AUTOTIX

2024
The Year of FaaS
Professional Fraud Goes Industrial

ANNUAL REPORT & Q4 HIGHLIGHTS

Table of Contents

Fraud-as-a-Service (FaaS)

(noun) /frɔːd æz ə ˈsɜːrvɪs/:

The commoditization of fraudulent activities, enabled by digital platforms that offer tools, templates, and automation to scale identity fraud, deepfakes, and cyberattacks.

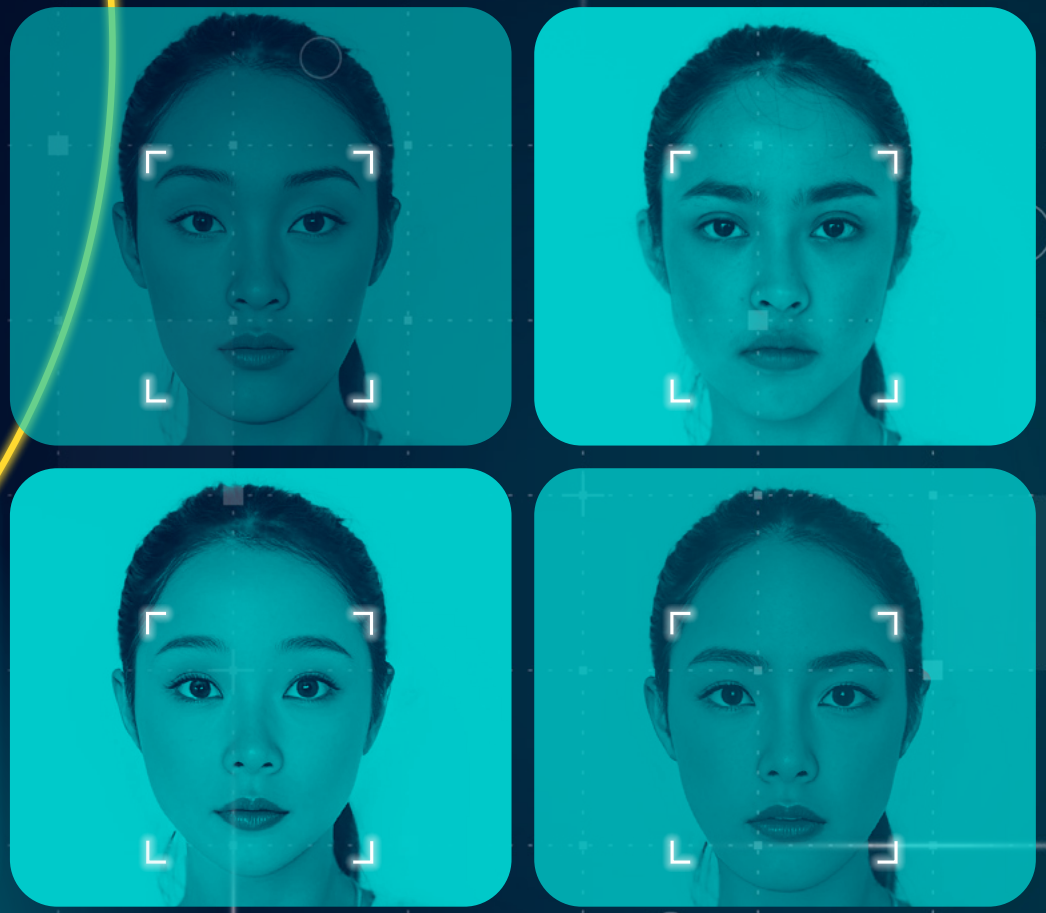
Foreword

2024 has been a game-changer in fraud prevention. Fraud-as-a-Service (FaaS) has taken cybercrime to a new level, enabling coordinated mega attacks that now average over 8,000 incidents each. With AI-powered tactics like deepfake selfies and synthetic identities, traditional defenses are being pushed to their limits.

But with challenges come opportunities. By embracing smarter fraud prevention strategies and layered defenses, businesses can get ahead of these threats and build stronger trust with their users. This report is here to guide you, offering practical insights to help you stay one step ahead.

Dan Yerushalmi, CEO, AU10TIX

FaaS: The Industry's Dark Engine



Disclaimer: This presentation contains AI-generated deepfake images. No real individuals are depicted; any resemblance to real persons is purely coincidental. These images are for demonstration purposes only.

Tools Fraudsters Access from FaaS Platforms

Deepfake Generators

Tools to create synthetic selfies and videos that may bypass liveness tests.

Botnets

Automate mass-scale credential stuffing and account takeovers.

Phishing Kits

Ready-to-use tools for email and web-based scams

Dark Web Marketplaces

A hub for buying stolen data and custom-fraud toolkits

FaaS enables plug-and-play kits, enabling even novices to execute complex attacks.*

*Source: BBC

We detected a single mega attack of **4580 unique permutations** spanning four geolocations and three industries.

AI-enabled FaaS scales attacks to **thousands** of accounts in minutes.

How FaaS Works

Imagine a fraudster operating from a remote location. They log onto a FaaS platform, select a “Pro Package”, and gain access to:

1. AI tools for generating synthetic identities
2. Bots for mass account creation
3. A deepfake generator to mimic ID liveness verification

It’s fast!

Within hours, the fraudster launches an attack targeting four continents and three industries.

A breakdown of FaaS operations:

Data Aggregators: Selling stolen identities and PII.

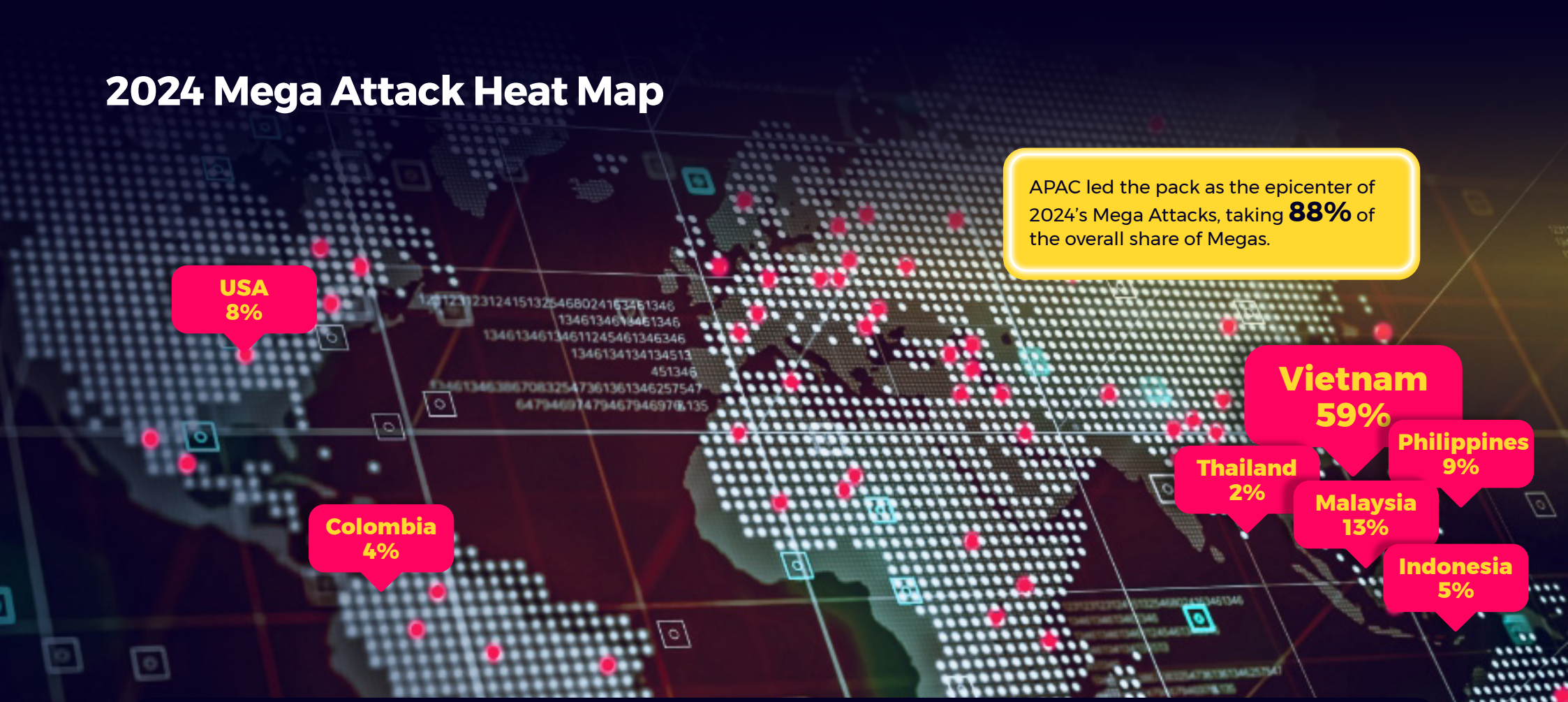
AI Synthesizers: Generating synthetic identities.

Bot Coordinators: Scaling and automating fraud attempts.

These advancements have led to substantial financial losses, with predictions of U.S. **fraud losses reaching $40 billion by 2027.***

***Source:** Wall Street Journal

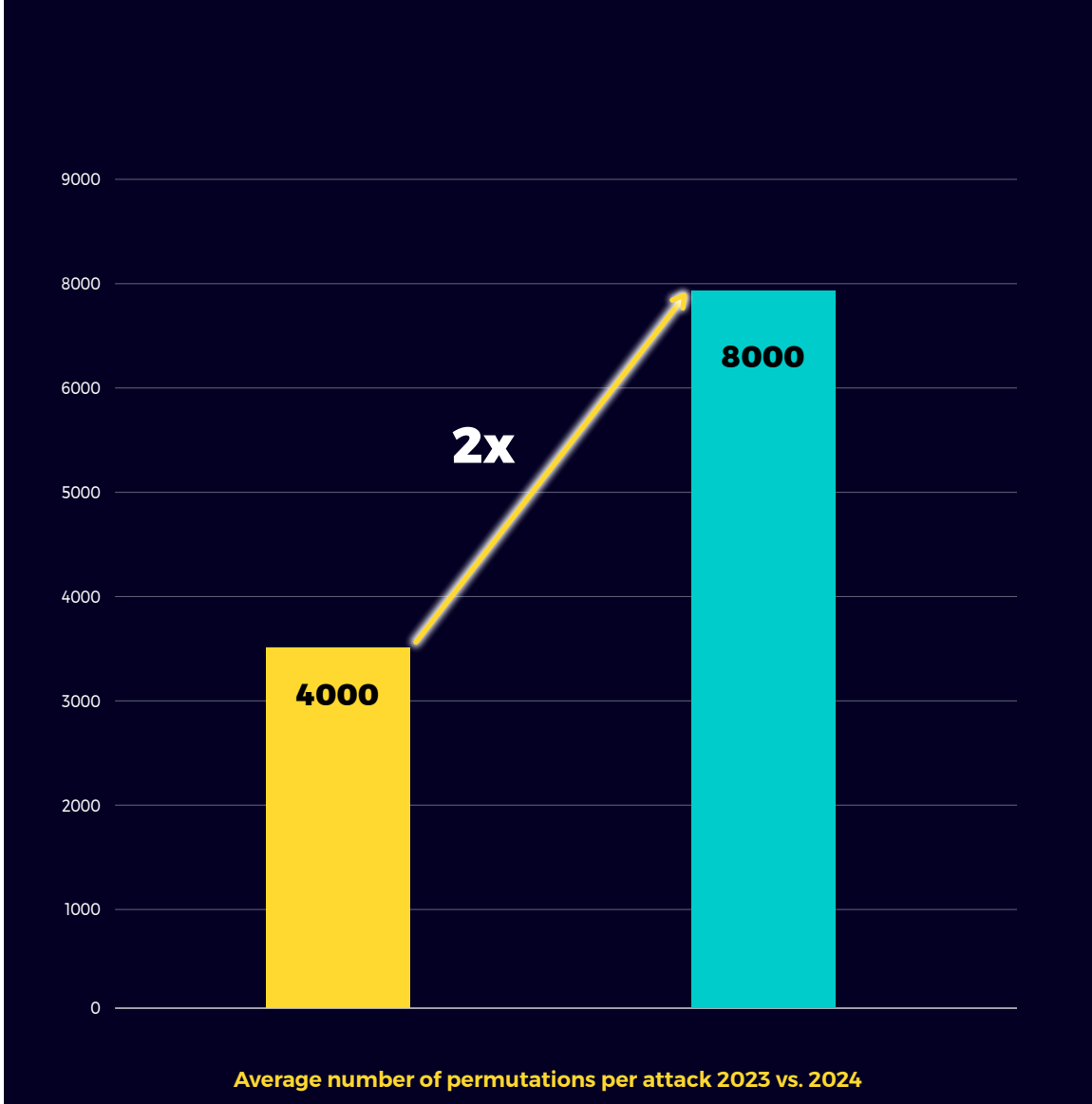
2024 Mega Attack Heat Map



APAC led the pack as the epicenter of 2024's Mega Attacks, taking **88%** of the overall share of Megas.

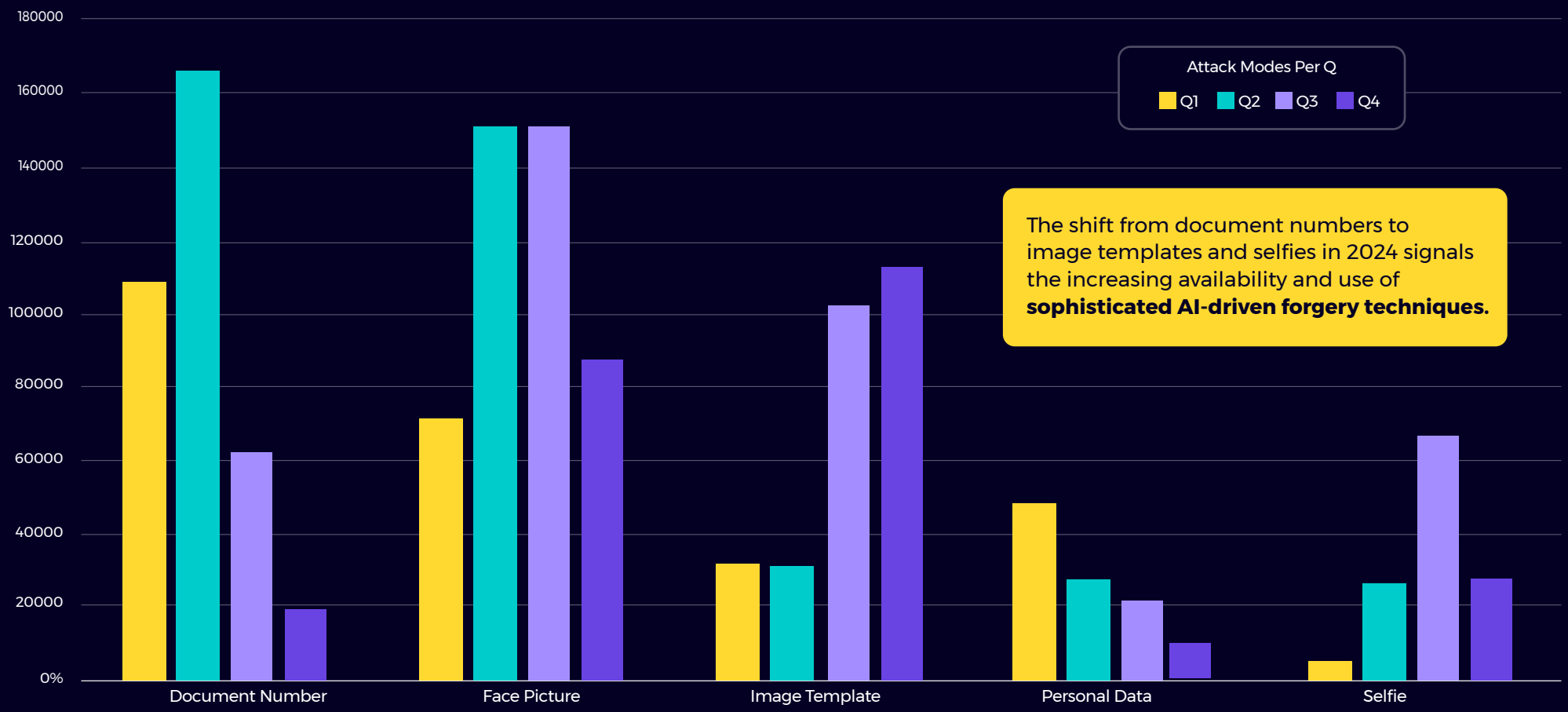
Our consortium validation solution Serial Fraud Monitor (SFM) identifies the country of origin for the document type used in an attack. Our Analysts have found a strong correlation between the document's country of origin and the actual geolocation of fraud attempts.

Mega Attacks doubled in size during 2024



Average number of permutations per attack 2023 vs. 2024

FaaS enabled a slick transition in modes of attack



The shift from document numbers to image templates and selfies in 2024 signals the increasing availability and use of **sophisticated AI-driven forgery techniques.**

Sector Analysis

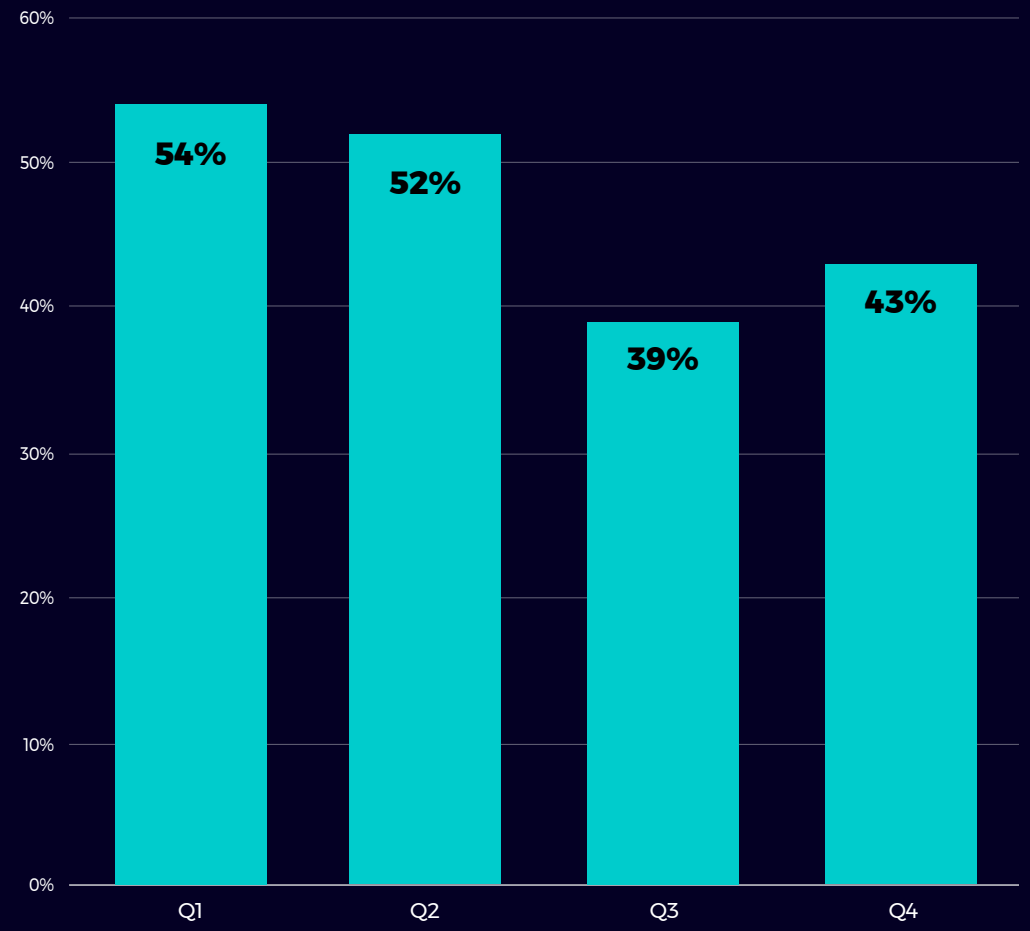
2024 in Review

Payments

Overall we saw a decrease in identity fraud attacks within the Payments sector in 2024.

As we reported, our Analysts attribute the decline to tougher law enforcement and a shift to the Social Media sector due to its ease of entry in some unregulated regions.

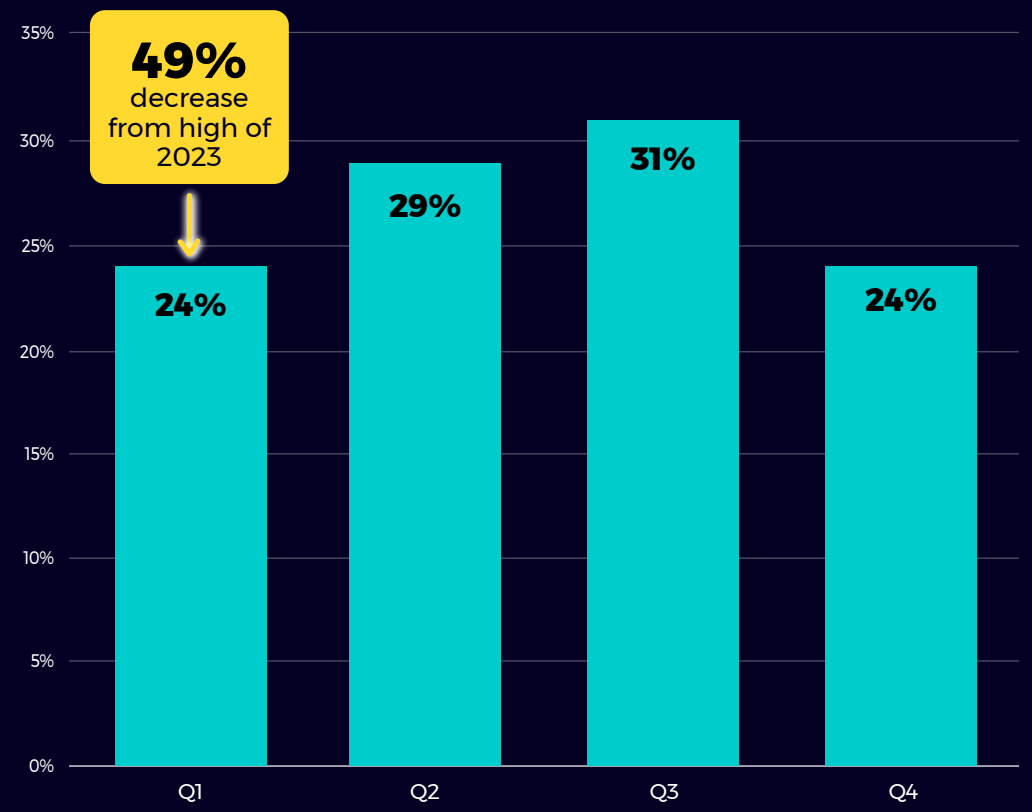
How are the two related? With users leveraging these platforms for e-commerce, fraudsters have an open door to conduct illicit activities that were once confined to payments, banking, crypto, and other fintech platforms.



Payments sector share of attack Q1 to Q4 2024

Crypto

Share of
attacks in the crypto sector decreased and stabilized
following the implementation if MiCA regulations in late 2023.



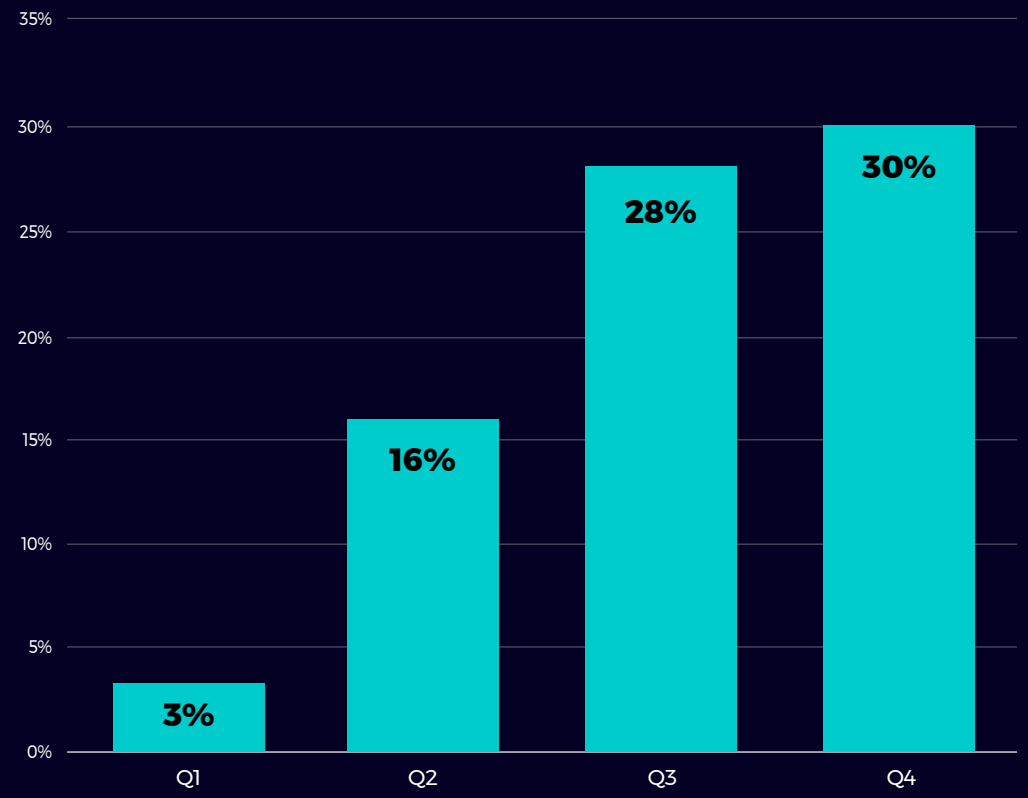
Crypto sector share of attack Q1 to Q4 2024

Social Media

This is the new big thing. Social media has become a critical battleground for fraud and misinformation.

According to a 2023 report by the World Economic Forum, trust in digital platforms has declined significantly due to rising concerns about fake accounts, manipulated content, and fraudulent activity.

Without proactive measures like robust identity verification and self-regulation, social networks risk losing credibility as users grow increasingly skeptical of the information they encounter.



Social Media sector share of attack Q1 to Q4 2024

Key Takeaways & Actionable Insights

Social Media Needs Smarter Fraud Detection

Sharper selfie detection and pattern recognition are critical for combating sophisticated fraud on platforms like social media, where deepfakes and synthetic identities threaten credibility.

Deploy enhanced selfie and fraud detection tools to protect social media engagement and ensure authenticity, preventing interaction risks posed by fake accounts.

Transparent Collaboration

Consortium validation and visual fraud simulations are powerful tools against FaaS-driven mega attacks, shifting from optional to essential defenses.

Leverage consortium insights to align stakeholders and add a robust second layer of protection for comprehensive risk mitigation.

The Future Belongs to the Proactive

Don't just react to what's here - prepare for what's next. Future-proofing means adopting AI-driven validation and multi-layer defenses to combat deepfakes, synthetic identities, and emerging threats.

Customers value security and seamless experiences, and the right strategy delivers both.

Conclusion

2024 marked a turning point in the fight against fraud, with FaaS driving mega attacks across payments, crypto, and social media platforms. These tools have made large-scale fraud easier to execute, putting platforms under pressure to innovate or lose user trust.

Social media, now a key target, must prioritize self-regulation and adopt advanced defenses like sharper selfie detection and consortium validation. These aren't optional anymore—they're essential to protecting authenticity and credibility.

The path forward is clear: invest in smarter fraud prevention and stronger collaboration. By doing so, businesses can safeguard trust and stay ahead of evolving threats.

Contributors

Ofer Freidman
Chief Business Development Officer
AU10TIX

Liron Levy
Director of Product Management
AU10TIX

Dror Shmuel
Business Analytics Manager
AU10TIX

Guy Yahav
Senior Business Analyst
AU10TIX

Amy Lurie
Senior Content Manager & Editor
AU10TIX

About AU10TIX

OUR VISION

To empower businesses with secure, seamless, and scalable identity verification solutions, combating fraud and establishing trust between businesses and Individuals.

OUR MISSION

To lead the future of identity verification by delivering innovative solutions, anticipating emerging fraud threats, and providing advanced technology that enables businesses to grow with confidence.

For more information, visit **AU10TIX.com.**

Media Contact:
Lisa Vestel
Head of Global Communications
lisa.vestel@au10tix.com

Ready to fight serious fraud?

Talk to us

Book a tech walkthrough with one of our experts to find out how you can protect your business from fraud.

Resources and further reading

THE Q3 2024 GLOBAL IDENTITY FRAUD REPORT, OCTOBER 2024
WORLD ECONOMIC FORUM DIGITAL TRUST INITIATIVE, JUNE 2023
GENAI INCREASINGLY POWERING SCAMS,THE WALL STREET JOURNAL, JANUARY 2025
TRIO BEHIND BANK FRAUD SUBSCRIPTION SERVICE GUILTY, BBC, SEPTEMBER 2024