

Behavioral Biometrics Prevents Massive New Account Opening Fraud Attack

Digital bank improves new customer onboarding process and increases fraud detection rates by 60% with BioCatch

A digital bank launched a marketing campaign offering high interest rates on savings and deposit accounts to attract new customers. Fraudsters took notice and pounced.

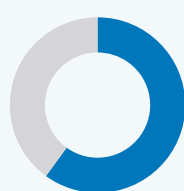
Problem

A digital bank found itself the target of a massive online account opening fraud attack after launching a marketing campaign intended to attract new customers. Traditional solutions and processes left the bank exposed, as fraudsters moved money from a compromised account into a new account that they now fully controlled, allowing them to quickly withdraw funds without the legitimate user noticing and creating significant liabilities for the new digital bank.

Solution

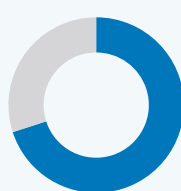
BioCatch's behavioral biometrics provided an added layer of visibility, closing the gap left by traditional fraud solutions. By analyzing user behaviors related to application familiarity, computer proficiency and data familiarity, the system generated real-time alerts that stopped the fraudsters and allowed the bank to resume normal operations. Today, the bank incorporates BioCatch into their main fraud prevention stack, maintaining a 30% sustainable uplift over the standard technologies and protocols.

Results



60%

Increase in fraud detection on top of the standard device reputation, email, location and KYC checks with BioCatch fully integrated into the technology stack.



70%

70% detection uplift during the attack period, as BioCatch identified unique behaviors to the crime ring.

As banks evolve to compete in a digital-only world, their top priority is how to gain market share as fast as possible by offering special incentives and making the onboarding process as easy as possible. However, by definition, opening a bank account online is an intricate process, but streamlining it and making it as user friendly as possible, is the key to success.

A new digital bank in the US allowed users to complete the account opening process entirely online, offering high interest rates on savings and Certificate of Deposit (CD) accounts to entice new customers. Identity verification involved traditional KYC personal data checks, device ID, email address validation and geolocation checks. In addition, a final step to validating user identity involved sending a small amount of money to the account that the user indicated they would be transferring money from, and then asking the user to report on the amount transferred. The idea was that this step would demonstrate that it was the legitimate user as they had control over the funding account.







It didn't take long for the fraudsters to figure out how to circumvent these steps and establish new accounts using stolen and synthetic identities, and then quickly cash out.

Within a short period of time, customer acquisition rates soared - about 10 times the normal volume. The feeling of success with their new offering quickly dissipated when they realized that they were actually the target of a very large, sustained, and potentially devastating online account opening fraud attack. **In fact, for every 100 good applications, there were 900 bad applications, each generating thousands of dollars in losses when fraudsters immediately withdrew their funds and disappeared.** This was clearly unsustainable. The bank would have to either stop accepting new customers or accept new customers but disallow them from withdrawing funds – a Hobson's choice.

Analyzing user behavior to understand the fraudsters' modus operandi

What was happening: Fraudsters used stolen and synthetic identities to open new deposit accounts at the digital bank, to be used as a holding account for funds they transferred from other compromised accounts. They did it by taking over another account and confirming the transfer at the end that was required to complete the online account opening process. Since they controlled both accounts, they were able to provide the proof of identity. The legitimate user of the originating account was not aware this was happening, and the digital bank was liable for the fraud as the funding request came from them.

The only way to address the attack was to stop the fraudsters from opening a new digital bank account. Analyzing user behavior with BioCatch behavioral biometrics provided the layer of visibility needed to do so. The system identified specific behaviors, relating to application fluency, proficiency with computer shortcuts and lack of data familiarity, delivering a 70% uplift over the traditional fraud checks and allowing the bank to continue normal operations. Since then, the BioCatch technology has been integrated into the overall fraud management stack, providing a 60% increase in fraud detection across the board, while preserving the desired user experience to ensure maximum customer acquisition.

Segmented Typing - Fraud		
05:57		Text Box > ssn > Left click
05:57		8 seconds of inactivity
06:08		Text Box > ssn > Typing 11
06:10		Text Box > ssn > Typing 11
06:12		Text Box > ssn > Typing 11
06:14		Text Box > ssn > Typing 11

A very specific criminal behavior

The cybercriminal gang responsible for the massive attack had very unique characteristics. It showed a remarkable familiarity with the onboarding process, which was several pages long and required a number of decisions and data points – this is not surprising given the fact they did open hundreds of fake applications per day. It also demonstrated lack of familiarity with the victim's data. All the data was typed using short-term memory, and the typing had pauses typical to someone who works off a printed list with many records.

Whereas a typical user types various data sets in a short period and without pauses, the criminals took much longer to enter the information and stopped several times along the way, demonstrating the use of short-term memory.

A game-changing uplift in fraud detection

Traditional fraud prevention solutions rely on static measures that are easily circumvented by fraudsters. Devices change regularly, locations can be spoofed and fraudsters have access to personal information available on the dark web. Applications are created using stolen or synthetic identities and can easily pass KYC data checks and even KBA (Knowledge Based Authentication) checks.

For account opening there are three primary methods of behavioral analysis: Application Fluency, Navigational Fluency and Data Familiarity.

How It Works



Application Fluency - Fraudsters repeatedly using compromised or synthetic identities demonstrate a high level of familiarity with the online application.



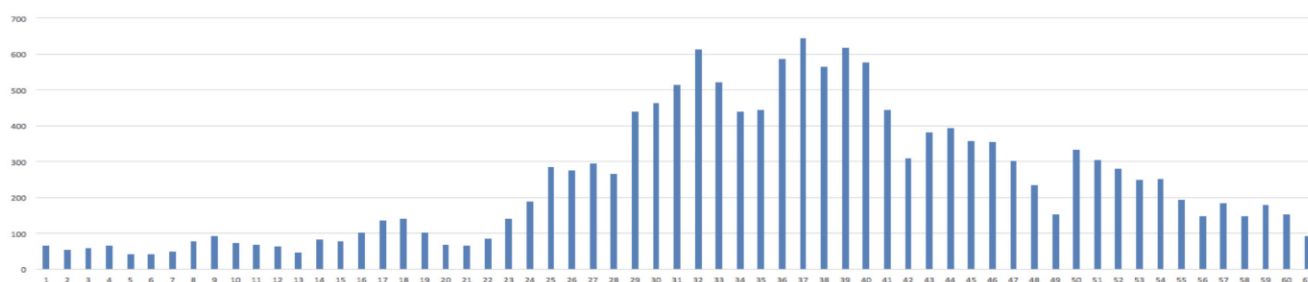
Navigational Fluency - Cybercriminals practice a proficiency with computer functions not typically seen with legitimate applicants.



Data Familiarity - Legitimate applicants exhibit intuitive knowledge of personal data.

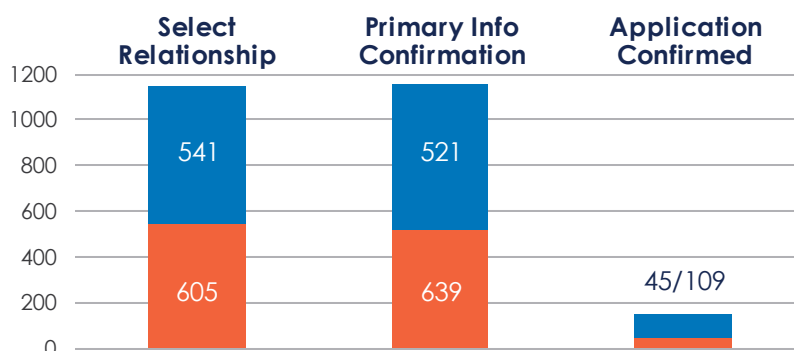
Using these combined artificial intelligence techniques, BioCatch provided this new digital bank a new layer of visibility. The attack timeline here shows the increase in applications plateaued and then began to decline, eventually going back to normal, once the bank adopted BioCatch.

Attack Period



The impact generated by BioCatch over the existing controls can also be understood by analyzing the detection uplift for each specific page that is filled out during the onboarding process as listed below.

Page in Account Opening Flow	Detection Uplift
Select_Relationship	89%
Primary_Info_Confirmation	82%
Application_Confirmed	41%
Congratulations	69%
Funding_Confirmation	144%



BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit www.biocatch.com

www.biocatch.com

[E: info@biocatch.com](mailto:info@biocatch.com)

[@biocatch](https://twitter.com/biocatch)

[in /company/biocatch](https://www.linkedin.com/company/biocatch)