

Datasheet

Xceed AI FRAML: Cross-Channel Fraud

More Payment Channels = More Fraud Challenges

Fraudsters perfect and scale their crimes using advanced technology, launching attacks and scams that are far more sophisticated and complex. By utilizing cross-payment channels, they can circumvent fraud prevention controls, defrauding financial institutions and customers. It is difficult for financial institutions (FI's) to connect, track, and intervene, especially when they are using legacy solutions or operating in silos. Unfortunately, fraudsters don't just stop at fraud. The same funds that touch multiple payment channels then end up involved in other nefarious schemes.

It's critical that FIs leverage AI to visualize the full story in real-time, enabling them to properly analyze and view behaviors and transactions across all channels. With NICE Actimize's Xceed Cross-Channel Fraud Detection solution you can catch cross-channel fraud before it even starts.

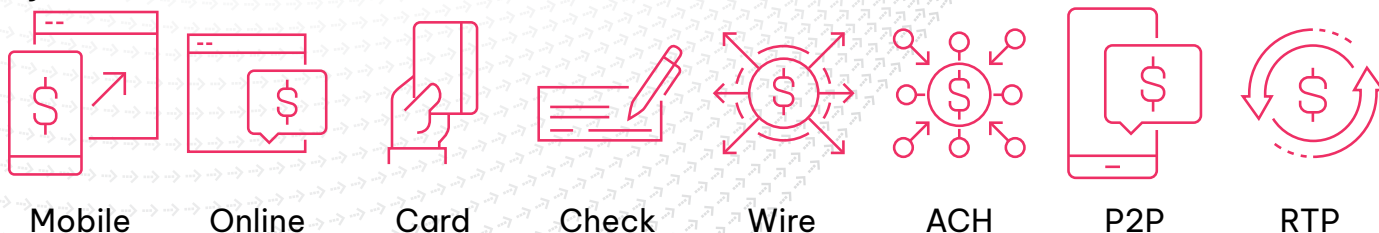
Examples of Cross-Channel Risk Factors:

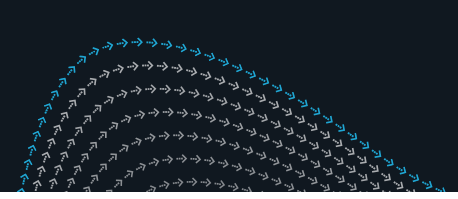
- Unusual transaction velocity
- Unusual activity across 2+ channels
- Unusual amounts
- Unusual payees
- Unusual locations
- Unusual check deposits

How Cross-Channel Fraud Occurs

A fraudster may deposit a counterfeit check in the United States and then immediately make multiple payments both domestically and internationally through different channels, such as wire and ACH. Based on the known customer behavior and transaction details, NICE Actimize's Cross-Channel Fraud Detection solution would return a high cross-channel risk score indicating risk factors and unusual activity across two or more channels.

Payments Channels include:





Faster Detection & Decisioning with Xceed

Xceed Cross-Channel detection and prevention solution uses advanced behavioral analytics and machine learning to monitor and detect customer behaviors and transaction details across multiple channels. Enabling the analysis of patterns and anomalies to identify transactions and activities that deviate from typical behavior.

Analysts are immediately notified of suspicious cross-channel events with easily identified indicators. Powerful visualizations including heatmaps and timelines enable investigators to see the full journey of the payment to make a quick and informed decision. The easy to navigate point, click, and drill capabilities of the UI along with the plethora of historical data makes the solution insightful.

With so many payments channels, the points of entry for a fraudster to commit fraud are endless. One fraudulent payment can end up touching multiple payment channels, many FIs, and can easily evolve into a money-laundering scheme. Stop it before it starts with NICE Actimize's Xceed Cross-Channel Fraud Detection solution.

Benefits of Cross-Channel Detection:

- Easily identify Cross-Channel Risk with real-time fraud risk scoring
- Immediate notification of cross-channel fraud through visual indicators
- Decrease losses and risk through early detection and prevention
- Seamlessly adapt to changing behaviors with machine learning
- Increased operational efficiency with a 360-degree view of risk

The screenshot shows the NICE Actimize FRAML Alerts interface. At the top, there are navigation tabs for Dashboard, Alerts, Cases, and Filings. A search bar and user information (City bank 2, #Customer ID) are visible. The main area displays an alert for ID 2022-10-001736, categorized as Fraud with a High priority and a Risk Score of 9.1. The alert is in an 'Open' status and is associated with account 65436258188 and channel ACHODFI. Below the alert, there is a 'Summary' section with tabs for Batch Entries, Subject Details, Attachments (3), Account Notes (2), Comments (3), and Audit. The 'Cross Channel Risk Factors' section lists several indicators: Wire (suspicious account, payment method change, beneficiary change), Check (duplicate number, ATM use, new account), ACH/RDFI (new location, suspicious account), and Transaction Monitoring (unusual amount, beneficiary). A table at the bottom provides details like Date Created, ODFI, Due Date, SEC Code, Company Name, and Company ID.

→ Request a Demo