Less Friction. Less Fraud.

Identity Proofing Case Study

A Top-5 Global Credit Card Issuer Detects New Account Fraud and Reduces False Declines with Behavioral Biometrics

Problem

Fraudsters use stolen personal information or synthetic identities to apply for credit cards. Existing solutions are based on static means of verifying identity – personal data, device ID, etc.

Solution

Add BioCatch behavioral biometrics technology into the online application workflow to act as another dimension in separating out legitimate users from fraudsters.

Results

- 33% less false declines
- 50% more accurate fraud alerts than existing solutions
- 100% alerts either confirmed as fraud or highly suspicious

This global credit card issuer has hundreds of millions of cardholders and is one of the most well-known issuers in the world.

The global card issuer uses a wide array of cyber defenses to monitor, analyze and prevent fraudulent activity during the card application process. Fraudulent activity may include the use of stolen or synthetic identities that rely on a combination of stolen personal information and false details, such as a real social security number and name with a fake address, phone and email. Then the fraudster can proceed to apply for a credit card and attempt to commit fraud.

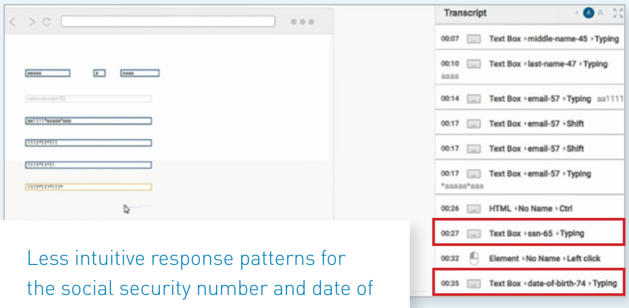
In recent years, credit card issuers have faced a variety of challenges in balancing between security needs and friction-related costs, most notably false declines. False declines translate into lost revenue over the full potential customer lifetime, is often not even measured in the account opening process but is a keen metric for customer acquisition teams.

In 2017, this global credit card powerhouse added the BioCatch behavioral biometrics capability on its credit card application website. Several months after the initial deployment, millions of applications were submitted with BioCatch's behavioral biometric solution running in the background. The user experience remained 100% seamless and frictionless, as BioCatch detected a significant amount of fraudulent applications that existing solutions did not flag and reduced false decline rates, which translates into immediate ROI and long-term customer value.

Behavioral Biometrics for Identity Proofing

BioCatch maps criminal behavior throughout the initiation process.
The BioCatch system distinugishes between a real user and an impostor by recognizing normal user behavior and fraudster behaviors. Understanding the way fraudsters behave allows the BioCatch system to identify human and non-human elements in a session in real-time and prevent a potentially fraudulent application from going through.

For identity proofing, there are three primary methods of behavioral analysis: **Application Fluency, Navigational Fluency and Low Data Familiarity.**



Transcript

00:07 Text Box › middle-name-45 › Typing

00:10 Text Box › last-name-47 › Typing
aaaa

00:14 Text Box › email-57 › Typing aa1111

00:17 Text Box › email-57 › Shift

00:17 Text Box › email-57 › Shift

00:17 Text Box › email-57 › Typing
*aaaaa*aaa

00:26 HTML › No Name › Ctrl

00:27 Text Box › ssn-65 › Typing

00:32 Element › No Name › Left click

00:35 Text Box › date-of-birth-74 › Typing

Less intuitive response patterns for the social security number and date of birth fields

Examining Data Familiarity: In this example (image taken from the system's analyst portal) BioCatch flagged an application as high-risk. The user was extremely familiar with the application flow, interacting with it almost instantly; they exhibited very low familiarly with information such as name, social security and date of birth, but had no problem with phone or email – which is a regular pattern in fraudulent applications as these tend to be not from the victim, but rather, the fraudster's own information.

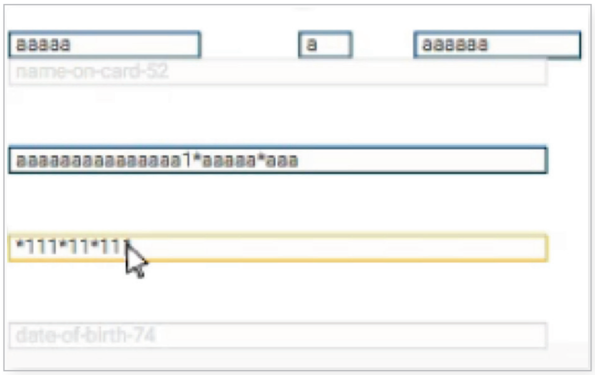
Reducing False Declines

Another important capability of the BioCatch behavioral biometric identity proofing technology is reducing false declines. The behavioral analysis can show positive signals such high data familiarity with personal details (such as name and date of birth), low familiarity with data that isn't normally top of mind (such as an airline's frequent flyer number), low familiarity with the application flow, and hesitancy around elements that require a though process to complete.

In the following example, an applicant was declined by the card company, who internally calculated a 96% chance of the application being fraud. BioCatch believed the application to be genuine as the user has shown several positive signs:

- The use of long-term memory as seen by typing, with no pause, a 9-digit SSN (fraudsters cannot type 9 digits in one go as short-term memory is limited to up to 7 digits; so, when they type a victim's SSN they would normally pause after a few digits, take another look at their record, and then complete the typing).
- This was an application for a hotel chain credit card, and the hotel's loyalty number was requested. Fraudsters normally come prepared an immediately provide the information, but users normally don't and have to look for the number as it's not top-of-mind. In this session there was a 58 second pause while the user was fetching the data.

Following BioCatch's alerts, the card issuer's fraud operations team contacted the user. It turns out they had a typo in the social security number; it mapped to a deceased person, which is why the application was immediately declined. After confirming all the details with the user, they were told that everything now checks and they can get the credit card. A false decline was prevented.



aaaaa a aaaaaa

name-on-card-52

aaaaaaaaaaaaaaa1*aaaaa*aaa

*111*11*111

date-of-birth-74

Through this display in the BioCatch Analyst Station, we notice that the user entered his SSN in one continuous sequence, without pauses or intervals - indicating authenticity. In addition, all personal information is anonymized in this portal with symbols