Sponsored Content

IDG

Innovating the Customer Experience Without Opening Fraud Floodgates

Financial services organizations must secure transactional activities amid increasingly sophisticated cyberattacks, while also providing frictionless customer service.

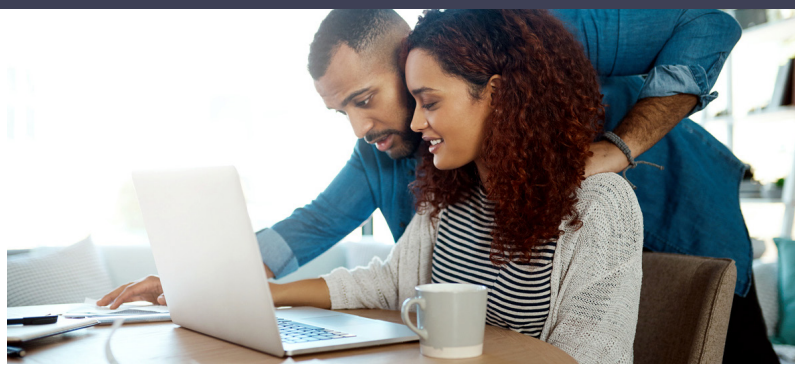
BioCatch

Financial institutions are struggling

with cybercriminals who exploit controls such as passwords, device IDs, one-time passcodes, and various authentication tools. Data breaches and phishing attacks have made it far too easy for criminals to harvest personally identifiable information to take over existing accounts or initiate new ones. Further, malware, remote access tools (RATs), emulator attacks, and other creative account takeover methods have contributed to a surge in fraud losses. At the same time, institutions are naturally reluctant to implement defenses that impede frictionless transactions and potentially alienate customers.

This dossier examines how behavioral biometrics can differentiate between legitimate and illegitimate activities in real time. The technology improves security while enabling organizations to accelerate digital offerings to customers without friction.

CONTENTS



Digital Financial Services Provide New Pathways for Criminals

Financial institutions are eagerly transforming business models to generate growth and success by providing innovative digital services that meet or exceed customer expectations. In parallel, they must shield themselves from risk as they potentially create targets of opportunity for cybercriminals.

The scope of risk is staggering:

- 85% of financial institutions experience fraud in the account-opening process, according to "The State of Digital Account Opening Transformation" by BankInfo Security (May 2020).
- $3,000 is the average loss per credit card application fraud incident, according to a top five US card issuer.
- McKinsey & Co. analysts assert that fraudsters using fictitious, synthetic IDs to draw credit "is the fastest-growing type of financial crime in the United States, accounting for 10% to 15% of charge-offs in a typical unsecured lending portfolio." The US Federal Reserve says this accounts for an average loss of $10,000 per incident.
- Social engineering and other scams frequently dupe legitimate users to authorize payments to illegitimate entities. In the UK, authorized push-payment fraud scams caused an estimated GBP 479 million in losses in 2020.

New services such as mobile banking and wealth management portals create new attack vectors for criminals seeking to take over existing accounts or fraudulently open new ones. Many of their numerous tools are available in "online supermarkets of cybercrime" that even come with free updates and tech support. Such sites offer software such as malware and RATs, as well as access to stolen credentials and personally identifiable information that can unlock user accounts.

Cybercriminals are continuously trying and fine-tuning social engineering tactics that can trick employees and customers into providing account and personal information or transferring funds into a criminal's account. Attackers can leverage stolen passwords and user IDs, and then attempt "credential stuffing" in the hope that users have duplicated their information across different accounts.

Financial institutions are also at risk from digital money mules recruited by criminal gangs, according to a report in the Wall Street Journal. They attempt to "open bank accounts, or use their pre-existing accounts, and move cash via electronic transfer" to launder funds in difficult-to-detect ways that hide behind data privacy requirements and lack of visibility into the end-to-end payment trail.

Prioritizing Customers' Digital Experience

Meanwhile, consumers are rapidly embracing payments through digital channels such as person-to-person (P2P) payments, with Zelle reporting more than 1.2 billion transactions in 2020 and PIX in Brazil reaching 1 billion transactions in its first six months. This trend, combined with the rise of digital-only banks, is leaving financial organizations with little choice but to transform.

Yet, individuals are unwilling to be constrained by risk management tools such as activation waiting periods and low transfer limits. Likewise, banks don't welcome the higher support costs of fielding calls from consumers struggling with security measures.

The balance between risk management and optimal customer experience is difficult to strike, and the risks are great:

- One bank's promotion for high-income prospects to obtain immediate approval for a deposit account and a credit card with a single application resulted in a subset of criminal applications. These were later tied to down-the-line credit fraud losses and exploitation of mule accounts.
- Social engineering voice scams cost a bank hundreds of thousands of pounds per month in authorized push-payment fraud as cybercriminals bypassed its comprehensive fraud technology stack.
- Automated account processes are susceptible to cybercriminals with access to stolen or synthetic identities, which can generate millions of dollars in fraud losses for individual institutions.

Weeding out criminal efforts

Traditional controls that rely on device or location can be spoofed. Also, device and location are largely irrelevant when the customer is not previously known to the institution.

When existing fraud protection programs and processes fail, financial institutions need to up their game. Behavioral biometrics from BioCatch analyze a user's physical and cognitive digital behavior to distinguish between genuine users and criminals to detect fraud and identity theft and improve customer experiences.

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

Cognitive analysis can uncover even the most advanced social engineering scams by determining whether a user is acting with purpose or under signs of duress. Furthermore, legitimate users and cybercriminals demonstrate very different behaviors that correspond to short- and long-term memory. A legitimate user, for example, will type continuously, while a fraudster is likely to pause or use copy and paste functions as they refer to unfamiliar information.

In addition, differences in how a senior citizen enters data can provide signals when a younger cybercriminal is trying to take over the account. Even if the profile seems to represent the physical traits and preference of a known legitimate user, certain microbehaviors give away the emotional state of the user.

In a large population of legitimate users, patterns associated with criminal behavior stand out. Some of today's most sophisticated attacks can be detected only when fraud protection solutions are continuously monitoring for the most subtle deviations in user behavior.

A Comparison of Static Biometrics and Behavioral Analytics

PHYSICAL BIOMETRICS are the primary method for identification, authentication, and access control. This involves fingerprints, face recognition, hand geometry, voice recognition, palm vein recognition, retina scans, iris recognition, and signature verification. However, using only one physical biometric to authenticate a user at login is essentially the same as adding a second static password that can never be changed if compromised.

Many financial institutions use static biometrics such as fingerprints, retina scans, and face recognition to authenticate customers. In many cases, however, the biometric is tied to the device and is only as strong as the PIN, which cannot provide suffcient visibility beyond login and when opening digital accounts.

Although static biometrics security is important, its integrity gradually erodes over time even when initial authentication is valid. This is due to sophisticated account takeover mechanisms, such as when a cybercriminal convinces a legitimate user to download a remote access tool (RAT) and log into a session. The only way to restore integrity is to require additional authentication actions, which causes friction that negatively impacts the customer experience.

Other challenges have emerged with physical biometrics:

- Criminals can capture and sell them for fraudulent use.
- Consumers and ethicists have raised concerns over racial bias in biometrics such as facial recognition and the need for consent to use biometric authentication.

Behavioral biometrics provides a dynamic solution that increases trust and reduces friction throughout online sessions while providing high levels of fraud detection.

The behavioral information that BioCatch solutions collect is not static. For example, user behavior can vary depending on:

- The type of device used.
- Mood and distraction levels.
- The user gaining fluency with a service over time.
- User setting (sitting behind a desk, walking outside, or even while carrying a cup of coffee).

Behavioral biometrics run continuously in the background to protect sessions post-login and to detect subtle anomalies based on risk. They are uniquely able to detect human and automated fraud threats including RATs, bots, social engineering, and other methods that bypass traditional controls.

The Engine Behind Behavioral Biometrics

BUILDING RISK MODELS that focus on identifying patterns for both legitimate users and cybercriminals offers unique insights that traditional fraud prevention tools do not. These can help protect and personalize the user experience while creating trust and ease of use in the digital channel.

The BioCatch Risk Engine analyzes digital behavior and calculates a risk score of 0-1,000, which specifies the degree of risk associated with every session. The BioCatch platform also reveals the leading behavioral indicators in this determination — for example, risky patterns such as app toggling and excessive deleting of personal information. Likewise, genuine behavioral patterns such as fluid typing and high familiarity with personal information indicate appropriate use.

Visualization tools allow fraud teams to reconstruct exactly how a user behaved during a session, including a step-by-step video breakdown. In addition, fraud teams can build rules using BioCatch insights such as risk score and leading indicators to take real-time action for both high- and low-risk events.

BioCatch continuously monitors and analyzes behavioral patterns throughout a user's time within an application. Doing so enables the solution to notify organizations of fraudulent behavior as soon as it's detected, allowing immediate action.

BioCatch continuously monitors and analyzes behavioral patterns throughout a user's time within an application.

BioCatch employs a multilayered risk analysis approach that arms organizations with key insights that enable real-time action for both high- and low-risk events. Regardless of an attacker's mode of operation, user behavior can't be stolen, spoofed, or replicated.

The Future Is Behavioral Insights

DIGITAL TOOLS ENABLE BAD ACTORS to exploit security weaknesses quickly, before defenders realize the extent of the problem. Such is the case with the digital money mule phenomenon.

Money mules are not new; however, in the wake of the COVID-19 pandemic, cybercriminals seek to exploit government stimulus programs and cash in on economic impact payments and unemployment benefits. To receive funds associated with these fraudulent claims, cybercriminals attempt to open new mule accounts. According to BioCatch research, high-risk applications for new accounts have exploded from a standard rate of 0.5% to between 10% and 50%.

Only an estimated 6% of financial institutions are actively investing in mule detection programs. One digital bank found that cybercriminals were exploiting a marketing campaign offering high interest rates to new customers, creating mule accounts to cash out funds from other compromised accounts. Using BioCatch behavioral insights, the institution experienced a 70% uplift in fraud detection during the attack period.

The financial industry has found success with behavioral biometrics in stopping mule accounts at the source. In one case study, a bank reported that biometrics:

- Detected more than 90% of account takeover fraud before a fraudulent payment could be made.
- Identified 2,000+ mule accounts in the first year.

With the rapid shift to digital solutions and the demand for fast payment, financial institutions require progressive technologies to prevent the flow of stolen funds. The BioCatch platform identifies mule accounts at account opening across existing accounts and helps financial institutions fight money laundering together through its consortium offering.

Another emerging use case in which behavioral insights have demonstrated strong results is business email compromise (BEC). The attacks are highly targeted against fewer victims, but the losses are often far more substantial. According to the FBI, BEC fraud accounted for $1.8 billion in losses in the US in 2020.

As with social engineering voice scams and authorized push payment, BEC fraud is difficult to detect, because a genuine user who is unaware of being scammed conducts the transaction or payment. By analyzing digital behavior patterns, BioCatch identifies changes in the user's emotional state, such as hesitation or confusion, as indicated by how the user interacts with the banking application in initiating a payment or transfer. BioCatch looks for flags such as high overall idleness of the mouse, keys, and clicks, and lengthy pauses in typing.

As financial transactions increasingly depend on digital channels to fuel growth, behavioral biometrics play a vital role in comprehensive defense layers, building trust and safety.

For more information, visit: www.biocatch.com

Credential Stuffing: Fraudsters Exploit Open-Banking Platforms to Launch Attacks

The rise in open banking is a huge opportunity for financial services organizations, but there are significant risks

By Gareth Campbell and Andrew Dunn

DESIGNED TO POWER INNOVATION in the banking landscape, the Second Payment Services Directive (PSD2) marked the start of open banking, allowing banks to deliver customers the convenience and experiences they want. By creating a path for banks and financial institutions to share their customers' data with third parties through the use of APIs, the opportunities presented by open banking to improve the digital experience – from customer onboarding to seamless payments – are endless.

The PSD2 regulatory framework has created a clearly defined pathway for open banking in the UK and Europe. Since 2019, open banking has exploded in the UK, with more than 300 providers joining the ecosystem. More than 2.5 million UK consumers and businesses now use open-banking-enabled products to manage their finances and make payments. Many other regions, including Australia and Hong Kong, have started to develop legislation to push open-banking initiatives while interest in the US for similar guidance is actively being explored.

While open banking has created incredible opportunities, banks are also presented with many new risks. One emerging risk is the exploitation of open-banking platforms to initiate credential-stuffing attacks.

Credential Stuffing Attacks on the Rise

Credential stuffing is the process of inputting compromised usernames, passwords, and other login information to gain access to an account.

These attacks have been on the rise. Between December 2017 and November 2019, there were 85.42 billion credential-stuffing attacks, of which 16.55 billion were targeted at APIs directly.

There are many contributing factors that make these attacks so successful. First, the abundance of personal information for sale on the dark web provides the fuel for testing. Second, consumers continue to re-use the same credentials across multiple sites, enabling high success rates. Finally, tools such as Sentry MBA, SNIPR, and Account Reaper have enabled fraudsters to automate credential stuffing at scale.

A Behavioral Perspective on Automated Attacks

BioCatch has also been seeing these types of attacks on the rise – with a twist. Fraudsters know that most prominent websites have some type of bot detection technology employed to prevent credential abuse and have started to change their tactics to circumvent these controls. BioCatch began to observe instances of fraudsters abusing legitimate open-banking platforms to test batches of credentials. In addition, they have reverted to testing smaller, more frequent batches instead of testing at scale.

During February 2021, one financial institution received reports from internal logs that they had suffered what looked like a brute-force attack. Looking at the overall volume of failed logins as well as the failed-to-successful ratio, we saw that two distinct events occurred.

All the login attempts were coming from a legitimate open-banking service provider. It's not known if the origin was the company itself or another third-party provider that leverages their services. What is clear, however, is that the attackers used the opportunity to hide their attacks behind a trusted source.

When reviewing what occurred in the login process of these sessions, we saw that the username and password were typed extremely quickly. Following a first attempt at login, a bot was programmed to wait 25 seconds, enter another password, and repeat this process multiple times. The login behavior is such that the username and password are not injected – they are entered using keypress events, and the element navigation is controlled by mouseclick events. The speed and concurrency of these sessions are far beyond what would be observed from a genuine connection from a human or from an open-banking provider (where connections are typically once per day per user), indicating a credential-stuffing attack.

Interestingly, during two notable attack events, a very small number of logins exhibited different behavior. These sessions, covering eight distinct users, had more human-like behavior. In comparison to the bulk of the credential-testing sessions, BioCatch detected remote access tools (RAT) and not bot activity. Success rates of the tested batches varied from 0% all the way **up to 23%**.

BioCatch advanced behavioral biometrics leverages user-device interaction data, such as mouse-clicks, swipes on mobile devices, and keystrokes, to analyze data using machine-learning techniques. The technology profiles both genuine and fraudulent activity as well as cognitive insights to distinguish between genuine and non-genuine users (automated or human) across multiple use cases and threat vectors.

While this may be an isolated incident, it is a potentially significant trend that BioCatch will continue to monitor. As with all forms of fraud, attackers are constantly changing their methods as new technology, such as open banking, comes into play.

As Digital Banking Grows in Southeast Asia, So Do the Security Risks

Exposed APIs, insecure customer mobile devices, insider fraud, and other criminal activities threaten online banking, but regulations and technology can help. | **By Zafar Anjum,** *CSO* **Feb. 28, 2021**

ONE OF THE KEY TRENDS in the Southeast Asian banking sector is the growing adoption of digital banking and the entry of new providers from nonbanking and tech backgrounds. Driving this adoption is evolving customer expectations and enhanced digital penetration, combined with the desire to serve the underbanked segments of society. But with that growth comes an increase in security risks for digital banks and their customers alike.

Why Digital Banking Is Growing in Southeast Asia

According to a report by the Boston Consulting Group (BCG) published in December 2020:

> *The COVID-19 pandemic has accelerated this trend, as enforced digital transitions have embedded a more immediate impetus for change. These drivers will see Southeast Asia's digital banking opportunity expanding significantly in coming years, reflecting a trend which has seen over 200 new digital banks established globally over the last decade.*

The rise of digital banking in Southeast Asia is part of a global trend. The BCG report highlights that "there has been a 190% increase in the number of [what it calls] Digital Challenger Banks since 2015, initially spurred by pioneering changes in regulation in the UK and Japan." As a result, 45% of digital banks are now based in the Europe and Middle East (EMEA) region, 35% in the Americas, and 20% in the Asian Pacific (APAC) region.

In Southeast Asia, Singapore is ushering the region into a digital banking future. While its rival, Hong Kong, had granted eight digital banking licenses last year, the Monetary Authority of Singapore (MAS) awarded digital-banking licenses to four new entities in December 2020. Malaysia and the Philippines are also reportedly readying the guidelines for issuing digital-banking licenses in their respective countries.

The Security Risks and Challenges of Digital Banks

The main security challenges include consumer protection and cybersecurity breaches.

The very nature of digital banks — most customer interaction happens on mobile devices — makes them vulnerable to cyberattacks.

"Everything from phishing attacks, man-in-the-middle attacks, mobile malicious hash, even ransomware have increased simply because of more use of the mobile channel," says Michael Araneta, an analyst at IDC Financial Insights. "Note also that a high percentage of mobile phones in use, especially those in developing markets of ASEAN, would have some malware in them. Banks cannot simply turn them off or not allow customers to not use them. That is the only means of interaction!"

"I feel any bank (digital or traditional) will always be a ripe target for cyberattacks," concurs Kunal Sehgal, a Singapore-based cyber evangelist. "The target audience here is millennials who are digital natives and are new to the financial world."

In the region, identity theft and fraud are the biggest threats, says Andrew Milroy, director at Veqtor8, a cybersecurity advisory firm.

The very nature of digital banks — most customer interaction happens on mobile devices — makes them vulnerable to cyberattacks.

"Data security has been one of the biggest threats in the banking industry," says Dewi Rengganis, an industry analyst for APAC telecoms and payments at Frost & Sullivan. She cites Japan's 7Pay as an example of security being a significant challenge for the broader adoption of digital banking for payment services. 7Pay was a cashless payment service rolled out in 2019 by 7-Eleven. It allowed users to pay for purchases at Japan's roughly 21,000 stores through a smartphone app. The app got hacked only days after its launch. More than ¥38 million (US $350,000) was confirmed missing from 808 7Pay user accounts. Because of this issue, 7Pay terminated its service at the end of September 2019 after losing user trust.

Governments and regulators are aware of these security threats. That's why, in Singapore's case, "the announcement of digital-banking licenses was eventually followed by the release of the updated IT Risk Management Guidelines for financial institutions in Singapore" by the MAS agency, Araneta says. "Although they were not necessarily contingent on the other, what Singapore has done is underscoring how banking (and competition) and the way we deliver banking (as in the IT guidelines) have really changed."

Milroy concurs: "In Southeast Asia, you need a strong regulator that forces banks to address security challenges. In Singapore, the MAS does this ... For other Southeast Asian nations, the regulators tend not to be as strong in enforcing best practices in security."

But Asian banks themselves are moving ahead to improve security, working with security technology providers, says Frost & Sullivan's Rengganis:

> *Digital banks have been constantly upgrading their risk management to ensure security is maintained and protect customers from criminal activity, such as fraud, and money laundering. Many banks have reevaluated their approach to cybersecurity by leveraging big-data analytics and blockchain technology. ... They need to add biometrics, device telemetry, and behavioral analytics to mitigate risk of identity theft. For fraud, they need to ramp up privileged access management [also called privileged identity management] and analytics.*

"Note that fraud often involves insiders," says Veqtor8's Milroy. "For identity theft, banks need to move beyond passwords, even one-time passwords. In fact, passwords are becoming a liability."

IDC's Araneta points out that many banks' security-related projects to date have focused on network security (securing the perimeter), but more and more of the banking activity (interactions and engagement) is happening outside the bank's traditional perimeter. "So the new tools of security really need to focus on securing those interactions as well," he says.

Banks can't do it alone; customers need to be better at security, Araneta says:

> *It is also about customer education — for the customer to know how to protect themselves as the ultimate threat vector or a vulnerable point of attack for cybercriminals. This is the reason banks must exert effort in customer education.*

Banks also need to help customers, such as by implementing multifactor authentication, despite the tradeoff in user experience it creates.

New APIs Emerging for Digital Banks

According to Gartner, attacks and data breaches involving poorly secured APIs are occurring frequently as each new API represents an additional and potentially unique attack vector into banking systems. The number of exposed APIs in apps has grown dramatically in just two years, making them a larger attack vector than the user interface. Gartner predicts that, by 2022, "API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications".

For digital banking, the open-banking API has been emerging in the Asia-Pacific region only recently, which will lead to more API adoption and thus possible attack vectors. The good news, Gartner says, is that API management and web application firewall vendors, as well as new startups, are aware of this shortcoming and are addressing it.

Asian banks themselves are moving ahead to improve security, working with security technology providers.

Besides secure API management, digital ID frameworks are also critical for the industry. Rengganis notes that digital ID frameworks have been implemented in countries across Southeast Asia, including Indonesia, Malaysia, and Singapore, that "can reduce the burden on banks for KYC [know-your-customer] processes."

The digital-banking opportunities are huge in Southeast Asia, and the organizations that are taking a plunge in this space will thrive as long as they ensure consumer protection, take steps to mitigate cybersecurity risks, and implement strong data protection.