SUCCESS STORIES

Consumer finance

Tags

Employees

Share this

Export as PDF →

The challenge

The solution

The outcome

The challenge

Narrow view of risk: The client's single-source point solution for verifying customer identity didn't go far enough in terms of assessing the risk associated with an identity. While they were using a single identity verification solution, the information was not being examined for additional risk signals that are often associated with fraudulent activity.

Surging synthetic identities: The threat posed by synthetic identities created by fraudsters has been growing, enabled by increasing numbers of data breaches. Fraudsters use compromised personal information in a piecemeal fashion, taking legitimate attributes from real identities and combining them with fake information to create an entirely new, non-existent identity. These fabricated identities are then used to access goods and services on behalf of the fraudster, who will often curate the identities over months and even years to bolster believability. Marked by increased VoIP usage, newly created mobile accounts and fraudulent emails, the client was challenged to combat this recent surge in synthetic identities.

Contactability: Without an effective way to verify contact information the client was facing a heightened risk of authorizing funding to fraudsters. Information such as deliverable address, email address, phone number and IP address were not being assessed for legitimacy, which provided an opportunity for first party-fraud (where an individual misrepresents their information to make a profit) as well as third-party, and synthetic fraud to take place. In addition, the client needed to keep customer data complete, and up-to-date, in order to meet KYC, anti-fraud regulations and data quality requirements.

Step-up authentication: The use of prepaid phones, sometimes associated with "burner phones," are commonly utilized to commit fraud. If a mobile account is prepaid and has a low tenure (along with other attributes) it may need to be "stepped up" to additional methods of authentication. The client was looking for a solution to address this scenario including a way to review account status (e.g., deactivated, suspended, lost/stolen device) as a helpful indicator of potentially fraudulent situations.

The solution

It was clear that the client required a solution that would deliver robust identity verification alongside accurate risk assessment to provide an additional layer of fraud prevention.

The solution also needed to be unobtrusive and selective to ensure legitimate customers would not be deterred by increased friction in the customer journey. Assessing and verifying the customer input data, already being captured as part of the onboarding process, ensured that the process remained streamlined.

ExpectID Identity Data Verification brings together physical and digital identity data from a wealth of authoritative sources, to instantly validate an identity with no added friction.

As an additional step, the client then introduced ExpectID Fraud Risk Signals, so that customer mobile numbers and email addresses could be assessed for indicators such as inactivity and deliverability, providing confidence in the client's ability to contact the individual. Mobile numbers are screened for high-risk indicators related to the account type (pre-paid or post-paid), tenure (the duration the account has been open), activity status (deactivated, suspended, lost or stolen device) and the device associated with the number (SIM swaps and port changes).

The IP address where an in-progress transaction is taking place is also cross-referenced against the known address of the corresponding identity, letting the client know if an individual is physically located where their identity would suggest.

The outcome

Through the ExpectID® platform, the client was able to effectively orchestrate acquisitions through multiple layers of risk assessment and verification. This layered approach meant that seemingly non-threatening identities could be checked for high-risk indicators, preventing fraudsters from getting access to funding further down the line.

By incorporating combinations of risk signals into their decisioning, the client was able to significantly increase their ROI. The client looked for consumers whose mobile number returned an “inactive” account status alongside risk signals associated with their address and were able to significantly increase ROI from 8:1 to 30:1. Non-existent email addresses alongside address risk signals also delivered an increase in ROI from 16:1 to 23:1.