feedzai

New Account Fraud

fiserv. Santander LLOYDS BANKING GROUP

The online account creation process can initiate a lifelong relationship with a legitimate customer and their financial institution. Or it can give criminals an opening to create money mule accounts, exploit promotional offers, or abuse financial services. Fraudsters use stolen personally identifiable information (PII), synthetic identity fraud, and bots to commit new account fraud digitally. Oftentimes, fraudsters can go undetected for months after account creation – leading to serious financial loss and even regulatory reprimand.

Stop Fraudsters at the Front Door

✓ **Identify fraudulent applications**
Leverage device intelligence, behavioral biometrics, and network data to quantify the risk of fraud. Defend your business from credential stuffing attempts, synthetic identities, bot attacks, and mule accounts.

✓ **Streamline digital account opening processes**
Gain clear, unified insights in one user interface to distinguish fraudulent applicants from genuine ones. Safely speed up the account creation process and create additional revenue by not turning away genuine customers.

✓ **Improve operational efficiency and save costs**
Consume risk indicators via a REST API that enriches downstream systems. Get contextual decisioning on the probability of a fraudulent account opening. Early detection of fraud in the onboarding process eliminates costly third-party identity verification steps.

Key Features

Device Intelligence

Determine if the device has been rooted. Investigate whether someone used it with other applications. Assess if the device is on a blacklist of known fraudulent devices. Quantify the likelihood of mule accounts, synthetic identities, or account opening credit abuse.

Network and Geolocation Analysis

Pinpoint anomalies in geolocation and IP addresses compared to the application data. Understand if someone previously used the network for other applications. Check whether a proxy, TOR, or VPN connection is masking the true network.

Non-human Behavior Monitoring

Identify usage of scripts, automation, or emulation for brute force attacks. Stop bots before they open hundreds of fake accounts within minutes.

Web and Mobile Coverage

Meet the user in their preferred onboarding channel. Implement Feedzai's SDKs and Javascript Collectors to perform accurate risk analysis on both web and mobile applications.

Behavioral Biometrics

Analyze the nuances in how the account holder interacts with your application. Fraud risk indicators include the user's keyboard shortcuts, suspicious browsing patterns, data entry fluency, and form expertise.

Awards and Recognition

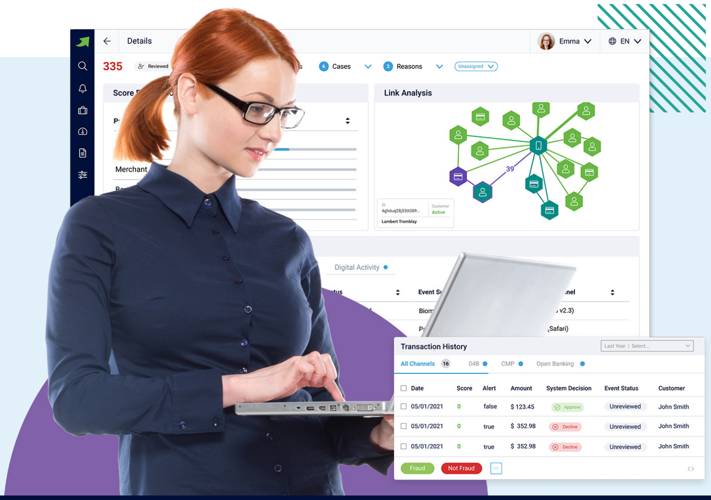
Quadrant Knowledge Solutions — Feedzai named a Behavioral Biometrics Leader

datos INSIGHTS — Feedzai named a Leading Contender in Behavioral Biometrics

FORRESTER® — Feedzai named Strong Performer in Enterprise Fraud Management

Are you ready to upgrade your fraud prevention strategy?

Speak with an expert



Transaction History

Last Year | Select...

All Channels 16 | 04B | CMP | Open Banking

☐ Date	Score	Alert	Amount	System Decision	Event Status	Customer
☐ 05/01/2021	0	false	$ 123.45	Approve	Unreviewed	John Smith
☐ 05/01/2021	0	true	$ 352.98	Decline	Unreviewed	John Smith
☐ 05/01/2021	0	true	$ 352.98	Decline	Unreviewed	John Smith

Fraud | Not Fraud | ···

feedzai

sales@feedzai.com info@feedzai.com feedzai.com