AU10TIX Global Identity Fraud Report

Special edition: the identity fraud mega attacks of 2023 and Q4 highlights

Table of Contents

Foreword

In May 2023, organized professionals executed a sophisticated, coordinated, and massive eight-month-long attack that was detected among the Serial Fraud Monitor consortium of 60-plus members.

Over 22,000 new users attempted to onboard with unique AI-generated variations of a **single** US Passport template. Fifty percent of the attacks happened in a matter of weeks.

This is what we mean when we talk about an organized mega-attack.

I am proud to say that AU10TIX's multi-layered inspection successfully detected the work of a sophisticated fraudster by the repetition patterns in the document and passed the knowledge to our consortium members.

Read on to learn the full scope of what we are facing in the modern world and what our future-ready technology is doing to fight fraud today.

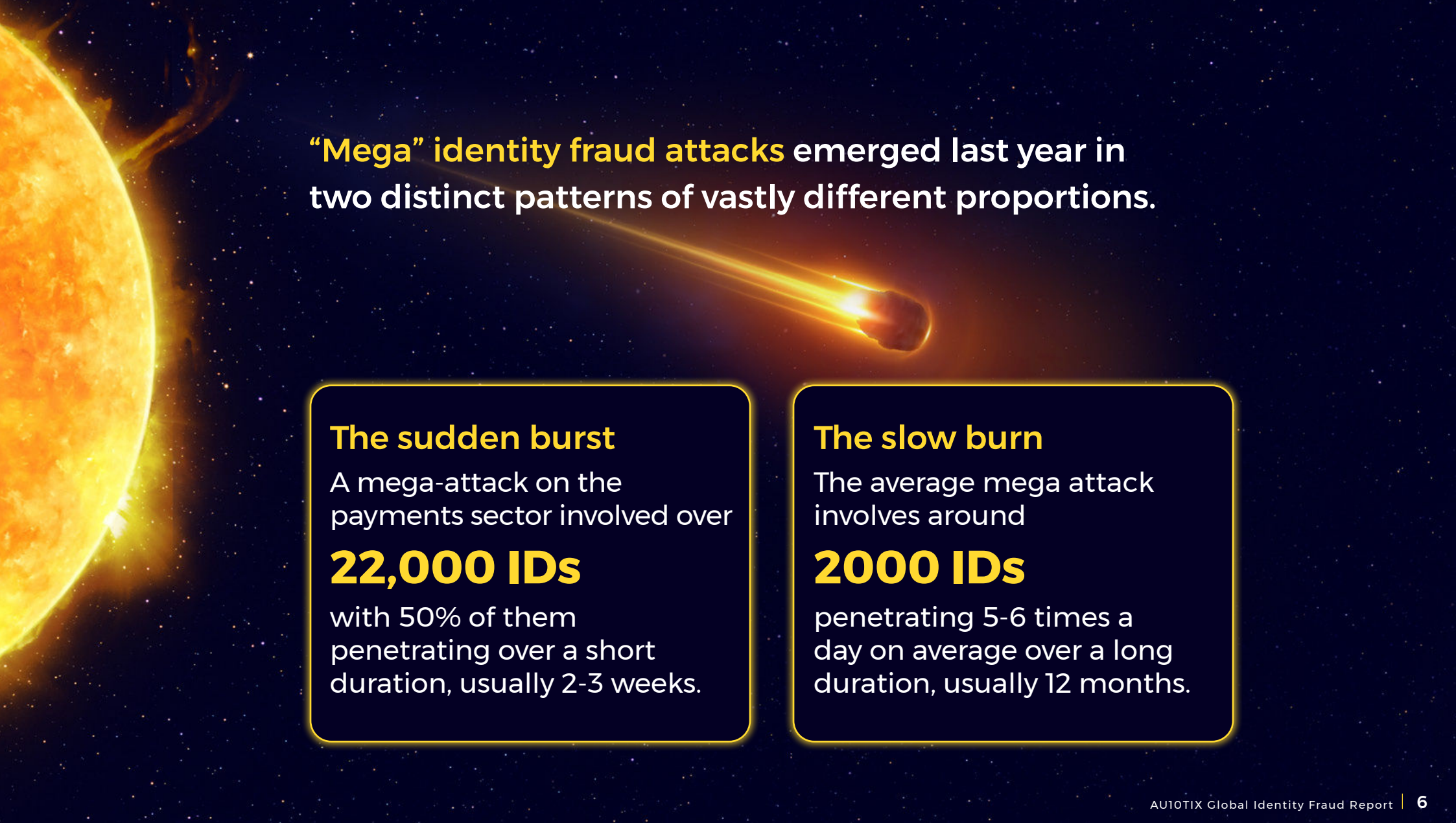
Dan Yerushalmi, CEO, AU10TIX

The MEGA Identity Fraud Attacks of 2023

MEGA Attack

(noun) /ˈmɛgə əˈtæk/:

A coordinated and extensive offensive maneuver, typically executed on a large scale, aimed at inflicting substantial damage or achieving strategic objectives.



“Mega” identity fraud attacks emerged last year in two distinct patterns of vastly different proportions.

The sudden burst

A mega-attack on the payments sector involved over

22,000 IDs

with 50% of them penetrating over a short duration, usually 2-3 weeks.

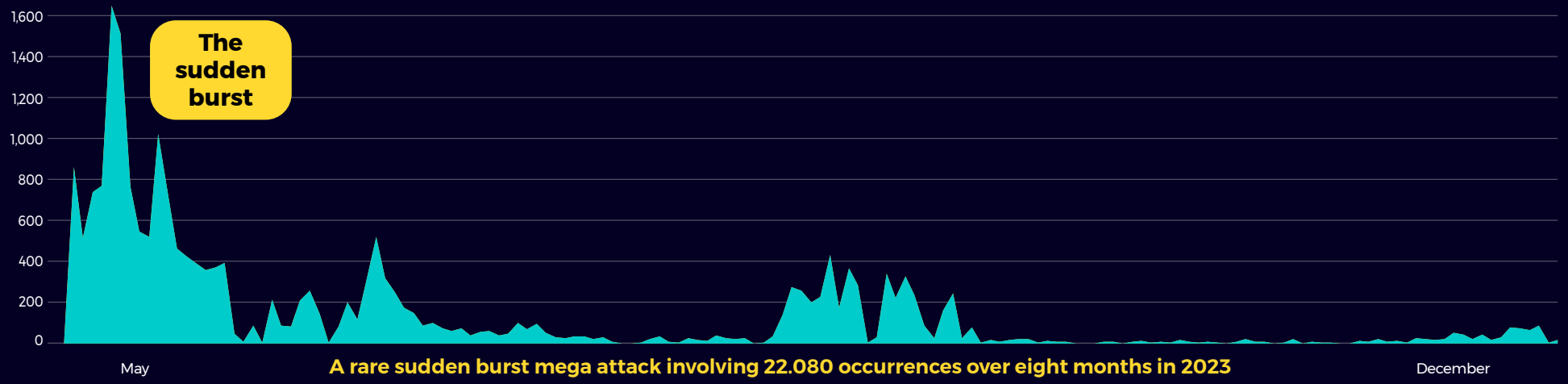
The slow burn

The average mega attack involves around

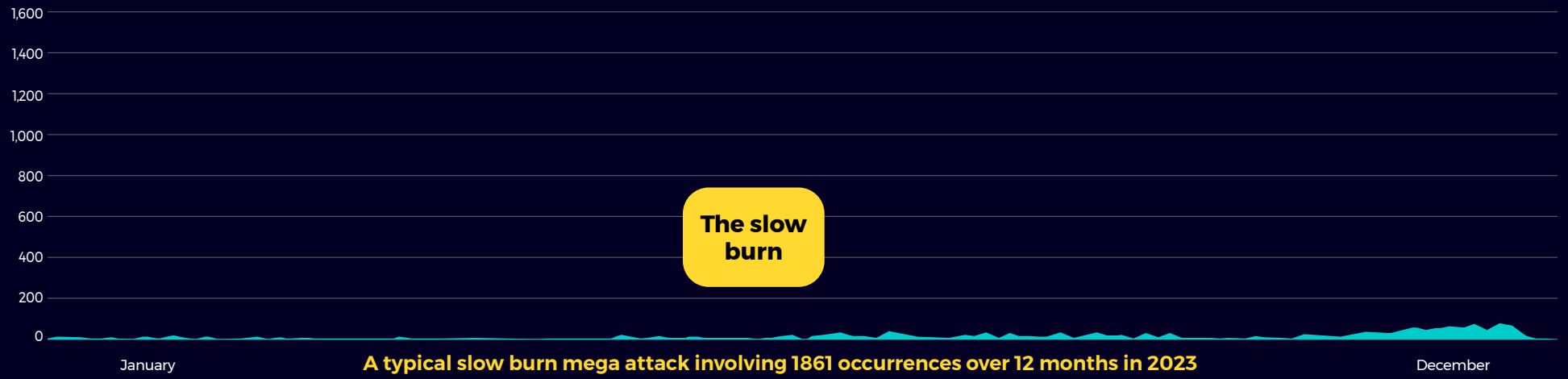
2000 IDs

penetrating 5-6 times a day on average over a long duration, usually 12 months.

We can observe their distinct behavior

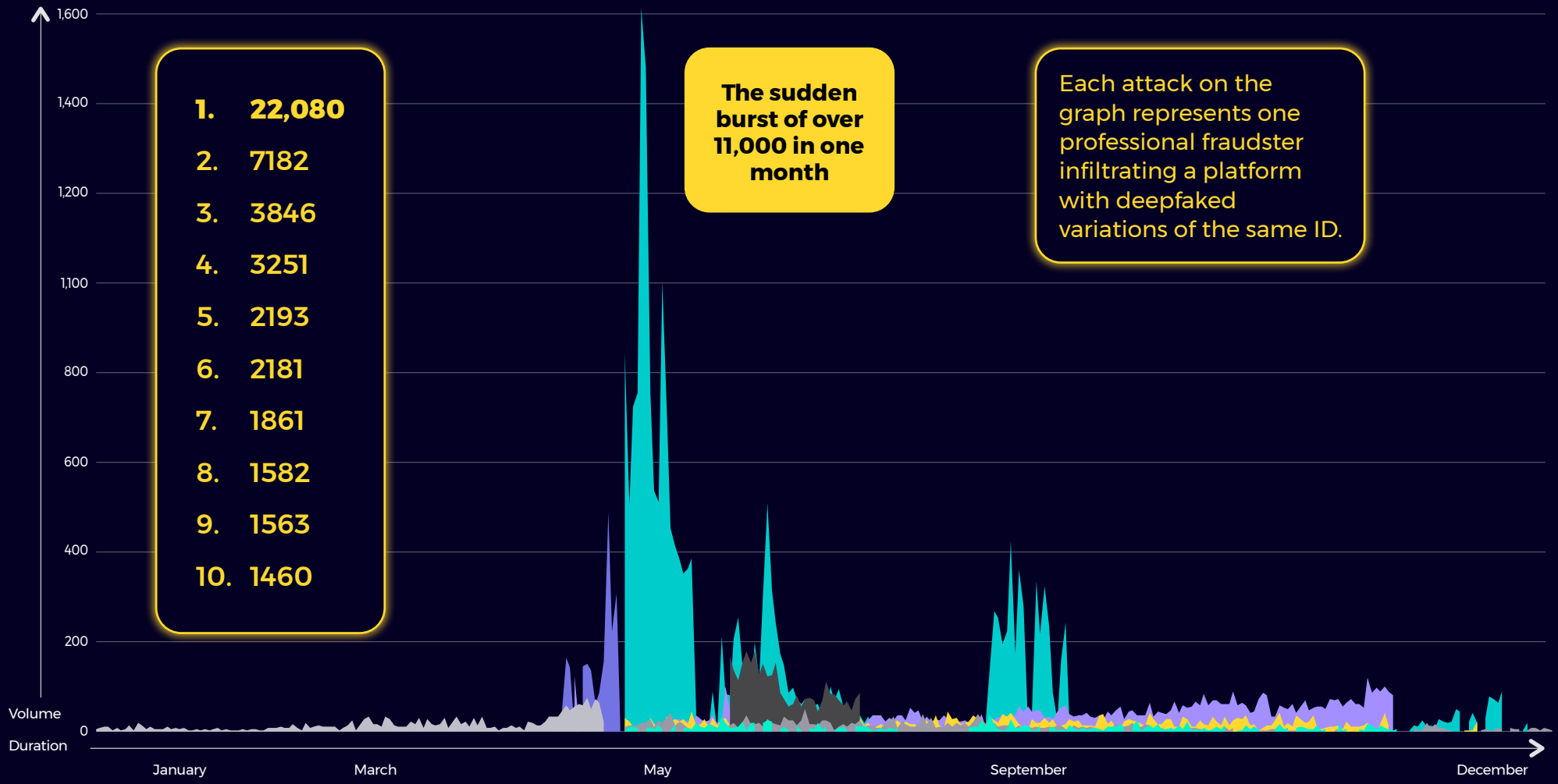


A rare sudden burst mega attack involving 22.080 occurrences over eight months in 2023

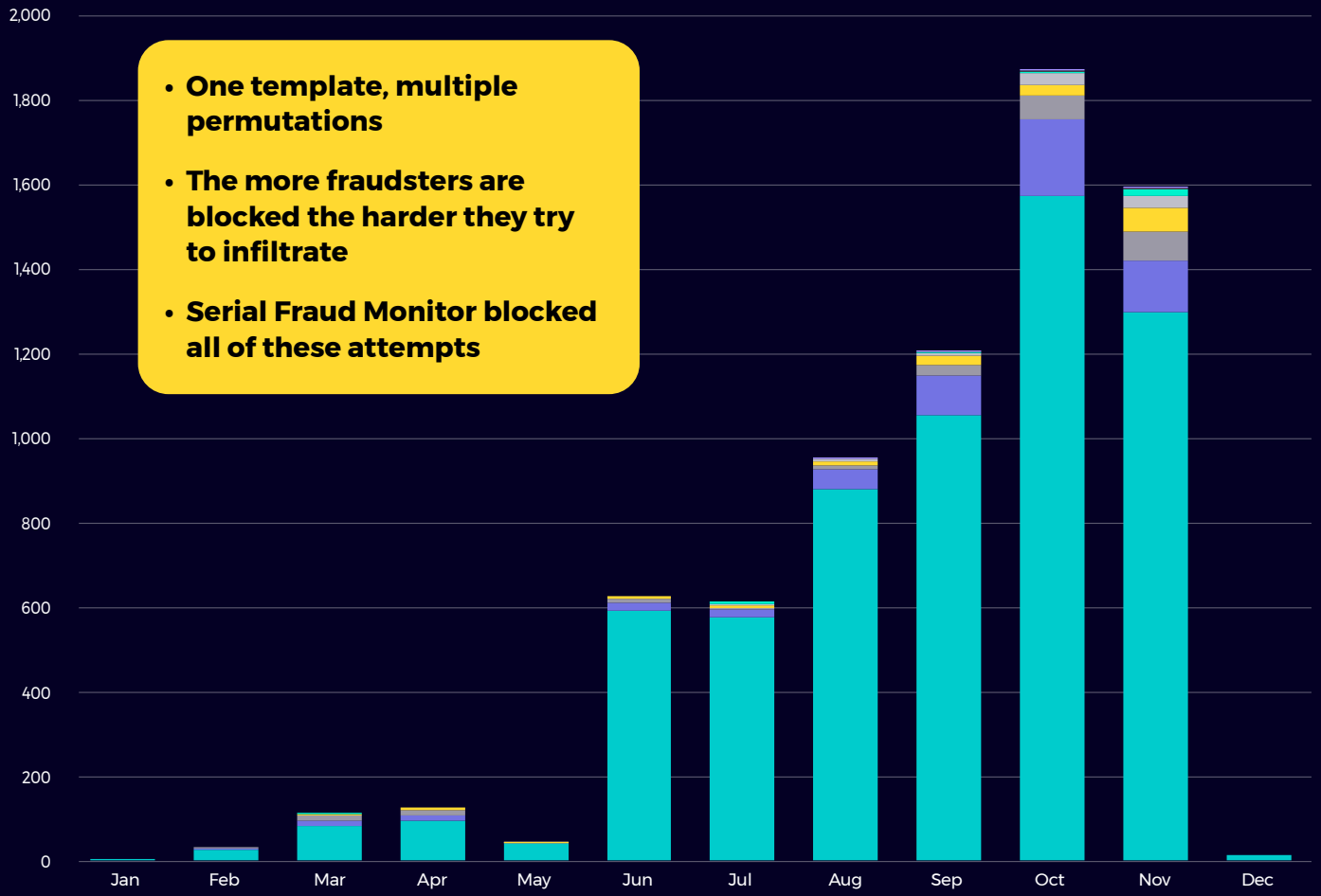


A typical slow burn mega attack involving 1861 occurrences over 12 months in 2023

Top ten professional identity fraud mega attacks of 2023



Pattern recognitions: the DNA of a mega attack from a single ID



- **One template, multiple permutations**
- **The more fraudsters are blocked the harder they try to infiltrate**
- **Serial Fraud Monitor blocked all of these attempts**

ID pattern recognitions in one mega attack over 12 months in 2023

Our consortium recognized four distinct elements of hashed PII (represented as A, B, C, and D) recombined eight ways:

- C,D
- B,C
- B,C,D
- C
- D
- A,B,C
- A,C,D
- A,B,C,D

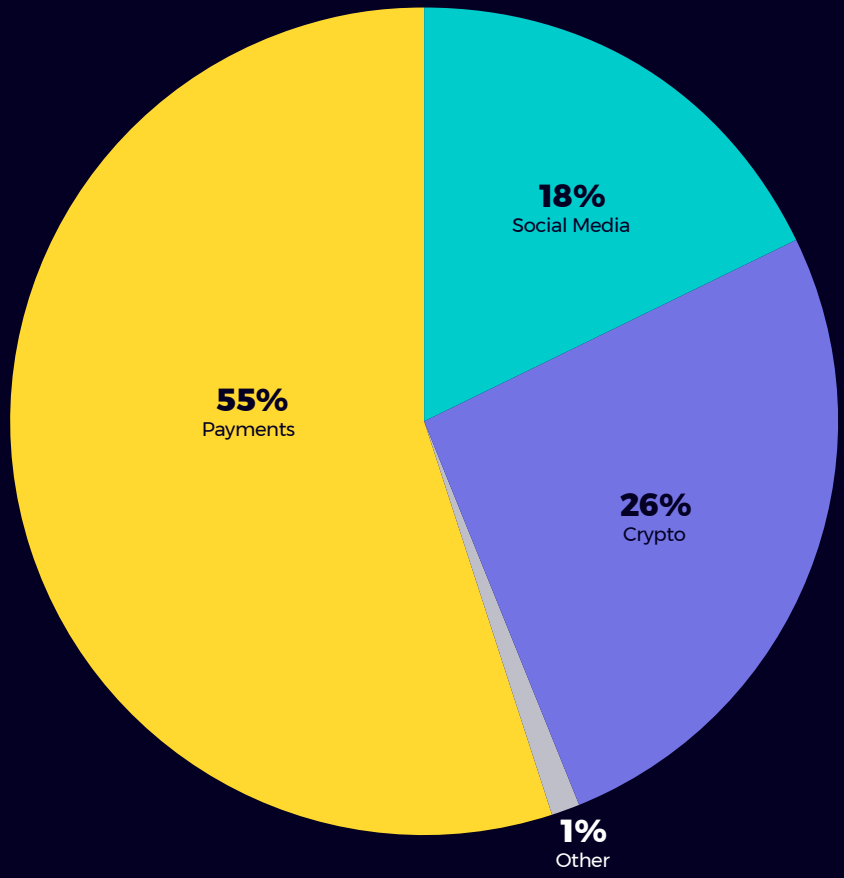
PII is hashed and therefore recognized by a unique identifier, preserving privacy in the consortium while providing the strongest detection against organized identity fraud attacks.

Sector analysis of the top ten attacks reveals a picture of organized crime at work

It is no surprise to see Payments and Crypto - the same two sectors hit hard by identity fraud attacks in our previous reports, come out on top in the analysis of the top ten attacks of last year.

The large proportion taken by the Social Media sector is a new development. Our analysts speculate the attention to social media makes sense. We know how easy it is for fraudsters to establish “credibility” through a fake digital footprint.

Social credibility is an easy way to “legitimize” fake accounts used by organized crime to launder money and finance terrorist activities.



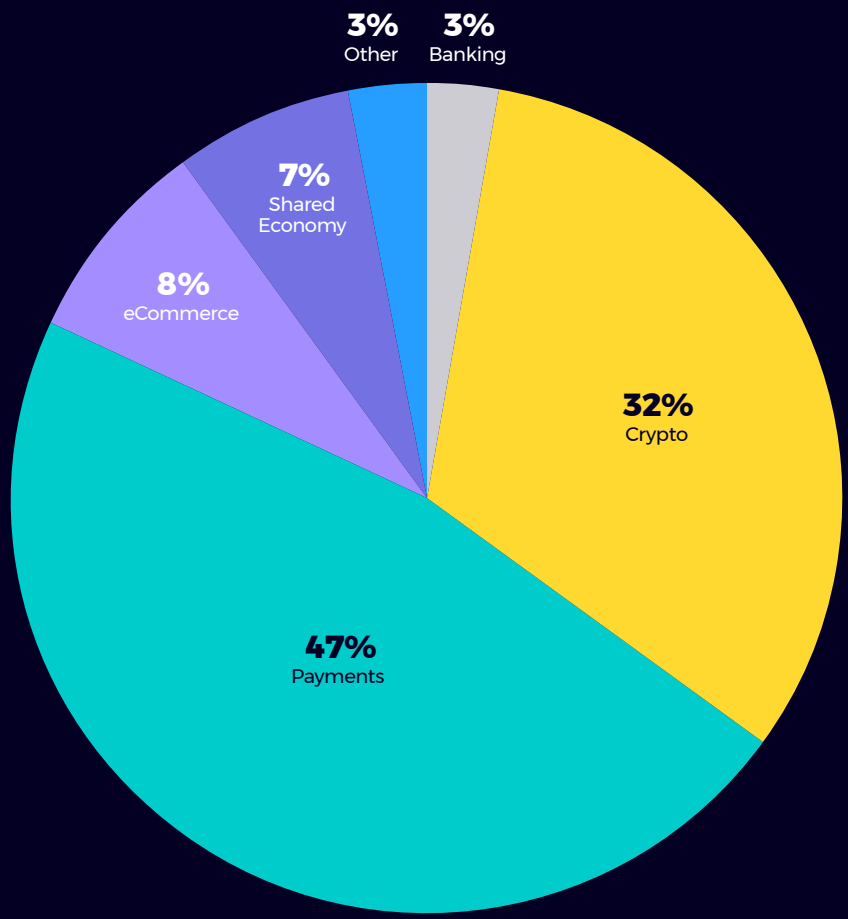
Distribution of the top 10 mega attacks across industries in 2023

Q4 Highlights

Q4 hotspots

The shift we spotted in the Q3 Report is still here.

The Payments sector still takes the lion's share in the attacks, and crypto follows close behind.



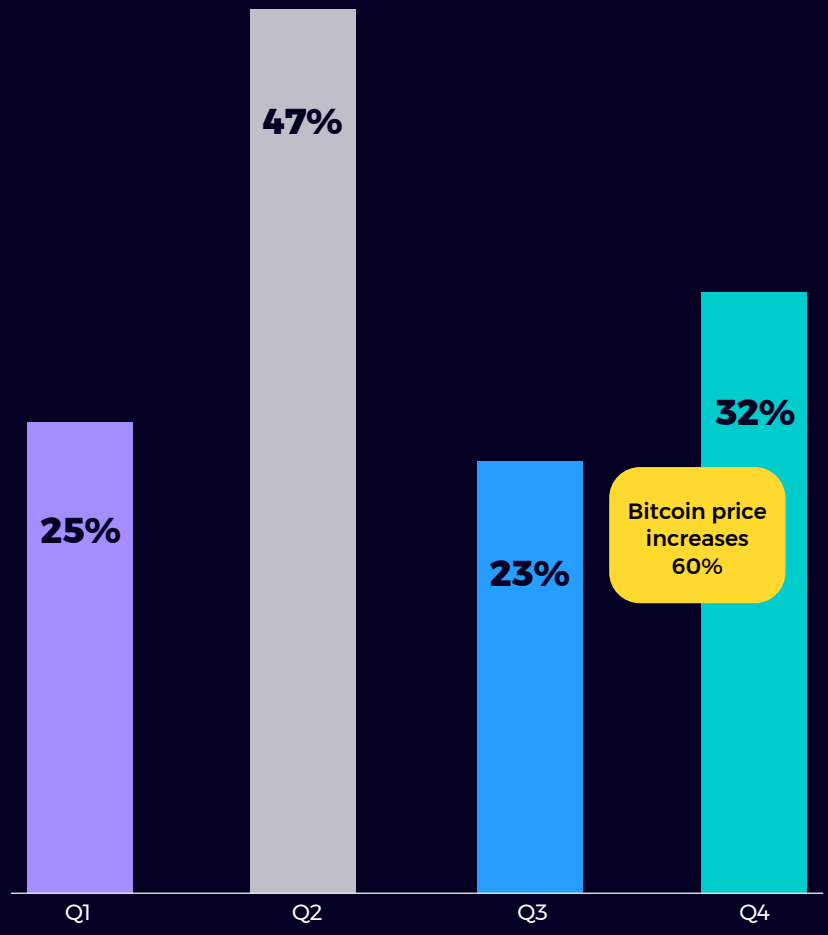
Top level overview: fourth quarter global attacks by industry

Despite a slight increase in crypto from Q3 to Q4, fraudulent activity still remains beneath the pre-MiCA Q2 spike

Last quarter, we reported a sharp decrease in Crypto-related identity fraud attacks that may be attributed to the Markets in Crypto Assets (MiCA) regulations adopted by the EU that require full compliance by mid-2024. Our analysts still hold this to be true and expect a decline in Crypto Asset fraud over the coming year.

We are optimistic that regulations such as the EU's MiCA will serve as a tough barrier to entry for criminal activities by requiring stringent KYC, KYB, and AML screening and tough penalties for non-compliant trading platforms.

The increase from 23% in Q3 to 32% in Q4 is attributed to the increase in the value of Bitcoin, alluring more legitimate players and scammers taking advantage of the increased trading traffic especially in North America and APAC.



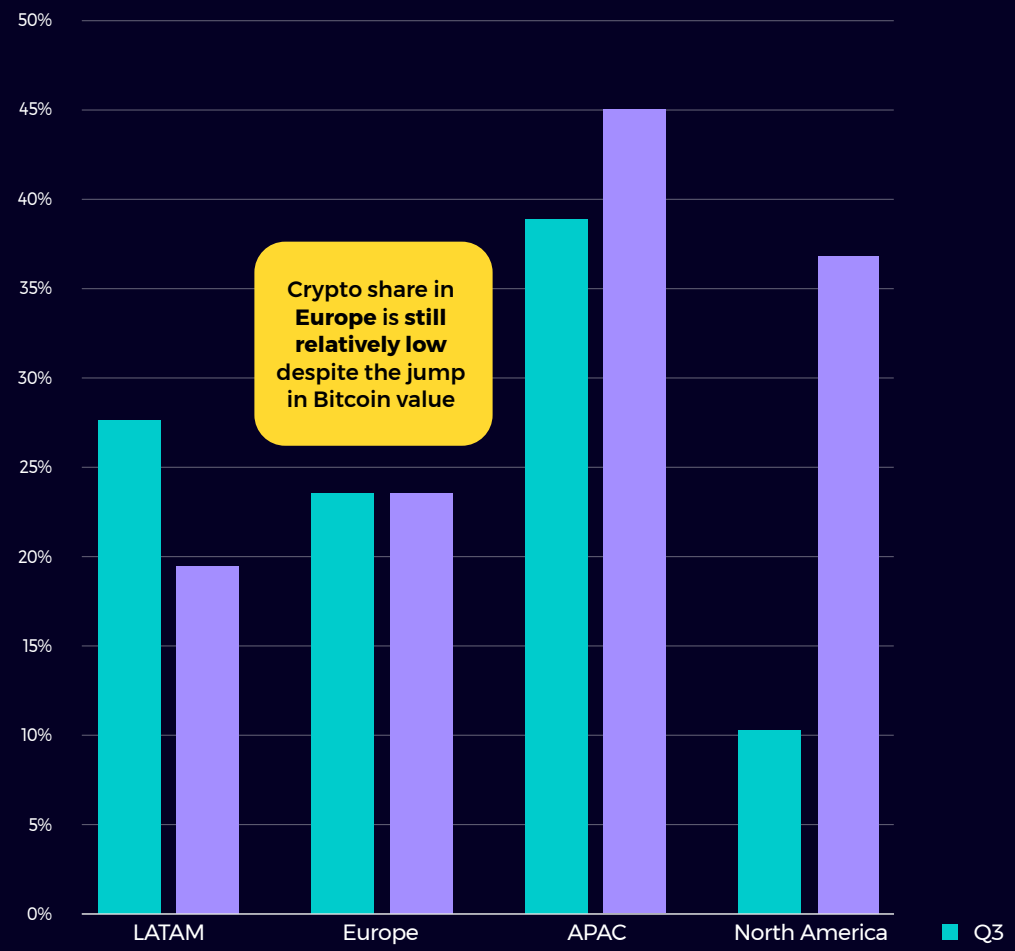
Crypto sector share of overall global identity fraud by quarter

Identity fraud within the Crypto sector share of overall identity fraud exhibits divergent trends across regions

In EMEA the implementation of MiCA has been impactful.

Meanwhile, North America and APAC experience heightened crypto activity fueled by surging Bitcoin prices and a lack of regulatory constraints.

The allure of potential profits and the perceived ability of bad actors to go unnoticed in the flux of trading has attracted a surge of market participants, including legitimate investors and opportunistic fraudsters seeking to exploit the hype.

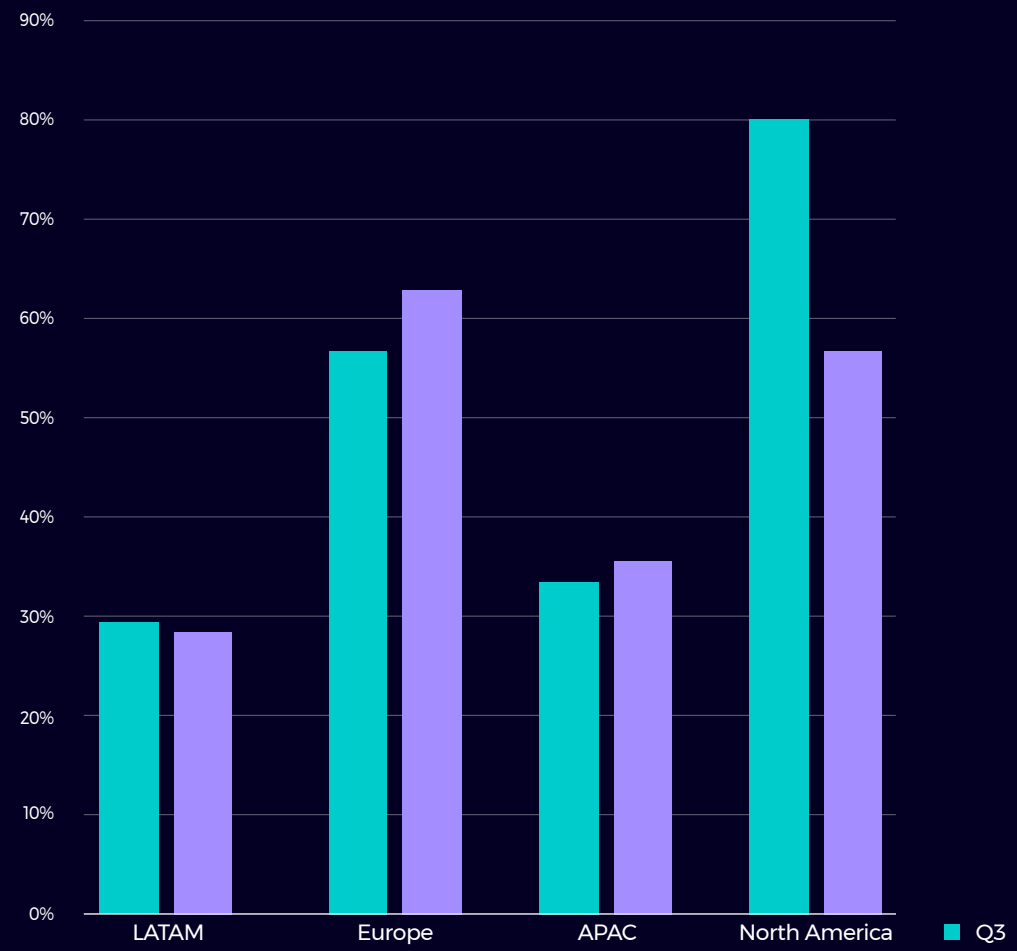


Crypto sector share of overall identity fraud by region H2 2023

Payments sector identity fraud persists across LATAM, Europe, and APAC but dropped in North America

Why the 30% drop in North America?

The data suggests that fraudsters shifted their focus from the Payments sector to Crypto to take advantage of the frenzy created by Bitcoin trading and work beneath the radar of activity.



Payments sector share of overall identity fraud by region H2 2023


Key Takeaways

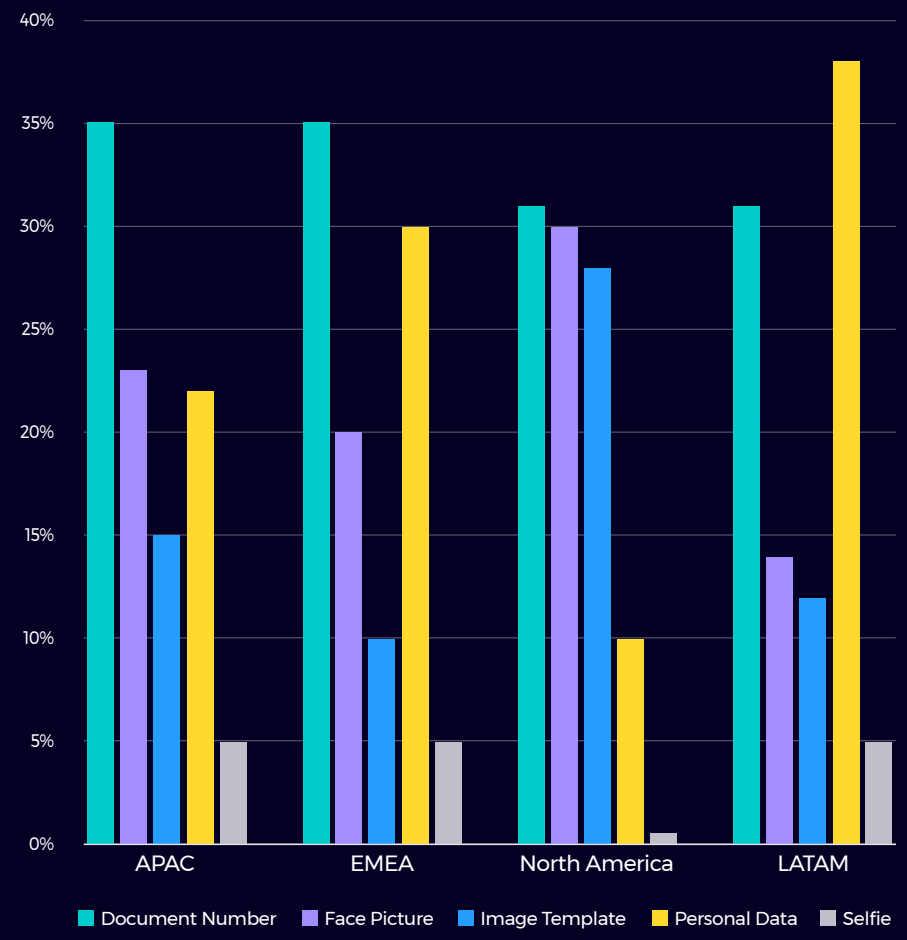
We can't say it enough: selfies as verification stop fraud

Gartner endorses facial image capture (selfie) as a "must-have" for identity verification vendors.*

Fraudsters know that fakes get recognized by adding a “take a selfie” step to the verification process.

Gartner®

* Source: Market Guide for Identity Verification, Gartner, 7 September 2023



2023 annual mode of attack per region

Now is the time to step up your IDV game with automated KYB, KYC, and AML screening

In the crypto sector, MiCA regulations are already working to combat professional identity fraud in Europe and LATAM.

The payments sector, however, does not have the benefit of a widespread and globally accepted regulatory framework, and there is an urgent need for service providers to implement self-regulatory tools like advanced KYB, KYC, and AML screening technologies alongside enhanced collaboration of the consortium validation between industry stakeholders to establish standardized best practices and information-sharing mechanisms.

Strengthening security protocols under the current absence of strong regulatory oversight safeguards the integrity of the payments ecosystem and protects consumers from fraudulent activities.

Consortium validation increases privacy and fraud detection

Consortium validation offers a robust solution for detecting identity fraud, particularly in the face of increasingly sophisticated synthetic and deepfaked identities.

The recent detection of a mega-attack by AU10TIX's consortium of 60–plus members exemplifies the power of collective expertise in identifying complex fraud patterns that may evade individual entities. By aggregating diverse data sources and insights, the consortium can effectively uncover subtle anomalies indicative of fraudulent activity, enhancing fraud detection capabilities.

Organizations can collaborate without compromising sensitive information by anonymizing and securely sharing data within a trusted network.

The consortium recognizes various elements we check and their repetition rate.

Actionable insights

Consortium validation increases privacy and magnifies fraud detection

Selfie-based biometrics are proven to be effective prevention against fake account onboarding

Robust KYB, KYC, and AML screening are must-haves to protect the reputation of your business

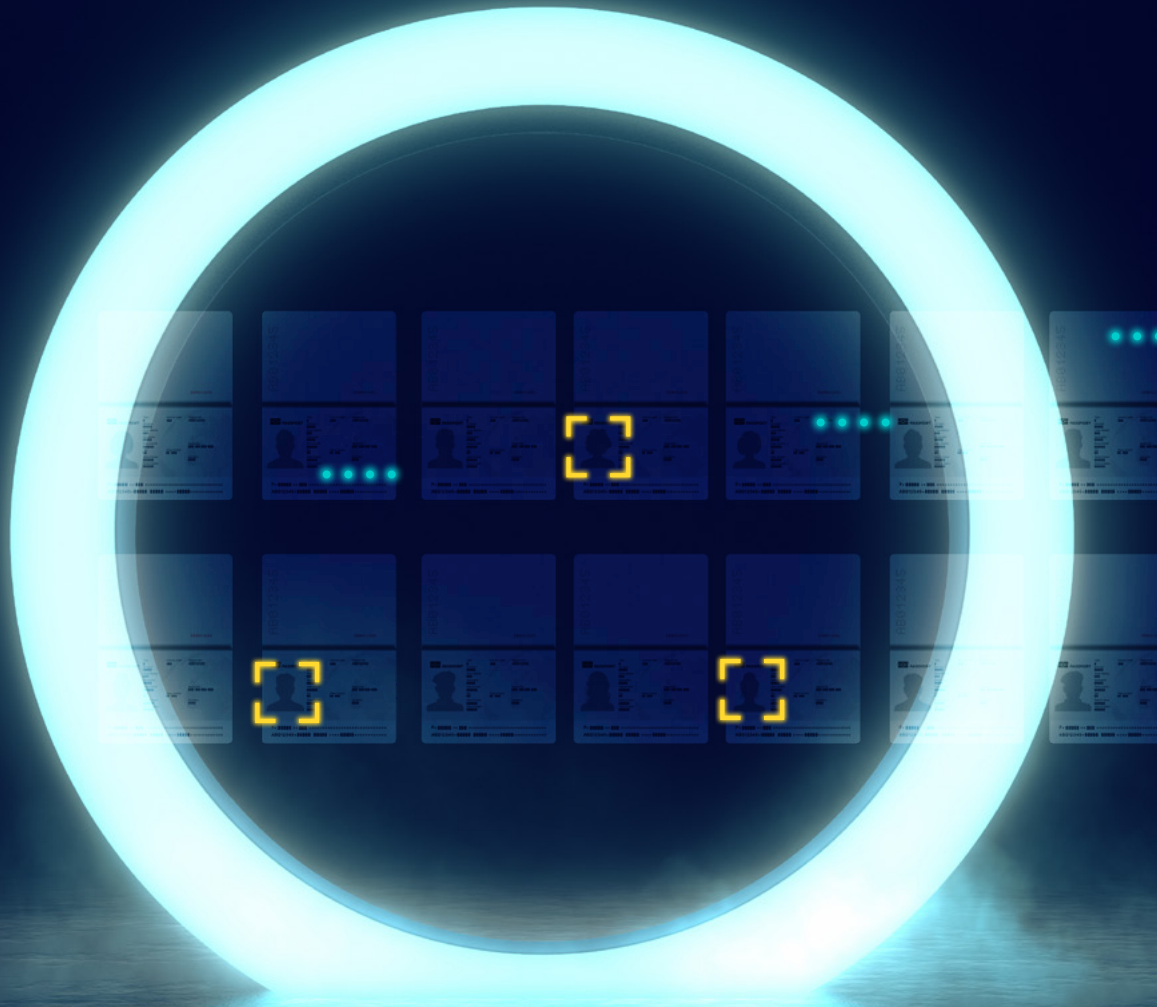
Fraudsters are using Social Media platforms to establish fake ID credibility

Conclusion

The recent mega-attack detected by the Serial Fraud Monitor consortium highlights the escalating threat of identity fraud, with over 22,000 attempted user onboardings using AI-generated variations of a single US Passport template.

AU10TIX's multi-layered inspection and consortium validation system successfully detected the attack, showcasing the critical role of consortium participation in combating fraud. Our consortium is based on pattern sharing, not PII sharing. Let's be clear - sensitivity to privacy is increasing, not decreasing.

Identity fraud remains prevalent in sectors like Payments and Crypto, emphasizing the need for robust KYB, KYC, and AML screening processes with biometric verification like selfie image capture. Moving forward, collaborative efforts between industry stakeholders and regulators are crucial to safeguarding the digital ecosystem and protecting consumers from fraudulent activities.



Contributors

Ofer Freidman
Chief Business Development Officer
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

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

Q3 2023 GLOBAL IDENTITY FRAUD REPORT, AU10TIX, December 2023

MARKET GUIDE FOR IDENTITY VERIFICATION, Gartner, 7 September 2023