August 2025

The 2025 Impact Awards in Fraud

Jim Mortensen

This report provided compliments of:

entersekt
The Financial Authentication Company.

Table of Contents

Executive Insights

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 and silver medalists of the 2025 Impact Awards in Fraud are as follows:

Best Authentication Innovation Category

- Entersekt: Best Authentication Innovation. Entersekt combines dynamic authentication methods with robust risk intelligence to combat banking and payment fraud while maintaining an exceptional customer experience. The platform analyzes hundreds of data points in real time to determine appropriate authentication methods based on risk levels and user preferences.

Datos Insights' 2025 Impact Awards in Fraud

The financial crime landscape continues to evolve rapidly, with criminals employing increasingly complex techniques to evade detection. Traditional approaches to AML and fraud prevention are often insufficient to keep pace with these evolving threats. FIs face mounting pressure to enhance their financial crime detection and prevention capabilities while improving operational efficiency and customer experience. In response to these challenges, technology providers are developing novel tools, capabilities, and solutions that leverage progressive technologies, such as data analytics, machine learning, and generative AI. These solutions aim to streamline processes, reduce false positives, uncover hidden risks, and provide more complete and accurate risk assessments.

> *"Datos Insights' 2025 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."*
>
> *Chuck Subrt*
> *Fraud & AML Practice Director, Datos Insights*

As financial crimes become increasingly mature and regulatory scrutiny intensifies, the need for new solutions to combat money laundering, fraud, and other illicit activities has never been greater.

The Fraud Market: Challenges and Opportunities

The breadth of fraud prevention technologies is expected to go beyond traditional capabilities to take on new market forces, combat expanding financial crime, and achieve regulatory compliance while elevating the customer experience and improving operational efficiency. Table A identifies several key fraud challenges that financial organizations and technology solution providers seek to address with forward-thinking tools and approaches.

Table A: Fraud Market Challenges and Opportunities

Fraud challenge	Impact
AI-driven fraud sophistication	Criminals increasingly leverage generative AI and deepfake technology to create fake and manipulated identities, forged identity documents, and convincing video and voice files. Legacy fraud prevention systems struggle to identify AI-generated content, creating vulnerabilities that fraudsters exploit through coordinated attacks and social engineering schemes that blend human psychology with technological manipulation.
Real-time payment vulnerabilities	The rapid adoption of instant payment systems such as FedNow, RTP, and Zelle creates new opportunities for fraudsters to exploit the immediacy and irreversibility of transactions. Traditional fraud controls designed for batch processing cannot deliver the submillisecond decisions required for real-time payments, while APP fraud and social engineering attacks target the speed and finality of these systems. Advanced platforms now provide real-time fraud detection with rapid response times while maintaining sophisticated behavioral modeling capabilities.
Cross-institutional blind spots	Fraudsters operate across multiple financial organizations, exploiting the lack of sufficient shared intelligence and coordinated defense mechanisms. Individual firms are often limited to seeing only their own transaction data, missing patterns that span institutional boundaries and enabling mule account networks to move illicit funds through legitimate accounts. Collaborative intelligence-sharing networks enable real-time risk assessment across institutions while maintaining privacy protections and regulatory compliance.
Authentication vulnerabilities in digital channels	Traditional authentication methods are proving inadequate against sophisticated social engineering tactics and account takeover attempts that exploit human psychology rather than technical vulnerabilities. Static security measures cannot adapt to evolving attack vectors, while customers increasingly expect frictionless experiences that don't compromise security. Context-aware authentication platforms now deliver dynamic risk-based authentication that adapts to user behavior, device intelligence, and transaction context in real time.
First-party fraud detection gaps	Traditional credit risk models cannot effectively distinguish between genuine financial hardship and deliberate intent to defraud, as first-party fraudsters use legitimate identities and established credit histories to commit bust-out schemes and application fraud. Cross-industry consortium approaches now provide broad visibility into consumer behavior patterns, enabling institutions to assess fraudulent intent before losses occur through predictive risk scoring and behavioral analysis.

Source: Datos Insights

Entersekt: Best Authentication Innovation

The winner of the 2025 Fraud Impact Award for the Best Authentication Innovation category is Entersekt for its authentication solution for fraud and scam prevention. This platform combines dynamic authentication methods with complex risk intelligence to combat the growing wave of banking and payment fraud while maintaining an exceptional customer experience.

Founded in 2008, Entersekt is a global provider of cross-channel fraud prevention, payments enablement, and digital security solutions. Entersekt protects key channels such as mobile apps and browsers, leveraging strong device identities and rich risk signals derived from those channels to secure and streamline customer interactions. In the past year, Entersekt has secured 7 billion transactions, demonstrating the scale and trust that major FIs place in its technology.

Datos Insights' Take

Traditional authentication methods are proving inadequate against modern threats, as financial fraud continues to evolve with increasingly convincing social engineering tactics and scam techniques. The industry faces an urgent need for approaches to fraud prevention that can adapt to the rapidly changing threat landscape, particularly as cybercriminals develop more robust techniques to exploit vulnerabilities in conventional security systems.

> *Entersekt's use of proprietary technologies, including multiple patented solutions such as Browser ID, Frictionless SCA, and Proximity Authentication-based step-up authentication, provides significant competitive advantages.*

Entersekt's holistic approach to fraud prevention considers the full context of each transaction rather than relying on isolated data points. By breaking down silos between channels and transaction types, Entersekt's solution can adapt to user preferences, risk levels, and interaction channels. This contextual approach is particularly critical given that a vast number of cyberattacks involve social engineering elements, requiring tools that can go beyond simple identity verification to assess transaction intent and user behavior patterns.

The quantitative results speak for themselves, with clients reportedly experiencing up to 99% reduction in phishing attempts and 90% reduction in APP fraud. Perhaps more importantly, these security improvements have been achieved while maintaining 98% frictionless authentication rates, demonstrating that robust security doesn't have to come at the expense of user experience. Entersekt's use of proprietary technologies delivers unique capabilities that differentiate it from many traditional authentication providers. Entersekt's ability to provide substantial fraud reduction rates while maintaining high authentication success rates demonstrates the effectiveness of its context-aware approach to authentication and fraud prevention.

Innovation: Authentication Solution for Fraud and Scam Prevention

Rather than treating authentication as a stand-alone security measure, Entersekt's authentication solution integrates advanced risk intelligence with dynamic authentication methods to create an end-to-end defense against modern fraud schemes. At its core, the solution embraces the notion that 98% of cyberattacks involve social engineering elements, going beyond traditional identity verification to assess whether the authenticated user should actually be making the transaction.

The platform's architecture collects, curates, enriches, and analyzes hundreds of data points across transactions, user behavior, context, device information, location data, and consortium intelligence, representing fraud indicators from billions of transactions globally. This thorough data analysis enables real-time fraud detection across critical workflows, including account changes, logins, and payment transactions. The solution's ability to process and analyze this large amount of data in real time represents a significant technological achievement that enables FIs to make informed decisions at the speed of digital commerce.

Table B lists key information about Entersekt and its award-winning solution.

Table B: Entersekt Authentication Solution

Category	Details
Organization	Entersekt
Date founded	2008

Category	Details
Headquarters	Atlanta and Cape Town, Western Cape, South Africa
Innovation	Authentication Solution for Fraud and Scam Prevention
Brief description	An authentication platform that combines dynamic authentication methods with advanced risk intelligence to combat banking and payment fraud while maintaining customer experience. The solution analyzes hundreds of data points in real time to determine appropriate authentication methods based on risk levels and user preferences.
Value proposition	Entersekt's solution enables FIs to achieve long-term financial growth through customer-friendly security, resulting in increased deposits, efficient investigations, effective risk management, and regulatory compliance while ensuring customer retention and trust.
Website	entersekt.com

Source: Entersekt, Datos Insights

The solution's novel approach centers on context-aware authentication, which dynamically applies the most appropriate authentication method based on multiple factors, including user preference, interaction channel, and associated risk level. This ensures strong binding between the user and device while enabling passwordless authentication, which improves both user experience and fraud detection capabilities.

Market Challenges and Needs

The authentication and fraud prevention landscape faces several critical challenges that Entersekt's solution addresses:

- Escalating fraud sophistication: Modern fraud schemes have evolved far beyond simple phishing attempts to include novel social engineering tactics, SIM-swap fraud, ATO, card-not-present fraud, and APP scams. Traditional authentication methods struggle to keep pace with these evolving threats.
- Balance between security and experience: FIs face the constant challenge of implementing robust security measures without creating friction that frustrates legitimate customers. Disruptive security approaches often result in customer abandonment and reduced transaction success rates.

- Siloed data and systems: Most FIs operate with disparate fraud detection systems that don't share data effectively across channels and transaction types. This fragmented approach limits visibility and reduces the effectiveness of fraud prevention efforts.
- Social engineering vulnerabilities: Amid a surge in social engineering, traditional authentication methods that only verify identity are insufficient. There's a growing need for solutions that can assess whether an authenticated user should actually be performing a specific transaction.
- Regulatory compliance requirements: FIs must navigate complex regulatory environments, including the Second Payment Services Directive, Strong Customer Authentication, and the General Data Protection Regulation, while maintaining effective fraud prevention capabilities.

Entersekt's authentication solution addresses these challenges through a unified platform that eliminates barriers, shares data across channels and transactions, and provides advanced risk rules and signals that deliver real-time context for each transaction.

How It Works

Entersekt's authentication solution leverages an enhanced architecture that integrates multiple data sources and authentication methods. The platform's key differentiator lies in its ability to consolidate information across various touch points and apply contextual intelligence to determine the most appropriate response for each transaction scenario.

Table C outlines the key features enabling Entersekt's approach to authentication and fraud prevention.

Table C: Authentication Solution for Fraud and Scam Prevention—Key Features

Key feature	Description
Context-aware authentication	Dynamic application of authentication methods based on user preference, interaction channel, and risk level, enabling personalized security experiences that balance protection with usability
Cross-channel data integration	Unified data sharing across channels and transactions, including originating channel, authentication channel, transaction context, historic patterns, and digital banking consortia

Key feature	Description
Advanced risk intelligence	Real-time analysis of hundreds of data points across transactions, user behavior, context, device information, location data, and consortium intelligence from billions of global transactions
Proprietary technology patents	Multiple patented innovations, such as Browser ID, Frictionless SCA, and Proximity Authentication-based step-up authentication that provide unique capabilities
Behavioral analysis	Assessment of user behavior patterns that identify anomalies indicating fraud or social engineering attempts, going beyond simple identity verification
Multimethod authentication	Support for various authentication approaches, such as risk-based authentication, silent authentication using device signals, out-of-band authentication, biometric authentication including passkeys, and proximity authentication
Consortium intelligence	Consolidated device and transaction context across organizations to determine normal and unusual behavior patterns, enhancing fraud detection capabilities through shared intelligence

Source: Entersekt, Datos Insights

The solution's architecture enables seamless integration across multiple use cases, such as digital access, push payments, and 3D Secure authentication. By integrating online fraud detection with authentication systems, the platform creates a feedback loop wherein fraud detection systems provide context to authentication processes, while authentication results feed signals back to fraud detection systems. This approach allows the platform to assess not just whether a user is who they claim to be, but also whether they should be performing specific actions, effectively addressing the social engineering component present in modern fraud schemes.

Key Quantitative and Qualitative Results

Entersekt's solution delivers enhanced customer trust and confidence, streamlined regulatory compliance, and improved operational efficiency through automated fraud detection and response processes. The platform's data analysis and reporting tools provide fraud analysts with the information needed to investigate and resolve fraud cases, significantly reducing investigation time and costs. Entersekt's authentication solution has delivered quantitative results across multiple fraud categories and client implementations:

- Account takeover prevention: One FI achieved a reported 99% reduction in phishing attempts within three months by replacing one-time password (OTP) with Entersekt's

Mobile Authentication. Another client experienced complete elimination of OTP phishing and SIM-swap fraud by replacing OTPs with push notifications.

- Payment fraud reduction: The platform has demonstrated notable performance in reducing various types of payment fraud, with person-to-person and real-time payment fraud reductions of 90% for one FI and up to 100% for credit unions. For APP fraud, Entersekt achieved a 90% reduction in fraud losses for a large U.S. bank.
- Enhanced user experience: The solution maintains 98% frictionless secure digital banking access on average for clients through Context-Aware authentication, demonstrating that security enhancements don't come at the expense of user experience.
- Operational efficiency: A top 20 U.S. bank reported a 70% reduction in fraud loss dollars and a 62% increase in authentication rate after deploying Entersekt's 3DS ACS, simultaneously driving down operational costs while achieving a 66% challenge success rate that improved customer experience.
- Comprehensive fraud prevention: The platform has proven effective against card-not-present fraud, with one client experiencing a 70% decrease within the first month of deployment.

Future Roadmap

Entersekt's product roadmap for the next 12 to 18 months is outlined in Table D.

Table D: Entersekt's Future Roadmap

Enhancement	Description
Use case orchestrator suite expansion	Development of pre-packaged orchestration and user journeys for digital banks, eliminating the need for banks to handle complex orchestration and fallback scenarios through simplified API consumption
Enhanced scam prevention capabilities	Expansion of the scam prevention solution with additional rules and signals, incorporating merchant signals, card network risk scores, and origin device signals for more multifaceted transaction evaluation
Advanced machine learning models	Improvement of machine learning model iteration and expansion of signals to enhance risk evaluation accuracy and adapt to emerging fraud patterns
Pre-configured rule sets	Development of pre-set rules based on specific client issues, enabling faster deployment and more targeted fraud prevention approaches

Enhancement	Description
Expanded use case coverage	Extension of scam prevention capabilities to include push payments, credential issuance, and identity verification across broader transaction types
Enhanced data enrichment	Integration of cardholder data, endpoint signals, and external consortia to provide more detailed transaction context and risk assessment
Improved decision orchestration	Enhancement of the platform's ability to make risk-based decisions with suggested actions, such as frictionless approval, step-up challenges, and transaction declines based on user preferences and optimal experiences

Source: Entersekt, Datos Insights

2025 Impact Awards in Fraud Methodology

In March 2025, Datos Insights solicited nominations for its 2025 Impact Awards in Fraud.

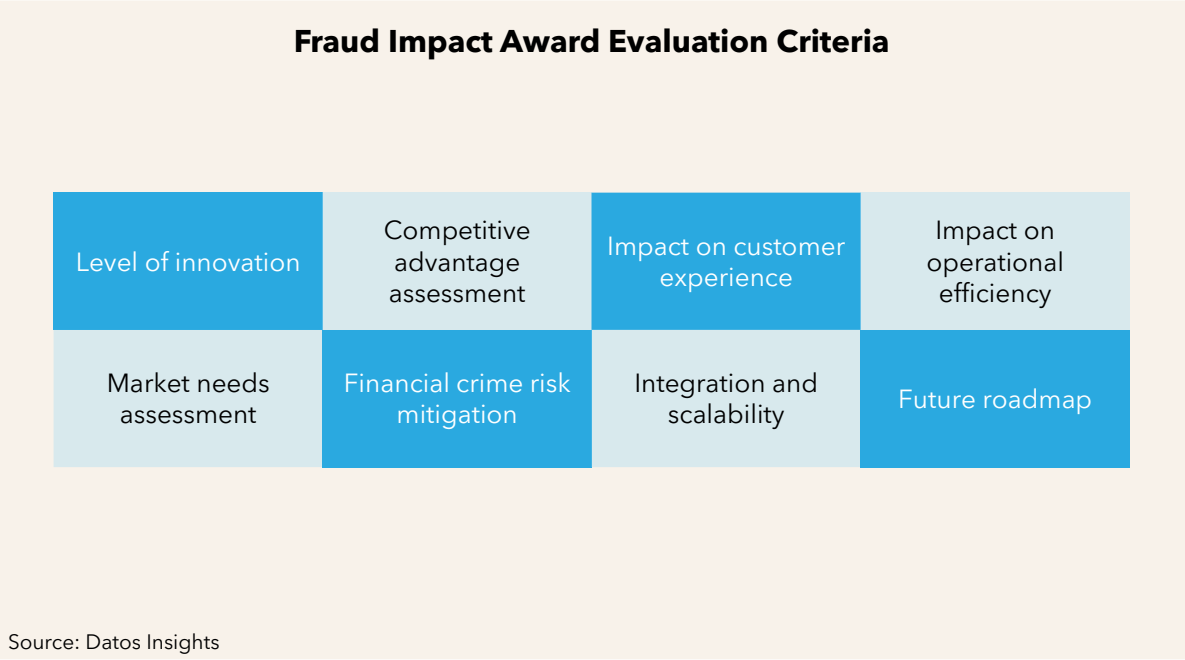
All nominated initiatives were required to be in production and must have been implemented within the last two years. Datos Insights designated the following five individual categories for its 2025 Impact Awards in Fraud, as well as the Best Innovation by a Financial Institution category:

- Best Authentication Innovation: This category features new solutions or innovations that deliver best-in-class identity-proofing or user authentication. These capabilities set new standards for verifying user identities and securing access to financial services.
- Best Transaction Fraud Monitoring and Decisioning Innovation: These are new solutions or innovations that deliver superior transaction fraud analytics, monitoring, detection, and case management that protect financial transactions. The winning technologies demonstrate advanced capabilities in real-time fraud detection and automated decision-making.
- Best Digital Identity Verification Innovation: This category spotlights new solutions or innovations that deliver exceptional identity verification. These cutting-edge solutions excel at confirming customer identities through digital channels while maintaining security and user experience.
- Best Scam and APP Fraud Prevention Innovation: These solutions deliver superior protection against scams and APP fraud threats. The recognized technologies demonstrate exceptional ability to identify and prevent APP fraud and social engineering attacks.
- Best First-Party Fraud Innovation: This category highlights new solutions or innovations that provide exceptional protection against first-party fraud. These advanced solutions excel at detecting when legitimate customers misrepresent information or engage in fraudulent activities using their own identities.
- Best Innovation by a Financial Institution: This category spotlights new solutions or innovations spearheaded by FIs that detect and deter financial crime. These internally developed or championed initiatives demonstrate how FIs can drive fraud prevention and compliance innovation.

Evaluation Criteria

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: Fraud Impact Awards Evaluation Criteria



Source: Datos Insights

About Datos Insights

Datos Insights is the leading research and advisory partner to the banking, insurance, securities, and payments industries—both the financial services firms and the technology providers that serve them.

In an era of rapid change, we empower firms across the financial services ecosystem to make high-stakes decisions with confidence and speed. Our distinctive combination of proprietary data, analytics, and deep practitioner expertise provides actionable insights that enable clients to accelerate critical initiatives, inspire decisive action, and de-risk strategic investments to achieve faster, bolder transformation.

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

Jim Mortensen

jmortensen@datos-insights.com

Contributing Author:

Gabrielle Inhofe

ginhofe@datos-insights.com