DATAVISOR

Case Study: Application Fraud

Financial Institution Implements Unsupervised Machine Learning to Stop Application Fraud

At A Glance

Customer Pain

A large US financial institution struggled with online application fraud from synthetic identities, stolen identities, and coordinated bust out attacks in its consumer portfolio.

DataVisor Results

30%
Increase in detection

90%
Detection accuracy

1.3%
False positives

$4M+
Annual fraud loss savings

About the Customer

DataVisor recently partnered with one of the largest banks in the U.S. that specializes in credit cards, home loans, auto loans, checking and savings products. Like many financial institutions, the bank had a concerted push to increase the number of new online account openings for its consumer portfolio.

Customer Challenges

Along with the explosive growth of new online applications for their consumer portfolio came the increased rise of fraudulent applications created using synthetic identities or stolen identities. Coordinated bust out fraud efforts further impacted their bottom line and threatened their brand. Fraudsters often were able to submit many applications with synthetic identities using the large scale of consumer information available for sale on the dark web following massive data breaches. They would then purchase goods to resell with credit cards they had no intention of paying. Or, they would pay credit card balances with fraudulent checking accounts.

The bank had an experienced internal review team that monitored new account applications. However, they struggled to catch the massive volume of fraudulent applications, especially dealing with fast-changing patterns from fraudsters. As a result, thousands of such accounts were created per month. Even worse, many fraudulent application losses were misclassified as credit losses.

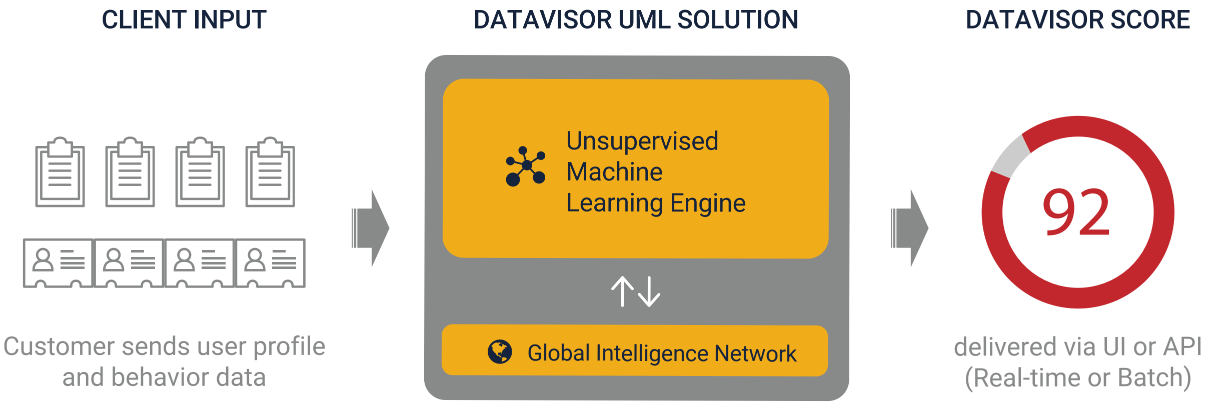
Traditional application fraud prevention processes, including business rules and supervised modeling approaches, could not effectively capture fast-changing fraud attacks leveraging advanced techniques. The bank needed a solution that could not only prevent different types of fraud attacks accurately, but could also decrease authentication steps for their good users applying for new accounts.

How DataVisor Helped

Fraudsters used advanced digital tools to look like normal accounts when viewed in isolation, such as cloud hosted infrastructure, email anonymizers, and mobile device flashing. DataVisor complemented the bank's existing solution with its patented Unsupervised Machine Learning (UML) Engine, which identified coordinated fraudulent applications at high accuracy and large scale. The UML Engine viewed all applications together, and then surfaced subtle suspicious correlations in real-time. Further, the UML Engine is able to capture and stop new attacks, since it does not make assumptions of what fraudulent applications look like. Among the additional fraudulent applications detected, many were misclassified as credit losses.

As a result, DataVisor detected **an additional 30% of fraudulent applications** at 90% accuracy and a low 1.3% false positives rate. Even more, DataVisor was able to capture fraudulent applications at least 1 day earlier by bypassing the bank's manual review process. This led to over $4M in annual savings. Among the additional fraudulent applications detected, many were misclassified as credit losses.

DataVisor also leveraged its Global Intelligence Network (GIN), which is aggregated anonymized non-PII data comprised of over 2 Billion accounts and 600 Billion events from customers across the globe. The GIN contained rich information about digital fields such as IP addresses, user agent strings, device types and OS, email, and more. Information from the GIN fed into the UML Engine to further improve the overall detection.



CLIENT INPUT

Customer sends user profile and behavior data

DATAVISOR UML SOLUTION

Unsupervised Machine Learning Engine

Global Intelligence Network

DATAVISOR SCORE

92

delivered via UI or API (Real-time or Batch)

Fraud Rings Detected

Third-Party Fraud Using Stolen Identities:

DataVisor identified a third-party fraud ring with over 200 applications. The bank looked at the applications individually and failed to decline over 90% of them since the fraudsters appeared legitimate in isolation.

Evasion techniques: The "applicants" had diverse demographic information and excellent credit worthiness. Their digital traces also looked legitimate from signal vendors, e.g. the applications utilized reputable email domains and different IP addresses.

Patterns Datavisor detected: All of the applications used T-Mobile IP ranges during the application process. However, the devices associated with those applications were desktop computers instead of mobile devices. The fraudsters tethered to use reputable IP ranges, bypassing IP reputation checks.

Synthetic Applications during Promotion Period:

DataVisor found a fraud ring taking advantage of account opening promotions and created over 300 accounts in under a week.

Evasion techniques: The "applicants" all worked for high paying bank positions. In addition, their addresses were all in a low risk region. The bank's existing solutions didn't notice anything suspicious in digital traces, because the fraudsters used Starbucks and other public IP addresses to sign up.

Patterns Datavisor detected: All of the applications had $100,000-$150,000 in income and the same email pattern. Their emails consisted of their first name, last name and a random number.