NuData Security
mastercard

Mitigating Card Application Fraud for Major North American Bank

CASE STUDY

Using passive biometrics, traffic anomalies, reputation data, and non-biometric anomalies to mitigate credit card application fraud in real time.

Key Points

- In one month, NuData Security's Online Account Opening (OAO) solution caught 2,000 otherwise missed fraudulent credit card applications for this major North American bank.
- Incremental to this bank's existing security tools, NuData's solution successfully caught:
  - 65% of missed third-party fraud[1], and
  - 28% of missed first-party fraud[2].
- This real time fraud mitigation resulted in a fraud loss reduction of millions of dollars annually for this bank.
- NuData was able to perform this identification and mitigation with only a 0.90% false positive rate.

[1] Third-party fraud is where an individual, or group of people, create or use another person's identity or personal details to open or takeover an account without the consent or knowledge of the person whose identity is being used.

[2] First-party fraud is where an individual, or group of people, misrepresents their identity or gives false information when applying for a product or service. This includes synthetic identity fraud, bust out fraud, and credit repair.

Industry Problem

OAO fraud continues to be a significant challenge for financial institutions across the globe. In 2018, the incidence of new account fraud was 1.25%, costing businesses worldwide a total of $3.4 billion[3]. OAO fraud typically manifests as either first-party fraud or third-party fraud.

The Client: A Top North American Bank

This client provides a wide range of investment, mortgage, trust, and payment services. A significant portion of its business is offered online, underscoring the importance of better recognizing new good users as either legitimate or fraudulent.

This institution, like many others worldwide, is experiencing sophisticated credit card application attacks at its various card application pages. Like most others, this bank has KYC check, fraud scoring, rules engine platform, and core risk engine technologies in place, but they still issue 1,400 credit cards per month to fraudsters, leading to an average monthly loss of about $500,000.

How NuDetect Helped This Client at OAO

This bank looked for an easy-to-integrate solution that could be combined with its current cybersecurity stack to detect fraudulent card applications that were being missed by their existing tools. NuData's award-winning technology was selected to provide enhanced protection leveraging passive biometrics technology at several of this bank's card application pages.

[3] According to Javelin's 2019 Identity Fraud Report.

Result

After this one-month proof of concept, the client detected additional **third-party fraud** and, the hardest one for the industry to mitigate; **first-party fraud**.

65%
of third-party fraud mitigated

28%
of first-party fraud stopped

0.9%
false positive rate

$6M
estimate annual savings

Third-party fraud

This fraud involves the use of automation to submit fraudulent applications with fake or stolen identities.

Out of all of the applications, NuDetect's OAO model ccurately identified 65% as high-risk. This evaluation happened in real time, allowing the client to prevent future fraud.

First-party fraud

This fraud involves synthetic identity, bust-out fraud, and credit repair applications and it is the most difficult to prevent for issuers. This is because the user is manually typing the information instead of using automated scripts.

The NuData model detected 28% of first-party fraudulent applications. This is a crucial increase for this client who couldn't detect these applications before it was too late.

False positive

Better capture numbers don't mean much if we can't ensure good users maintain the streamlined experience they deserve. While the fraud detection rates for credit card application jumped up, the false positive rate stayed consistently under 0.9%. This means that only 90 BPS of all good user applications were flagged by NuDetect for further review.

Based on the information shared by the institution, NuData's monthly estimated savings for this client are $500,574. Annualized, this amounts to *$6 million*.

The direct **monthly** cost savings to this bank are explained in the table below.

FRAUDULENT CARD APPLICATIONS - CAPTURE PERFORMANCE - PER MONTH

	Third-party fraud	First-party fraud	Total
Total Fraudulent Applications	2,802	637	3,439
NuData Capture %	65%	28%	
Applications Caught	1,821	178	1,999
$ Average Direct Loss Per Application	$ 135	$ 1,428	
$ Saved with NuData	$ 245,876	$ 254,698	$ 500,574[5]

The savings totals calculated above are conservative since they do not include:

- the manual review costs incurred for those fraudulent applications that were caught before being issued
- the processing and operational costs6 of those cards tied to fraud that were issued.

[5] These savings are incremental to the fraud loss savings that result from all other tools that this bank already had in place.

[6] This includes the cost of issuing a card, creating the plastic, credit checks, posting the card, and sending any declination letters.

How Does it Work?

NuData's OAO solution uses hundreds of behavioral, reputation, traffic, and passive biometric data points to determine whether the applicant is genuine or malicious. NuDetect's OAO solution detects fraudulent applications and calculates a risk score for individual form completion attempts before they are submitted.

The solution uniquely finds attributes that collectively separate fraud from non-fraud using complex models – this process leverages machine learning to further train these models. The complex models we use is a tree-based ensemble model called xgboost (eXtreme Gradient BOOSTed trees). We run up to 2,000 trees, many with up to 9 branches in depth. This enables class separation in contexts where simpler approaches would fail.

NuData uses its input data to create a range of over 300 features (and counting) – data attributes that capture user behavior in useful ways. The features collected include:

- Cadence of completing the form
- Method of moving through the form (click or tab)
- Progression through the form, field order and 'circle back' behavior
- Cadence and speed of user typing
- Form focus and window-switching behavior
- Detail-checking and pausing behavior
- Dynamics of mouse and touch interactions (when available)
- Device orientation and accelerometer (when available)
- Form field autocomplete or copy-paste behavior
- Familiarity with the form, e.g. omission of optional fields and error incidence rate. ▸

EXAMPLE

NuData's OAO Solution in Action

The passive biometrics and behavioral analytics technology deployed in NuData's OAO solution plays a key role in providing these ground-breaking results for card application fraud capture. Below is an example of how these technologies were instrumental in detecting a particular fraudulent credit card application for this client.

1. A user applied for a credit card.
2. Dozens of behavioral indicators capture typing, touch and mouse interaction.
3. This application presented a broad range of behavioral anomalies, including:
    - A high degree of familiarity with the bank's form.
    - The applicant pasted content into each field rather than typing it manually.
    - The applicant performed rapid tab-based navigation, suggesting form familiarity.
    - The applicant did not pause to review the form content.
    - The entire application form was completed in 46 seconds (compared to population average of 5 minutes).
4. NuDetect's OAO solution successfully identified this application as high-risk in real time.

Hungry for more results?

Read how we've helped another financial institution against automated attacks. →

ABOUT NUDATA

NuData Security, a Mastercard company, is an award winning passive biometrics and behavioral analytics solutions provider, based in Vancouver, B.C.

We were born with the belief that customers deserve a seamless online experience that keeps them protected. Our technology identifies users based on their online interactions behavior that can t be replicated by a third party.

We have proudly pioneered the field of passive behavioral biometrics and are tirelessly evolving to keep our clients protected from growing online risks.Today, NuData is trusted by some of the largest global brands in the world to verify users, keep environments safe, and bring trust and innovation to the online space.

NuData Security
mastercard