SPOTLIGHT ON HIDDEN GEOGRAPHICAL
AND INDUSTRY TRENDS

Q2 2023 Global Identity Fraud Report

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

Gain actionable insights on organized identity fraud

Gartner has identified fraud and identity risks as one of the top emerging security risks within Generative AI. But, while digitization and Generative AI technology become avenues for criminals to engage in identity fraud, they also present an opportunity to outmaneuver fraudsters at their own game.

At AU10TIX, our unique ability to monitor serial fraud activity positions us as the only identity verification solution capable of detecting and analyzing coordinated fraud attacks at the incoming traffic level that are undetectable by our competitors. We are preventing the fraudster from acting on the customer's platform through detection. Detection is key to prevention.

Our objective in compiling this report is to show the geographical regions, industry sectors, and identity modes experiencing the most acute attack rates and provide a look into how organized, professional identity fraud appears in the data so businesses can take action to protect their customers.

This data reveals which markets professional fraudsters consider the most vulnerable with the most potentially lucrative return and the modes they use to infiltrate. We hope that by compiling the report and sharing our analysis regularly, we can contribute to the global reduction of ID fraud.

Dan Yerushalmi
CEO, AU10TIX

Fraud by **Geolocation**

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

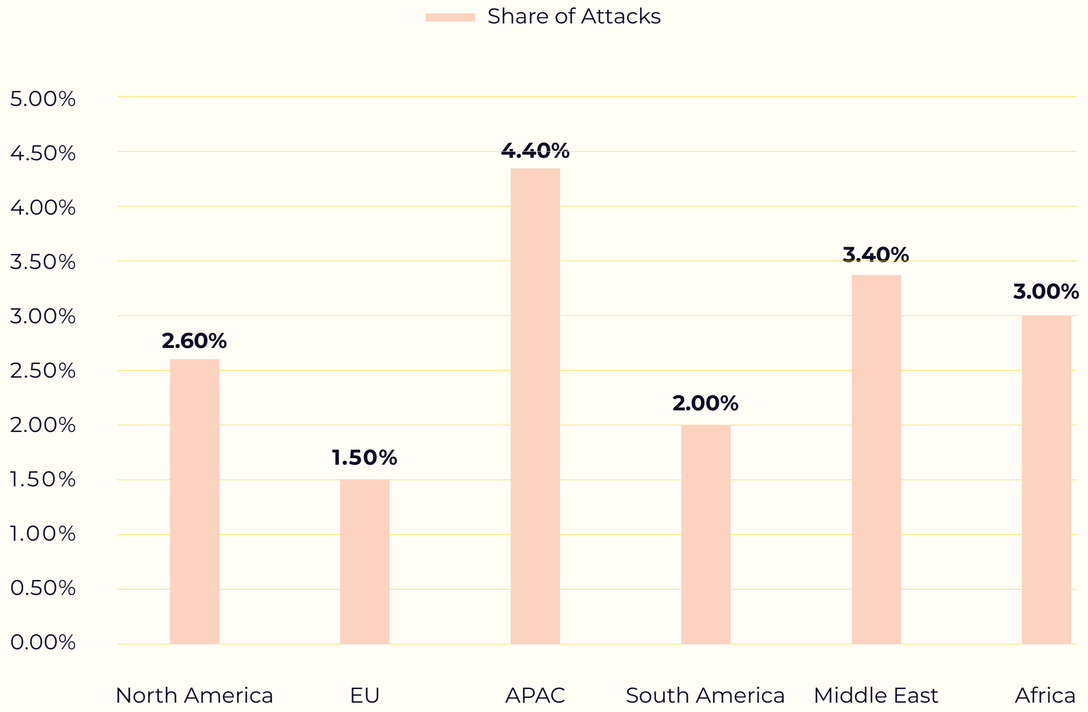
North America and APAC are big targets of organized fraud

While North America's **2.6%** take of professional attacks seems low compared to other regions, it represents a conspicuous surge of **44%** in orchestrated identity fraud cases, indicating a notable escalation from the **1.8%** we saw in Q1. So why don't we see a similar trend across all regions? Simple - the economic recuperation of the US has inadvertently created an environment that empowers proficient syndicates specializing in identity fraud.

During this period of heightened activity, the Asia-Pacific region has surfaced as the prime focus for malicious actors, with more than **4%** of transactions being identified as instances of identity fraud. This notably elevated percentage far exceeds the prevalence observed in comparable global regions. AU10TIX associates this concerning trend with the historically weaker anti-fraud measures in the Asian market, designating it as a vulnerable target that entices malicious individuals.

Entities based in the EU and South America encounter a relatively lower attack rate of **1.50%** and **2.0%**, respectively, primarily attributed to their proactive approach of verifying identifications against robust government databases. This practice establishes a stronger defense against fraudulent activities.

Q2 ID Fraud Professional Attack Rate by Region



This data represents the percentage of fraud transactions out of the total transactions of each region.

Fraud by **Industry**

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

Crypto and payments more attractive to professional fraudsters

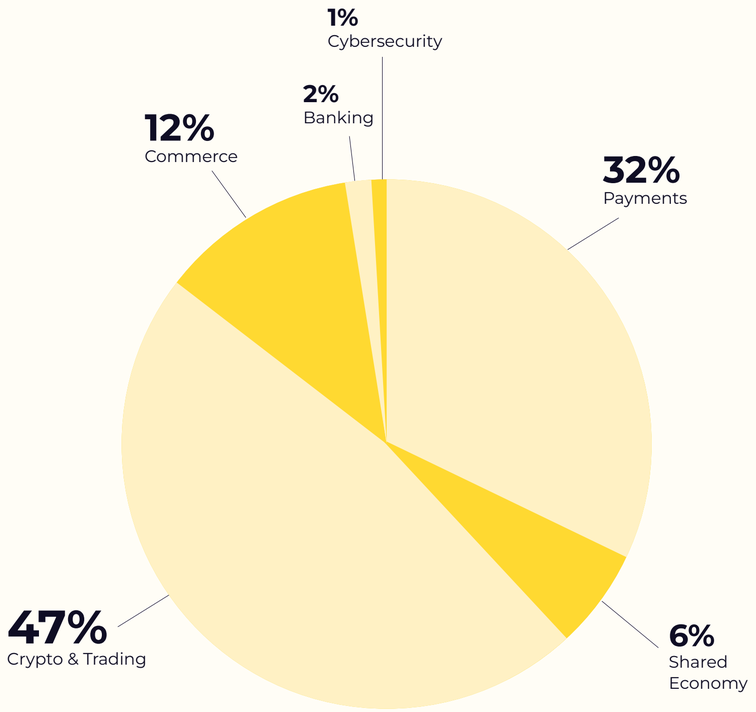
Among the sectors scrutinized, cryptocurrency and trading are the most highly targeted, making up 47% of the attacks detected by AU10TIX in Q2. These industries attract professional fraudsters due to their perceived high-profit prospects and inherent anonymity.

Furthermore, payments appear to be more attractive to organized fraudsters than Commerce, with 32% of attacks from this sector compared to the latter's 12%. This divergence is likely attributable to the assumption that financial institutions invest more significantly in robust protective measures.

An undeniable indicator of the flourishing success within the realm of payment service providers (PSPs) is the heightened susceptibility to financial crimes. If left unaddressed, this susceptibility could jeopardize the very existence of PSPs. Regulatory scrutiny is inevitable as perceived vulnerabilities in the controls implemented by electronic payment platforms draw regulatory attention.

Moreover, banks are increasingly anticipating robust anti-money laundering (AML) and fraud prevention measures from the PSPs within their network. Rather than passively awaiting new regulatory mandates, PSPs can take proactive steps by assimilating insights from the banking sector's experiences and leveraging AU10TIX's technological expertise.

Attacked by Industry



Mode of **Attack**

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

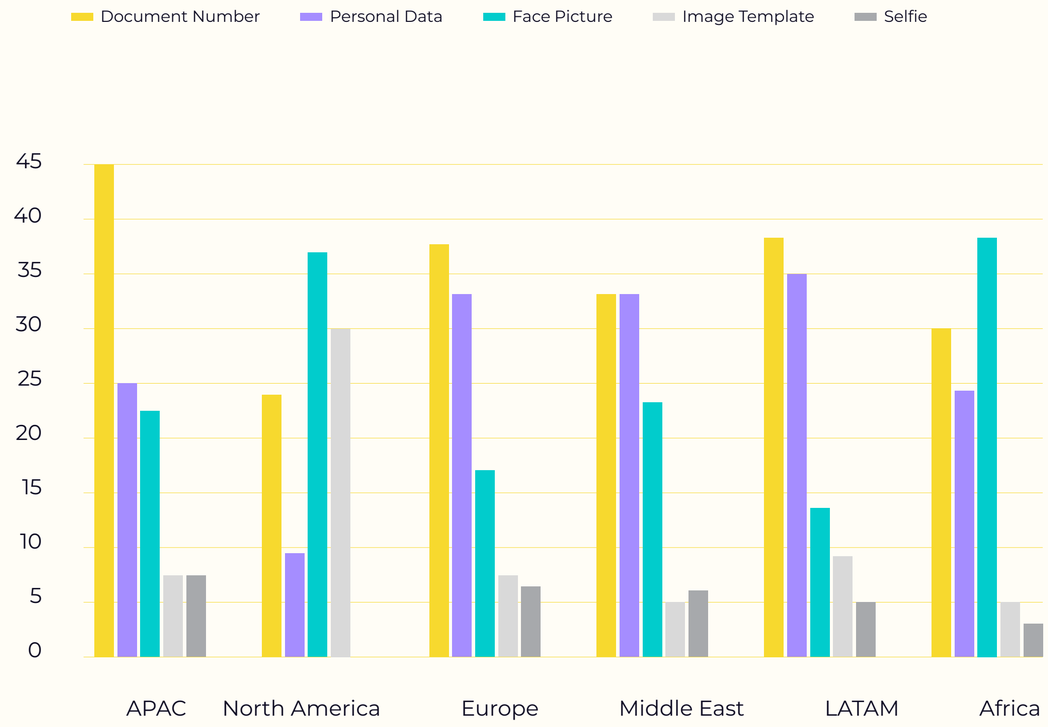
Advanced biometrics that include liveness detection and consortium validation as part of a multilayered defense strategy prove crucial in the defense against professional fraud rings.

The data analysis underscores a significant and notable discrepancy in attack modes based on document verification (averaging 37%) compared to attacks using selfies (averaging 5%).

This stark contrast highlights the importance of implementing a multilayered identity verification system incorporating liveness testing, biometric verification, and consortium validation, and demonstrates that professional fraudsters are still using traditional modes such as personal data and document numbers to generate synthetic identities used in coordinated attacks.

We track all types of anomalies, including visual and data (significantly higher than other competitors) as well as repetitions and conflicts based on non-ID data.

Attack Modes Per Region



Targeted **Documents**

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

In Q2, Permanent Residency Cards are fraudster's top pick this quarter

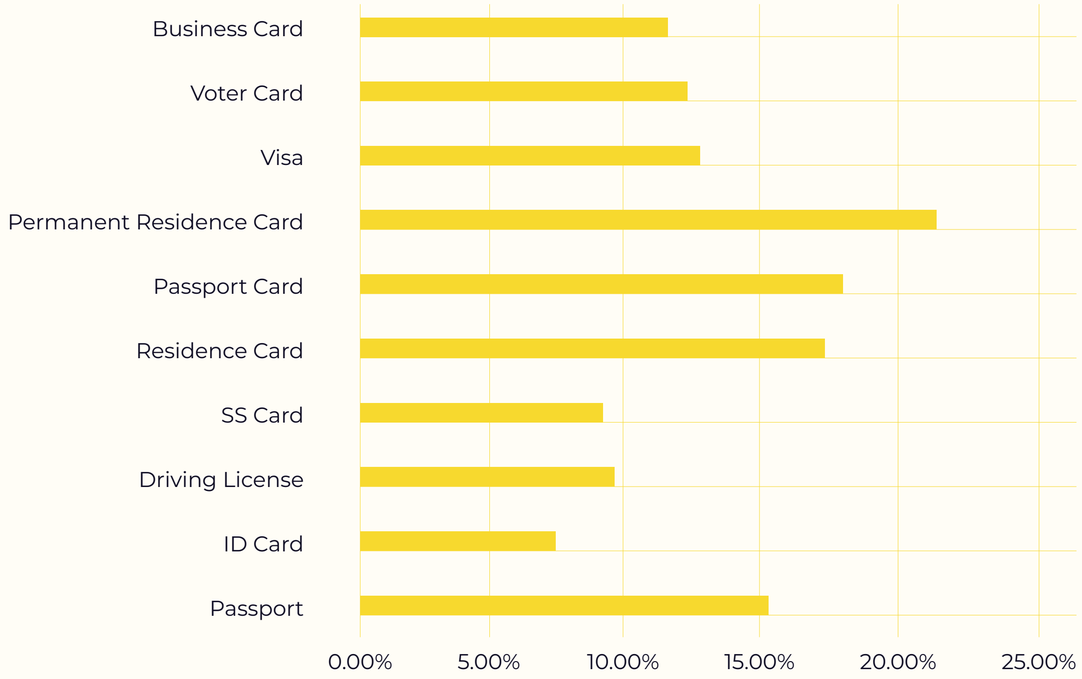
This quarter, fraudulent activities involved the misuse of Permanent Residency Cards. Our data reveals that 22% of all Permanent Residency Cards submitted for identity verification were spotted as counterfeit by AU10TIX. This starkly contrasts with Q1, where passports ruled the charts at 28% and Permanent Residency Cards hovered at 20%.

Why Permanent Residency Cards?

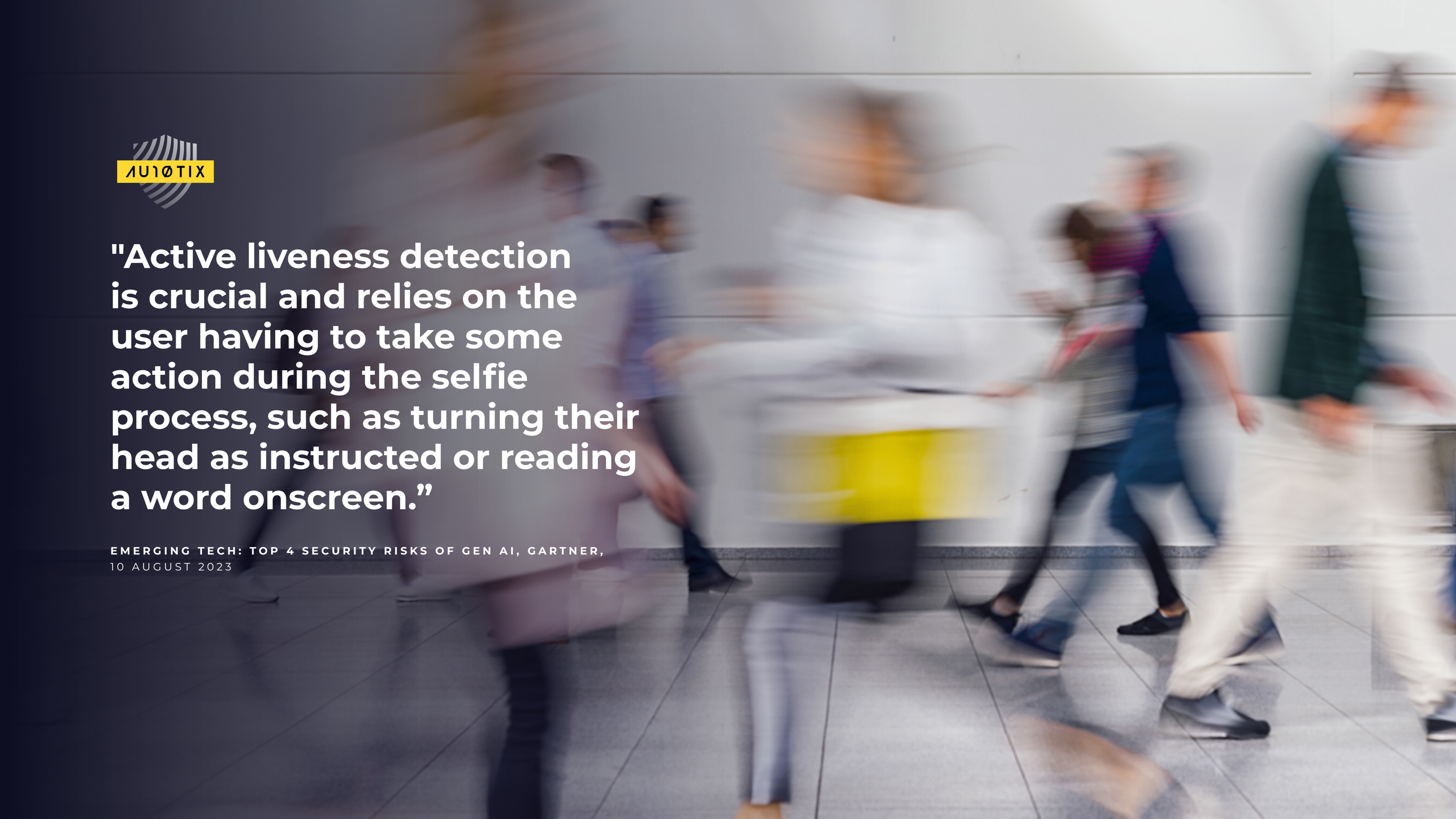
1. Simpler to Forge
Permanent Residency Cards are perceived to have simpler security features, making them an easier target for forging compared to more sophisticated IDs like passports.

2. Less Scrutiny
Due to lower familiarity, Permanent Residency Cards may face less scrutiny during verification processes, allowing fraudsters to exploit this lack of attention to detail.

Q2 Top 10 Most Forged Documents



Percentage of forgeries detected per document type



"Active liveness detection is crucial and relies on the user having to take some action during the selfie process, such as turning their head as instructed or reading a word onscreen."

EMERGING TECH: TOP 4 SECURITY RISKS OF GEN AI, GARTNER,
10 AUGUST 2023

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

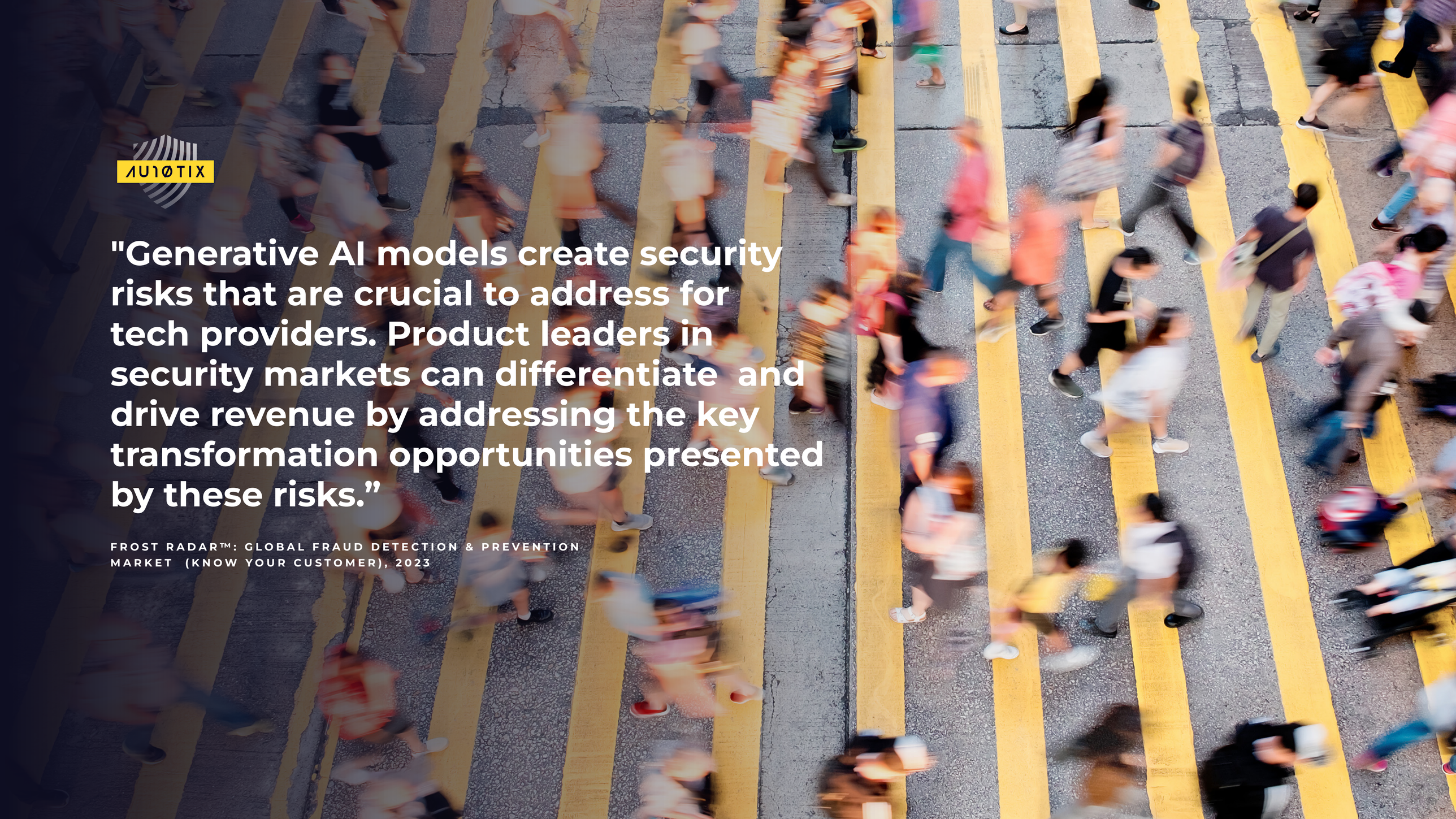
Are you ready to face the future of AI-generated fraud?

The integration of Gen AI and intelligent malware is elevating the efficacy of malicious actors, introducing a higher degree of automation, and amplifying the independence of attacks. Concurrently, this advancement substantially bolsters the toolkit available to both attackers and defenders.

AU10TIX's Serial Fraud Monitor has detected telltale signs of escalating organized criminal activity. The patterns identified by this proprietary tool distinctly differentiate between sophisticated, professional fraud and more amateurish attempts, providing crucial insight into the evolving nature of fraudulent activities at a traffic level.

AU10TIX recognized the role of Generative AI on identity fraud and is utilizing advanced recognition algorithms to detect synthetic content.

Ron Atzmon, Active Chairman, AU10TIX



"Generative AI models create security risks that are crucial to address for tech providers. Product leaders in security markets can differentiate and drive revenue by addressing the key transformation opportunities presented by these risks."

FROST RADAR™: GLOBAL FRAUD DETECTION & PREVENTION MARKET (KNOW YOUR CUSTOMER), 2023

SPOTLIGHT ON HIDDEN GEOGRAPHICAL AND INDUSTRY TRENDS

It is increasingly difficult to tell reality and fiction apart...

There is an overall increase in sophisticated fraud. Why? Gartner has identified fraud and identity risks as one of the top emerging security risks within Generative AI. LLMs (Large Language Models) and chat interfaces have enhanced malicious actors' ability to mimic genuine sources and complicate the task of differentiating between forgeries and the real thing. This underscores the necessity for solution alignment that focuses on detecting and defending against a surge in prompts and injection attacks on LLM and API interfaces.

AU10TIX fraud detection tools, most notably Serial Fraud Monitor, detected an upswing in professional organized attacks utilizing various attack modes across geopolitical regions and industries, most notably in the United States and in the vulnerable crypto trading and payments verticals.

Serial Fraud Monitor is the only fraud detection tool of its kind on the market. Its analyst-recognized award-winning technology enhances your tech stack with the big picture on traffic patterns and offers the flexibility of closed garden, network, or consortium level validation.

AU10TIX stands at the forefront, equipped with a cutting-edge suite of services dedicated to combatting identity fraud and ensuring a secure digital realm. Our commitment to safeguarding the digital landscape through restless innovation empowers us to offer future-proof technology that outsmarts fraud.

One of our recent Serial Fraud Monitor customer success stories:

99.83%

Achieved 99.83% precision in fraud detection.

21,000

Discovered 21,000 falsely approved serial fraudsters out of 27,000 during the pilot stage since December 2022

4

Identified four countries accounting for 90% of total indications: Sri- Lanka: 71% (19,000), Morocco: 7 (1,900), Vietnam: 6% (1,600), Malaysia: 6% (1,600)

“[AU10TIX] leading position on the Frost & Sullivan Innovation Index reveals its investment commitment to research and development, focus on homegrown technologies such as neural network ML for detection, and detection AI models to protect against advanced synthetic forgeries.”

FROST RADAR™: GLOBAL FRAUD DETECTION & PREVENTION MARKET (KNOW YOUR CUSTOMER), 2023

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:
Mark Prindle, Fusion PR
au10tix@fusionpr.com

Resources and Further Reading

FROST RADAR™: GLOBAL FRAUD DETECTION & PREVENTION MARKET (KNOW YOUR CUSTOMER), 2023

EMERGING TECH: TOP 4 SECURITY RISKS OF GEN AI, GARTNER, 10 AUGUST 2023

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.