VISA SECURITY SUMMIT 2024

Media Round Table Summary

Introduction

The Visa Security Summit 2024, which took place in Dubai on March 6th and 7th, brought together over 350 attendees from 50 markets across Central and Eastern Europe, the Middle East, and Africa. This annual event welcomed C-suite executives and key decision-makers from issuers, acquirers, merchants, and fintech companies. Featuring two days of keynotes, panel discussions, and interactive breakout sessions, the summit served as a platform for Visa's global and regional executives, as well as top payments experts and risk leaders from the region and beyond, to discuss the redefinition of the security landscape.

In this report, we delve into the key insights and takeaways from the media round table.

Steering the New Security Paradigm

Charles Lobo, Regional Risk Officer, CEMEA, Visa

The pandemic accelerated e-commerce growth, compressing years of digital progress into months. Despite a post-pandemic return to face-to-face commerce, eCommerce continues to thrive. This **digital shift** reduced cash usage significantly, promoting inclusive growth by swiftly onboarding more people into digital commerce[1]. Notably, fraud rates have decreased alongside this growth[2], with contactless payments and tokenization enhancing transaction security. However, **consumers remain vulnerable**, necessitating ongoing industry efforts to combat evolving cyber threats amidst an increasingly complex payments ecosystem.

In 2023, Visa's **Stay Secure** campaign surveyed 6,000 individuals across 17 CEMEA markets, revealing concerning trends. Despite 56% claiming to be scam-savvy, 90% failed basic fraud tests, highlighting **costly overconfidence**. Additionally, 87% would respond to scam message types, demonstrating a need for heightened awareness. Furthermore, only 33% check critical communication details for fraud signs, emphasizing the consumer's role as the weakest link[3].

Cyber threats continue to evolve, with notable increases in purchase return authorization attacks, ransomware attacks, and enumeration attacks in the CEMEA region[4]. Visa's Global Fraud team employs AI-driven models and invests billions to counter these threats swiftly. Moreover, the rise of deep fakes and **AI proliferation poses new challenges**, with voice cloning[5] and polymorph malware becoming prevalent.

Ecosystem integrity and complexity have grown[6], evidenced by a 50% increase in registered payments facilitators and a 30% rise in transaction laundering identifications. **As merchants collect sensitive data**, tokenization emerges as a key security measure, with a 4.5X growth in network tokenization level[7] – above the 48% growth in credential-on-file merchant volume[8]. However, 84% of consumers surveyed seek assurance regarding their data protection before engaging with e-commerce merchants[9].

Key Takeaways:

- Visa prioritizes AI investments to combat fraud, ingesting vast datasets to identify crucial identifiers efficiently.
- The company enhances cyber defense capabilities through Risk-as-a-Service and collaboration with cybersecurity experts.
- Visa ensures ecosystem integrity by adapting programs to the evolving payments landscape, emphasizing trust as its foundation.

Spot a Scam – Understanding the Evolving Landscape

Michael Jabbara, Global Head of Fraud Protection, Visa

[1] Source: Adoption rates are based on VisaNet, Collections Only (excluding Cash) for CEMEA for December 2023 in comparison to December 2022
[2] Source: VisaNet, Collections Only and TC40 Data for CEMEA for 2020 – 2023 calendar years
[3] Source: Visa CEMEA Stay Secure study 2023
[4] Source: Visa CEMEA Stay Secure study 2023
[5] https://www.microsoft.com/en-us/research/project/vall-e-x/
[6] Source: Visa CEMEA Ecosystem Integrity database of program identifications for 2023 calendar year
[7] Source: VTS CoF Tokenization PV share in total CoF PV for CEMEA region in Q4 2023
[8] Source: VisaNet, Collections Only Card on File Payment Volume Data for CEMEA for Q4 2023 vs Q4 2022
[9] Source: Visa CEMEA Stay Secure study 2022

In 2025, cybercrime is projected to cost **$10.5 trillion globally**[10] – if this were a nation's GDP, it would rank as the world's third-largest economy.

Threat actors pursue two main avenues:

• **Exploiting vulnerabilities** in large service providers through network breaches and ransomware.

• Employing sophisticated **social engineering** tactics to target individual cardholders and compromise payment data.

Fraudsters innovate using open-source technology to streamline their operations. One prevalent method involves creating enticing **marketing materials** that prompt users to click on fraudulent links. Additionally, they provide **coding assistance**, simplifying the creation of fraudulent scripts. Dozens of tools and apps have emerged, covering various areas from audio synthesis to code generation.

Consumer-targeted scams are increasing in complexity and volume, resulting in an estimated **$1 trillion in financial losses in 2023**[11]. These include imposter scams, online shopping scams, social media/messaging platform scams, and prize/sweepstakes/lottery scams. A significant portion of consumers in CEMEA reported falling victim to online scams. In CEMEA, **52% of surveyed consumers** said they have been a victim of an online scam, 15% of them multiple times[12].

Visa responds by deploying top-tier tools, expertise, and processes to identify and mitigate fraud, investing over **$10 billion in technology** over the past five years. The Global Fraud team integrates security at the network level, focusing on addressing human vulnerabilities through technology.

With access to petabytes of data, Visa analyzes transaction patterns in real-time to identify potential compromises. Experienced risk analysts provide comprehensive 24/7 monitoring, offering real-time threat containment, rapid remediation, and comprehensive threat detection across cyber and payment fraud.

The impact of Visa's efforts[13] is evident:

• Blocking $40 billion in fraud payment value.

• Preventing 80 million fraudulent transactions.

• Averting over $122 million in estimated e-commerce fraud through malware detection.

• Blocking over $7 million in attempted fraud through AI and machine learning for a single client.

Looking ahead, threat actors will:

- Continue targeting consumers, exploiting their vulnerability as the easiest avenue for scams.
- Leverage global scale, orchestrating scams across regions with sophisticated organization and monetization strategies.
- Innovate social engineering tactics, evolving customer service impersonation schemes and exploiting compromised data.
- Exploit AI technologies, facilitating more widespread and sophisticated attacks.

<u>Key Takeaways:</u>

Visa continues to work with all industry players to empower consumers with:

- Personalized security through data insights and giving controls to end user (e.g. Visa Transaction Controls - allowing consumers control of specific category of merchants).
- Innovative solutions for intelligent authentication and verification.
- Convenience through secure device-based experience (Tokenization - enabling fast and secure payment experience).
- Zero liability is key to Visa's brand promise, with consumers given iron-clad assurance that they will not be held liable for fraudulent transactions outside of their control.

[10] Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[11] Source: Biannual Threats Report, December 2023. A Payment Ecosystem Report by Visa Payment Fraud Disruption
Global States of Scam Report, GASA
[12] Source: Visa Stay Secure study 2023
[13] Sources: Visa Payment Fraud Disruption Source; Visa Payment Fraud Disruption scorecard

Talking Tokens, Transacting Trust

Mehret Habteab, Head of Products and Solutions, Visa Europe

In today's rapidly evolving commerce landscape, the convergence of **trust, data, choice, and experience** is paramount. As consumers demand greater value from brands, factors such as brand alignment with personal values, sustainability efforts, and support during times of need are increasingly scrutinized[14].

The shift in consumer behavior towards seeking community trust and influencer validation for **financial decisions** underscores a desire to **minimize risks**[15], especially among younger generations like Gen Z and Gen A, who value autonomy and innovation.

Against this backdrop, trust emerges as a critical currency in the digital realm, essential for fostering confidence in digital payments. Fraud, a key detractor of trust, affects consumers across age groups, with **over 60%** of victims falling in the **18–44 age bracket**[16].

For Visa, trust forms the bedrock of its operations, underpinning its commitment to innovation, education, and ecosystem security. Tokenization, a foundational pillar of Visa's digital services, facilitates seamless and secure experiences by replacing sensitive card details with tokens. This technology not only **boosts sales conversion by over 5%** but also slashes fraud rates by **30-50%** compared to non-tokenized transactions.

Beyond traditional payment methods, **tokenization extends to diverse applications**, from in-car payments to personalized holiday offerings, offering consumers unprecedented control and convenience. With tokenization witnessing a surge in adoption across various domains, including e-commerce, it has emerged as a linchpin in Visa's quest to redefine the future of commerce.

As the ecosystem collaborates to drive consumer-centric experiences, Visa remains committed to building a trusted open network, empowering clients, and partners to deliver innovative solutions that cater to evolving consumer preferences, thereby shaping the commerce landscape of tomorrow.

Key Takeaways:

- Trust is pivotal: In the digital commerce landscape, trust serves as a cornerstone, fostering consumer confidence in payment transactions and brand interactions.
- Tokenization revolutionizes security: tokenization, a key aspect of Visa's digital services, replaces sensitive card data with tokens, enhancing security, boosting sales conversions, and slashing fraud rates.
- Consumer empowerment through choice: consumers, especially younger generations like Gen Z and Gen A, seek autonomy and innovation, driving demand for personalized and seamless experiences.
- Diverse tokenization applications: tokenization extends beyond traditional payment methods, facilitating in-car payments, personalized holiday offerings, and enhanced consent management for consumers.
- Collaboration drives future commerce: Visa advocates for collaboration across the ecosystem, empowering clients and partners to leverage innovative solutions that cater to evolving consumer preferences, ultimately shaping the future of commerce.

[14] Source: Value: Relationships Under Duress, CSpace and Hall & Partners, 2023
[15] Source: Kantar Global Monitor, November 2022; Kantar US Monitor Q2 2022; Kantar Global Youth Spotlight – GenZ & Retail
[16] Source: https://navigate.visa.com/europe/security/stepping-up-the-fight-against-fraud/