September 2023

The 2023 Impact Awards in Fraud

Fraud & AML Practice

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

Datos Insights' Impact Awards in Fraud aim to identify and recognize those organizations and vendors leading the industry and pioneering new and disruptive financial crime products and capabilities. Award recipients and their innovations are bringing the financial services industry one step closer to triumphing over fraud, money laundering, and other illicit activity.

The winners of the 2023 Impact Awards in Fraud follow:

- **Incognia: Best Digital Identity Verification Innovation.** Incognia's Fraud and Risk Platform harnesses device intelligence and precise location data to provide risk analysis and actionable insights that help businesses prevent fraud, protect users, and build customer trust. The platform has proven invaluable in lowering false positives, reducing identity fraud upon new account creation, and reducing account takeover (ATO) fraud losses.

Introduction

Datos Insights' 2023 Impact Awards in Fraud aim to identify and recognize those financial organizations and vendors leading the industry with new and disruptive financial crime products and capabilities. Award recipients and their innovations are bringing the financial services industry one step closer to triumphing over fraud, money laundering, and other illicit activity.

Datos Insights designated the following four individual categories for its 2023 Impact Awards in Fraud:

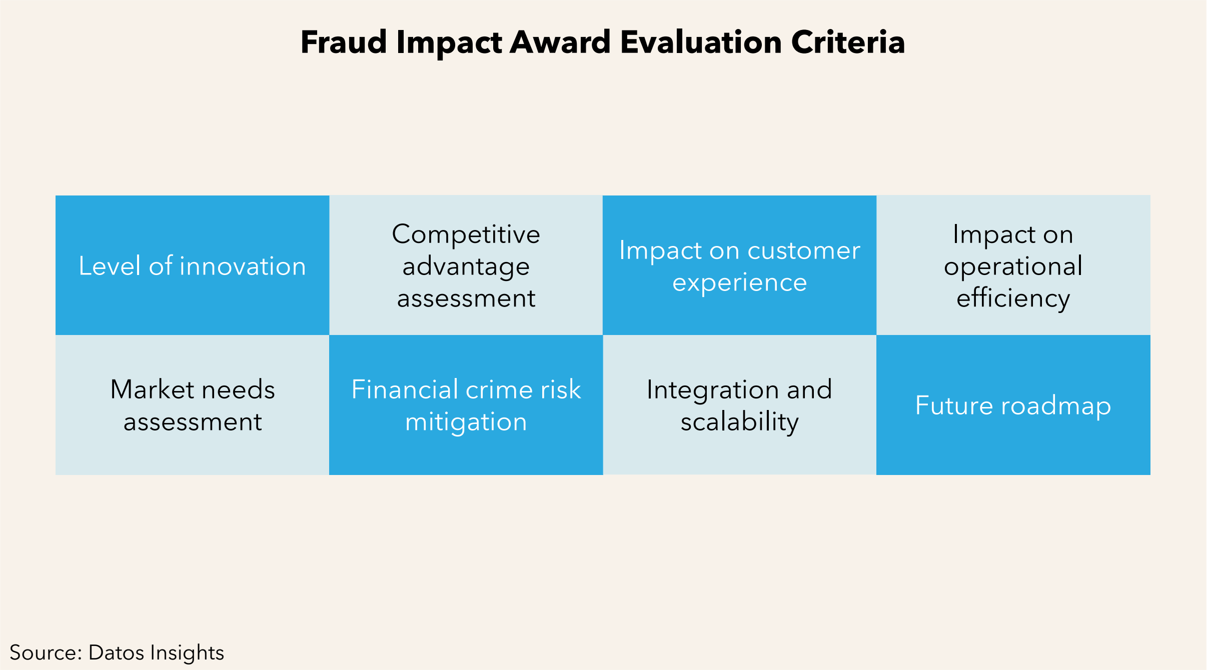
- **Best Authentication Innovation:** New solutions or innovations that deliver best-in-class identity proofing or user authentication
- **Best Transaction Fraud Monitoring and Decisioning Innovation:** New solutions or innovations that deliver superior transaction fraud analytics, monitoring, detection, and case management that protect the financial transaction
- **Best Digital Identity Verification Innovation:** New solutions or innovations that deliver exceptional individual identity verification
- **Best Innovation by an FI:** New solutions or innovations developed and implemented by an FI that deliver robust fraud mitigation while supporting elevated customer experience and operational efficiency

Qualification and Evaluation Methodology

In April 2023, Datos Insights solicited nominations for its 2023 Impact Awards in Fraud. All nominated initiatives were required to be in production and must have been implemented within the last two years. Strategic Advisors from Datos Insights' Fraud & AML practice, along with an external panel of subject matter experts and industry thought leaders, evaluated the submissions and determined the individual category winners.

Each fraud nomination was evaluated across several criteria (Figure 1).

Figure 1: Impact Award Evaluation Criteria



Fraud Impact Award Evaluation Criteria

Level of innovation	Competitive advantage assessment	Impact on customer experience	Impact on operational efficiency
Market needs assessment	Financial crime risk mitigation	Integration and scalability	Future roadmap

Source: Datos Insights

The Fraud Market: Challenges and Needs

Sustaining effective financial crime risk management remains extremely challenging and complex. The breadth of fraud technology solutions must go beyond traditional capabilities to take on new market forces and combat expanding fraud while elevating the customer experience and uplifting operational efficiency.

Table A identifies several key fraud challenges that financial organizations and technology solution providers seek to address with innovative tools and approaches.

Table A: Fraud Market Challenges

Fraud Challenge	Impact
Greater sophistication and volume of fraud and scams	As more people and organizations conduct business online, new fraud vectors have emerged for financial criminals to exploit. Fraud and scams such as APP and ATO are on the rise, and emerging technologies like generative AI are helping criminals refine their techniques and make social engineering more sophisticated. Liability for fraud losses is shifting from the consumer to the FI. These factors are motivating FIs to replace legacy solutions with newer, sleeker ones that can address fraud risks across the customer life cycle. Solutions that harness automation, ML, and other cutting-edge technologies are invaluable in navigating the ever-evolving threat landscape. Further, FIs are turning towards solutions that allow for the sharing of data.
Increasing customer experience expectations	Customer experience expectations are becoming more stringent as they increasingly interact with digital channels, from online banking to e-commerce. Customers can be unforgiving in the cases of slow service, clunky authentication, and a decline due to suspected fraud. FIs cannot merely look to bolster their fraud defenses; they must seek to provide frictionless customer experiences alongside risk mitigation. Solutions that offer fast, behind-the-scenes fraud prevention are critical in today's financial crime landscape.

Fraud Challenge	Impact
Emergence of new payment types	Peer-to-peer (P2P) and real-time payments are gaining in popularity. FIs are thus responsible for devising new fraud risk management approaches to these methods while still elevating their approaches to legacy payments such as checks and cash. The emergence of digital-asset payments has led FIs to rethink their fraud mitigation protocols, as the digital assets industry has fueled new methods of carrying out fraud and scams.

Source: Datos Insights

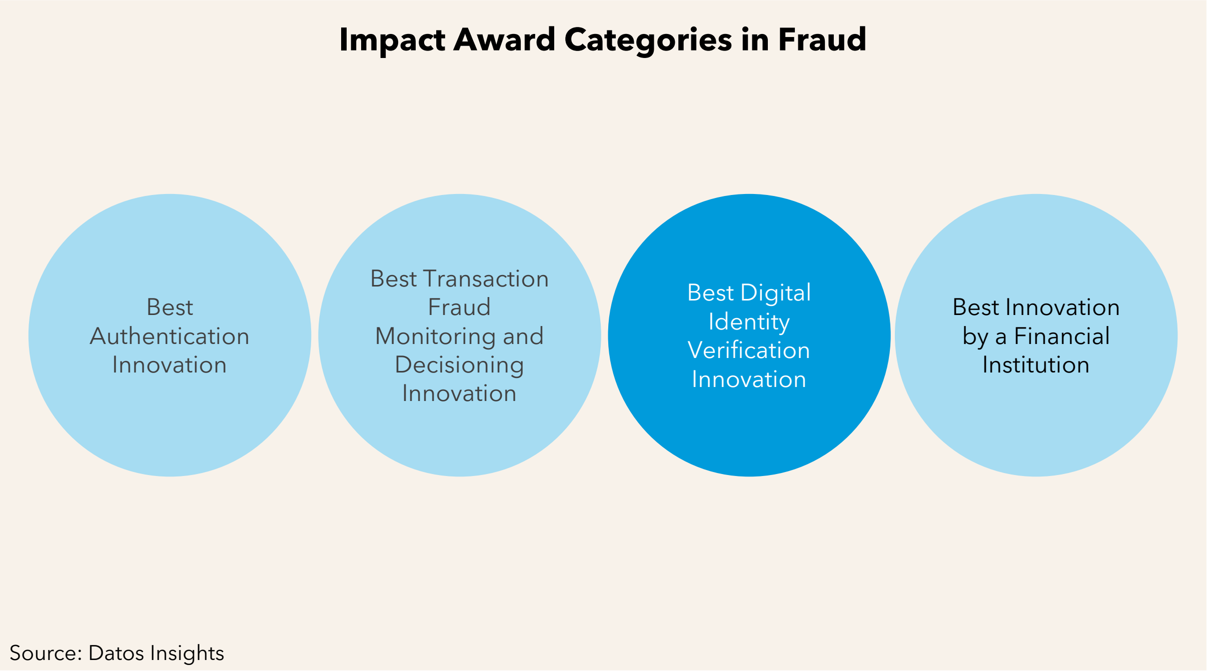
Incognia

By: David Mattei

Incognia is an innovator in location identity solutions that deliver cutting-edge user verification and account security across the digital journey. Incognia's novel approach leverages over a decade of expertise in location technology to provide frictionless experiences using device intelligence and precise location data. Incognia enables customizable risk analysis and actionable insights from day one, empowering consumer-focused businesses to prevent fraud, protect users, and build customer trust.

Incognia is the recipient of the Impact Award for Best Digital Identity Verification Innovation (Figure 2).

Figure 2: Impact Award for Best Digital Identity Verification Innovation—Incognia


Impact Award Categories in Fraud
Best Authentication Innovation
Best Transaction Fraud Monitoring and Decisioning Innovation
Best Digital Identity Verification Innovation
Best Innovation by a Financial Institution

Source: Datos Insights

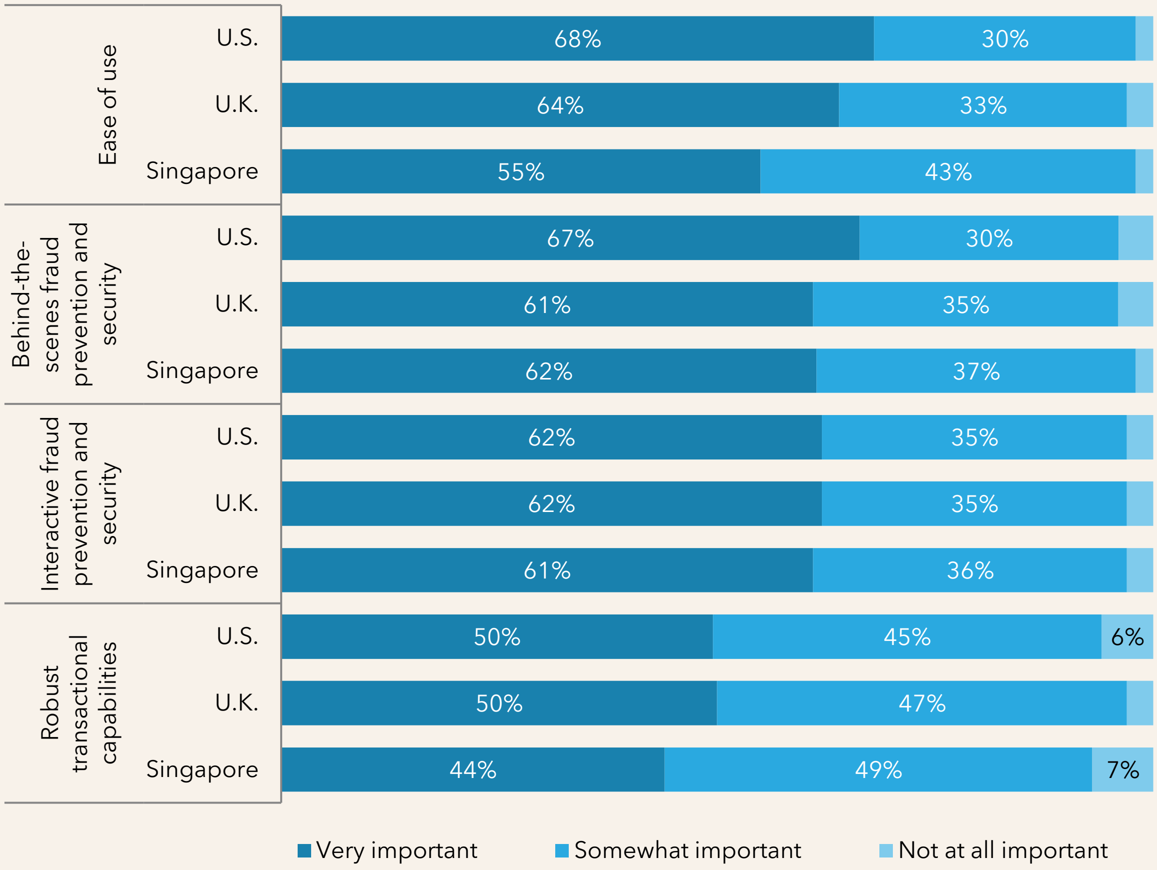
Market Challenges and Needs

Fraud executives are realizing that stopping the fraudster at the point of the financial transaction is too late in the overall process. It is becoming increasingly harder to stop fraud at that stage and a never-ending game of whack-a-mole. Fraud practitioners realize that fighting fraudsters needs to occur much earlier—at the authentication stage—thus keeping fraudsters out of the banking system. Doing so requires a careful balance of security, accuracy, and good user experience. Achieving all three is a challenge.

In a Datos Insights consumer survey of 2,276 consumers in the U.K., U.S., and Singapore in Q3 2022, the two most important criteria for online banking services cited were ease of use and behind-the-scenes fraud prevention and security (Figure 3).[1] Delivering on these expectations while protecting the FI requires a carefully crafted plan.

Figure 3: Consumer Values in Digital Banking Services

Q. How important the following to you when you're considering using your FI's online banking services?
(Base: 1,025 U.S. consumers, 901 U.K. consumers, and 350 Singapore consumers)



Source: Datos Insights survey on consumer online authentication methods, Q3 2022

[1] See Datos Insights' report Global Consumers' Authentication Preferences: Between Fraud and Friction in Digital Banking, March 2023.

Consumers are becoming more digitally savvy and have high expectations of their online banking and shopping experiences. Industries outside financial services are developing smooth and seamless user experiences, shaping consumer expectations. FIs should not benchmark their digital banking channel against other FIs. Rather, FIs need to look beyond the financial services world to industries that deliver optimal user experiences.

Innovation: Incognia's Location Fingerprint

Incognia has approached the authentication problem by tracking a user's location and creating a location signature that tends to be unique for each individual. Table B lists key information about this innovation.

Table B: Location Fingerprint

Category	Details
Firm	Incognia
Innovation	Incognia introduced a cross-device fingerprint that leverages an innovative new attribute, exact location, to offer the next-generation device recognition solution. Its passive user verification and authentication, high precision, and low false positive rates prevent account takeover fraud and verify identity.
Official launch date	May 2023
How it works	The innovation uses a combination of GPS, WiFi, Bluetooth, and connected devices, along with frequently visited location information and device attributes, to verify and authenticate a user with ultra-low false positives.
Key benefits	The top three benefits include tamper resistance, persistent device recognition, and frictionless user experience: • It detects several app and device manipulation techniques, such as root access, app cloning, emulation, and GPS spoofing • It uniquely identifies a device across all clients, and even when the user resets the device to factory defaults • As a passive authentication solution, it runs in the background, transparent to the user
Future roadmap	• Smarter and more integrated solution for digital banking (online and mobile) • Expansion into new industry verticals that are location-focused

Source: Incognia, Datos Insights

Incognia's Location Fingerprint uses multiple data points to ascertain a user's precise location and information about the user's mobile device. Its location triangulation creates signal environments using GPS, WiFi, and Bluetooth, assigning these environments context based on the device's behavior. This offers a precise geolocation reading for every device.

Users are creatures of habit, and there are patterns in the locations they visit (e.g., home, work, and shopping). This information is included with the location data to determine whether a location is in or out of pattern for each user.

Target Market

The Incognia solution works best when deployed on mobile devices, though it still delivers value in an online/web environment. It focuses on banks, credit unions, fintech firms, and cryptocurrency companies, which commonly have a mobile app. The solution works well for gig economy firms, such as food delivery and peer-to-peer marketplaces. It has expanded into other industries where location is important.

How It Works

A client deploying Location Fingerprint typically uses the provided software development kit (SDK) to integrate the Incognia solution into the client's mobile app. Users are prompted to consent for their location data to be used for fraud mitigation. The SDK collects data through the mobile device's sensors to create a unique profile for each user based on location behavior. A risk score and supporting evidence are provided to the client so they can take appropriate action. This process does not store personal identifiable information (PII) data, making it a data-privacy-centric solution.

Many device fingerprinting solutions have a one-to-one relationship between a user and the user's device. If a user switches devices, the solution will recognize that this is a new device but is unaware that it is the same user. Therefore, a new user is created within the solution. Leveraging the user's location information, Incognia recognizes that this is the same user with a new device, providing continuity within a fraud or authentication solution.

In most deployments, a prospective client begins with a proof of value in which the SDK is embedded in the mobile app and allowed to run for 30 days to collect data. Unlike traditional proofs of concept, Incognia's proof of value allows businesses to test Location Fingerprint in production, analyze its performance, and measure potential ROI without disrupting clients' existing processes. Afterward, known good and known fraud data is shared with Incognia to measure two aspects of the system's performance.

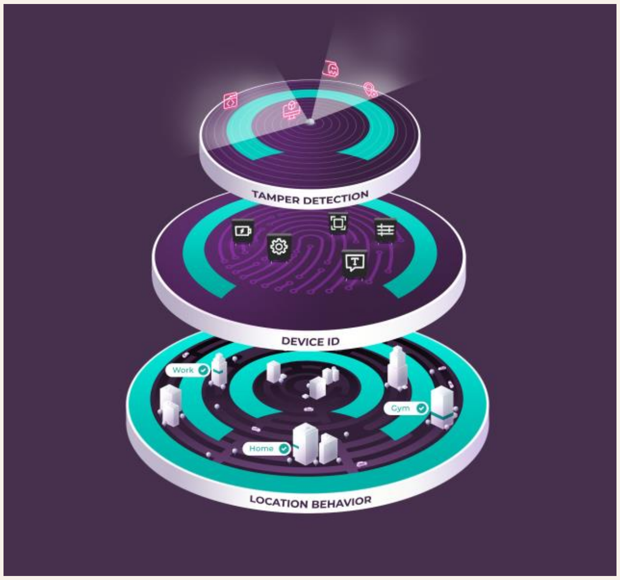
- Incognia will compare the client's known fraud data with its fraud markers to determine how much of it would have been identified upfront.

- Using the known good data, Incognia can estimate the number of stepped-up authentications that could have been avoided or the number of legitimate accounts that could have been opened without requiring the user to provide documentation.

ML models are another core component of Location Fingerprint used to improve location accuracy and recognize fraud patterns. This is useful when analyzing location data in densely populated areas. The ML models can even differentiate between apartments within the same building. This is critical to reducing false positives and ensuring a good experience for legitimate users while at the same time detecting bad actors. Figure 4 provides an overview of Location Fingerprint.

Figure 4: Incognia – Location Fingerprint

Incognia – Location Fingerprint



Source: Incognia

Location Fingerprint works on mobile apps, mobile devices, and browsers running on a PC-based device. However, the data available on a mobile device is much richer than a PC-based browser. Location accuracy on mobile is within 10 feet; on PC-based devices, location accuracy is within 30 feet.

Tuning the system for a client involves configuring various system parameters and writing fraud rules similar to other commercial fraud systems. Rules and ML models handle edge cases, while location data handles more mainstream location identification needs.

It takes one user interaction to uniquely identify a new device. In a scenario where a new user is on a new device in a residence Incognia hasn't seen before, it could take between three and five user interactions to uniquely identify the person. However, if the FI shares users' home addresses with Incognia, the user can be uniquely identified on the first interaction.

Key Quantitative and Qualitative Results

In today's world, where data privacy concerns abound, Incognia's solution is interesting because it uses only one piece of PII: location. Location Fingerprint leverages location and non-PII data collected from the mobile phone in combination with its consortium of device information, including device reputation and history.

Many solutions on the market for identity proofing and user authentication are device-centric instead of user-centric. For example, risk is assessed based on the device's attributes, history, and association with bad behavior. When a user upgrades or resets the device to its factory defaults, these solutions see it as a new device and a new user. They cannot recognize that it is the same user with a new or reset device. Location Fingerprint is user-centric; it assesses a user's reputation and knows their history across device resets and new purchases.

Across its client base, Incognia has shared that its customers have achieved the following benefits:

- Location Fingerprint uniquely identifies 99.9999% of users with just three location data points, making it a powerful identification signal.
- False positive rates are as low as 0.01%.
- Identity fraud at the time of new account creation is reduced by up to 95%.
- It has a 97% success rate at identifying emulated devices, which is common with fraudsters using sophisticated software to mimic a mobile device rather than possessing one.
- There is a 90% reduction in ATO fraud losses.

Future Roadmap

Incognia solutions are available for both mobile app and browser-based services. By integrating these channels, Incognia plans to build a more comprehensive fraud prevention platform to enhance its financial services offering. Incognia is continually developing its device ID and fingerprinting solutions to provide a highly persistent and reliable device recognition solution.

Datos Insights' Take

There are numerous categories of commercial authentication solutions and multiple vendors within each category. Location Fingerprint stands out in the authentication space for its novel method of uniquely identifying an individual. While not sufficient to serve as the only tool in an authentication control framework, Location Fingerprint should be able to address the majority of use cases (mainly new account creation and account logins) and reduce the need for stepped-up authentication. Location Fingerprint will identify instances when there is ambiguity of who the user is and additional tools are needed.

Several factors make Incognia's offering deserving of an Impact Award for Best Digital Identity Verification:

- Passive authentication provides an elevated user experience.
- Consumers tend to be creatures of habit, including where they live, work, and shop. These patterns and behaviors, especially when combined with connected devices, create a unique signature of an individual, which is ideal for user verification and authentication.
- The precision of Location Fingerprint can go as far as to identify individuals within an apartment building, including those with good or bad intent.
- Device fingerprinting, location data, and Incognia's consortia data can provide strong risk signals that can be leveraged across its client base. Few device fingerprinting solutions offer this capability today.

With its Location Fingerprint solution, Incognia is gaining traction in the user verification and authentication space. As more roadmap items come to market, it will deliver a strong combination of unique identification, strong risk signals, and a good user experience via its low-friction approach.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author Information

Gabrielle Inhofe

ginhofe@datos-insights.com

Contributing authors:

David Mattei

dmattei@datos-insights.com