LEVERAGING AI TO SECURE FINANCIAL SERVICES ORGANIZATIONS FROM DIGITAL FRAUDS

What FSOs need to secure digital onboarding from fraud

NICE Actimize

Infosys®
Navigate your next

Customer onboarding is the first step in preventing the fraud and financial crime cycle in any financial services organization (FSO).

While onboarding customers, there is always the prospect of letting in bad actors who could expose the organization to potential abuse. Such manipulation and illegal activities fall under the purview of fraud and financial crime. This paper examines how a strong customer onboarding process, complemented by new-age digital technologies, can go a long way in enabling robust fraud management at FSOs.

Introduction

The threat from financial crime and fraud is rising globally. Driven by the economic volatility and social disruptions from the COVID-19 pandemic as well as the accelerated digitalization of FSOs, the growing fears over financial crime are fast becoming a reality. The massive shift to digital channels has led to a staggering rise in application fraud. Application fraud starts with manipulated identities and involves a variety of criminal activities against an account. It refers to opening an account that is then used, directly or indirectly, for fraudulent acts.

Application fraud can variously manifest itself as identity theft, synthetic identity fraud, and new account fraud.

About the Authors

Anu Beri heads the Regulatory Technology segment for the FS domain consulting group at Infosys. She has a work experience of 25 years – working for global FIs out of India and London. Her expertise lies in IT solution design and in managing and delivering large IT projects. She has in depth knowledge of the various aspects of the FS Industry ranging from capital markets to wealth management to retail lending to reg implementations.

Rob Rendell is Global Head of Fraud Market Strategy & Fraud Prevention, Subject Matter Expert. He brings 13 years of banking experience as a Fraud Practitioner. Before joining Actimize, Rob was a VP of Payment Solutions & Product SME at Feedzai. His career has been focused on payments, financial crimes, fraud, cyber vulnerabilities, and platform transformation. He's held management roles at IBM, Citi, Bank of America, Wells Fargo, and legacy Wachovia. Rob brings his industry knowledge to further advance Actimize's positioning as market leader in the space of Fraud and Financial Crime to combat ever-changing trends and threats.

Challenges during Customer Onboarding

FSOs strive to provide customers with smooth and fast onboarding. At the same time, they need to barricade their systems against cyber-criminals posing as customers. This is critical not only to prevent loss from fraud but also safeguard the organization against regulatory non-compliance.

Synthetic identity fraud can be more challenging to detect. Conventional tools and techniques used by FSOs fail to perceive fraud and avert financial damage once a synthetic identity manages to gain entry into their systems. Customer onboarding calls for a powerful strategy and adequate coverage against all forms of application fraud.

Leading anti-fraud practitioners and FSOs require robust solutions that can aid them in:

- Quantifying associated fraud risks throughout the entire customer lifecycle
- Automating system controls to optimally allow for accurate and intelligent distinction between legitimate and stolen identities

Beyond reducing operational costs and fraud losses, organizations must explore the potential of technology as an enabler for digital banking and creating differentiated customer experiences.

How Can FSOs Prevent Fraud?

With accelerated digitalization leading to diversified fraudulent activities, FSOs must invest in solutions that protect them against all kinds of potential threats. They need a strategy that enables establishing identities accurately, identifying anomalies in transactions, and deploying real-time, dynamic fraud prevention measures throughout the customer lifecycle. A multi-layered approach, powered by advanced analytics, artificial intelligence (AI) and machine learning (ML), can ensure effective fraud prevention.

Multi-layered Approach

1 Data corroboration

The first step in the multi-layered approach is identity proofing and data corroboration to authenticate legitimate applicants. Identity proofing includes validating phone numbers and email IDs, establishing real-time possession or accessibility, verifying device-persona connection as well as proof of existence, and ensuring that this data matches the applicant's age, occupation and nationality. ML models, trained and developed using high-quality historical data, best facilitate data corroboration thereby enabling repeatable, reliable, and data-driven outcomes.

2 Risk assessment

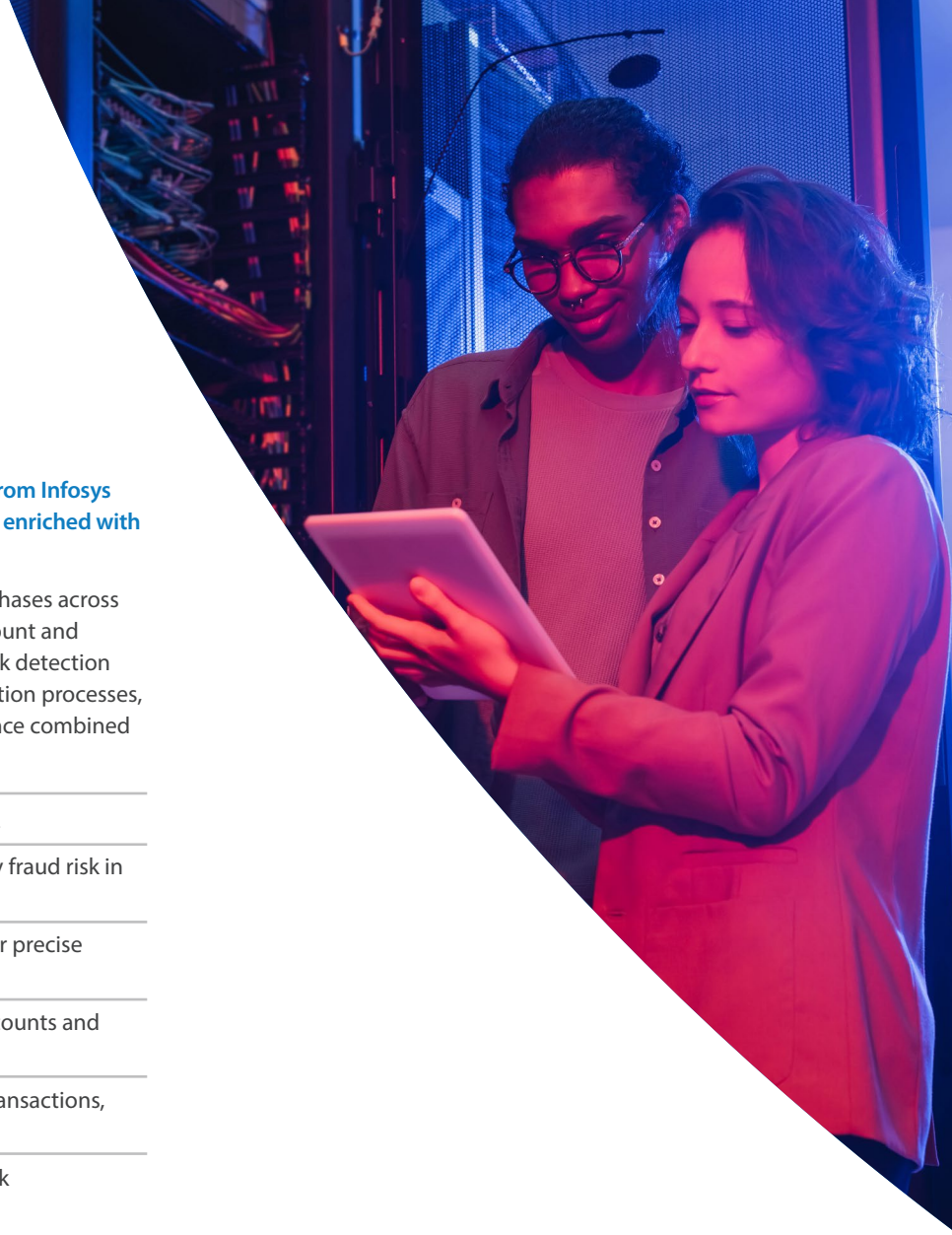
The second step in preventing fraud is to assess risk and thwart potential threats from defrauding customers. At the time of application, the customer origination gateway correlates the real-world data with a customer's digital identity to establish legitimacy. FSOs must enrich customer data with additional information such as social media presence, devices used and their corresponding IP addresses, as well as behavioral analytics.

ML models can make use of profiling techniques to build more reliable rules for risk assessment. For example, customers without social media presence should be flagged for further investigation. Online presence can be probed by checking email addresses and phone numbers against social media platforms. Profiling techniques can also check customer browsers for privacy-focused tools as well as match IP location with the submitted address. Risk assessment is critical to customer scoring, which can determine potential customer journey friction.

3 Fine-tuning models with additional data

The third layer involves passive data collection to build digital identity profiles. The data points created by legitimate interactions are used as a verification benchmark, doing away with transactional customer friction touchpoints. By adopting sophisticated clustering techniques, such as Agglomerative Hierarchical, K-Means, Mean-Shift, and DBSCAN, among others, customers are grouped by jurisdiction, profession, estimated net worth, and other parameters, enabling high-quality KYC risk assessment.

IFM-X's New Account Fraud Solution from Infosys and Actimize



The AI-powered IFM-X's New Account Fraud solution from Infosys and its partner Actimize provides identity intelligence enriched with behavioral and transactional analytics.

The solution optimizes risk detection during discrete phases across the customer lifecycle — from origination to early account and ongoing monitoring. It helps with synthetic identity risk detection during the new account phase by streamlining verification processes, using identity risk scores and identity-related intelligence combined with behavioral analytics. **It provides:**

- A multi-layered solution using advanced AI and ML
- Dedicated analytics to cover identity and first-party fraud risk in digital origination channels
- Orchestration and corroboration of identity data for precise identity risk matrix
- Early account monitoring to identify fraudulent accounts and stop fraud losses
- Holistic view of customer risk: identity, accounts, transactions, and associated risks
- Entity-level view of identity and first-party fraud risk

Conclusion

Identity verification is vital to a holistic customer journey from account opening to verification and continual transactions. Connecting identity verification and data corroboration with enterprise fraud management can be transformational for FSOs, providing the much-needed solution to digital account opening challenges. Transforming the digital account opening process can act as the pivot to an organization's growth and profitability.

Effective customer onboarding can prevent fraudulent customers from getting into the system, benefitting the financial services ecosystem at large. A thoughtfully conceived customer profile at the time of onboarding can hold the key to bringing about several benefits to FSOs, including:

1. Reduced friction, leading to lower abandonment and application rejection rates, driving new digital account growth
2. Enhanced interconnected network of data and point solutions for identity verification (IDV) and fraud management
3. Reduced direct fraud losses and prevention of downstream fraud losses across the organization

The future of digital fraud is already here. FSOs must enable rapid digitization while protecting their sensitive, high-value assets against growing complex threats. As organizations prepare for the next iteration of digital maturity, they need a smart onboarding solution to fuel effective fraud management and drive a holistic approach to fraud detection and prevention.

For more information, contact askus@infosys.com

Navigate your next

Infosys.com | NYSE: INFY

Stay Connected