BioCatch

4 Ways Financial Scammers Are Getting Ahead

BioCatch

Fraud Forward 2022

Recent global developments have created ample opportunities for cybercriminals to take advantage of vulnerable and even traditionally non-vulnerable individuals. The COVID-19 pandemic amplified the use of digital channels for everyday banking, while other services including digital payments, contactless and cashless payments, and buy now pay later (BNPL) services were embraced by consumers around the world. Last year, 93% of consumers used one or more digital payment methods[1], such as Zelle, and made nearly $100 billion in purchases using BNPL services[2]. Not to mention government stimulus programs created unusual cash flows that were ripe for the taking by scammers.

93% of consumers used one or more digital payment methods in 2021

Every financial institution strives to stay ahead of scammers in order to protect customers against financial loss and preserve their reputation and brand. However, the dynamic nature of cybercrime makes the practice of managing fraud risk a considerable challenge. What will the fraud landscape look like moving forward in 2022?

This e-book will explore four ways financial scammers are getting ahead including the tactics they are using, the targets that are most vulnerable, and the limitations of existing fraud controls. We'll also discuss how financial institutions can fight back.

BioCatch

1 Social Engineering and the Modern Scammer

Social engineering is by no means a new occurrence, but it continues to be an effective method for scammers to achieve a desired outcome. BioCatch research shows that social engineering scams increased 57% last year and is present in one out of every three cases of account takeover fraud. Most scams that involve social engineering require some interaction in order to get a user to divulge personal information, download malware onto their mobile device, or provide a one-time passcode that will allow a scammer to bypass multi-factor authentication. Here are some of the social engineering tactics that scammers are using to stay ahead.

Social engineering scams increased **57%** in 2021

Smishing

SMS phishing, also commonly referred to as smishing, is a form of social engineering attack that targets victims on their smartphones. A smishing attack uses text messages that appear to come from a legitimate organization and most often contain a link that drives a user to a phishing site. More recent smishing cases send direct messages to consumers alerting them to fraud or some other problem on their account in order to elicit a response. Once a user responds, the scammer will contact them on their mobile phone claiming to be someone from their bank.

Smishing has increased significantly across the globe and complaints about SMS spam increased over 140% last year[3]. Smishing remains a big concern as users spend so much time on their mobile devices – an average of five hours per day in 2021[4]. In addition, the ability to launch a smishing attack has gotten easier with scammers able to reach thousands of potential victims in minutes, and SMS bots that can be used to intercept the one-time passcode most banks use for step-up authentication.

Voice scams

Voice scams are not an entirely new strategy, yet their success is resulting in a global expansion of this scamming tactic. While earlier financial scam strategies were focused primarily on vulnerable customers such as the elderly, younger customers who value convenience over privacy are increasingly falling prey. This method of social engineering is not difficult for scammers to perform, but it can be very challenging to detect since the scammer does not interact directly with the banking platform and instead convinces the user to perform an action. For example, authorized push payment fraud is one of the most prevalent types of voice scams where a user is convinced to make a payment or transfer into an account controlled by the criminal.

35% of impersonation voice scams involves a payment greater than $1,000

Remote access scams

Financial scammers have advanced their strategies to multi-layer hybrid scams that go far beyond simply coaching a target through performing a transaction. This is often the case where remote access tools are involved. For example, a scammer might start out with a social engineering voice scam and then shift tactics to coerce a target to download an app to their phone that is actually a software that enables a criminal to gain remote access to their device. The methodology behind switching or blending techniques is designed to slip past bank security controls and even gain access to additional personal or account information.

Key Takeaway

As the modern consumer has outsmarted old scamming tricks, the modern scammer has become more sophisticated. Social engineering scams have evolved to understand human inclinations and tendencies and have been reworked to target consumers at the exact right moments with the right methods. Legacy-based fraud prevention measures that rely on device, IP or network attributes are no longer a match on their own for scammers who have learned to bypass or spoof them, and new approaches that provide deeper visibility into risk across a digital session are required.

BioCatch

2 The New "Vulnerable Customer"

While anyone with a bank account, credit card and access to the internet is a potential financial fraud victim, some consumers are more vulnerable to scammers. The UK Financial Conduct Authority (FCA) defines a vulnerable customer as "someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care." Customer vulnerability is driven by four factors—health, life events, resilience, and capability—and that vulnerability can either be transient or continuous depending upon life events, capability, and health. Major world events that have impacted everyone combined with the advancement of scamming techniques have evolved the idea of the "vulnerable customer" to become much broader.

Elderly customers

While there are a number of new "vulnerable customers," elderly customers remain a top target for financial scams. Elderly customers have always been a primary vulnerable demographic as they are known for having better credit and more funds, tend to be more trusting, and lack familiarity with new digital technologies. They are also less likely to report incidents of fraud out of embarrassment or shame. It is estimated that seniors are scammed out of more than $3 billion each year[5], with a median loss of $600 per victim over 60, and up to $1,600 per victim over 80.

The methods by which to scam seniors have become more prevalent with romance scams, impostor scams and sweepstakes and lottery scams topping the list. Account opening fraud is also a significant type of fraud for this demographic. BioCatch fraud data reveals that 40% of third-party fraud victims are people born before 1960.

40% of third-party fraud victims have a declared age over 60

78% increase in account holders under 21 that indicate signs of money mule activity

Generation Z

While elderly customers have typically been the primary target for financial crimes, the demographics have expanded significantly into younger generations. The global pandemic spurred what has become to be known as the Great Resignation, with millions of global workers quitting their jobs. Generation Z has led the charge with generous government stimulus payments and unemployment benefits prolonging job searches. Social media has also made it increasingly easy for mule herders to connect with young people. Many of the young people recruited into laundering schemes are less complicit, needing quick, easy cash, but not fully understanding the legality of what they're being asked to do.

Regulatory protection

Governing agencies are acutely aware of the new dangers of financial scams targeting vulnerable groups. As a result, they have recently increased regulatory and consumer action group pressure to protect vulnerable and elderly customers. For example, the FCA released new guidance in 2021 for vulnerable customers and aging populations in areas where physical bank branches are being closed and migrated to digital channels. The FDIC has also taken an interest in protecting vulnerable customers, especially the elderly, launching the Money Smart for Older Adults Program to raise awareness among seniors and their caregivers to prevent elder financial exploitation.

Key Takeaway

The financial industry is taking major steps in creating an environment where seniors and other vulnerable populations can transact in an environment free of fraud. With increased regulatory scrutiny across the globe, some financial institutions have already started to get ahead of the problem by forming internal groups dedicated to addressing vulnerable customers. Industry groups, such as The Knoble, have also been formed to identify best practices for detection and data sharing requirements within financial institutions to combat financial crimes such as elder scams. Technology that leverages machine learning and an understanding of human behavior will be a critical element in protecting vulnerable customer populations.

BioCatch

3 Mobile Malware on the Move

With the increased use of mobile devices, mobile internet access, and mobile apps, it should not come as a surprise that mobile malware is making a comeback. As banks, retailers and other consumer service providers look to meet their customers where they are, scammers have adapted their strategies as well. The use of multi-factor authentication on mobile devices has created gaps for technologically capable attackers to step in at key moments undetected and hijack the operating system or steal personal and financial information with the goal of committing fraud.

Remote access tools are detected in **1 out of every 24** mobile fraud cases

While mobile malware is not as prevalent as it was a few years ago, it is much more targeted and well-developed. FluBot and TeaBot were two of the most common families of financial malware targeting mobile users last year and are still prevalent in the wild. The malware is mainly spread to users via mockups of fake apps such as parcel delivery services and continues to largely be distributed throughout Europe and Australia.

Remote access capabilities are common in financial malware. Specifically, TeaBot leverages RAT capabilities that enable keylogging, interception of OTP codes and harvesting of other data contained on an infected device. The malware caters to many languages and the list of targeted applications is increasing at pace.

While a majority of mobile malware still targets Android devices, largely due to Google's open systems for development and distribution of apps, scammers have found new ways to circumvent Apple security measures to target iOS devices. For example, as iOS does not allow for remote control of a device, scammers have worked their way around this control with remote access-like tools, such as Zoom, AnyDesk, and TeamViewer. Scammers coerce users into using one of these tools and sharing their screens so that the scammer can more effectively coach them through a scam. BioCatch refers to this attack method as a Passive Remote Access scam and has discovered over 80% of iOS reported remote access cases contain this positive screen broadcast feature. This means that the passive remote access was being broadcast to multiple screens to better complete the scam process.

Key Takeaway

Mobile malware is just another method scammers are using to bypass legacy fraud controls and commit account takeover. Detecting malware on mobile devices has relied heavily on traditional anti-virus (AV) scanning technologies which looks for the name of the suspicious package and regularly monitors apps and their hashes for the malware. However, the technology itself has limitations as malware files change frequently, and financial institutions do not have control over the end user device so even if they were able to offer this service to customers, adoption would be sporadic at best. Financial institutions need to look beyond the device itself and consider behavior-based fraud controls for detecting mobile malware. As malware behaves in ways much different than the genuine user population, and these indicators are common in most malware families, behaviors indicative of malware can be uncovered in actions such as navigation paths, accelerometer data, and touch and swipe patterns.

BioCatch

4 Scammers Got Smarter. Authentication Methods Not So Much.

As scammers got smarter about their approach to committing fraud, financial institutions are still struggling to keep pace. Legacy fraud prevention methods still largely rely on passwords, device ID and SMS one-time passcodes which remain susceptible to scammer intervention. The replacement of traditional user authentication methods is highly unlikely due to their global deployment and acceptance by consumers. However, their limitations to detect social engineering, malware and other advanced scams must be acknowledged. As a result of the increase in scam-based fraud, financial institutions require solutions that can look beyond device, IP and network-based attributes and instead at the user themselves.

Regulators in the UK recognized the vulnerability of one-time passcodes and knowledge-based authentication early on for complying with the Payment Services Directive II (PSD2). In 2021, the UK Information Commissioner's Office embraced the use of behavioral biometrics technology as an adherence factor for strong customer authentication. In Singapore, a recent spate of smishing attacks that resulted in millions of dollars in losses caught the attention of financial regulators who took immediate action such as requiring financial institutions to remove links from all customer communications.

Higher consumer expectations, greater business risk

Consumers have developed greater expectations of protection from their banks and financial institutions including the expectation to be reimbursed for losses associated with fraud or scam activity. However, the risks associated with cybercrime are much greater than financial loss. Consumers are exponentially offended when they feel their financial data has not been sufficiently protected, and their complaints can very quickly lead to reputational damage and customer attrition.

Financial institutions have also taken great strides to improve customer experience and communications in recent years. Cybercrime directly impacts their ability to deliver the convenience and personalization customers have come to expect in digital channels, and the last thing they want to do is compromise these efforts by adding more friction or limiting how they communicate and market new products and services.

"Continuing to insist that customers jump through multiple hoops to prove themselves worthy of a business relationship ignores the reality that customers today have multiple options available. For many customers, convenience is a greater driver than security of their day-to-day decisions."

Gartner, Don't Treat Your Customer Like a Criminal, July 2021

Key Takeaway

Between the wide availability of stolen personal and financial information for sale in the black market and attack methods that leverage malware, remote access tools and social engineering, the weaknesses of traditional user authentication methods when taken on their own have been exposed. In addition, user experience and convenience are increasingly at the center of new fraud detection projects thus technology that can address a range of fraud use cases while introducing a frictionless journey for a majority of good users will drive future authentication strategies.

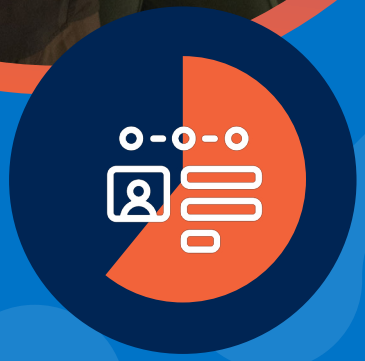
BioCatch

Financial Protection That's Smarter Than Scammers

Financial fraud detection has certainly gotten more advanced in recent years, but lately it feels like scammers remain one step ahead. Rather than continuing to be reactive to cybercrime attacks, it's time for the tables to turn and for financial institutions to proactively dictate the future of protection for their customers and themselves.

The only way to do that is to stay on top of what's going on in the industry and to fully embrace the strategies, technologies, and solutions that will have the greatest impact in future-proofing customer protection. BioCatch behavioral biometrics is currently delivering extraordinary results for organizations, including 25 of the world's Top 100 financial institutions, and exposing the most advanced fraud attacks.

Behavioral biometrics works passively in the background of a user web or mobile session to monitor thousands of parameters such as the way a person holds the phone, the pressure they use when they type, how they scroll or toggle between fields and how they navigate an application or form. As each person's interactions with a device or application are unique, behavioral biometrics can differentiate between the activities of a genuine user and the activities of a scammer.



64% of confirmed cases of account opening fraud indicated a lack of familiarity with personal data

Use Cases for Banking and Payments

BioCatch

The Risk: Account Opening Fraud

The Solution: *Gaps in existing solutions are leaving blind spots in the account opening process. For example, in cases where a customer has no prior relationship with the organization, most legacy fraud prevention controls do not have the historical data to identify a good or bad applicant. Behavioral biometrics does not require an existing relationship and detects high-risk applications by looking for patterns such as high application fluency, low data familiarity and age analysis.*

The Risk: Account Takeover

The Solution: *Account takeover comes in many forms capable of bypassing most existing authentication and fraud prevention controls. Behavioral biometrics looks for anomalies in digital interactions that can indicate both human and non-human attacks such as malware, bots, remote access tools and manual account takeover methods.*

The Risk: Mule Account Detection

The Solution: *Identifying mule accounts is challenging because in some cases, it involves a genuine account and a genuine account holder's actions. Behaviors associated with a mule account will vary depending on the level of complicity and the stage of the digital banking journey. BioCatch has developed a unique approach to uncover mule activity by identifying five mule personas. each which exhibit different patterns of behavior and are meant to align with the kinds of mules typically observed to operate within financial institutions. Behavioral biometrics can be used to distinguish between behaviors that are far more common in mules than in users who are opening legitimate accounts or accessing their own accounts for legitimate reasons.*

The Risk: Social Engineering Scams

The Solution: *Many social engineering scams go undetected because it is the actual genuine user making the payment at the direction of a scammer. The ability to detect subtle changes in digital behavior to suggest a victim may be acting under coercion or being guided through a session is key to stopping real-time social engineering scams. Behavioral biometrics looks at factors such as session length, typing segmentation, hesitation, and device displacement to determine if a user's intention is legitimate or suggestive that a social engineering scam may be at play.*

ABOUT BIOCATCH

BioCatch is the leader in Behavioral Biometrics, which analyzes an online user's physical and cognitive behavior to protect users 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 of use 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 experience analyzing data, more than 60 patents and unparalleled anti-fraud expertise, BioCatch continues to innovate to solve tomorrow's problems. For more information, visit www.biocatch.com.

1 Chase Bank
2 Cornerstone Advisors
3 US Federal Communications Commission
4 ZDNet, "We spent 5 hours a day on our mobile devices in 2021," January 2022
5 Consumer Affairs

© 2022 BioCatch. This content is a copyright of BioCatch. All rights reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following:

- You may print or download to a local hard disk extracts for your personal and non-commercial use only.
- You may copy the content to individual third parties for their personal use, but only if you acknowledge the document and BioCatch as the source of the material.
- You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system without our express written permission.

BioCatch