AUTOTIX

Q2 2024

Global Identity Fraud Report

ATTACK OF THE IMPERSONATION BOTS

Table of Contents

Foreword

The numbers don't lie: bot attacks using deepfakes have become a major plague, overshadowing the usual deepfake fraud.

We're witnessing a dramatic transformation in how these attacks are carried out. Automated bots and deepfake tech are letting criminals automate complex scams that used to take a lot more effort, making them incredibly efficient and dangerous.

Cybercriminals are shifting their focus as new regulations make committing fraud in the crypto and payments industries tougher. They're leveraging social engineering on social media to establish credibility before diving into criminal activities on more traditional platforms.

With social media platforms now reaching 5 billion of the world's population, they've become a playground for fraudsters. This report not only covers the bases but also dives into these new threats, breaking down their impact and showing you how to tackle them head-on.

Dan Yerushalmi, CEO, AU10TIX

Q2

IMPERSONATION BOTS
are the new deepfake

32%
of all internet traffic is malicious bot driven

* IMPERVA BAD BOT REPORT, 2024

Share of fraudulent attempts in Social Media increased close to

3X

17%
decrease in Payments industry attacks since INTERPOL bust

2024

Impersonation Bots

(noun) /ɪmˈpɜː.səˌneɪ.ʃən bɒts/:

Automated programs designed to mimic real human identities and behaviors, often enhanced with deepfake technology to create highly convincing fake profiles.

Impersonation Bots are changing the way criminals use deepfakes

Efficiency

- Rapid creation of fake profiles.
- Spread of disinformation.
- Manipulation of online interactions.

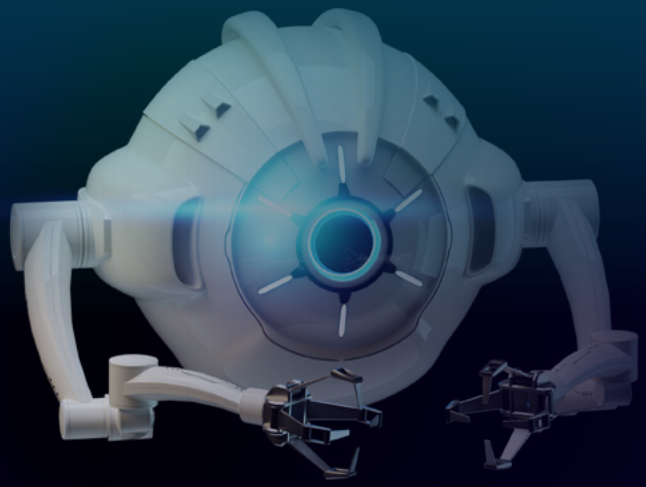
Impact

- Realistic fake videos and images.
- High potential to deceive individuals.

Sector-Specific Effects

- **Social Media Chaos**
  - Distorted public discourse.
  - Increased spread of misinformation.
- **Financial Sector Threats**
  - Creation of fake accounts.
  - Execution of sophisticated fraud schemes.
- **Challenges in Detection**
  - Seamless integration into fraud strategies.
  - Increased difficulty in identifying fraudulent activities.

The evolution of Impersonation Bots



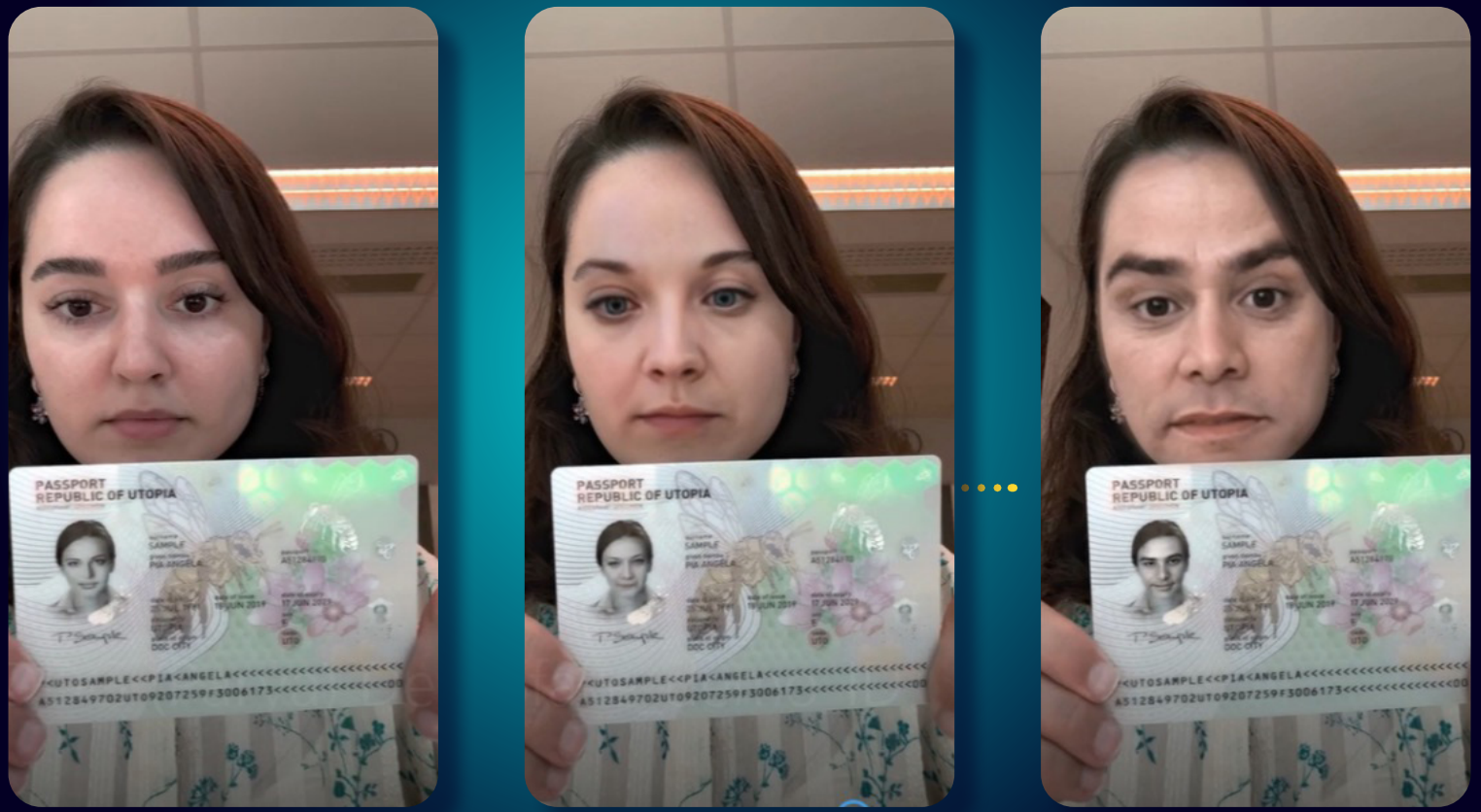
Level of impersonation sophistication

Overall, the danger lies in the bots' ability to mimic human behavior with enough variability to bypass traditional detection methods, making them a potent tool for fraudsters.

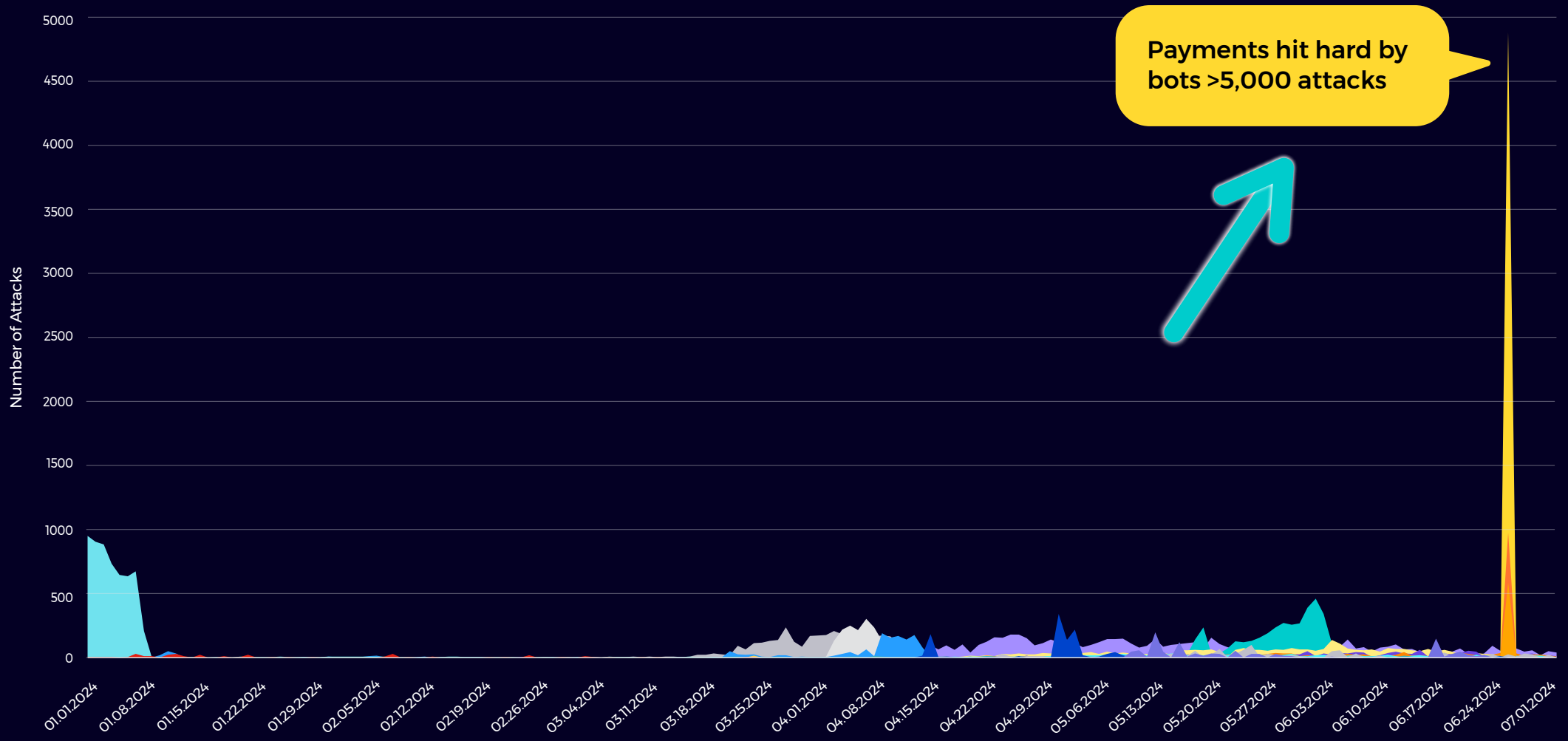
ID Doc | Gen AI/Face | Liveness | Liveness Randomization | Avatar | Avatar Randomization

Types of Impersonation Bots

A liveness Impersonation Bot at work...



Caught by consortium: APAC focused bot-led mega attack



APAC's vulnerability to financial-related identity fraud

Here's what we've uncovered:

Skyrocketing Fraud Rates

APAC now holds the highest fraud rate globally at **3.27%** with a notable **24%** increase from 2022 to 2023.

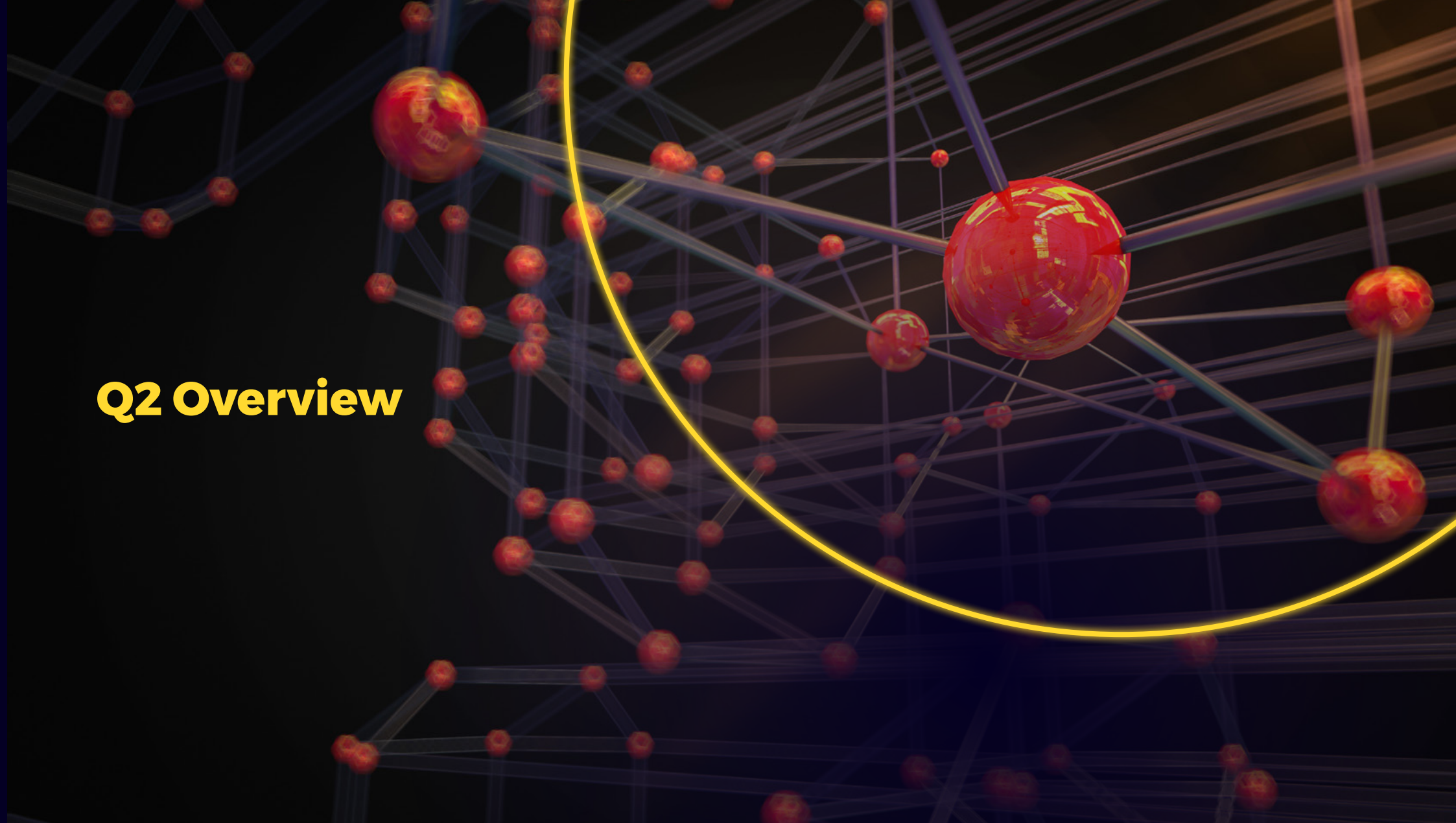
Cultural Trust Exploited

Scammers take advantage of the perceived cultural inclination towards **trust.**

Automation of Fraud

The advent of **FaaS** (Fraud-as-a-Service), powered by AI, is enabling large-scale attacks.

Source: Fintech News Singapore, 2024



Q2 Overview

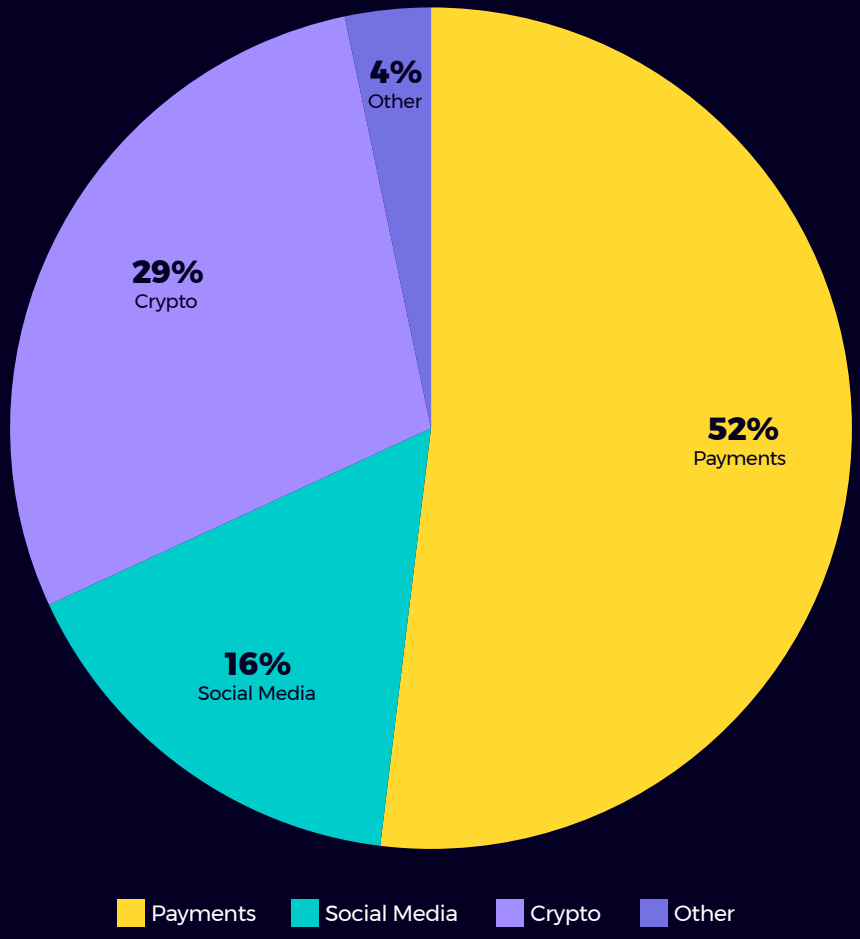
Q2 hotspots

The trends we reported last year are clearly depicted in the data generated by our consortium during the second quarter.

Social media share of attacks surged to **16%**

Fraud attempts against the **Payments sector** exceed those in all industries, although it dropped **>17%** from Q1.

Keep reading to learn what our analysts have to say about these numbers.



Top Level Overview: Second Quarter Global Attacks by Industry

Cybercriminals use bots to exploit social media for identity fraud

Key Social Media Statistics

New Accounts (2023) ***259 Million**

Growth Rate **5.4%**

New Users per Second **8.2**

Global Users (by April 2024) **62%** of the **population**

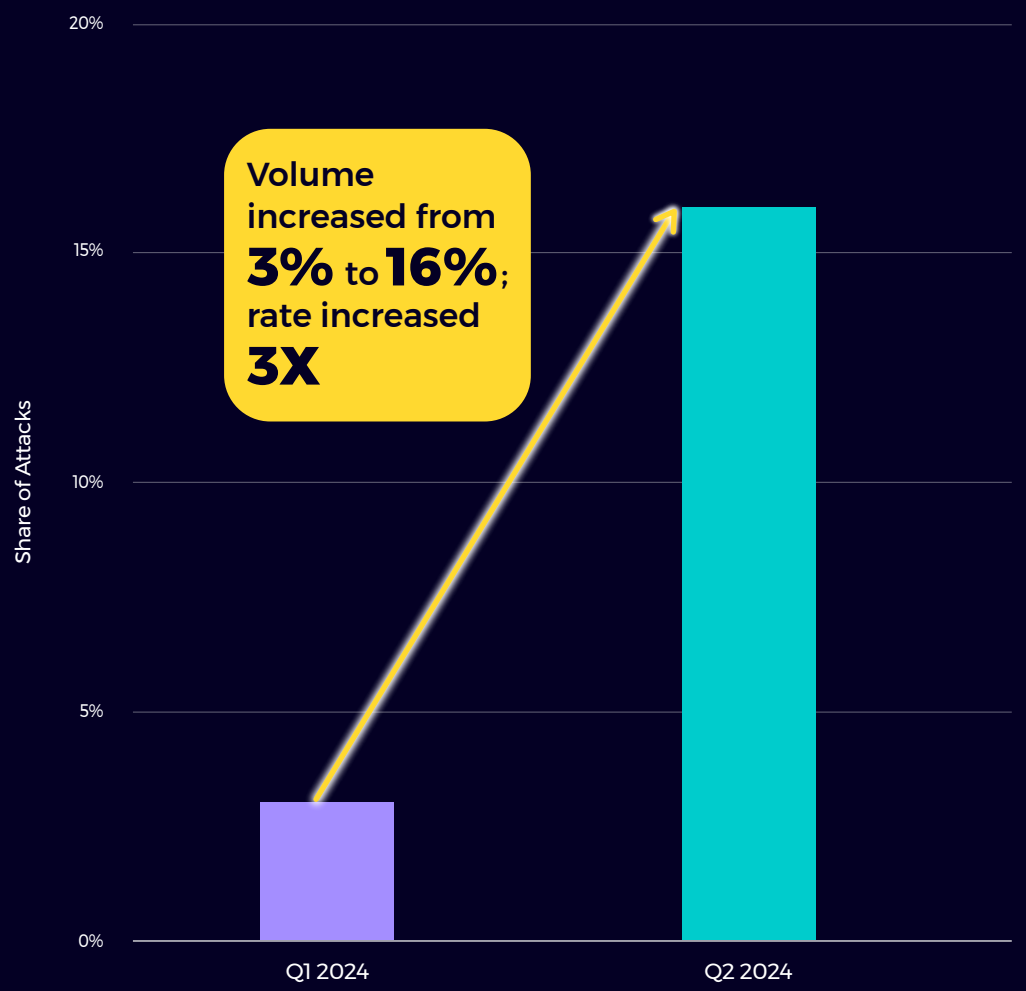
Cybercriminal Tactics

- **32%** of all internet traffic is bot generated
- Highest ever number of bot attacks this quarter on social media
- Bots generate fake profiles, spread malware, and manipulate interactions

Urgency for Enhanced Security

- AI-driven bots can increase influence on public opinion, especially with upcoming US elections

Source: Kempner 2024; imperva



Social Media sector share of overall global identity fraud from Q1 2024 to Q2 2024

The rise in Social Media identity fraud

In Q2, we recorded the highest number of attacks on the social media sector to date. Automated bots predominantly carried out these attacks. Social media has become a critical gateway for broader fraudulent payments, cryptocurrency, and banking activities.

The Threat of Bots

Bots automate tasks that amplify cybercriminal activities. They spread malware, follow users, join groups, and boost messages. The lack of regulations lets bots run wild, continuously threatening social media users.

Social Engineering Tactics

Cybercriminals use social engineering to make fake accounts look legit. They trick victims into believing these accounts are real, exploiting this trust for further malicious activities.

Influence on Politics and Public Opinion

Social media shapes political opinions and candidate credibility but can be manipulated by fake accounts, bots, and government interventions. Examples include the bot-driven promotion of polarizing content during elections and the use of fake accounts to influence public opinion during political protests. Fake news from unverified accounts exacerbates tensions in the Middle East conflict, highlighting the role of social media in shaping geopolitical narratives.

Implications

In addition to influencing public opinion, fake profiles often lead to the creation of fraudulent accounts in payments, cryptocurrency, and banking sectors. These fraudulent accounts are then used for money laundering, highlighting the critical need for enhanced security measures.

Are the INTERPOL crackdowns working?

Our Analysts speculate INTERPOL's HAECHI IV and First Light operations in Q4 2023 and Q1 2024 disrupted criminal operations in the payments industry.

Significant Impact

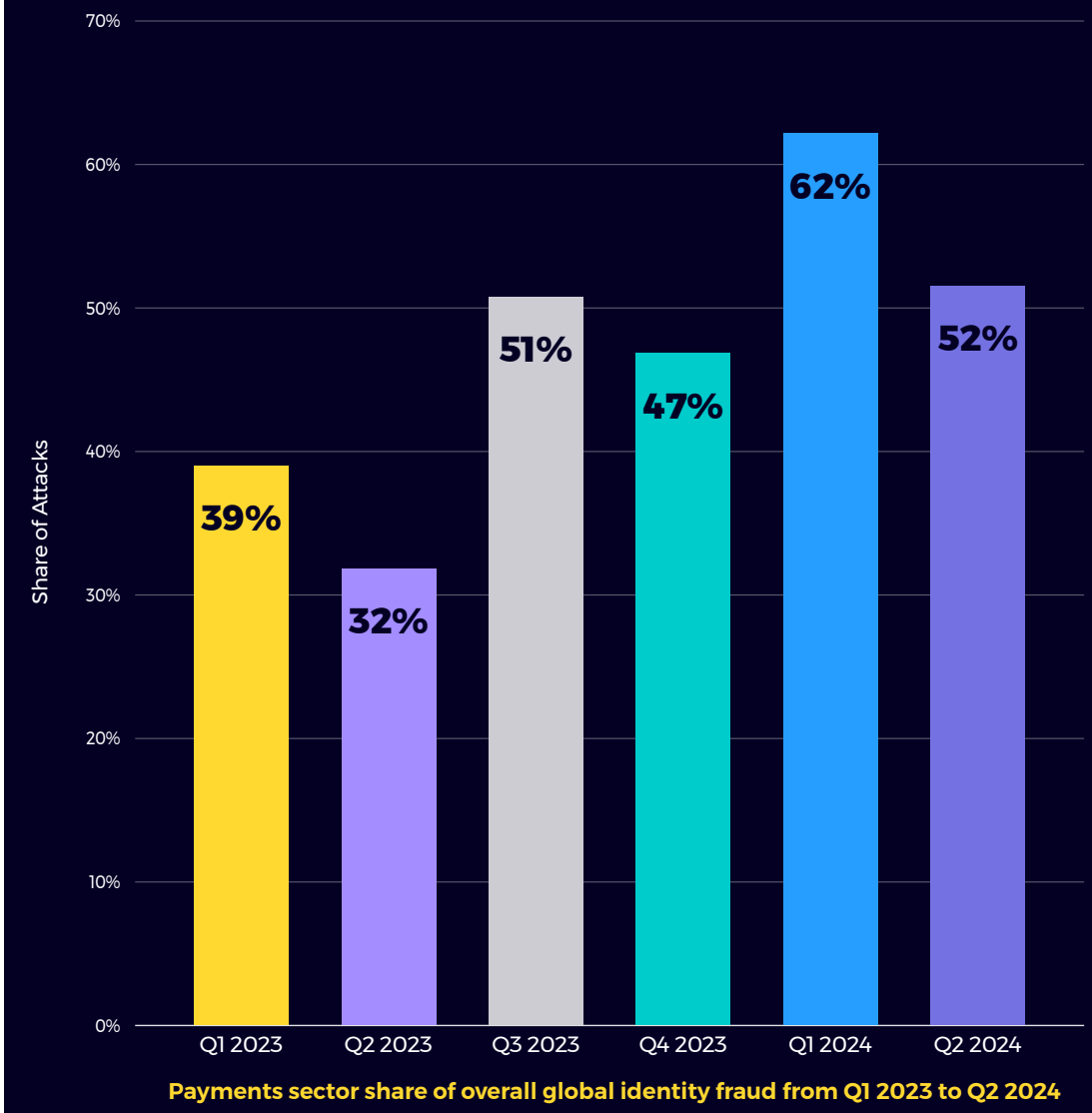
In the absence of regulations, payments providers are advised to self regulate with **robust KYC**

17% decline in fraudulent attempts detected by AU10TIX consortium

"The results of this global police operation are more than just numbers-they represent lives protected, crimes prevented, and a healthier global economy worldwide (and) also deal a significant blow to the transnational organized crime groups that pose such a serious threat to global security."

Dr Isaac Kehinde Oginni, Director of INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC)

Sources: INTERPOL; Cybernews.com

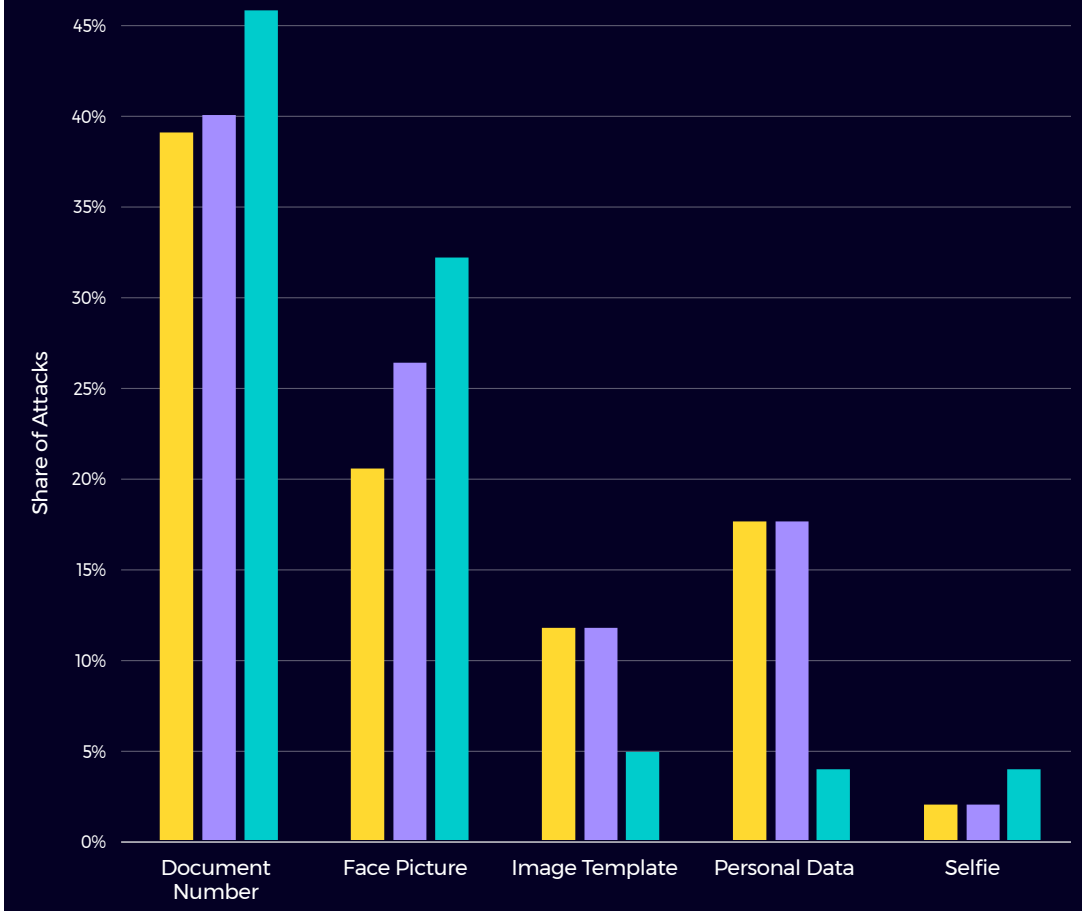


Payments sector share of overall global identity fraud from Q1 2023 to Q2 2024

Modes of attack

Nothing out of the ordinary here. **Selfies stop fraud.**

The numbers show that deepfake synthetic fraud (variations on document numbers and face pictures) is becoming more common, while verification through selfies has repeatedly proven to deter attempts at identity fraud.



Proportion of Modes of Attack Detected from Q4 2023 to Q2 2024

Actionable insights and recommendations

Adopt Multi-layered Authentication Measures

Implementing multi-layered authentication measures, such as Serial Fraud Monitor, KYC/KYB solutions, and biometric verification, can significantly enhance an organization's defenses against social media identity fraud.

Leverage Advanced Fraud Detection Technologies

Utilizing technologies like deepfake detection and consortium validation can effectively combat the rising threat of social media impersonation.

Social Media Should Self-Regulate

Maintain your credibility among the public by requiring platform users to authenticate their identity.

Conclusion

The shift from traditional fraud methods to sophisticated bot-led attacks and deepfake technologies marks a new era of challenges. These threats are not confined to one industry but spread across social media, payments, and beyond. The clear evidence of bots automating fraud on an unprecedented scale means we must rethink our defense strategies.

AU10TIX is committed to leading this fight with cutting-edge solutions. By harnessing advanced technologies like deepfake detection and multi-layered authentication, we provide robust defenses against these modern threats. Our comprehensive verification processes ensure that only legitimate entities pass through, helping to maintain trust and security across digital platform.

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

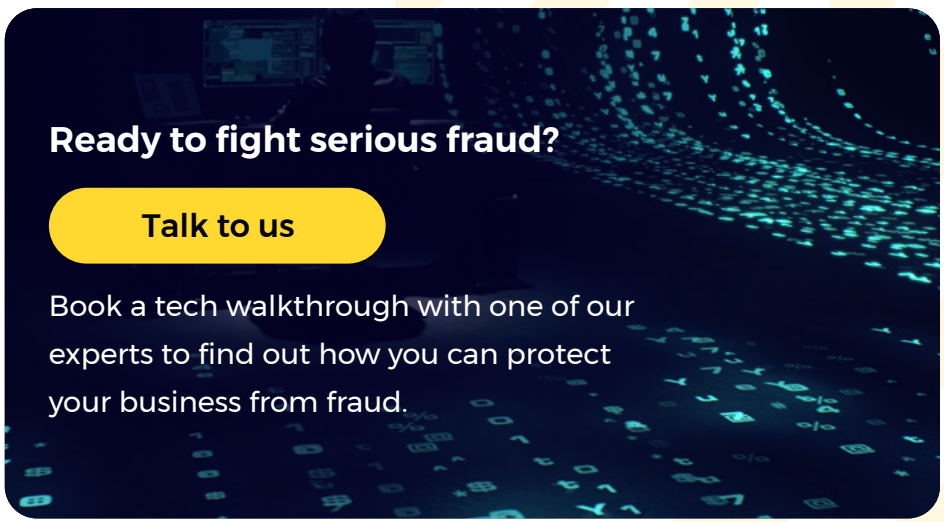
Amy Lurie
Senior Content Manager & Editor
AU10TIX

About AU10TIX

AU10TIX, a global identity intelligence leader headquartered in Israel, is on a mission to obliterate fraud and further a more secure and inclusive world. The company provides critical, modular solutions to verify and link physical and digital identities so businesses and their customers can confidently connect. Over the past decade, AU10TIX has become the preferred partner of major global brands for customer onboarding and verification automation – and continues working on the edge of what's next for identity's role in society. AU10TIX's proprietary technology provides results in less than 8 seconds, enabling businesses to onboard customers faster while preventing fraud, meeting compliance mandates, and, importantly, promoting trust and safety. AU10TIX is a subsidiary of ICTS International N.V. (OTCQB: **ICTSF**).

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

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



Resources and further reading

IMPERVA BAD BOT REPORT

KEMPNER

INTERPOL

FINTECH NEWS SINGAPORE

CYBERNEWS.COM