are often utilized by actors to conduct ATM cashout attacks by deploying malware on a victim issuer network, accessing the cardholder data environment, and increasing limits on a select number of payment accounts. These accounts are then used by mule networks to withdraw significant amounts of cash from ATMs. Additionally, threat actors use similar methods to take over a customer account and change contact information which enables the threat actors to bypass OTP authentication during a transaction.

Nation States and the Political Environment

Ongoing Security Situation in Eastern Europe

The payments ecosystem threat landscape in the past six-month period was significantly influenced by the ongoing security situation and conflict in Eastern Europe.

While the situation continues to unfold, the payments ecosystem has not experienced unusually disruptive or concerted attacks. Payments ecosystem targeting predominantly occurred in the form of Distributed Denial of Service (DDoS) attacks against Western financial institutions prompting warnings from several government organizations, attacks against Russian financial institutions from activist threat groups such as Network Battalion 65 (NB65), and scam / phishing operations utilizing the situation as a lure to attract prospective victims.

The scam / phishing operations were identified frequently over the past six months, and generally consisted of scam charities created under the guise of facilitating monetary donations

to Ukrainian families, businesses, and refugees. This is a common tactic that is regularly used by threat actors to take advantage of natural disasters or other disruptive global events. The prevalence of these type of scams over this time period also prompted a warning from the FBI, which includes recommendations to spot and avoid such scams.

Geopolitical developments in Eastern Europe continue to unfold and, as such, the threat landscape is expected to be heavily influenced by political and security developments, such as Finland and Sweden applying for North Atlantic Treaty Organization (NATO) membership.

Eastern European-Based Ransomware Actors

In early 2022, various law enforcement, government, and private sector operations led to an overall reduction in ransomware attacks against organizations of every industry vertical. Visa Payment Fraud Disruption (PFD) also identified this trend of decreasing ransomware attacks specifically against payments ecosystem participants. However, ransomware attacks have again returned to the prolific levels witnessed throughout 2021, and many of the most active actors have a nexus to Eastern Europe.

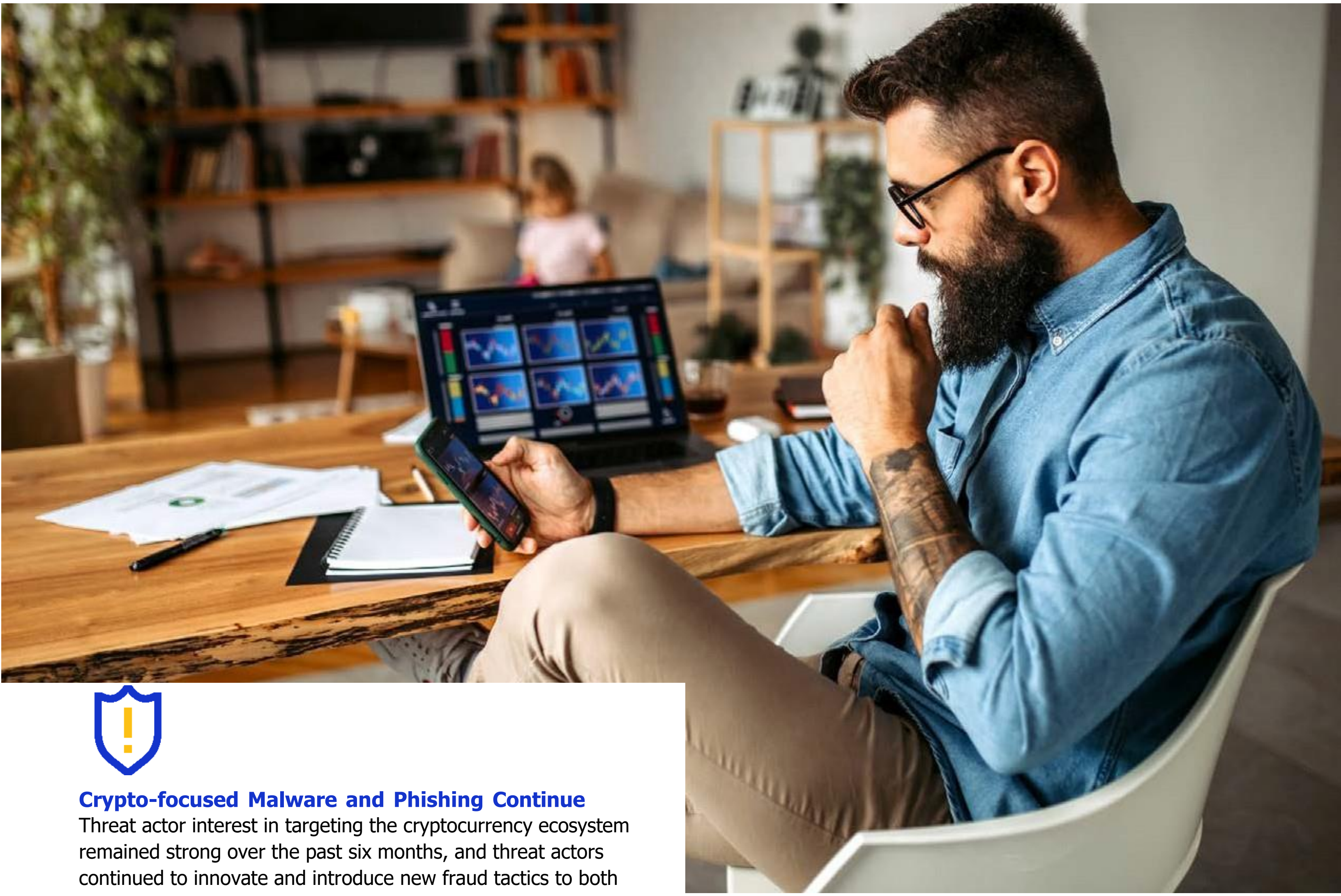
One particularly notable development in the ransomware threat landscape was the alleged arrests of 14 actors within the REvil ransomware operation by Russian authorities. However, despite the alleged arrests, security researchers recently identified the return of REvil and their prolific ransomware campaigns. Additionally, Conti remains among the most active ransomware operations, and RagnarLocker's continued campaigns prompted an alert from the FBI in March.

Concerted ransomware attacks against the payments ecosystem have not been identified in this period, and ransomware actors appear to remain opportunistic in targeting any data to which they obtain access. The general regional nexus of these ransomware groups and intelligence supporting political influences on the group's operations makes ransomware a focal point in the monitoring of the ongoing security and political situation in the region, especially with regards to any impact on the payments ecosystem.

Cryptocurrency and Digital Payments

General Update

2021 saw a surge in global interest in cryptocurrency, and threat actors consequently capitalized on the increased interest and payment volume.



Crypto-focused Malware and Phishing Continue

Threat actor interest in targeting the cryptocurrency ecosystem remained strong over the past six months, and threat actors continued to innovate and introduce new fraud tactics to both the fiat and crypto payment ecosystems.

- In February 2022, threat actors deployed a new malware designed to steal cryptocurrency from victims' browser extension wallets. The new malware, called Mars Stealer, directly targets over 40 types of cryptocurrency digital wallets that work as browser extensions, as well as targeting popular two-factor authentication (2FA) extensions.
- In March and April 2022, two distinct phishing attacks using unique, crypto focused lures targeted user's cryptocurrency wallets to steal funds.

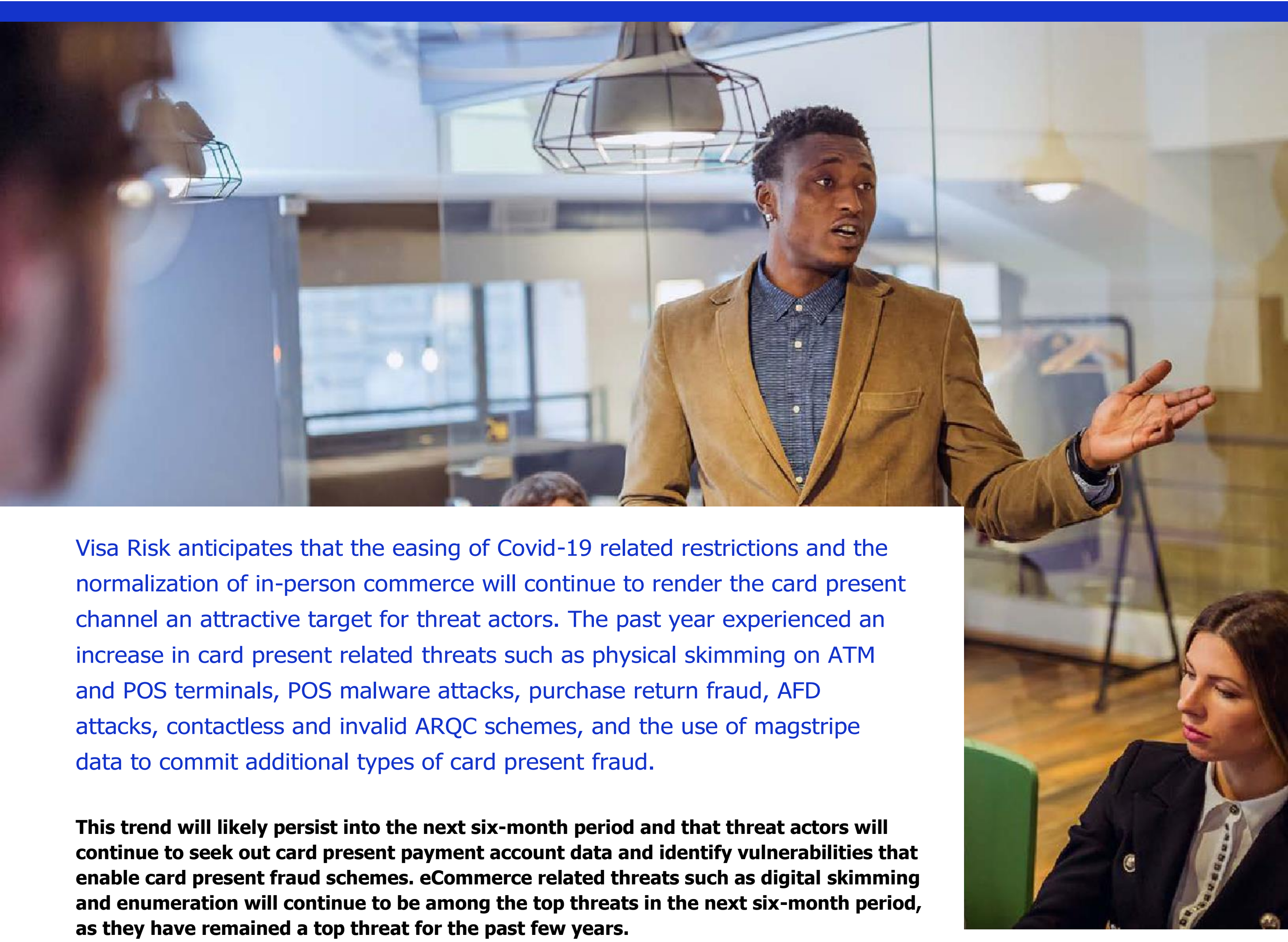
Phishing campaigns and the use of social engineering tactics to compromise victims' data and steal funds remain top threats across the fiat and cryptocurrency ecosystems. Visa provides guidance on preventing social engineering attacks and published a blog post with anti-phishing best practices, as well as a Visa Business News article on mitigating the risk of Account Take Over.

Bridge Service Thefts

In addition to new crypto-focused malware, over the past six months, threat actors targeted crypto bridge services in their fraud efforts. From January through February 2022, three sizeable thefts exploiting vulnerabilities in various bridge services netted threat actors over US$400M.

The thefts all involved cross-chain platforms, known as bridge services, that allow users to transfer cryptocurrency across different blockchains. Bridge platforms operate these 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. These recent crypto thefts illustrate threat actors' increased interest in targeting smart contracts, Decentralized Finance (DeFi), and cross-chain bridge services to steal funds.

Threats Landscape Forecast



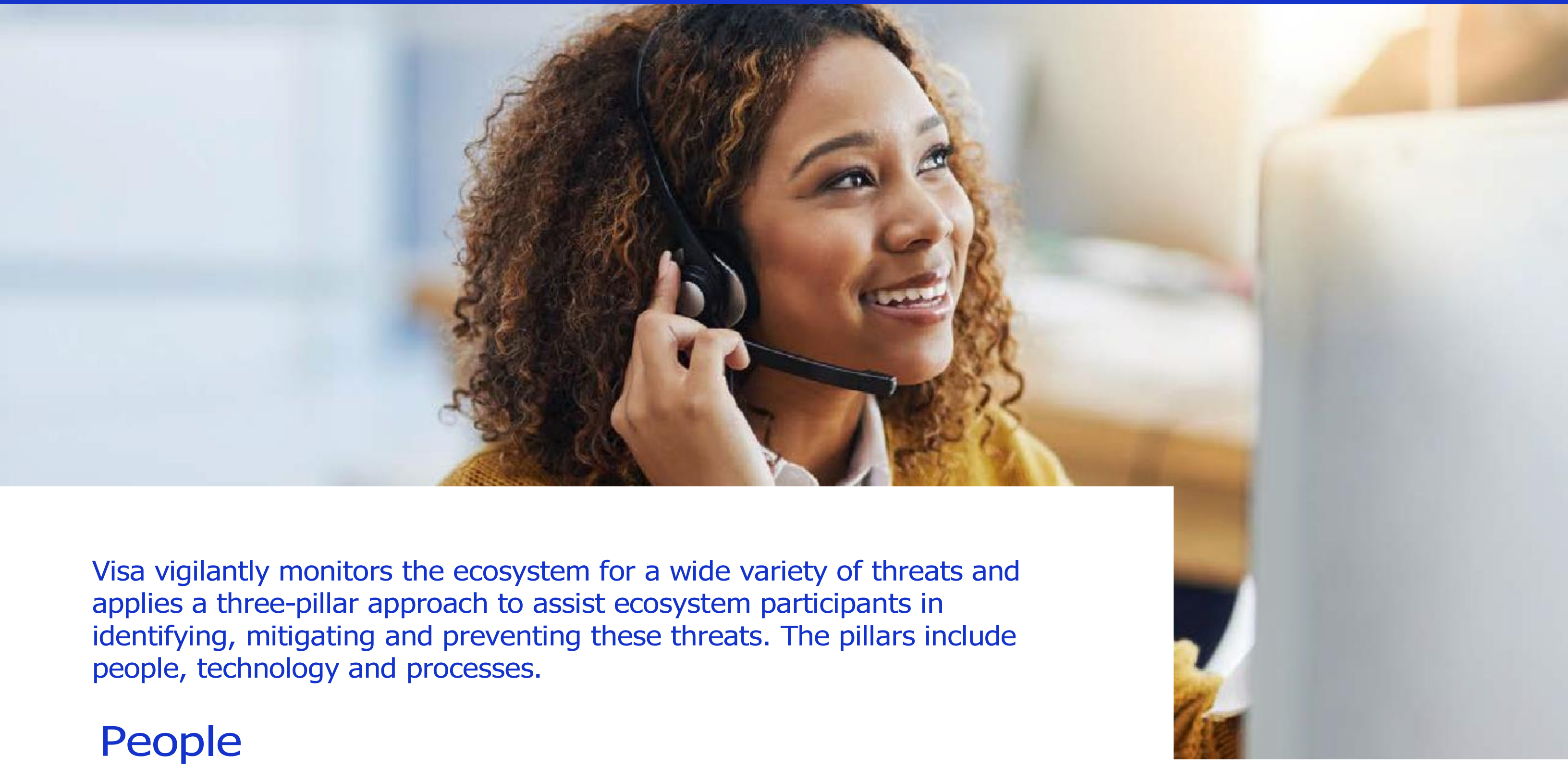
Visa Risk anticipates that the easing of Covid-19 related restrictions and the normalization of in-person commerce will continue to render the card present channel an attractive target for threat actors. The past year experienced an increase in card present related threats such as physical skimming on ATM and POS terminals, POS malware attacks, purchase return fraud, AFD attacks, contactless and invalid ARQC schemes, and the use of magstripe data to commit additional types of card present fraud.

This trend will likely persist into the next six-month period and that threat actors will continue to seek out card present payment account data and identify vulnerabilities that enable card present fraud schemes. eCommerce related threats such as digital skimming and enumeration will continue to be among the top threats in the next six-month period, as they have remained a top threat for the past few years.

The takedown and disruption of numerous underground carding shops and marketplaces, where compromised payment account data was bought and sold, significantly affected the availability of compromised payment data as there are now fewer reputable carding operations. As a result, actors appear to be identifying vulnerabilities within payment processing and conducting targeted fraud to exploit these vulnerabilities rather than purchasing bulk accounts from underground carding shops. Indeed, most successful fraud attacks seen over the past six-month period, as detailed throughout this report, pertained to various processing or other technical/business misconfigurations that enabled threat actors to conduct the fraud schemes. This is expected to continue into the next six-month period. However, despite the takedowns of these marketplaces and carding shops, the underground economy is still thriving and rife with fraud, thus it is expected to remain a significant consideration in the payments threat landscape.

Threat actors will also continue to innovate their methods to target cryptocurrency and other emerging digital payment types. Actors will invariably use new tactics, technology, malware, and other tools to target the payments ecosystem and conduct fraud. PFD remains vigilant in proactively detecting, mitigating and preventing such threats. Visa Risk and PFD also remain committed to working with clients, partners, law enforcement, and the overall payments ecosystem to combat fraud threats posed to the global ecosystem.

How Visa can Help



Visa vigilantly monitors the ecosystem for a wide variety of threats and applies a three-pillar approach to assist ecosystem participants in identifying, mitigating and preventing these threats. The pillars include people, technology and processes.

People

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

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.

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 deep transaction data analysis, cybercrime underground 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 ideally 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 that provides 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.

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

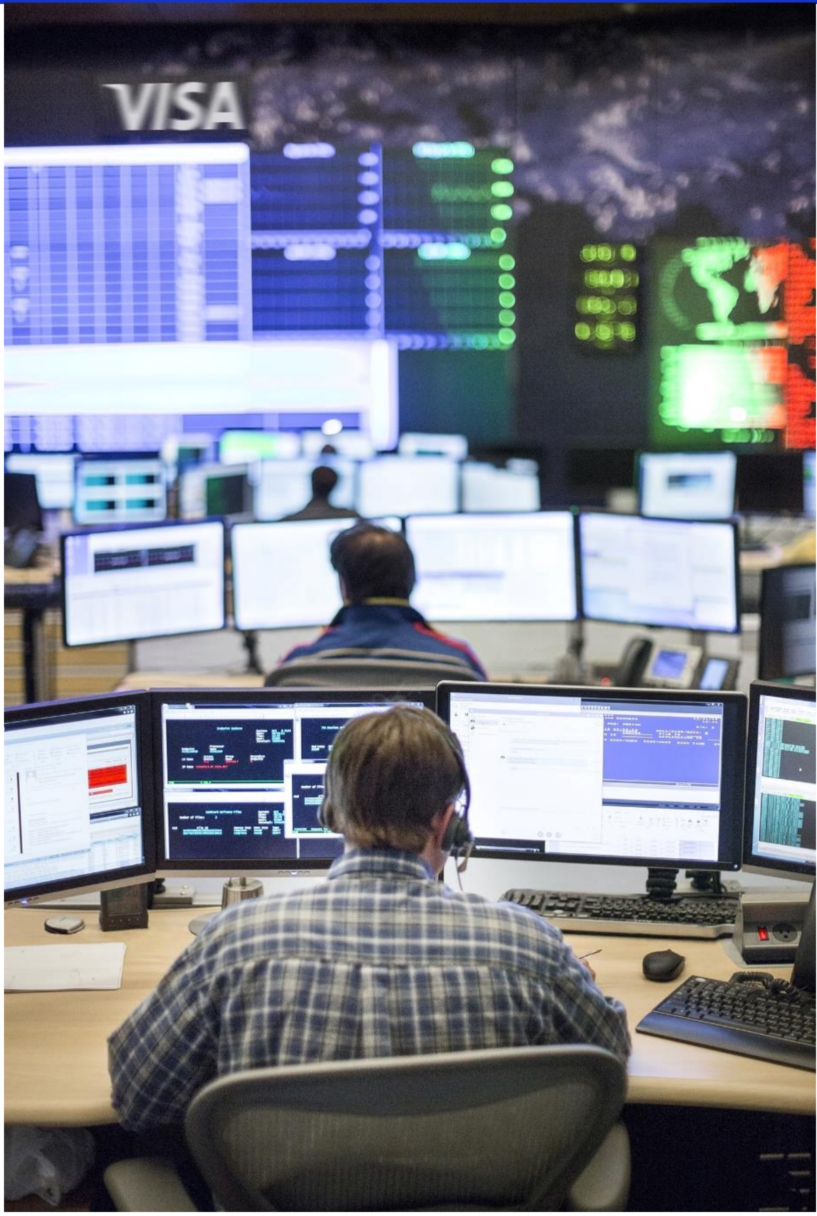
Additional Visa Risk technologies are deployed that monitor for transaction anomalies in the card-not-present / eCommerce, ATM, and point-of-sale channels, and Visa is constantly developing new technologies to prevent attacks occurring from OTP intercepts and authentication bypass by pursuing the development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

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)
- Visa Business News Article published on AFD attack schemes
- Visa Business News Article containing best practices for mitigating risks of Account Take Over (ATO) fraud

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.