BioCatch

White Paper

Account Opening Fraud:

How to Uncover When New Customers Are Not

White Paper

Account Opening Fraud:

Table of Contents

The Rise of the Digital Bank	Pg. 3
Cybercriminals Follow the Money, Jeopardizing the Digital Migration	Pg. 3
Uncovering the Blind Spots in Traditional Fraud Controls	Pg. 4
When Digital Business Objectives Collide	Pg. 5
Stop Criminals, Not New Customers: A Fresh Approach to Protect Account Opening	Pg. 5
Behavioral Biometrics Gets Real Results	Pg. 6
Conclusion	Pg. 7

BioCatch

The Rise of the Digital Bank

Digital banking has become the single most effective channel for financial institutions to drive growth, increase revenue and attract new customers. The global rise of neobanks, or digital-only banks, has proven this point. Not only are they growing rapidly, they are challenging traditional banks. Because they do not have to operate physical branches, neobanks have lower costs and can offer higher rates. But more importantly, they offer an innovative and personalized user experience that appeals to younger generations.

The competition is steep, and traditional banks have prioritized digital transformation to catch up to and surpass more savvy players. The investment in digital channels has accelerated even further as a result of the COVID-19 pandemic. With access to physical branches greatly limited, or even completely shut down, consumers had no choice but to move their business online. A top 5 U.S. bank reported a 23 percent jump in the number of customers using digital banking during the peak of the pandemic[1].

Now that consumers are more accustomed to digital channels, demand is growing. Besides everyday banking transactions, such as checking their balance, bill pay or sending a payment, online account opening has more than doubled at most banks since last year[2]. Recent studies suggest that consumers are voicing a growing demand for more online services and touchless banking since the pandemic, with 79% of consumers citing a preference for their banks to offer more all-digital services[3].

These consumer lifestyle changes present a game-changing opportunity for banks to grow their customer base and attract new or underbanked populations. This is good news from a cost efficiency perspective. The acquisition cost for a digital customer is $77 per account while the cost for acquiring a non-digital customer is more than 50% higher, or $138 per account[4]. The demand is there, but do the benefits outweigh the risks?

Cybercriminals Follow the Money, Jeopardizing the Digital Migration

There is no question that digital channels offer banks a tremendous business opportunity to acquire more customers at a fraction of the cost. But the digital migration has also introduced more risk. Cybercriminals are following the money right into the online account opening process. Today, a staggering 85% of financial institutions experience fraud in the account opening process[5], a problem that is increasingly difficult to detect when there is no prior profile or relationship with the customer.

From credit cards and bank accounts to a wide range of lending products, cybercriminals are sparing no effort to turn a profit by exploiting weaknesses in the account opening process. Several challenges have emerged when managing fraud risk in account opening, including:

Synthetic Identity Fraud - This occurs when a cybercriminal combines legitimate data with synthetic data not associated with a real person to create a whole new identity. According to the Federal Reserve Bank, synthetic identity fraud cost lenders around US $6 billion and was cited as 20% of all credit losses in 2016, the most recently available numbers.

[1] Source: ABA Banking Journal, Digital Transformation, Accelerated, September 2020
[2] Source: ABA Banking Journal, Digital Transformation, Accelerated, September 2020
[3] Source: Lightico, COVID-19: Consumers Demand a New Digital Banking Normal, May 2020
[4] Source: American Banker, The What and Why of Digital Account Opening, October 2018
[5] Source: BankInfo Security, The State of Digital Account Opening Transformation, March 2020

Mule Accounts - While typically used as a way to move stolen funds from compromised accounts, mule accounts are increasingly being opened to establish a relationship with a bank so a criminal can later apply for credit. One large bank in Asia found that 70% of their credit card lending fraud cases had come from "trusted" customers that were later identified as mule accounts[6]. The lack of industry standards and best practices for detection and monitoring has contributed to an ideal environment for mule accounts to flourish.

Buy Now, Pay Later - The "buy now, pay later" financial model is booming globally. These services offer an interest-free platform for consumers to make purchases at online storefronts and pay the costs in small, affordable installments over time with a debit or credit card or bank account. Cybercriminals use stolen identities and financial information to open new accounts and initiate fraudulent purchases. These FinTech platforms are still in their infancy, so there is little data that has been reported on estimated fraud losses tied to the service. However, it is one to watch.

Uncovering the Blind Spots in Traditional Fraud Controls

The rapid growth and adoption of digital banking services has left fraud and risk management teams running to keep up. With the laser focus on digital experience and customer acquisition, fraud management has taken a back seat with existing "good enough" technology and controls expected to deliver the same results. Gaps in existing solutions, however, are leaving blind spots in the account opening process.

Know Your Customer (KYC), or knowledge-based identity proofing mechanisms, have been ineffective for some time. Data breaches and phishing scams have generated a wealth of personal data available for sale on the black market, and the ease of searching online public databases and social media profiles for information has deemed knowledge-based methods as too easy to defeat.

Device ID or IP/geo-location based solutions are widely used, but they have increasingly come under scrutiny after cybercriminals have demonstrated the ease of taking over a device or hiding their use of one. A secondary challenge is how frequently users change their devices. New models come out, mobile devices break, and devices like a home laptop can be shared among multiple users. Regular device changes fail the requirement for identity proofing to be fixed and stable. In the case of account opening, device ID on its own is not able to identify a good or bad applicant as a new customer does not have a prior relationship or profile with the organization.

"While losses to fraud would be avoidable in an ideal world, most organizations reluctantly accept the level of fraud-related loss they experience. However, fraud leaders with a trust and safety focus often have other intentions. These include not insulting customers by incorrectly identifying legitimate interactions as fraudulent and not making interactions intolerable through repeated high-friction challenges."

***- Gartner**, "Creating Trust and Safety on the Internet," July 2020*

| [6] Source: BioCatch, **Top Asia Bank Case Study**, September 2020

When Digital Business Objectives Collide

Technology isn't the only reason for the gaps. Organizational challenges also exist that must be addressed. Digital transformation has created new priorities for financial institutions, and fraud management is no longer just a function of information security or risk management. More stakeholders have become involved in the process, including line of business owners. Often these lines of business have different objectives and levels of maturation, and the means of identifying fraud and connecting the dots between disparate lines of business creates issues.

Conflicting business objectives are hard to overcome, and different metrics are used to measure success. For example, as fraud leaders seek to collaborate with other internal stakeholders, they are required to shift their mindset from loss prevention to revenue growth. Instead of focusing solely on stopping fraud, they must also consider how controls they implement could potentially stop customers.

Let's consider this in the context of online credit card opening. According to a Top 5 card issuer, the average loss per incident of a fraudulent credit card application is US $3,000. On one hand, a fraud leader might say, "We stopped 1,000 fraudulent applications and prevented $3M USD in potential losses due to the fraud controls we implemented." The objective of a fraud leader is reducing the impact to the P&L statement.

On the other hand, a digital product owner, looking at average customer lifetime value of US $3,000, might say, "Those fraud controls added friction to the process thus increasing application abandonment. As a result, we lost 1,000 new customers and $3M USD in potential revenue." The objective of the line of business owner is increasing customer acquisition and revenue.

Looking ahead, the question that all financial institutions most resolve is: How can you trust a customer that you have never seen before?

> *"Through cognitive analysis, BioCatch helps reduce instances of Account Opening fraud, which is particularly challenging to detect when the user is a new user and doesn't have a historical digital footprint with the organization."*
>
> ***- John Tolbert** , Lead Analyst and Managing Director, KuppingerCole*

Stop Criminals, Not New Customers: A Fresh Approach to Protect Account Opening

In our digital world, behavior tells all. During account opening, typing speed, swipe patterns, and every click of the mouse tells a story — one of criminal activity or genuine user behavior. Each of these patterns can be quickly spotted through behavioral biometrics, an innovative technology that provides financial institutions with a fresh approach to effective fraud detection in the account opening process while maintaining a low-friction customer experience.

Behavioral biometrics looks at account opening fraud through a different lens, focusing on how information is entered into an online form, and not what information is entered. Behavioral biometrics has a high degree of accuracy and pulls together data to empower fraud teams with increased visibility into risk through behavioral insights. Even in the case of a new customer, behavioral biometrics recognizes trusted behaviors, creating a smooth journey through the account opening process.

Examples of patterns that behavioral biometrics looks at during the account opening process to identify fraud include:

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 does not demonstrate knowledge of 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.

Age Analysis - Does the human-device interaction align with the common behavior patterns associated with users of a certain age group?

Some behavioral patterns shift with age, such as the time required to shift from the Control key to a letter key during data input, mobile device orientation and swiping patterns.

***Did You Know**: 64% of confirmed account opening fraud cases detected with behavioral biometrics showed behaviors indicating lack of familiarity with personal data.*

Behavioral Biometrics Gets Real Results

Identity proofing is critical for managing risk in the account opening process, and behavioral biometrics is delivering results. Global organizations have achieved reduced fraud risk and customer friction and increased digital acquisition after implementation. These success metrics make the case.

Reduce Fraud Risk - Managing fraud risk encompasses much more than just loss prevention. Mule accounts is one example. When a fraudulent deposit account is opened to serve as a mule account to move money from other compromised accounts, that comes with both regulatory and reputational risks in addition to the financial impact. Behavioral biometrics helped a large bank in Asia detect hundreds of fraudulent account openings in the first four weeks of deployment, with potential annual fraud savings estimated at over USD $7M.

Minimize High-Friction Interactions - Eliminating points of friction in the digital account opening process can be especially challenging. The experience should be centered on treating new customers like an old friend, but that is difficult in cases where no pre-established relationship exists. A large digital bank undergoing a massive attack deployed behavioral biometrics and was able to detect 70% more new account fraud without impacting good customers in the process.

Increase Digital Acquisition- This is the ultimate risk and reward question. Fraud prevention solutions should provide measurable fraud reduction while also allowing more good applicants to be approved with confidence. A Top 5 U.S. card issuer leveraging behavioral biometrics was able to reduce false declines, gaining an additional USD $1M in otherwise lost annual revenue from genuine customers who had abandoned the application during the high-friction control process.

Conclusion

The surge in digital channel usage brought on by COVID-19 forced financial institutions to accelerate digital transformation to address growing demand. With previous investment weighted toward customer experience, financial institutions have had to re-evaluate their digital strategy with a renewed focus on identity proofing as a core requirement of maintaining and growing digital operations.

An effective strategy for tackling today's threats requires a layered solution that builds trust with customers, manages risk across digital channels, and limits financial losses from cybercrime. Behavioral biometrics is helping financial institutions deliver a comprehensive fraud management strategy and build an online environment where customers feel safe to interact.

BioCatch

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers 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, over 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch