BioCatch

New Account Opening Fraud:

3 Ways Behavioral Biometrics Can Spot Criminals and Protect Customers

When New Customers **are Not Customers**

New account fraud has continued to accelerate as financial institutions, e-commerce merchants, and other businesses deliver more products and services through digital channels. New account fraud occurs when cybercriminals use stolen credentials or synthetic identities to create a new account with the intent of committing fraud.

There are several different types of new account fraud that can be perpetrated. Some of the most common are:

1 Application Fraud

Application fraud occurs when a cybercriminal applies for a new credit card, bank account, loan, or other financial product with someone else's identity or a synthetic identity. Data breaches and phishing attacks provide the fuel for committing application fraud: personally identifiable information (PII). Data, such as Social Security numbers, emails, addresses, phone numbers, and even device and network attributes, can be used to exploit weaknesses in applications and establish fraudulent accounts.

Synthetic Identity Fraud Designated Fastest Growing Financial Crime

Synthetic identity fraud is the fastest growing financial crime, according to leading consultants at McKinsey, accounting for 10 to 15 percent of charge-offs in a typical unsecured lending portfolio. Synthetic identity fraud combines fake data with real data to create a synthetic identity that is used to open new accounts. For example, a cybercriminal may use a real Social Security number combined with a fake name and date of birth. Despite Know Your Customer (KYC) rules, cybercriminals have been able to meet these requirements using real stolen information combined with other falsified data that will not trigger reg flags. According to the Federal Reserve Bank, synthetic identity fraud results in $6 billion in losses per year to banks and lenders.

2 Mule Accounts

Mule accounts are accounts opened for the sole purpose of moving stolen funds. Mule accounts are critical to the cash out process and a central component to the fraud supply chain infrastructure. The lack of industry standards and best practices for detection and monitoring combined with the increase in P2P platforms and faster payments have created an ideal environment for mule accounts to flourish.

3 Credit Card Testing

Credit card testing occurs when cybercriminals create new accounts to check the validity of stolen payment cards. This type of new account fraud predominantly impacts e-commerce merchants in the form of chargebacks when cybercriminals use the stolen cards to make fraudulent payments and purchases. Checking the validity of the card to determine if it is "live" also raises its value when offered for sale in black market forums.

Banks Turn to Behavioral Biometrics to Stop Mules from Opening New Accounts

50%

of financial institutions do not track mule activity or lack the information and resources to do so

Source: Aite Group

1,000

The number of mule accounts identified by a large bank within the first few months of deploying behavioral biometrics

Source: BioCatch Customer Case Study

Less Friction. Less Fraud. More Customers.

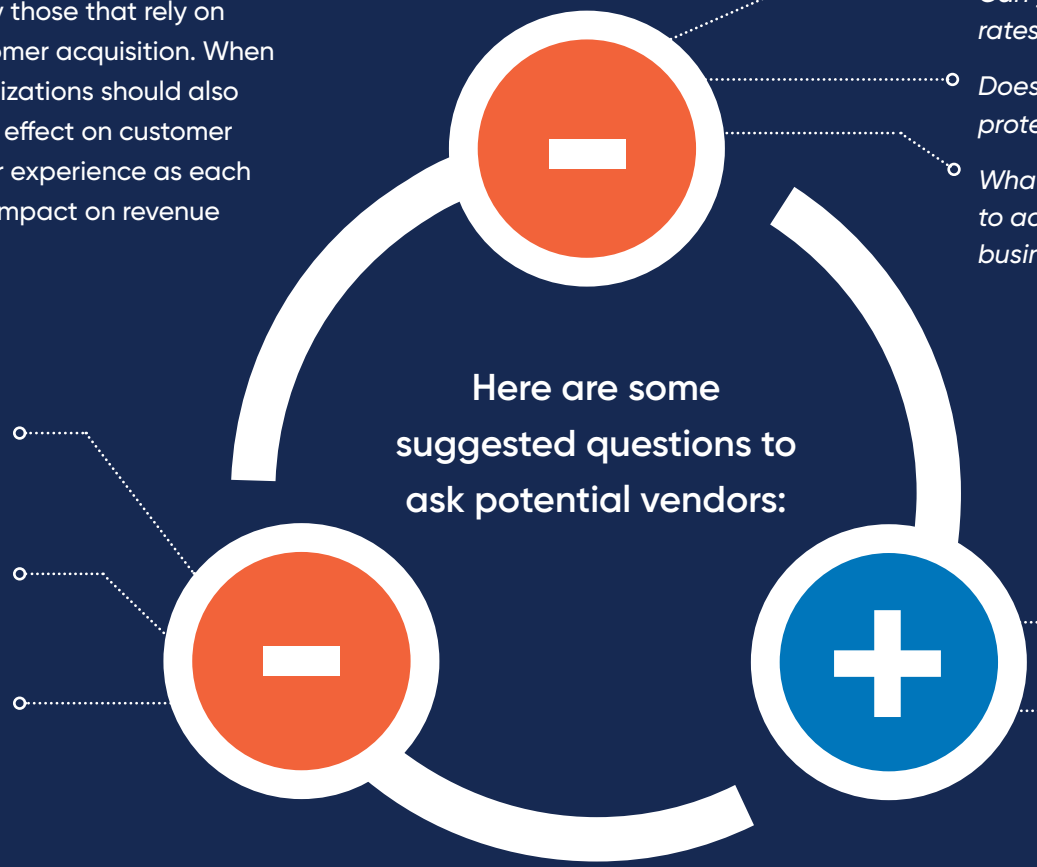
New account fraud prevention can directly impact the bottom line and threatens new digital business models, especially those that rely on growth through rapid customer acquisition. When evaluating solutions, organizations should also take into consideration the effect on customer acquisition and overall user experience as each can have an even greater impact on revenue due to abandonment.

LESS FRAUD

Can you demonstrate high fraud detection rates while minimizing fraud alerts?

Does your solution provide continuous protection for a broad number of use cases?

What capabilities does your solution have to address emerging threats and evolving business requirements?



LESS FRICTION

How does your solution enable less friction and reduce abandonment?

Does your solution analyze user behavior throughout the digital session?

Does your solution identify risk for both payment and non-payment activity across the account lifecycle?

MORE CUSTOMERS

What is your false decline rate? False positive rate?

Does your solution support multiple digital channels?

New Account Fraud in Numbers

85%

Percent of financial institutions that experience fraud in the account opening process[1]

$2.1 Billion

Total losses from credit card application fraud projected in the U.S. in 2020[2]

$3,000

Average loss per incident from credit card application fraud[3]

80%

Percent of credit card fraud losses related to synthetic identity fraud[4]

$10,000

Average loss per incident from synthetic identity fraud[5]

33%

Increase in new account opening fraud cases in 2020[6]

Behavioral Biometrics:
Build Trust and Reduce Fraud

Traditional controls leverage identity proofing methods that require knowledge of personal information and device intelligence. Data breaches and phishing scams have generated a wealth of personal data for sale in the black market, and the ease of searching online public databases and social media profiles have deemed knowledge-based methods ineffective and easy to defeat. Device intelligence offers very limited protection during the new account opening process because new customers rarely come from a "known" device.

Behavioral biometrics offers a fresh approach to new account fraud protection, picking up where knowledge and device-based fraud prevention solutions leave off. There are very clear behavior patterns associated with genuine and fraudulent activity that manifest within the account opening process that behavioral biometrics can quickly spot with a high degree of accuracy by applying cognitive analysis.

64% of confirmed account opening fraud cases detected by BioCatch showed behaviors indicating lack of familiarity with data

HOW IT WORKS

The BioCatch Behavioral Platform leverages machine learning algorithms to analyze physical and cognitive digital behavior of users across digital channels. The model analyzes real-time physical interactions such as keystrokes, mouse movements, swipes and taps, and profiles both legitimate users and cybercriminals on the user level and population level to identify patterns associated with genuine and fraudulent activity.

Applying more than 2,000 behavioral indicators to analyze the online account opening process, BioCatch can distinguish between legitimate, criminal, and non-human users. Here are three examples of ways that BioCatch analyzes user behavior associated with the new account opening process to identify fraud:

Application fluency: *How familiar is the user with the account application process?*
A cybercriminal repeatedly using compromised or synthetic identities will demonstrate a high level of familiarity with the new account opening process compared to a legitimate user.

Low data familiarity: *How familiar is the user with personal data?*
A cybercriminal is not familiar with the personal data and may display excessive deleting or rely on cut and paste techniques or automated tools to enter information that would be intuitive to the legitimate user.

Expert behavior: *Does the user display advanced computer skills compared to the general population?*
A cybercriminal often demonstrates advanced computer skills that are rarely seen among the legitimate user population. Common examples include the use of advanced shortcuts, special keys or application toggling.

Advanced Behavioral Biometrics: A New Frontier in Fraud Detection

Behavioral biometrics has evolved profoundly in the last decade. What started as the analysis of user behavior based on clicks, swipes and typing patterns has developed into a technology that relies on deep knowledge of neuroscience and cognitive analysis that ventures into the unchartered areas of the human mind. The ability to distinguish between the good and the bad based on analysis of short-term and long-term memory and how this impacts human-device interaction requires more than just good machine learning models. Expertise in online user behavior as well as the psychology of cybercrime and social engineering is key for developing the models that produce highly accurate behavioral biometric profiling to detect fraud.

Here are some unique insights that advanced behavioral biometrics platforms can produce:

Age Analysis: *Does the human-device interactions align with the common behavior patterns associated with users of a certain age group?* There are clear patterns that emerge across a large genuine user population that are directly linked to age.

Short and Long-term Memory: *How familiar is the user with the data*? Legitimate users and cybercriminals demonstrate very different behaviors that correspond to short and long-term memory. In a large population of legitimate users, patterns associated with criminal behavior stand out like a sore thumb

User Intent: *What is the intent of the user?* This level of cognitive analysis can be used to uncover even the most advanced social engineering scams by showing whether a user is acting with purpose or under signs of duress.

THE BIOCATCH ADVANTAGE

2+ billion
The number of monthly transactions analyzed by BioCatch

150+ million
The number of users protected by BioCatch

50+
The number of patents attributed to BioCatch technology

CASE STUDY

BioCatch

Top Asia Pacific Bank Rapidly Deploys BioCatch to Protect Account Opening and Saves Millions of Dollars Per Year

OVERVIEW

A top Asia Pacific bank experienced an increase in lending fraud. After deeper investigation, the bank found that more than 70% of their lending fraud cases were coming from what appeared to be existing "trusted" customers. In this case, cybercriminals were opening new bank accounts with the intention of establishing a relationship with the bank and later applying for credit.

SOLUTION

The bank required a solution that would enable them to detect fraudulent bank account openings and reduce losses from subsequent lending fraud. In addition, they needed to be able to deploy quickly in order to minimize further impact to their bottom line and reputation.

RESULTS

The bank achieved the following results by leveraging BioCatch in the account opening process:

$7 MILLION
Projected annual savings in potential fraud losses

90%+
Achieved over 90% accuracy rate on new account fraud alerts

1:1
Achieved a better than 1:1 genuine to fraud ratio for credit card applications

100s
Detected hundreds of fraudulent account openings within four weeks of implementation

CASE STUDY

BioCatch

Top 5 Card Issuer Increases Customer Acquisition and Drastically Reduces Account Opening Fraud

OVERVIEW

A Top-5 credit card issuer was experiencing millions of dollars in fraud losses caused by the use of stolen personal information or synthetic IDs in the application process. Their existing fraud detection model was based on traditional means of verifying identity including personal data and device reputation.

SOLUTION

The issuer adopted the BioCatch behavioral biometrics platform to capture user cognitive and physical digital behavior and leverage real-time risk scores and behavioral indictors within their machine-learning based model. This added a new layer of visibility, enabling them to decipher between legitimate applicants and cybercriminals with a greater level of confidence.

RESULTS

The issuer achieved the following results by leveraging BioCatch in the account opening process:

$10 MILLION

Annual uplift by detecting new account fraud and safely acquiring more customers

99.93%

Percent of applicants approved by BioCatch were confirmed genuine, increasing customer acquisition rates

90%+

Increased new account fraud detection rates to over 90%

CASE STUDY

BioCatch

Behavioral Biometrics Stops Massive New Account Opening Fraud Attack

OVERVIEW

A top digital bank launched an aggressive marketing campaign offering high interest rates in order to attract new customers. Cybercriminals started to take advantage of the promotion and figured out how to circumvent the controls required to open a new account. Using both stolen and synthetic identities, cybercriminals opened a high volume of new accounts which were used as a holding account for funds they transferred from other compromised accounts which they used to quickly cash out.

SOLUTION

New customer acquisition had soared ten times the normal volume, but the bank soon discovered that for every 100 legitimate applications, there were 900 fraudulent ones. Adopting the BioCatch Behavioral Platform, the digital bank was able close the gaps left by their current fraud prevention solutions. BioCatch quickly identified specific behavior patterns associated with fraudulent activity related to application fluency, proficiency with computer shortcuts and lack of data familiarity, that allowed the bank to get fraud under control and continue normal operations.

RESULTS

The bank was able to achieve the following results from adding BioCatch to its technology stack:

70% uplift in fraud detection
during the attack period

60% increase in fraud detection
when deployed on top of existing fraud prevention tools following the attack

Increase in customer acquisition
while preserving the desired user experience

ABOUT BIOCATCH

BioCatch pioneered behavioral biometrics which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Protecting more than 100 million users, organizations around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, more than 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, visit www.biocatch.com.

1 BankInfo Security, The State of Digital Account Opening Transformation, March 2020
2 Aite Group
3 Top 5 U.S Card Issuer
4 U.S. Federal Reserve Bank
3 U.S. Federal Reserve Bank
6 BioCatch

BioCatch