Current Payment Ecosystem Threats

Megan Munroe

Ph.D., Intelligence and Cybercrime Sr. Consultant

Visa Payment Ecosystem Risk and Control

Notice of confidentiality

This presentation is furnished to you solely in your capacity as a customer of Visa Inc. and/or a participant in the Visa payments system. By accepting this presentation, you acknowledge that the information contained herein (the “Information”) is confidential and subject to the confidentiality restrictions contained in Visa’s core rules and product and service rules/or other confidentiality agreements, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non public information would constitute a violation of applicable U.S. federal securities laws.

Disclaimer

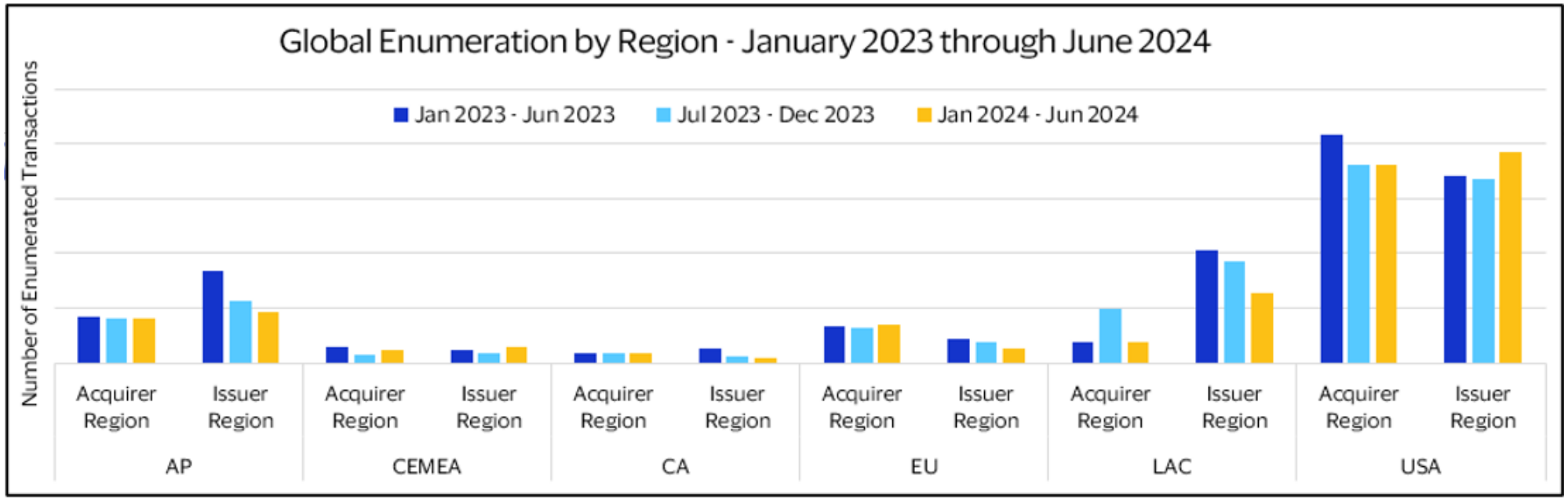
Case studies, research and recommended practice recommendations are intended for informational purposes only and should not be relied upon for marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances The actual costs, savings and benefits of a card program may vary based upon your specific business needs and program requirements. Visa makes no representations and warranties as to the information contained herein and member is solely responsible for any use of the information in this presentation in connection with its card programs.

Agenda

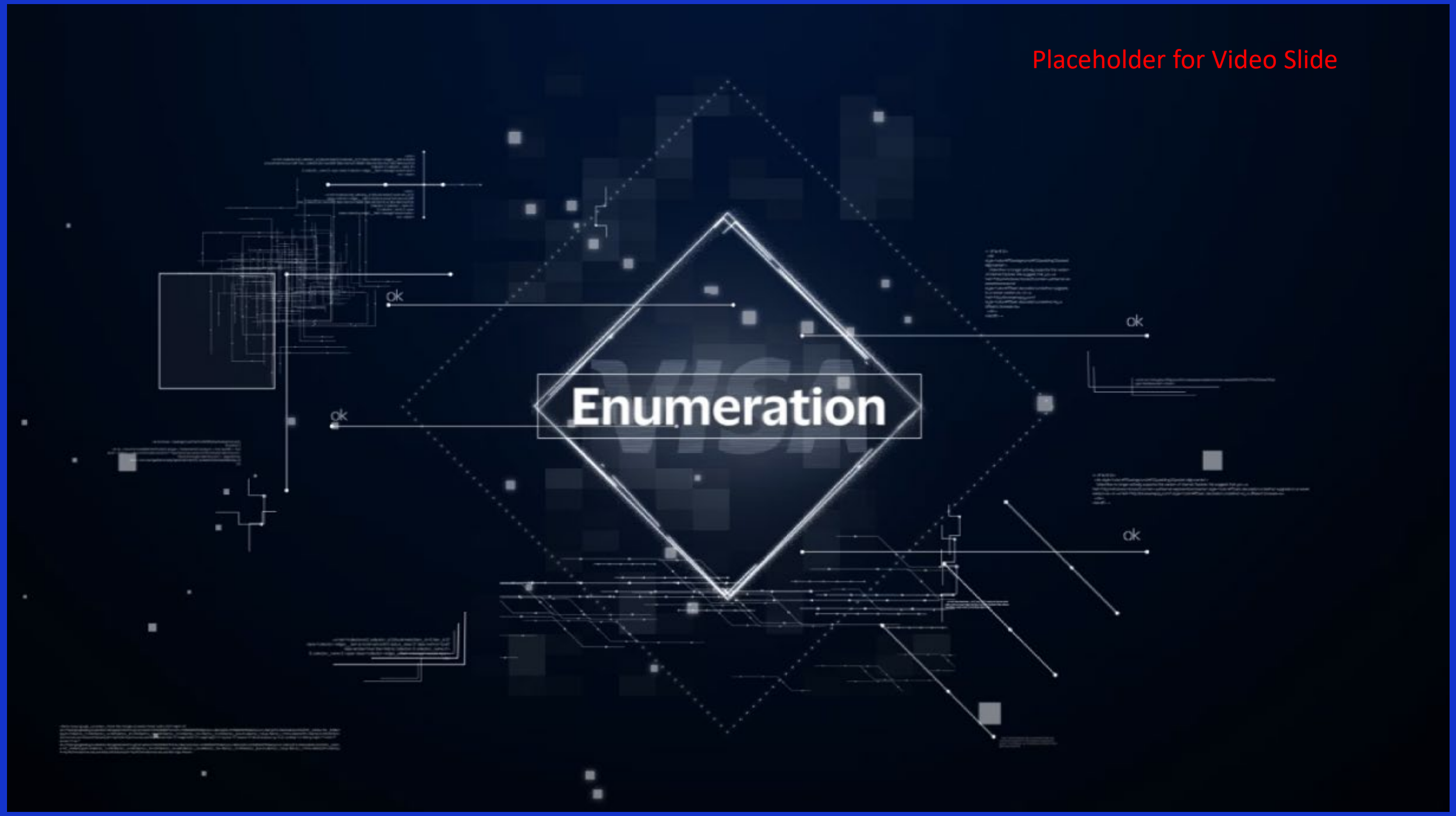
1. Enumeration
2. Exploitation of System Misconfigurations
3. Targeting of Consumers
4. Increase in Scams
5. What Can We Do

Enumeration

Enumeration and Account Testing



Visa PFD vigilantly monitors for enumeration attacks through the **Visa Account Attack Intelligence (VAAI)** capability using machine learning to identify enumeration attacks. VAAI then analyzes the details of the attack and enables Visa to notify affected acquirers/merchants and help affected acquirers/merchants block egregious attacks.


Placeholder for Video Slide
Enumeration
ok
ok
ok
ok

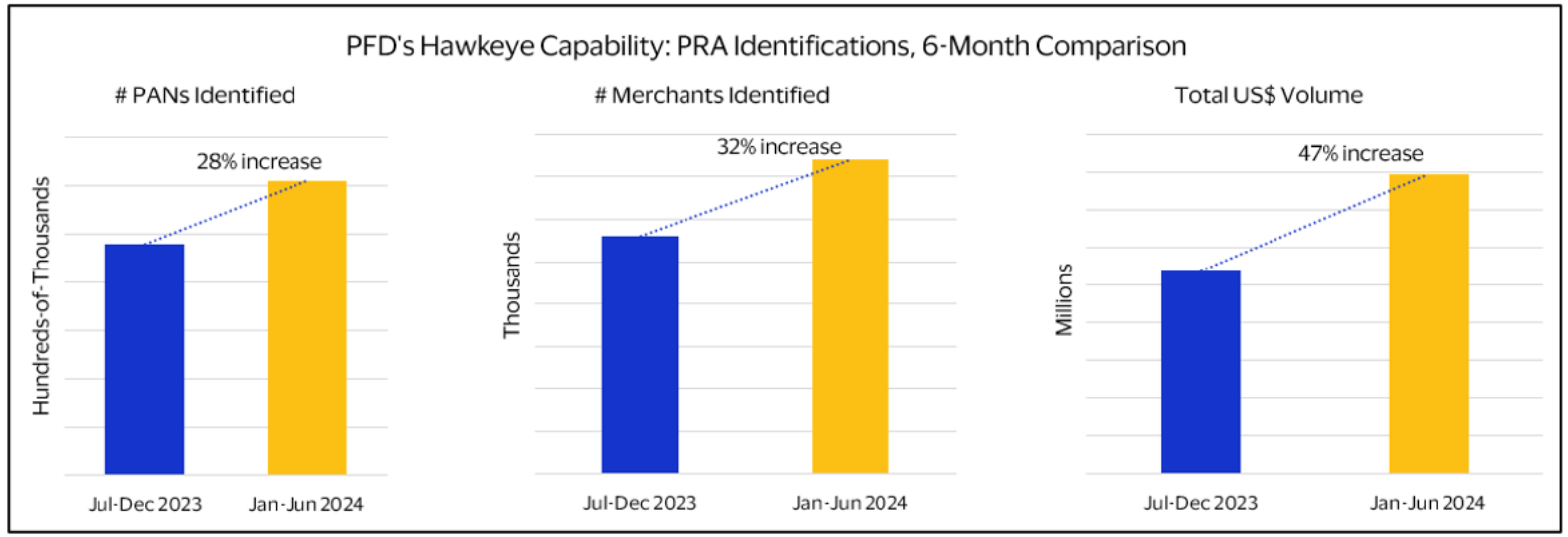
Exploitation of System Misconfigurations

Exploitation of System Misconfigurations

- Automated Fuel Dispenser Fraud
  - **373% increase** from the assessed fraud total From Jan-Jun 2024 compared to Jul-Dec 2023

- NFC code used in malicious app “offline transaction” fraud
  - https://www.texasbankers.com/fcic-issues-bulletin-on-merchant-processing-app-crimes/

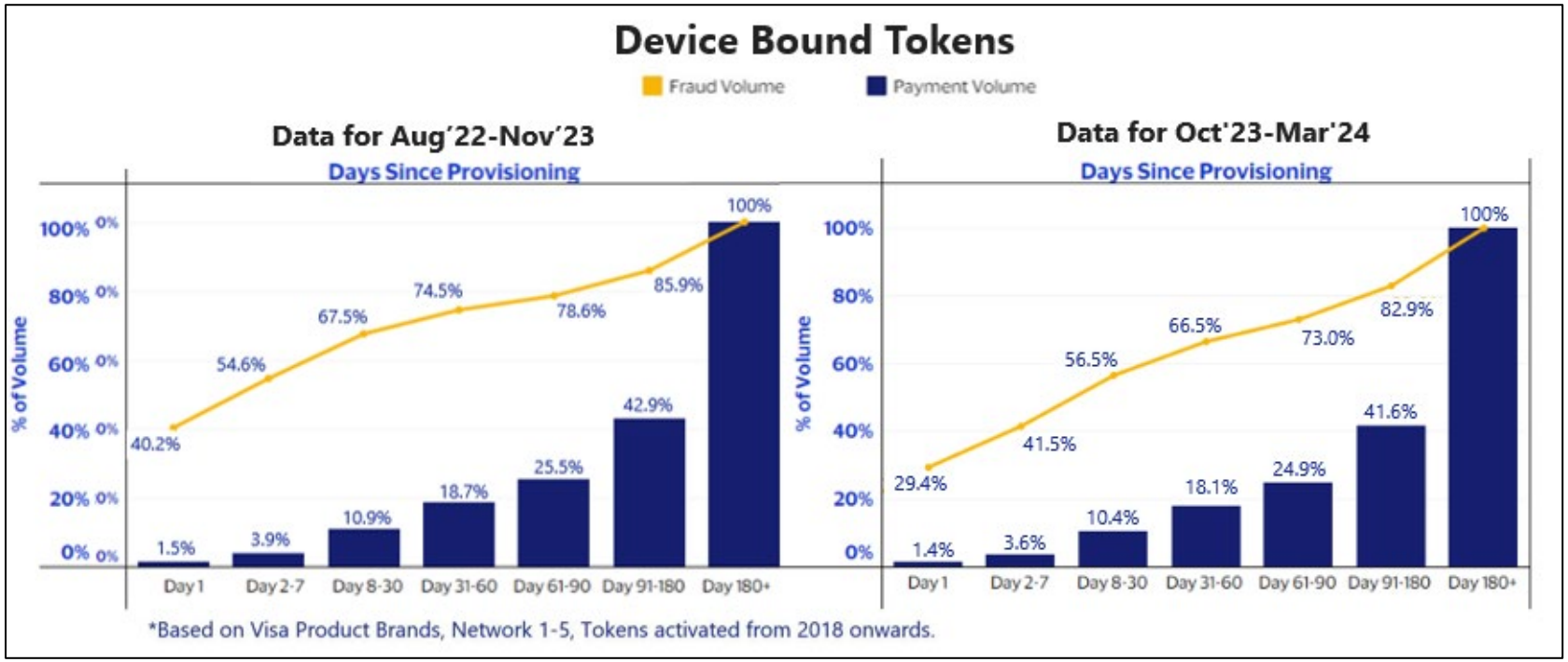
- Purchase Return Authorization Attacks



Targeting of Consumers

Threat Actors Increasingly Target Consumers

- Cashout times increase in provisioning fraud



- OTP-bypass scheme targets digital wallets with relay activity: "**Ghost Tap**"
  - https://www.threatfabric.com/blogs/ghost-tap-new-cash-out-tactic-with-nfc-relay

- Threat actors target **travel and holiday periods** with consumer-focused scams

VISA

Top Holiday Threats

What Fraudsters Want

Account Takeover

Scammers take over accounts by convincing victims to hand over data, such as one-time passcodes (OTPs), that allows them to bypass account authentication. They often use phishing and social engineering to trick victims into providing OTPs.

Theft of Data

Scammers steal payment data and personal information through social engineering and malware. Tactics include phishing, fake websites, and infecting victims' devices with malware.

Theft of Funds

Scammers use stolen data and account takeover to withdraw funds, buy goods to resell, or transfer money. They also create fake online stores and websites to steal money from victims.

Top Holiday Threats

Top 5 Ways Fraudsters Will Try to Get What They Want This Holiday Season

1. Phishing and Social Engineering

Email Phishing: Common holiday scams include discounted goods/shopping deals or fake black Friday deals, heavily discounted travel deals, and spoofed well-known and in-demand brands/merchant emails.

Phone Phishing: Common holiday phone scams include bank impersonation scams, utility/services impersonation scams, and charity/donation scams.

Text Message Phishing: Common holiday scams include package delivery scams, prize or free giveaway scams, and financial/account problem text messages.

Social Engineering: Common holiday scams include seasonal job scams, fake charities and donation scams, and year-end flexible spending account schemes.

VISA

Top Holiday Threats

Top 5 Ways Fraudsters Will Try to Get What They Want This Holiday Season

2. Scam Merchants

Scammers create ***fake merchants*** and advertise heavily discounted popular or luxury items on social media and other platforms to lure shoppers to their websites. One third of 2023 holiday shoppers polled in the 18-44 age group said they experienced fraud from purchasing a product they found by clicking a ***social media advertisement.***

3. Holiday Travel Scams

- ***Fake Travel Websites***: Pretending to offer travel services or spoofing airlines
- ***Phishing Emails***: Impersonating airline officials to send fake flight cancellations
- ***Call Center Scams***: Using malicious advertising to promote fake sites, leading victims to chat with fake customer service reps who steal payment details
- ***Fake Rental Listings***: Posting fake accommodation listings with stolen photos and descriptions, often at below-market prices. Victims pay for non-existent rentals.

Top Holiday Threats

Top 5 Ways Fraudsters Will Try to Get What They Want This Holiday Season

4. Malicious Holiday Apps

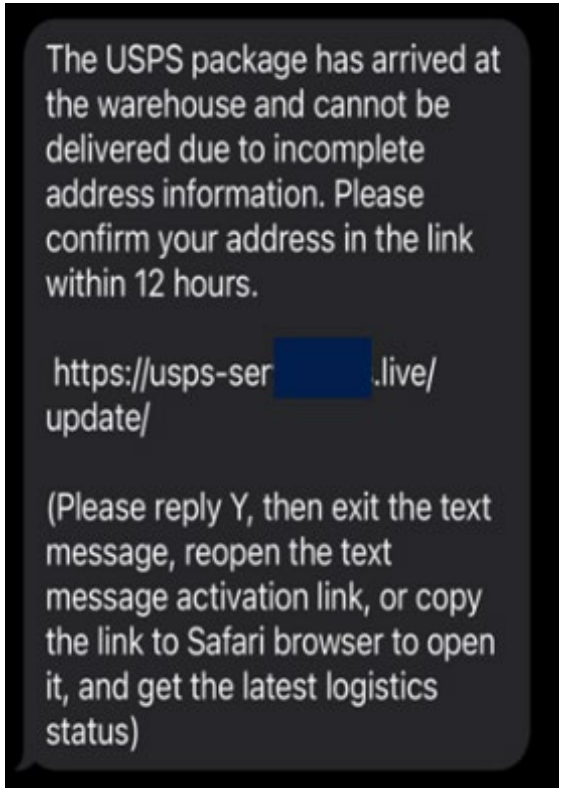
That adorable Santa tracking app that you see advertised on social media that has few or no reviews and requires you to download it by clicking a link rather than visiting a known and trusted app store…*Beware*! Scammers create new apps or ***imitate legitimate apps*** that, when downloaded, ***infect devices*** and ***steal sensitive data*** like login credentials and payment information.

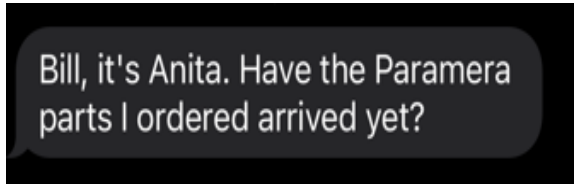
5. Physical Theft

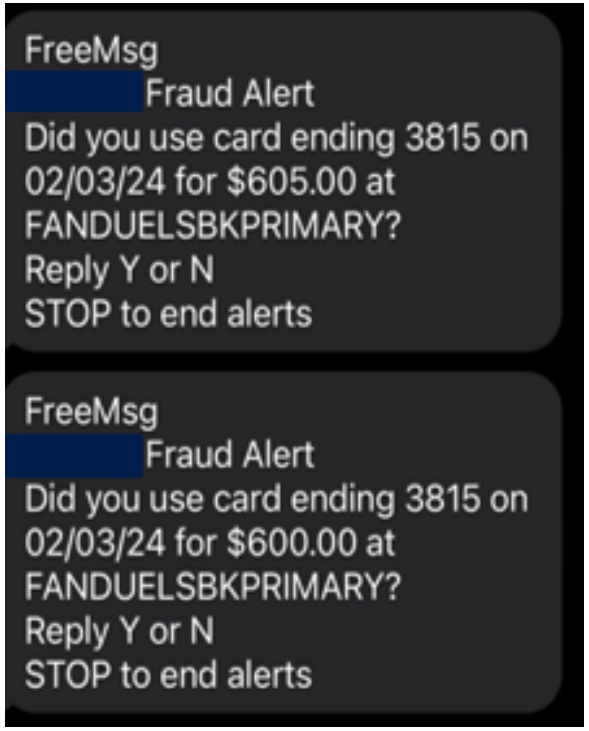
- ***Physically steal payment cards*** or phones from consumers in crowded stores, malls, or parking lots.
- Steal card data by targeting ATMs and POS terminals with ***skimming attacks***.
- Steal money through "***digital pickpocketing***" - using mobile point-of-sale devices to conduct fraudulent contactless transactions by tapping against a victim's purse, wallet, or pocket.

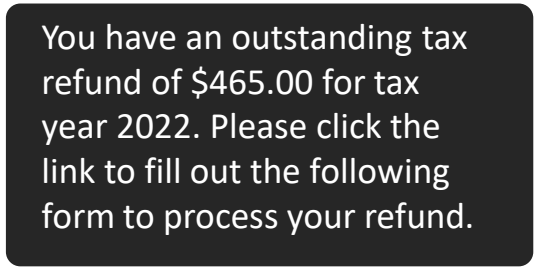
Increase in Scams

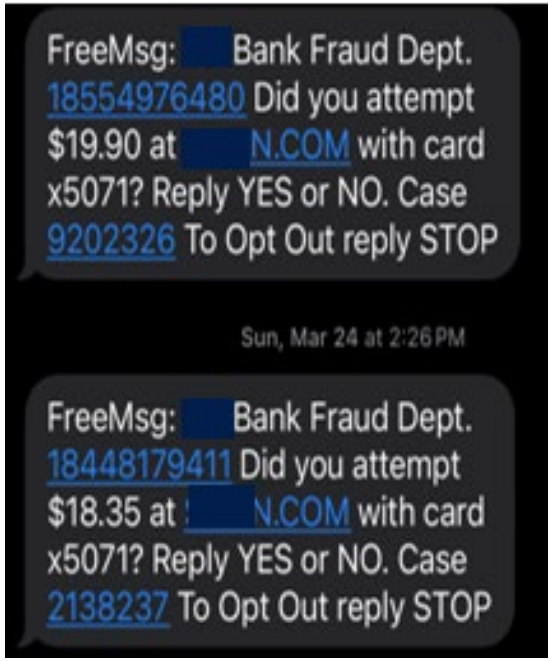
Smishing Scams

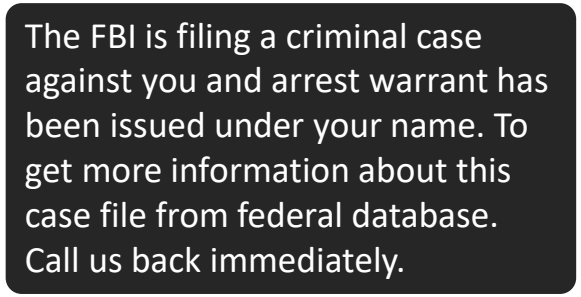




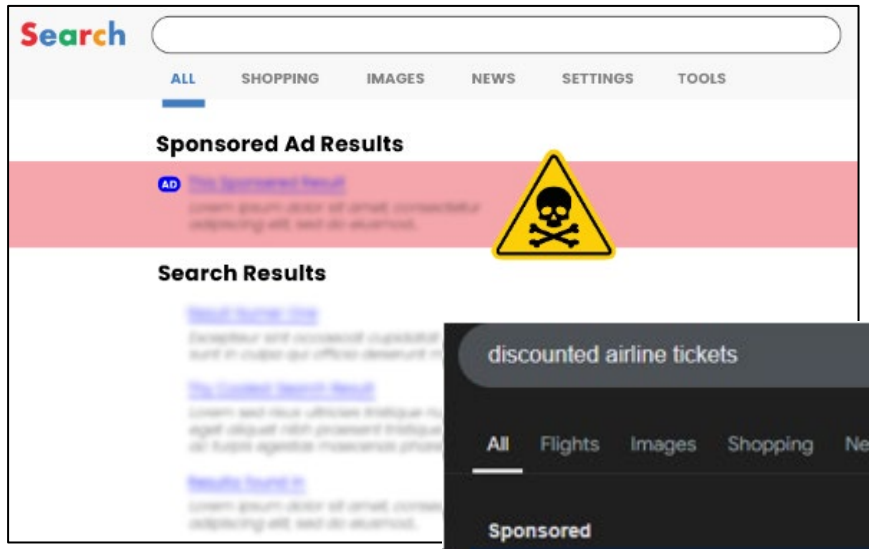




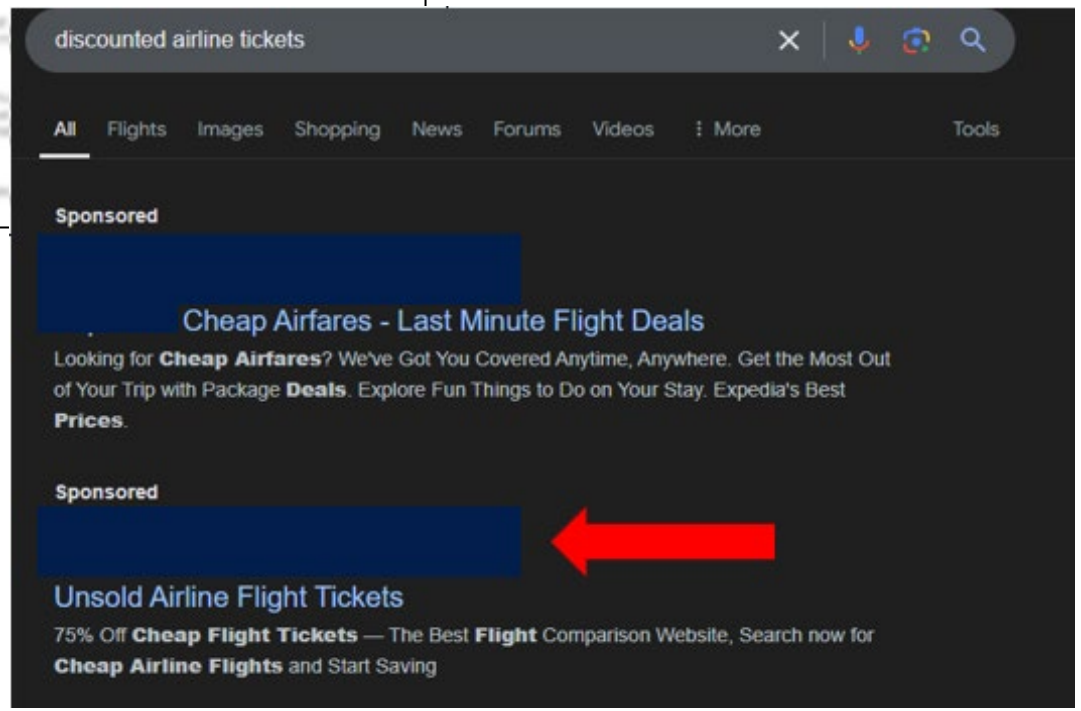


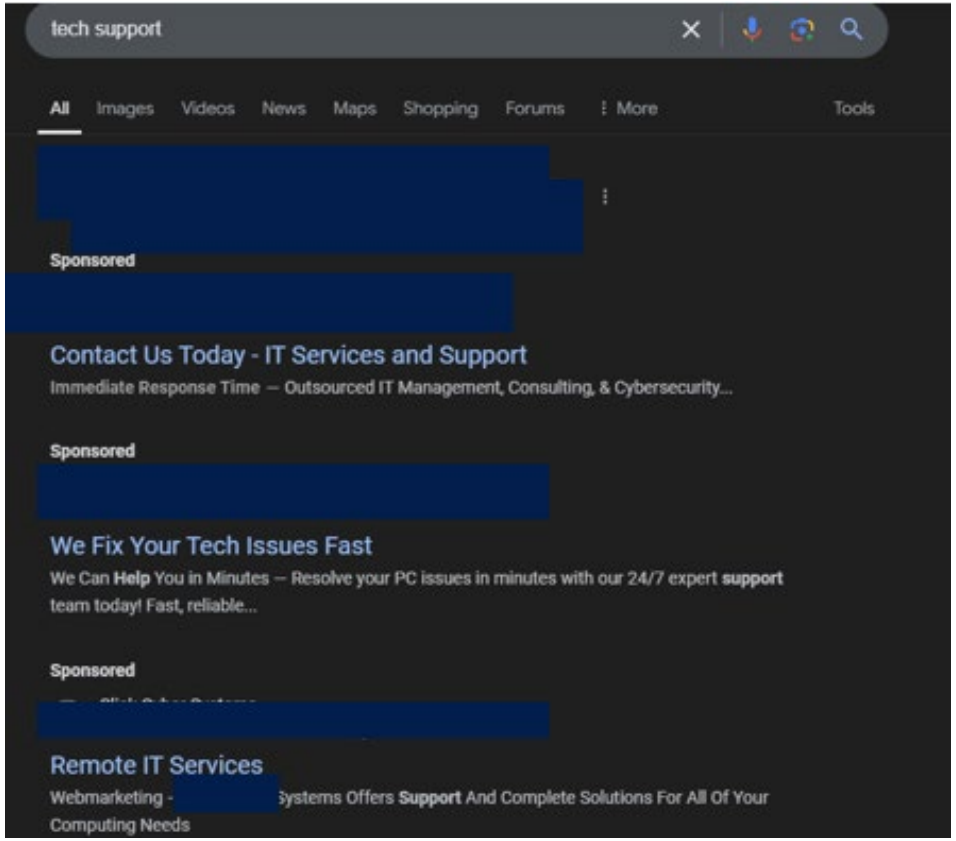


Malicious Advertising and Illicit SEO



Visa PERC identified a **284% increase** in fake and spoofed merchant websites as compared to the prior 4 months.



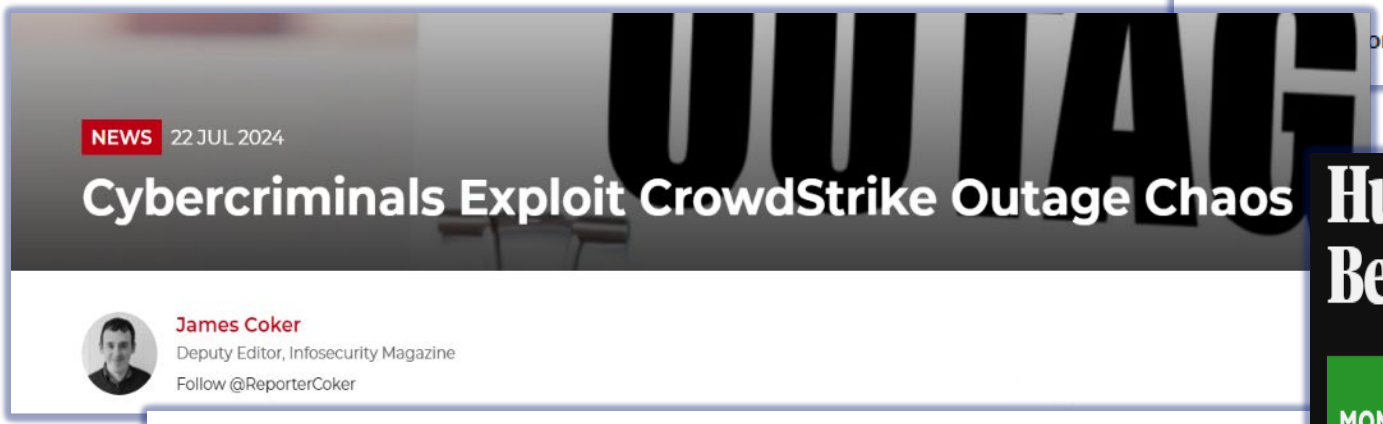


Opportunistic Scams

Ukraine war: Investigation finds hundreds of fake charity websites

5 May 2022

ord & Tony Smith



Hurricane fraud is on the rise, feds warn. Beware these scams.

MONEY WATCH

By **Megan Cerullo**
Edited By **Alain Sherter**
October 8, 2024 / 4:41 PM EDT / CBS News

Home > News > Security > Ticket Heist fraud gang uses 700 domains to sell fake Olympics tickets

Ticket Heist fraud gang uses 700 domains to sell fake Olympics tickets

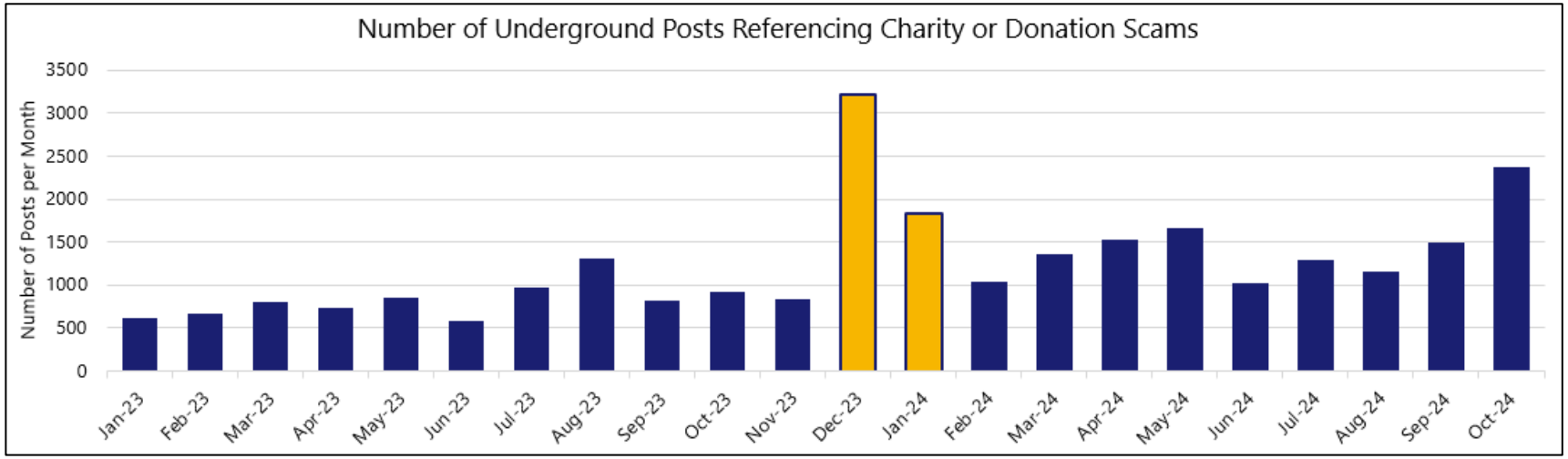
By **Ionut Ilascu** July 10, 2024 06:33 AM 0

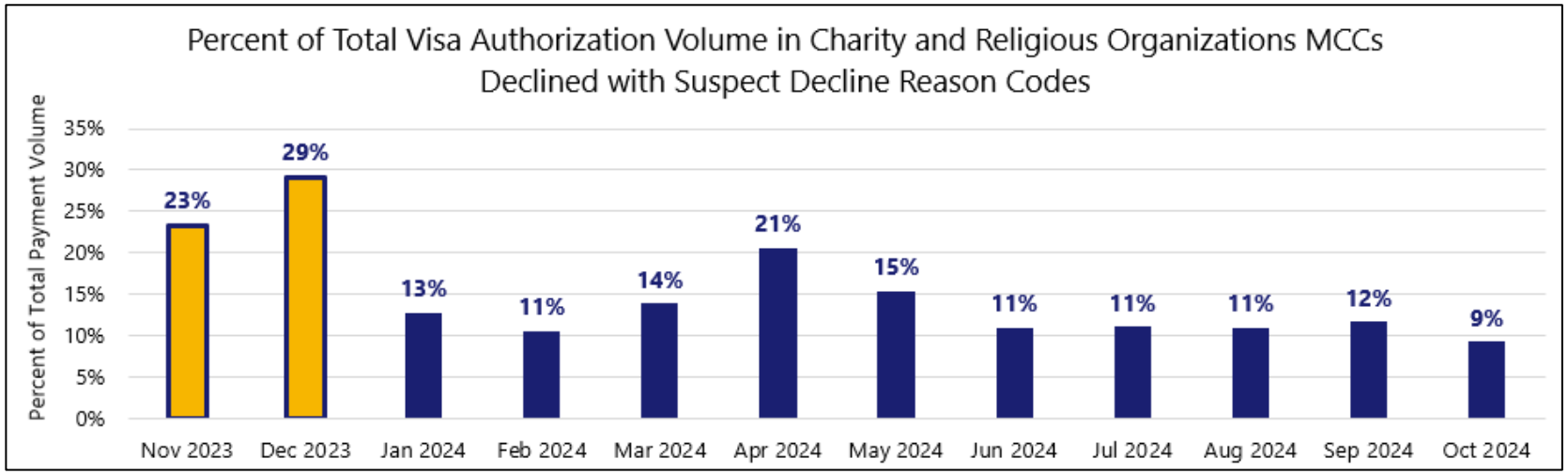
VISA

Charity and Donation Scams

- **Fake Charities**
- **Spoofed Real Charities**

- Phishing
- Matching Scams
- Celebrity Impersonation
- Exploitation of Conflicts & Disasters





What We Can Do

Scam Prevention: What can consumers do?

Scam Prevention Recommendations

- **Do not act immediately.** Stop and talk to someone you trust about the situation and seek guidance from the organization's official website.
- **Watch for scam indicators in the method of payment being requested**: scammers often ask for payment in formats that can be more difficult to trace, such as reloadable or prepaid gift cards, cryptocurrency, or money transfers, which can be initiated with a debit or credit card transaction. Sending cash or initiating wire transfers or other types of money transfers are also popular requests from fraudsters.
- **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.
- **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 an unknown caller**, or via email or SMS text message, and never install Remote Access software unless instructed by a trusted system support provider.
- **Review bills, bank statements, and credit reports** to identify unauthorized charges, and sign up for purchase alerts with your card issuer to notify you of suspicious activity.
- **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.

Use cybersecurity best practices

- **Enable 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.
- **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 from legitimate and verified sources.
- **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.

How Visa is Helping

Ecosystem Protection and Risk-as-a-Service

1. **Around-the-clock Global Vigilance:**
   24x7x365 global monitoring and actioning of fraud risk performance by trained Visa risk professionals via Risk Operations Center.

2. **Enumeration & Contextual Defense:**
   Service that identifies and helps clients block enumeration attacks to detect fraud transactions in specific contexts (e.g. high-risk MCCs or specific fraud balanced with legitimate transactions)

3. **Proactive Vulnerability Testing:**
   Testing service that helps proactively identify vulnerabilities before they can be exploited and monetized by criminals

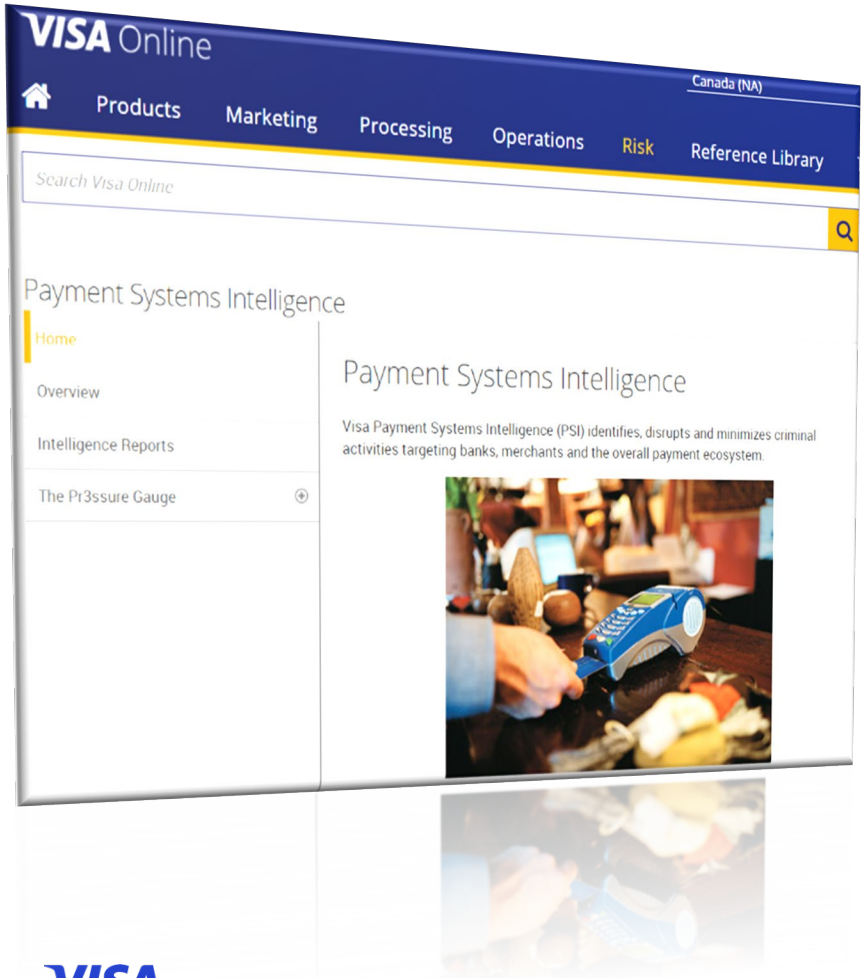
4. **Fraud Intelligence and Analytics:**
   Gather and analyze intelligence on how fraudsters exploit vulnerabilities; use intel to shape fraud defenses both proactively and retroactively

5. **Client and Consumer Education:**
   Publication of security alerts, public notices, best practices, and coordination with media to help educate consumers

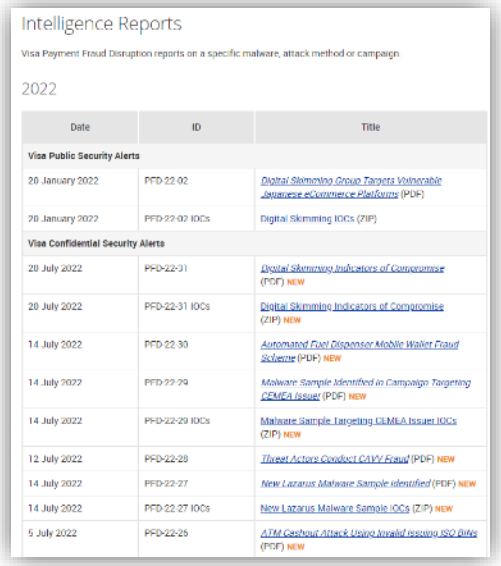
VISA

Stay informed of Security Alerts from Visa's Payment Fraud Disruption team

Visa Access Page: Payment Systems Intelligence is updated weekly – Reporting Repository



Intelligence Reports


Intelligence Reports

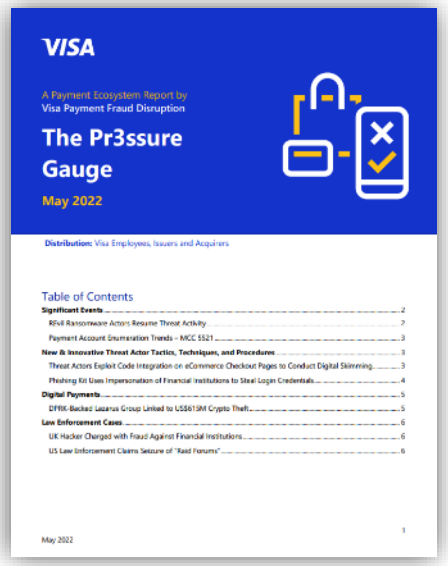
Visa Payment Fraud Disruption reports on a specific malware, attack method or campaign.

2022

Date	ID	Title
Visa Public Security Alerts		
28 January 2022	PFD-22-02	*Digital Skimming Group Targets Vulnerable Japanese eCommerce Platforms* (PDF)
28 January 2022	PFD-22-02 IOCs	Digital Skimming IOCs (ZIP)
Visa Confidential Security Alerts		
20 July 2022	PFD-22-31	*Digital Skimming Indicators of Compromise* (PDF) NEW
20 July 2022	PFD-22-31 IOCs	Digital Skimming Indicators of Compromise (ZIP) NEW
14 July 2022	PFD-22-30	*Automated Fuel Dispenser Mobile Wallet Fraud Scheme* (PDF) NEW
14 July 2022	PFD-22-29	*Malware Sample Identified in Campaign Targeting CEMEA Issuer* (PDF) NEW
14 July 2022	PFD-22-29 IOCs	Malware Sample Targeting CEMEA Issuer IOCs (ZIP) NEW
12 July 2022	PFD-22-28	*Threat Actors Conduct CNP Fraud* (PDF) NEW
14 July 2022	PFD-22-27	*New Lazarus Malware Sample Identified* (PDF) NEW
14 July 2022	PFD-22-27 IOCs	New Lazarus Malware Sample IOCs (ZIP) NEW
5 July 2022	PFD-22-26	*ATM Cashout Attack Using Invalid Issuing ISO BINs* (PDF) NEW

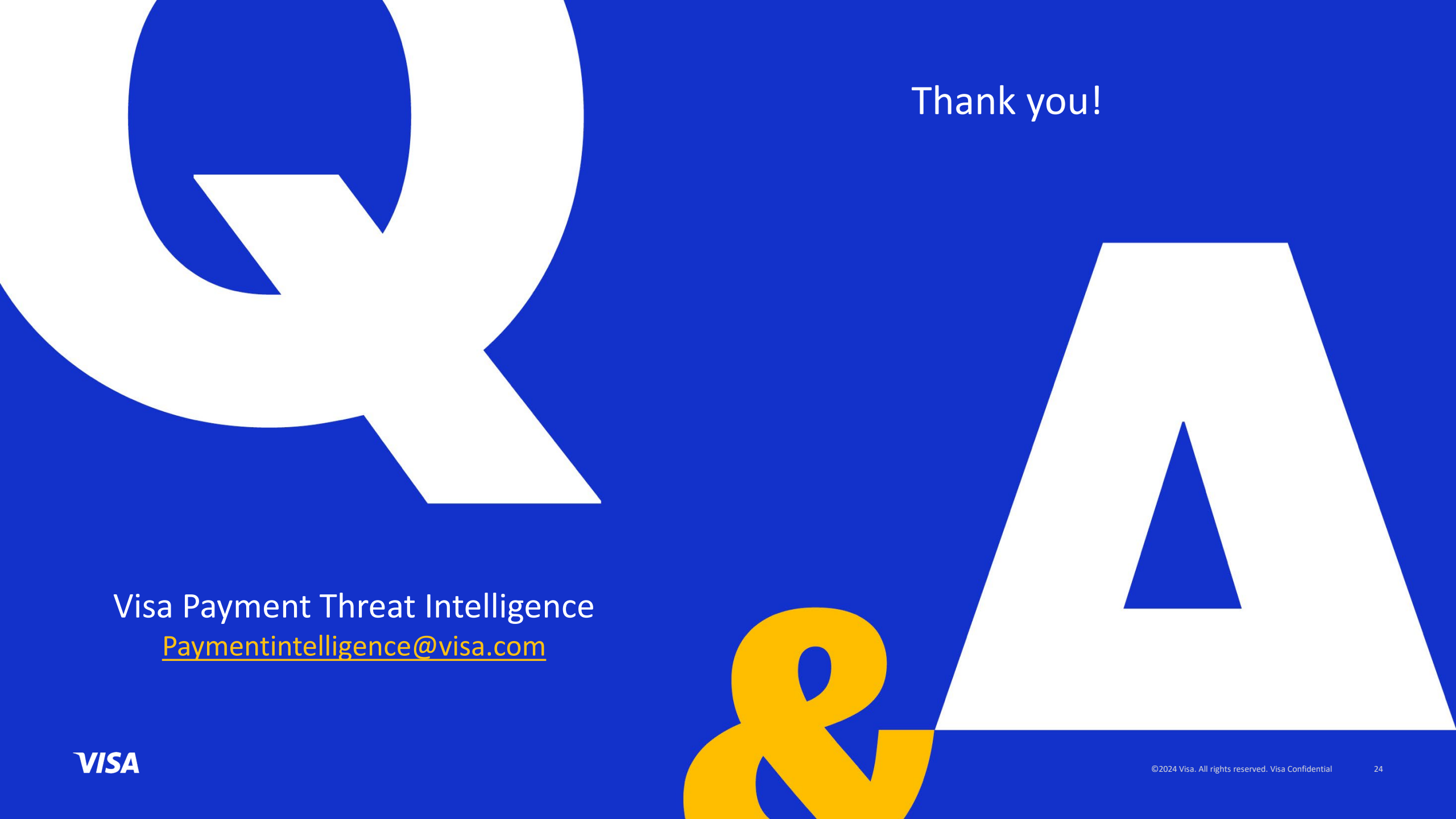
Biannual Report

The Pr3ssure Gauge



Contact Paymentintelligence@visa.com or your Visa Account Executive for subscription

Thank you!



Visa Payment Threat Intelligence
Paymentintelligence@visa.com

VISA