BioCatch

CASE STUDY

A Top 5 UK Bank Drastically Reduces Account Takeover Fraud and Creates an Adaptive Customer Experience

A Journey to Less Friction and Less Fraud with Behavioral Biometrics

Problem:

Account takeover (ATO) attacks were bypassing existing fraud prevention controls and generating extensive losses. In addition, the solutions and controls deployed across multiple layers of the account lifecycle were creating high levels of friction. For example, a one-time passcode was still being sent via postal mail to confirm account changes. The bank was looking for a solution that could work on top of existing solutions to reduce ATO fraud and eliminate friction to improve the digital experience.

Solution:

The bank deployed BioCatch behavioral biometrics initially to protect against threats targeting the payment process. After realizing the tremendous value behavioral biometrics brought to the payment flow, they started to look for ways to solve other security challenges across the account lifecycle. The use of behavioral biometrics was expanded to protect additional activities such as login, password resets, account changes, and instant loans.

Results:

30%
Up to 30% reduction in fraud alert volumes

95%
Reduction in friction during the credential re-enrollment process with a risk-based approach

£300k
Average savings per month from detection of authorized push payment fraud

£1.5M
Losses prevented over six months from instant loan fraud

For every £1 invested in behavioral biometrics the bank was able to reduce fraud by £4. In addition to a decrease in fraud, the bank also realized a significant reduction in user friction and fraud alerts which low er operational costs of investigation.

First Step: Battling Account Takeover Threats

Account takeover fraud continued to affect a Top 5 UK bank despite multiple layers of protection already in place, including device intelligence and transaction monitoring. The bank sought a solution that could increase visibility and enhance detection of account takeover fraud in the payment process.

Authorized Push Payments

One type of fraud that has seen an alarming 30% percent increase in the UK and other parts of Europe is a form of social engineering scam known as Authorized Push Payment (APP) fraud. In this attack, cybercriminals call victims pretending to be a representative from a legitimate organization, most often a bank or government agency. Following instructions from the cybercriminal, victims are coerced into initiating payments to an account owned and operated by the criminal. According to the UK Finance organization, losses due to APP scams rose to £456 million in 2019.

These attacks are difficult to detect because it is the legitimate user taking action, using a legitimate device and potentially know location. Traditional fraud prevention tools that use device-based or activity-based cannot detect such attacks because the transaction or payment takes place within an authenticated session, from a trusted device and location, and does not use any form of malware. By implementing BioCatch across the account lifecycle and deploying advanced behavioral insights, the bank was able to detect APP fraud in real-time. In fact, BioCatch observed that at least 35% of all fraud came from such attacks.

Remote Access Tool (RAT) Attacks

When a cybercriminal calls victims and convinces them that they are calling on behalf of the bank in an APP scam, the question remains: how do they have access to financial information? Working with BioCatch, the bank observed something alarming. Prior to a social engineering scam, cybercriminals were using remote access tools to access customer accounts. When a legitimate user would log in, authenticate and perform transactions, the cybercriminal would use remote access tools to gain visibility into the account and user activity, information that would later be used in the scam. To prevent such fraud, the bank deployed alerts for proactive prevention, resulting in £100K-£500K per month of fraud savings, at a 4:1 genuine to fraud ratio.

New Digital Offers Create Unintended Consequences

Amidst the string of targeted account takeover attacks, the bank had launched new digital services, including a promotional offer for a pre-approved loan. When a customer would log in to the account, they would receive a pre-approved offer, and after completing a short application, up to £50K in funds would be made available in the account within hours. This campaign became a big target for cybercriminals.

The bank decided to leverage behavioral biometrics to calculate fraud risk before granting a loan. Leveraging the BioCatch Account Takeover Protection models, the bank was alerted to potential instant loan fraud. As an outcome, the bank saw a savings of £1.5 million over six months and a 30% increase in detection over previous controls.

Step Two: A Journey to Less Friction and Less Fraud

By adding behavioral biometrics to their technology stack, the bank achieved the additional visibility needed to combat ATO fraud. Cybercriminals continued to look for new ways to target the bank, and despite new methods that have emerged, the bank has effectively mitigated these attacks. Confident in having risk under control, the bank turned their attention to identify other use cases where behavioral biometric could be integrated to reduce customer friction and improve the digital experience.

One priority the bank had was to create a modern, secure process to support account updates which is an extremely sensitive activity that may seem innocuous but can actually pose a high level of risk. For example, it is common for cybercriminals to make changes to an email address or phone number on record in an account before initiating a fraudulent payment.

The bank has continued to deploy BioCatch to reduce friction across the account lifecycle for multiple use cases including changes in account details, new payees and internal transfers.

Before deploying BioCatch, a change of phone number online often required a one-time passcode (OTP) to be sent via postal mail, a long and outdated process. Since the bank uses phone OTP for authentication, this re-enrollment process is critically sensitive. While it was highly effective in stopping fraud, it created a horrible customer experience.

By leveraging BioCatch risk scores as part of the process for account changes, the bank created a risk - based, adaptive customer experience. For high-risk scores, the old process was maintained. For medium risk scores, digital phone change is possible, but the use of its activation is delayed for a couple of days. For low -risk scores, which accounts for almost 95% of cases, digital phone change is possible for immediate use, providing a great customer experience and very low fraud risk.

Another process that was generating friction was password resetting. To create an adaptive experience, the bank evaluated the effectiveness of existing solutions in their technology stack and compared it with BioCatch's behavioral insights. They realized that the BioCatch risk scores were most effective in closing this gap for cybercriminals while also providing customers with a safe and seamless experience to instantly change their password. The bank has continued to deploy BioCatch to reduce friction across the account lifecycle for multiple use cases, including changes in account details, new payees, and internal transfers.

Next Stop on the Journey

Recognizing the power of behavioral biometrics, the bank continues to work in partnership with BioCatch to find new ways to reduce fraud and friction across various use cases and digital channels including how behavioral insights can be used as part of a layered strategy to reduce fraud in 3D-Secure transactions and across the mobile channel.

www.biocatch.com E: info@biocatch.com @biocatch in /company/biocatch

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

Tel Aviv | New York | Boston | London | São Paulo | Santiago | Mexico City | Melbourne | Mumbai | Singapore