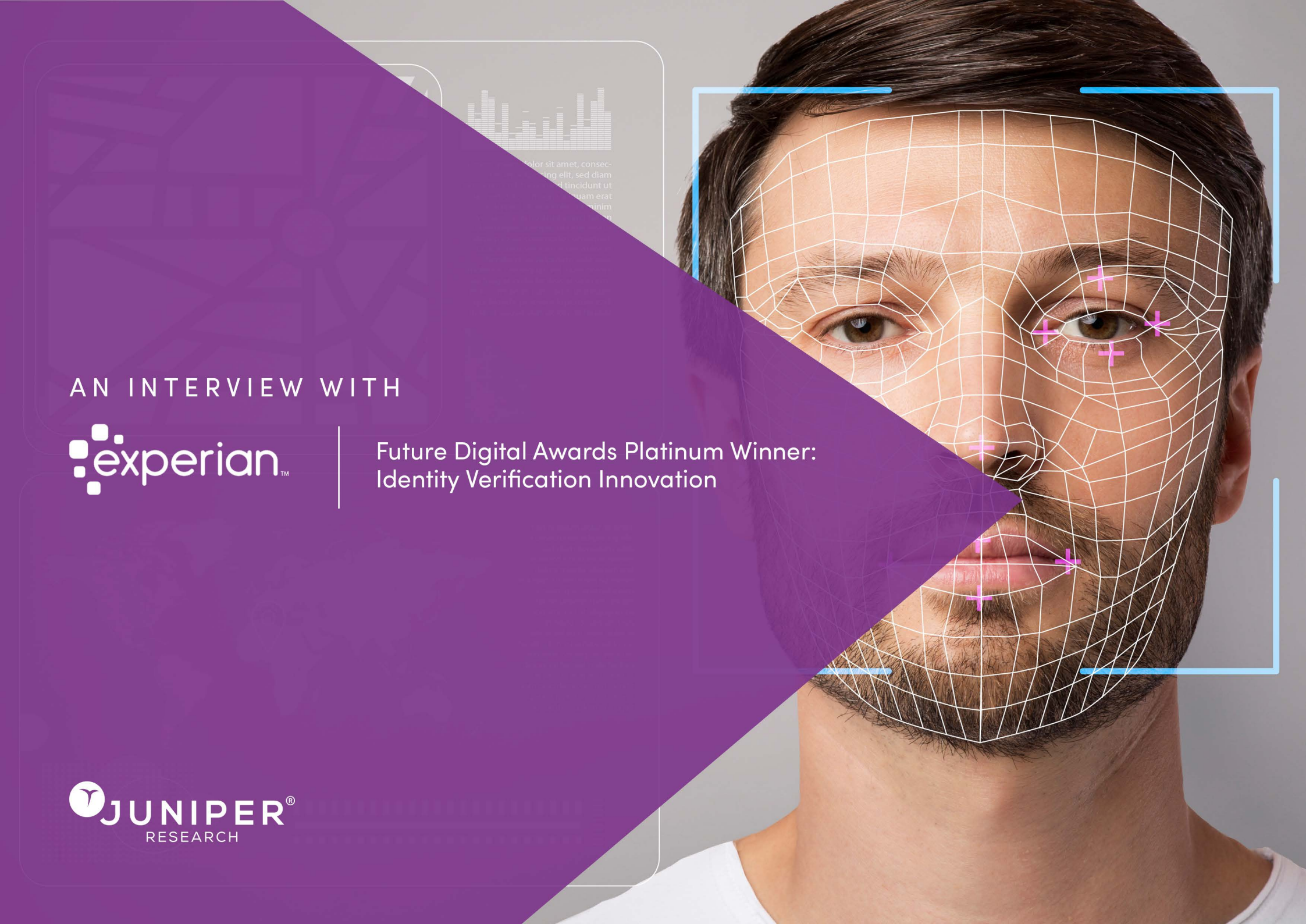
AN INTERVIEW WITH

experian™

Future Digital Awards Platinum Winner: Identity Verification Innovation



JUNIPER® RESEARCH

Mover & Shaker Interview with Experian: Future Digital Awards Platinum Winner, Identity Verification Innovation

Juniper Research interviewed Keir Breitenfeld SVP, Fraud & Identity, North America in December 2024.

Keir Breitenfeld currently serves as Senior Vice President of Experian's Fraud and Identity line of business within the North American region, leading product management and portfolio marketing teams.

Keir has been with Experian for more than 18 years, most recently as Senior Vice President of Portfolio Marketing strategy and execution. He has also held various individual and leadership roles in product management, consulting, and go-to-market strategy.

Keir's background prior to joining Experian in 2005 includes serving as a Director of Product Management with both HNC Software and Fair Isaac Corporation and leading fraud detection and prevention units at both Fleet/Advanta Credit Card Services and Capital One Financial Corporation. Keir also spent time with FinTech start-up, Trulioo, a global identity bureau, where he worked with partners worldwide to maximize market penetration and operational performance in KYC/AML related use cases.

Keir holds a B.S. degree from Auburn University and an M.B.A. from Duke University. Prior to entering the information services and technology arena, he served in the United States Navy as a Surface Warfare Officer aboard the guided missile frigate USS Estocin (FFG-15).

How do Experian's AI-powered fraud solutions differentiate between legitimate customers and bots?

With the growing fraud threat, it is important that companies review many different signals in order to balance potential threats with customer experience. Leading companies are starting to use behavioral analytics look at attributes that are truly unique to each consumer and are difficult for a bot to replicate.

Experian leverages NeuroID's behavioral analytics to analyze user typing patterns, mouse movements, navigation behaviors, and hundreds of other interactions to differentiate between bots and legitimate customers. Our behavioral analytics detect deviations from typical human behavior, such as the hyper-speed and consistency patterns of bots. Experian's behavioral analytics identify intent and risk without relying on personal identifiable information (PII), making it highly effective against bots that are able to evade traditional defenses.

How frequently does Experian update its AI models to adapt to new bot and fraud techniques?

The pace of change across our industry continues to increase with advancing technology. Updates have to be tailored to individual needs and market changes, not just on a specific schedule.

Experian's behavioral analytics are updated depending on fraud trends and customer needs. We look at a constant feedback loop to incorporate real-world outcomes and feedback from extensive fraud data assets, ensuring our models stay ahead of evolving fraud tactics, including those leveraging next-gen bots that were built to beat behavior.

What types of data does Experian use to train its AI models for bot detection?

The need for a comprehensive range of data inputs to accurately distinguish genuine user interactions from automated, fraudulent bot attempts is incredibly important. This includes traditional data used to track identity and fraud, but also cutting-edge data like behavioral analytics.

Experian's NeuroID has translated more than a trillion behavioral data points to help differentiate between legitimate customer behavior vs. bots behavior, for fraud detection without sacrificing conversions or adding friction. Experian behavioral analytics use a combination of behavioral data (e.g., keystroke dynamics, mouse movements, and interaction timings), device intelligence (e.g., device fingerprinting and IP information), and network data. When behavior is combined with device, these data points are anonymized and synthesized with historical fraud patterns to build predictive models. Generative AI-enhanced bot attacks are specifically countered with dynamic datasets that can capture next-gen bot risk.

How does Experian's AI technology balance bot detection with minimising false positives for legitimate users?

It is important for organizations to find the right balance between risk appetite and customer experience, which is why our AI-driven fraud technologies are engineered to find the ideal equilibrium between stringent security measures and a seamless user experience.

The key lies in layering multiple data signals - behavioral, device, and identity - at different points in the customer journey. Behavioral analytics serve as a pre-submit checkpoint, creating a nuanced risk profile before a user even completes a form, while high-fidelity, deterministic signals are then calibrated into a granular risk score, allowing organizations to automate decisions, fast-track legitimate users, and introduce additional verification steps only when strictly necessary. By measuring interactions against a baseline of legitimate user behavior, businesses can flag bots with more precision, for fewer false positives, ensuring that trust, growth, and conversion aren't compromised for security.

How well can Experian's AI solutions detect and prevent fraud attempts using generative AI to create synthetic identities?

Synthetic identity is a growing problem and some that we believe many organizations do not fully understand the extent of today. Experian's behavioral analytics combat synthetic identity fraud by analyzing a user's interaction patterns, instead of relying on personal identifiable information (PII) that can be easily spoofed with generative AI. It identifies deviations from legitimate user behaviors, such as overly consistent or unnaturally fast actions.

Even when identity documents appear authentic, behavioral signals can detect abnormalities that signal a fraudster or bot. Additionally, persistent device and network analysis help detect even advanced synthetic identities.

How does Experian's platform incorporate bot detection into its broader fraud prevention strategy?

There are a number of different data points and signals to take into account when looking at the various types of fraud and overall fraud prevention. It is important for these different signals to connect with each other and to maintain a feedback loop to understand changes as they are happening in the market.

Experian offers a full set of fraud capabilities, integrated through a single platform, that combats all types of fraud risk at account opening to a client's portfolio management. Our best-in-class strategy orchestrates multiple fraud prevention tools, including behavioral analytics, device intelligence, and network-based risk assessments detection. This combination is integrated anywhere user interaction occurs, with a best practice being to implement at the top of the fraud stack, enabling Experian to flag likely bot behaviors early. This reduces downstream costs and ensures higher accuracy in subsequent layers of fraud detection, such as KYC and compliance checks. The platform's modularity enables businesses to adapt and layer additional tools as fraud tactics evolve.