A Payment Ecosystem Report by Visa Payment Fraud Disruption

PFD Biannual Report

April – September 2020

Distribution: Public

VISA

Table of Contents

Executive Summary

Throughout the second half of 2020, the payments threat landscape was largely influenced by the ongoing COVID-19 pandemic. Threat actors continued to employ tried and true threat methodologies such as phishing, payment account enumeration, eCommerce skimming, ransomware, among others, and adjusted these methodologies to exploit the ongoing pandemic. Actors also developed new and novel techniques to carry out fraud and used cryptocurrency exchanges, exploited unemployment insurance benefits and stimulus payments from governments around the globe, and found new ways to obtain and monetize payment accounts.

The global pandemic forced the world into an uncertain and constantly adapting environment and fundamentally changed the way the world conducts business. Threat actors similarly adapted to the new environment and remained immensely active in carrying out cyber and fraud threat campaigns. This report utilizes Visa Payment Fraud Disruption (PFD) team's first-hand operational experience to describe the most significant developments in the payments threat landscape, as well as the adapted tactics employed by threat actors.

PFD incorporates a fast-paced, multi-faceted approach in the fight against attacks targeting the global payment ecosystem. Compromised of five primary functions, the team utilizes best-in-class cyber and fraud capabilities and personnel to preserve the integrity of Visa's payment system and support global growth.

Threat Landscape Developments

Threat actors remained active in traditional fraud channels, such as enumeration and point-of-sale (POS) fraud, however the tactics employed by actors were adapted for the changing payments landscape and included new target areas, such as government disbursement programs.

Pandemic Unemployment Assistance Fraud

Visa Payment Fraud Disruption (PFD) identified threat actors taking advantage of the rise in pandemic-related US government assistance programs to conduct various types of fraud. From May through October 2020, Visa PFD published numerous security alerts regarding prolific Pandemic Unemployment Assistance (PUA) fraud arising out of the COVID-19 pandemic and subsequent high unemployment rate. These alerts detail various tactics, techniques and procedures (TTPs) employed by threat actors to carry out unemployment insurance fraud. In identified schemes, the threat actors obtain personally identifiable information (PII), known colloquially in the underground as 'fullz', which generally contain the victim's full name, address, date of birth, social security number, driver's license, and payment account information.

The actors then use the fullz to fraudulently apply for unemployment insurance and load the funds to prepaid and/or virtual payment accounts. Subsequently, the accounts are monetized both domestically and cross-border and include purchases of cryptocurrency, gift cards, electronics, and other forms of person to person transfers often utilizing mobile payment applications. A significant amount of these purchases occur as contactless (payment entry mode 07) but also include magstripe (entry mode 90) transactions. PFD also believes criminals conduct fraudulent card not present (CNP) / eCommerce transactions.

The U.S. Financial Crimes Enforcement Network (FinCEN) and Federal Bureau of Investigation (FBI) released independent alerts regarding COVID-19 related impostor scams/money mule schemes, and the significant increase in unemployment insurance related fraud. PFD continues to closely monitor the various unemployment insurance fraud schemes related to the COVID-19 pandemic and work with the payments ecosystem and law enforcement to ensure the schemes are quickly identified and addressed.

To combat fraud on government disbursement programs, PFD has:

- regular collaboration with banks and FinTechs involved to discuss fraud trends and mitigation best practices,
- continuous implementation and improvement to comprehensive monitoring within the payments ecosystem to identify, mitigate and prevent PUA fraud,
- curated analysis and observation of the payments ecosystem for novel and emerging fraud schemes that exploit the ongoing COVID 19 pandemic and associated unemployment programs.

Visa Law Enforcement Engagement

In response to PUA related unemployment insurance fraud, Visa and federal law enforcement embarked on a public education campaign through the media to remind consumers to protect their personal information. Visa shared information on ways to identify possible phishing scams that may target them through a phone call, email, text message, webpage, or social media.

PFD remains actively engaged with the law enforcement and ecosystem partners in an effort to disrupt pandemic related fraud. This partnership has resulted in the identification, pursuit and arrest of threat actors operating in pandemic fraud.

Curbside Pickup Fraud

Merchants around the globe quickly adapted business models to accommodate consumer spending trends as a result of the COVID-19 pandemic. Among the most significant trends was the increase in payment volume within the eCommerce channel due to the restrictions on crowds and brick and mortar merchant activity. As a result of these restrictions, numerous merchants with large brick and mortar operations shifted their business model to curbside pickup wherein customers purchased goods on the merchant's website and subsequently picked up the ordered goods at the brick and mortar location without leaving their vehicle.

Merchants that employed this model effectively transitioned to eCommerce-only in a short amount of time. As such, certain elements of the curbside pickup model were vulnerable to fraud, such as the method of order verification and lack of controls during the pickup process. For example, merchant employees often only required the order verification number and did not check cardholder ID or implement additional authorization checks. Banks also had to adapt fraud models to account for this significant shift in activity, which made capturing fraudulent activity in this channel difficult. Consequently, fraudsters quickly picked up on these vulnerabilities and exploited curbside pickup processes to conduct high volumes of fraud.

> Consequent to the emergence of this fraud scheme, Visa Payment Fraud Disruption (PFD) expeditiously worked with payments ecosystem participants to identify and remediate vulnerabilities.

While the majority of curbside pickup fraud was identified in North America, merchants that are not properly implementing fraud controls around curbside pickup are vulnerable to this type of attack.

Enumeration Attacks Remain Prevalent

Throughout the second half of 2020, enumeration, which is the scalable and programmatic automated testing of common payment fields via eCommerce transactions to effectively guess the full payment account number, CVV2, and/or expiration date, remained one of the leading threats to the payments ecosystem. Threat actors adapted to the COVID-19 pandemic by illicitly creating and subsequently using COVID-19 related merchant names to conduct enumeration attacks, as well as targeting donation related merchants.

Cashout via Cryptocurrency

Monetization of fraud schemes via conversion to cryptocurrency is becoming an increasingly popular option for threat actors. The number of individuals using digital wallets and merchants accepting cryptocurrency have been increasing, as has the installation and use of Bitcoin ATMs globally. As the adoption and use of cryptocurrency continues to rise, fraudsters will increasingly look to use this innovative financial avenue to monetize stolen and scammed funds.

Ransomware and Malware

Ransomware Actors Exfiltrate Payment Account Data

Ransomware actors continued to pose a prolific threat to organizations across the globe in the second half of 2020 and increasingly targeted the payments ecosystem. In February 2020, PFD reported on an emerging ransomware trend whereby the threat actors began targeting financial institutions and exfiltrating payment account data, in addition to encrypting sensitive systems to disrupt the target's business operations.

Threat actors use the exfiltrated payment account data to extort the ransom payment from victims. This is an attempt to compel victims to pay the ransom in the event that the victim refuses to pay for the decryption key. The threat actors created websites on which they release the exfiltrated data if the victim does not pay the ransom. This ransomware trend is expected to persist, and ransomware attacks against financial institutions should be treated as a data breach.

REvil and Maze

In addition to commonly used phishing campaigns, PFD research shows ransomware actors often exploit insecure remote desktop protocol (RDP) ports, utilize malvertising or watering hole campaigns, disguise malware as legitimate downloads or installation files, or exploit specific Common Vulnerabilities and Exposures (CVEs). Ransomware threat groups REvil and Maze, two cybercrime groups that actively targeted the financial sector in the second half of 2020, commonly exploit RDP and CVE vulnerabilities along with employing phishing campaigns.

On 1 November 2020, the threat actors behind the notorious Maze ransomware group announced that the group will end its ransomware operations. The announcement also alleges that while the group is ending its operations, "there will be more projects like Maze to remind you about secure data storage." Security researchers reported that many of the Maze affiliates appear to be moving away from Maze after this announcement and potentially using the ransomware variant Egregor. Egregor has many similarities with Maze, such as the malware's source code and tactics used by the actors. Egregor campaigns also threaten to release sensitive exfiltrated data taken from the victim's network if the victim does not pay the ransom. Currently, PFD has not confirmed whether Egregor data exfiltration includes payment account data.

Point-of-Sale Malware

Threat actors largely focused on eCommerce channels to obtain compromised payment accounts, however, brick and mortar merchant compromises still accounted for a small percent of incidents.

Alina POS

In August 2020, PFD released a security alert regarding analyzed malware samples recovered from the compromise of a North American brick and mortar merchant. The malware variants were identified as Alina POS, Dexter POS, and TinyLoader. These variants were deployed on the merchant network in an effort to harvest track 1 and track 2 magstripe payment card data from the merchant's point-of-sale environment. However, **the targeted merchant had EMV® Chip enabled point-of-sale terminals.** The implementation of secure acceptance technology significantly reduced the usability of the payment account data by threat actors as the available data only included primary account number (PAN), integrated circuit card verification value (iCVV) and expiration date. Thus, provided iCVV is validated properly, the risk of counterfeit fraud was minimal. Additionally, many of the merchant locations employed point-to-point encryption (P2PE) which encrypted the PAN data and further reduced the risk to the payment accounts processed as EMV® Chip.

After gaining initial network access, the actors deployed keylogging malware to harvest credentials and facilitate privilege escalation and lateral movement within the corporate network. Multiple merchant's store locations were affected by the attack, and the malware variant used differed depending on the store location.

TinyPOS & PwnPOS

In June, PFD analyzed malware samples recovered from the independent compromises of two North American merchants. In these incidents, criminals targeted the merchants' point-of-sale (POS) terminals in an effort to harvest and exfiltrate payment account data. Subsequent to analysis, the first attack was attributed to the malware variant TinyPOS, and the second to a mix of POS malware families including RtPOS, MMon (aka Kaptoxa), and PwnPOS. The recent attacks exemplify threat actors' continued interest in targeting merchant POS systems to **harvest track 1 and track 2 card present payment account data,** even with the decrease in card present transaction volume due to the ongoing COVID-19 pandemic.

Prilex

In August 2020, PFD analyzed a malware sample recovered from a threat campaign targeting merchants in Latin America. Subsequent to analysis, the malware was determined to be Prilex, which is attributed to the financially motivated cybercrime group Prilex Group. The group's primary objective is to target financial institutions to cashout via ATMs or point-of-sale (POS) systems. The group is suspected to be of Brazilian origin, based on observed targeting and the fact that many debug strings and function / variable names in the malware are written in Portuguese. The POS variant of Prilex has not been often used in threat campaigns since its discovery. However, **the recent attacks in Latin America provide evidence that Prilex is currently being used to target POS systems and harvest payment account data.**

New eSkimmers Identified by PFD

Baka

In August, PFD was the first to identify a new JavaScript skimming malware variant and subsequently dubbed the malware '*Baka*'. PFD's investigation revealed seven command and control (C2) servers hosting the *Baka* skimming kit. The skimmer contains expected features offered by many eCommerce skimming kits (e.g., data exfiltration using image requests and configurable target form fields), however, the *Baka* skimming kit's advanced design indicates it was created by a skilled developer. The most compelling components of this kit are a unique loader and obfuscation method. The skimmer loads dynamically to avoid static malware scanners and uses unique encryption parameters curated for each victim to obfuscate the malicious code. PFD assesses that this skimmer variant avoids detection and analysis by removing itself from memory when it detects the possibility of dynamic analysis with Developer Tools or when data has been successfully exfiltrated. This unique skimmer was identified on several merchant websites across multiple global regions using Visa's eCommerce Threat Disruption (eTD) capability, which analyzes and detects threats targeting eCommerce merchants.

Pipka-like skimmer

In June, security researchers observed a new self-destructing JavaScript skimmer variant on a North American merchant website. The skimmer, designed to steal customers' payment details at checkout, uses an obfuscation technique similar to the *Pipka* skimmer Visa discovered and reported on in 2019, which is able to remove itself from the HTML of a compromised website after it executes, decreasing the likelihood of detection. PFD reported on the discovery and mechanics of the *Pipka* eCommerce skimmer in November 2019.

Anticipated Threats

Payments Ecosystem Threats Over the Next Six Months

- **Enumeration** is anticipated to remain a top threat across global regions. Cybercriminals are taking advantage of big data and machine learning to find and exploit new vulnerabilities. To counter this, PFD continues to improve and update the Visa Account Attack Intelligence (VAAI) capability to quickly identify and halt sophisticated enumeration attacks.
- Cybercriminals will continue to innovate and evolve tactics in developing **eSkimmers** for eCommerce merchants, and eSkimming innovation will remain a persistent threat to the eCommerce space. This is especially true in the context of COVID-19 as many brick and mortar merchants are still not operating at full capacity due to government restrictions and lockdowns. By proactively scanning the front-end of eCommerce websites for skimming malware and hunting for new malware variants, PFD's eCommerce Threat Disruption (eTD) capability remains an effective solution to cybercriminals' efforts to steal card data from eCommerce sites.
- While threat actors will continue efforts targeting payment data in the eCommerce space, **point-of-sale** (POS) systems remain attractive targets for threat actors. Even as transaction volume shifted to favor card-not-present (CNP) during the pandemic, PFD observed actors continuing to target card present data. Lack of EMV® implementation contributes to POS systems remaining worthwhile targets, however, the adoption of this secure acceptance technology continues to increase. This will likely result in threat actors attempting to target non-EMV® terminals and networks as quickly as possible. PFD continues to analyze and report on new malware variants and indicators of compromise (IOCs) and publishes client and publicly available reports on new developments regarding POS malware.
- As the pandemic situation persists, we will likely see sustained contextual and opportunistic **cyberattacks** leverage the state of the pandemic. Given the success fraudsters had in 2020, fraud schemes targeting new or extended **government stimulus programs**, such as Unemployment Insurance benefits, will continue. Even when the COVID threat subsides, criminals will continue to leverage pandemic related lures e.g., vaccination lures. As more countries begin to shift to post-COVID operations, threat actors will likely shift their tactics to exploit the latest developments impacting global and regional economies.

Across all regions and using a multitude of tactics, criminals are expected to innovate and advance in their efforts to target financial institutions, consumers, and payment data. To protect the payments ecosystem, PFD capabilities continuously evolve to detect, analyze, and disrupt new threat schemes. As fraudsters leverage technology to attack consumers and financial institutions in new ways, PFD will persist in efforts to anticipate and counter new threats to the ecosystem.

Fraudsters remained immensely active during the pandemic and throughout 2020. While these actors employed many tried and true fraud techniques, such as ransomware, eSkimming and POS malware, the actors adapted their methods to coincide with the changes in the payment landscape due to the ongoing pandemic. The above fraud schemes and techniques will persist into 2021, and PFD assesses that fraudsters will continue to adapt to the changing environment and develop new and novel techniques to commit fraud.

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.*