Visa Security Alert

November 2023

POTENTIAL INCREASE IN HOLIDAY SHOPPING FRAUD SCHEMES

Distribution: Visa Issuers, Processors and Acquirers

Summary:

For the upcoming 2023 holiday season, Visa Payment Fraud Disruption (PFD) anticipates threat actors will conduct a variety of both card-present (CP) and card-not-present (CNP) schemes in attempts to obtain cardholders' sensitive information, including their personal identifiable information (PII) and payment account data, such as the primary account number (PAN), CVV2, and expiry. Throughout 2023, PFD has observed both novel and commonplace techniques used by threat actors to compromise sensitive cardholder information. **PFD assesses actors will conduct tried and tested tactics that are often seen across the payments ecosystem to facilitate fraud during the holiday season, but will take advantage of season-specific commerce, such as an increase in travel, and discounted goods and services, to facilitate fraud during the holiday season.** This report identifies those schemes which PFD assess may be the most popular tactics employed by threat actors during the 2023 holiday season, between November 2023 and January 2024.

1. Threat Overview

PFD expects threat actors to deploy many different methods to compromise cardholder information over the next few months. Due to the rapid influx in both eCommerce activities and in-person shopping at brick-and-mortar retailers and hospitality merchants, threat actors will seek to exploit lax security protocols implemented by cardholders, issuers acquirers and processors. Below are some of the more likely schemes which PFD anticipates threat actors will execute:

- **Digital Skimming:** In a digital skimming attack, threat actors deploy malicious code onto a merchant website which targets the checkout page of the merchant's site and harvests payment account data, such as primary account number (PAN), card verification value (CVV2), and expiration date, and often the personally identifiable information (PII), entered into checkout forms by the merchant's customers. **During the holiday shopping season, threat actors may target merchant websites selling in-demand goods or services where they may benefit from skimming more payment accounts since the in-demand goods/services website will receive higher customer traffic.** PFD anticipates an increase in digital skimming attacks against eCommerce merchants as online shopping increases during the holiday season. This creates a greater opportunity for actors to successfully compromise and monetize compromised payment account data stolen from the checkout pages of these merchants.
- **Phishing and Social Engineering:** PFD forecasts phishing attacks will continue to increase. In phishing attacks, threat actors create phishing websites, often using malvertising and other search engine optimization (SEO) tactics on retail or service websites to entice victims. When the victim attempts to make a purchase on the phishing websites, the threat actor steals the victim's payment account details and uses those payment details on another website. **With merchants offering discounts and sales to increase holiday shopping purchases, threat actors will likely attempt to impersonate well-known retailers to trick consumers into accesses**

the phishing websites and obtain their payment account data. Merchant sectors often spoofed and used for phishing during the holiday season include popular large retail and/or electronics merchants, airlines and other travel booking sites, hotel and hospitality sites and other travel-related customer service sites, and luxury goods retailers.

The advancement of artificial intelligence (AI) over the past year provides threat actors with the ability to create highly customized phishing campaigns and lures that closely mimic the impersonated brand and are typically free of any spelling or grammatical errors, meaning cardholders may fall victim to phishing attempts at a higher frequency than in previous years. Threat actors may also use SEO techniques to 'push' their phishing websites, which commonly impersonate legitimate merchants' websites, higher in search engine results in order to increase the likelihood of a cardholder accessing their phishing site. The threat actors will then obtain payment account details or PII from the cardholders who visit their phishing webpage.

Additionally, threat actors will create fake merchants that can operate phishing websites and place advertisements, usually showing heavily discounts prices on popular or luxury items, on social media and other platforms to entice cardholders to visit their website. When the cardholder initiates a purchase on the fake merchant's checkout page, the threat actors obtain their payment account data and PII and also receive funds into their merchant account.

- **ATM / POS Skimming: With the increase in foot traffic at brick-and-mortar merchants and ATMs due to the increase of in-person shopping and travel during the holiday season, threat actors will also likely seek to target ATM and POS terminals with skimming attacks.** In these skimming attacks, threat actors place a removable device, known as a "skimmer", on an in-store, fuel pump, or ATM point-of-sale (POS) terminal to harvest the magstripe track data from payment accounts that are used at the targeted terminals. The threat actors will extract the compromised PANs from these skimmers and conduct fraudulent transactions at various retailers or cashout to their own accounts. Actors increasingly utilize "deep insert" skimmers skimmers to perpetrate ATM and POS skimming. Deep insert skimmers are thin devices placed inside the ATM or POS card reader and are much more difficult to detect as compared to skimming overlay devices, which are placed on top of the card reader. **Due to the physical increase in customer volume experienced during the holiday season by many brick-and-mortar merchants, threat actors can use the cover of a crowded shop to place a skimming device on a POS machine out of line-of-site of store employees. Additionally, as customers sometimes purchase a larger number of goods at brick-and-mortar merchants during this period, threat actors often hide their installation of a skimming device behind an armful of large products or blocked by an associate creating a disturbance or carrying a large amount of goods.**
- **OTP Bypass and Provisioning Fraud:** One-time-passcode (OTP) bypass is a method by which threat actors obtain the OTP provided to a cardholder during the user-authentication process by their issuing bank. PFD identified many OTP bypass schemes employed by threat actors to obtain cardholders' OTPs and gain access to cardholder accounts, including phishing campaigns, where threat actors create OTP templates sent to the victims during the purchase on phishing websites appearing to be associated with the purchase the victim is intentionally making. The victim provides the OTP into the phishing template and the threat actor then uses the OTP to complete their fraudulent purchase or transaction. **Due to the general increase in fraud monitoring that occurs during the holiday period, it is likely threat actors will use this increase as a phishing lure, pretending to be an issuing bank fraud center, or merchant where goods were "fraudulently" purchased using a stolen account, to contact victims in efforts to obtain sensitive information, such as OTP to bypass authentication or provision a stolen payment account.**
- **Physical Theft:** As consumers visit brick-and-mortar stores more frequently during the holiday season, threat actors may attempt to physically steal payment cards and/or phones from unsuspecting consumers in crowded retail stores, shopping malls, or parking lots. Threat actors will likely target unattended bags and purses, such

as those placed in shopping carts, or wait for cardholders to exit a retail store. As the cardholder is exiting, the threat actor will attempt to steal the cardholder's physical payment card and then re-enter the store to make a purchase on a high-end luxury item using the stolen card.

- **Shopping Bots:** Online merchants will likely see an increase in bot attacks during the holiday season. Bots are increasingly more complex and strive to imitate humans as well as circumvent security measures like IP blockers and CAPTCHAs that are intended to identify and prevent bots on a merchant's site. Bots-as-a-service offerings made it possible for anyone to easily purchase and deploy bots. **There are several types of bots popularly used by threat actors during the holiday shopping season: Grinch bots, for example, buy the popular toys or items of the holiday season then resell the items at a higher price. "Freebie" bots hunt for items that are mismarked at low prices. There are also bots that target limited-edition items to buy in bulk and resell.** Despite efforts made to combat the bot problem in eCommerce, retailers strive to find a balance between ease of user experience and checkout security.

2. Recommendations

Visa recommends the following **consumer best practices** to prevent financial and scam-related fraud:

- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Maintain device and software security by keeping software patched and up-to-date.
- Ensure Multi-Factor Authentication (MFA) is implemented on all sensitive log in environments.
- Use cybersecurity best practices, including enabling anti-phishing protection on your web browser, adding multi-factor authentication to account log ins, using unique, strong passwords for different accounts, not clicking on unsolicited links, and remain vigilant of the URLs you are visiting.
- Contact your bank directly by using the phone number or website listed on the back of your card, rather than following guidance from an email, phone call, or text message you received.
- Never provide a one-time-passcode to a caller, or via email or SMS text message, and do not install Remote Access software unless instructed by a trusted system support provider.
- Check shipping details on accounts. Be aware of details in the 2nd or 3rd lines of the shipping addresses that might be used to reroute packages.
- Review bills, bank statements, and credit reports to identify anomalies that could indicate fraud, identity theft, or if someone else has access to your account.
- Sign up for purchase alerts with your card issuer. Purchase alerts are customizable, can be received via email or text, and can be used to confirm legitimate purchases or notify you of suspicious activity.
- Look for the "s" – When paying online, check the URL to ensure it begins with "https://". The "s" at the end indicates a secure connection. Additionally, check that the name of the web page does not contain spelling errors or strange characters.
- Update system and application software – Install the latest software on your computer, tablet, or phone.
- Use tokens when possible. A token can be viewed as a "secret code" that contains no customer or sensitive data, which can be used to transmit a payment. Use of a token for a purchase, or tokenization, is the digital equivalent of using a card's chip for in-person purchase. The value of the token changes with each transaction, making them more resistant to use by fraudsters.
- Take advantage of identity and credit monitoring services. These services may be provided by your bank/credit union, credit card provider, employer, or insurance company.

- Watch for scam indicators in the method of payment being requested: scammers often ask for payment in the form of wire transfers or other money transfers, reloadable or prepaid gift cards, cryptocurrency, or sending cash, since these formats are more difficult to trace.
- If you suspect a scam, stop and talk to someone you trust about the situation and seek guidance from the organization's official website before acting on the suspected scammers request.
- Use caution when posting on social media. Be aware that sharing sensitive personal information can provide criminals with clues to answer your security questions or craft believable, targeted scam messages.

Visa recommends the following best practices **for banks** to prevent phishing and related fraud:

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Verify recent changes to customer and cardholder account information by contacting through established channels and methods.
- Employ the principle of least privilege and grant personnel only the access needed to complete job requirements. Segment sensitive network environments, such as the cardholder data environment, from other corporate networks to prevent lateral movement by threat actors.
- Ensure Multi-Factor Authentication (MFA) is implemented on all administrative user accounts and across the enterprise, and utilize strict password policies.
- Require Multi Factor Authentication (MFA) when provisioning a PAN to a mobile device and use secure one-time-passcode delivery methods such as dedicated one-time-passcode applications.