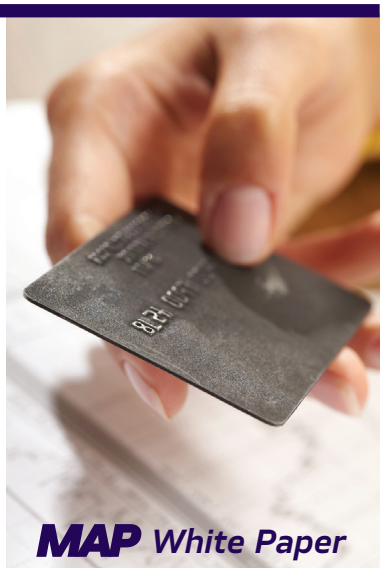
MEMBER ACCESS PROCESSING

Dynamic Payment Solutions. Trusted Results.



Importance of Cybersecurity Amid Shifting Threats

Whether in-person or online, cybercriminals target payments touchpoints with sophisticated fraud techniques

Cybercriminals are showing no signs of slowing down as they employed a variety of schemes to defraud consumers, acquirers, card issuers, and merchants, according to Visa Inc.'s 2023 Biannual Threats Report. While fraud early on during the COVID-19 pandemic was concentrated on online scams, in-person attacks are now trending higher as criminals widen their scope to once again capture physical targets. The past year experienced an increase in card-present threats such as physical skimming on ATM and point-of-sale terminals – a trend that will likely persist. For instance, from June – November 2021, Visa saw a 176% increase in physical skimming devices over the previous 12-month period[1].

Cryptocurrency can be a prime place for cybercriminals.
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. 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.

Skimming attacks are becoming more common.
We've seen a major uptick in skimming over the past six months. In fact, skimming cases increased 174% in the June 2022-November 2022 period when compared to December 2021 May 2022. Digital skimming, which is when threat actors deploy malicious code onto a merchant website targeting their checkout pages to steal account data entered by

consumers. These digital skimming attacks are often the result of misconfigurations or lack of security controls, and merchants of every size can help prevent these attacks by ensuring their software is up to date.

The U.S. is the primary target for enumeration attacks.
Enumeration, which is the programmatic, automated testing of common payment elements via ecommerce transactions to effectively guess the full payment credentials, remains among the top threats to the payment ecoysystem. Interestingly, 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).

Still, the digital commerce environment – vastly accelerated by the pandemic – remains the richest target for cybercriminals.

Nearly three-fourths of fraud and data breach cases investigated by Visa's Global Risk team involved e-commerce merchants – often social engineering and ransomware attacks. Digital skimming attacks targeting e-commerce platforms and third-party code integrations are common.

These attacks shine a light on the need for stringent security controls on merchant websites and checkout pages, ensuring external code is not enabled in sensitive cardholder environments. In fact, 42% of respondents in the MIT Technology Review Insights report say security measures are important for their customers, with 59% acknowledging that cybersecurity threats are the biggest challenge to expanding digital payments. Many are prioritizing advanced security capabilities like digital tokens (32%), artificial intelligence and enhanced authorization (43%).

Beyond attacks on traditional currency, threat actors are employing new tactics to defraud cryptocurrency users, including new malware focused on browser extension wallets for crypto users as well as innovation in phishing and social engineering schemes. Crypto bridge services are also a target. From January through February 2022, three sizeable thefts exploiting vulnerabilities in various bridge services netted cyber thieves over $400 million.[2]

Protection Is Visa's promise
While cybercrime persists, Visa has increased its efforts to mitigate fraud. Over the past five years, Visa has invested more than $9 billion on network security. Visa employs more than a thousand dedicated specialists protecting Visa's network from malware, zero-day attacks and insider threats 24x7x365. Visa also deploys AI-enabled capabilities and always-on experts to protect its ecosystem, proactively detecting and preventing billions of dollars of attempted fraud. In fact, Visa's real-time monitoring with AI blocked over $4.2 billion in fraudulent payments volume in the last 12 months, preventing many from ever knowing they were at risk of a potential fraudulent transaction.

To read more of the Payment Fraud Disruption report, visit Biannual Threats Report (visa.com). To read the full MIT Technology Review Insights Moving Money in a Digital World report, visit Moving money in a digital world | MIT Technology Review.

---

1. Visa Global Risk Investigations, June - November 2021

2. Visa Biannual Payment Fraud Disruption Report

As the nation's only aggregator of the Visa Debit Processing Service platform for credit unions, Member Access Processing is in the forefront of providing industry-leading products and services to credit unions. MAP's special role in the marketplace provides our client credit unions the unique opportunity to leverage the Technology, Security, and Service of Visa for their members.

450 Alaskan Wy S - STE 246 | Seattle, WA 98104 | 866-598-0698 | www.MAProcessing.com