WHITE PAPER

CONSUMER-CENTRIC DIGITAL AUTHENTICATION

How Financial Institutions are Reducing Friction and False Positives in the Digital Channel

neustar®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Are your authentication methods eroding customer loyalty and satisfaction? That's a critical question today's banks and credit unions must ask themselves as a growing number of people migrate to digital first as a way to interact with financial institutions.

While conducting business via digital channels drives down acquisition costs, it's a largely anonymous interaction that creates a critical vulnerability for fraud. Authenticating the customer behind the device without adding undue friction can be a challenging balancing act.

In today's environment, financial institutions must deliver convenient, frictionless and secure services, while embracing a multilayered strategy that focuses on securing the identity of their digital users and ensuring the integrity of the devices their customers use.

To help financial institutions navigate this delicate balancing act, this white paper outlines three best practices to mitigate risk while delivering legitimate customers the frictionless experience they deserve.

1 UNDERSTAND THE THREATS

In today's increasingly connected world, consumers have grown accustomed to conducting business online and their financial institutions are no exception. In fact, a 2019 survey conducted on behalf of the American Bankers Association revealed that nearly three-quarters of Americans most often access their bank accounts via online and mobile platforms.[1]

Going forward, one can expect this shift to continue as the number of digitally native, younger generations (millennials and Gen Z) ascend in the workforce and increasingly secure financial products like checking accounts, credit cards and loans. By 2028, these younger generations are projected to make up 58 percent of the workforce.[2]

Unfortunately, sophisticated fraudsters are lurking in the shadows waiting to steal from consumers and businesses alike. Painting a disturbing picture of this reality, the Federal Trade Commission, in 2019, processed 1.7 million fraud reports, totaling $1.9 billion in losses. Among the top 10 report categories: Identity theft, telephone and mobile services, and banks and lenders.[3]

Financial institutions are justifiably fearful of the threats facing online and mobile platforms, not to mention the attacks that threaten channels like call centers. However, as the saying goes, "Knowledge is power." Understanding the threats can better position your financial institution in the fight against fraud. Here's a look at some common threats seen today:

Spoofing

The word "spoof" is defined as deceive or hoax. When applied to technology, spoofing is when hackers attempt to use a computer or device to impersonate a legitimate source. Successful attacks can lead to data breaches, infected computer systems and networks, and/or loss of revenue.

There are various types of spoofing that hackers have in their arsenal, including phone spoofing. Thanks to the accessibility of spoofing tools and the ability to purchase personally identifying information (PII) on the dark web, fraudsters can disguise themselves to make call center agents believe the call is coming from the phone of a genuine customer.

This once popular criminal tactic, however, has taken a back seat to a growing account takeover threat: call virtualization.

Virtualized Calls

Virtualized calls (e.g., web-based calling services like Skype; Google Project Fi, which is a phone carrier operated by Google that, in the U.S., gives you data service on T-Mobile, Sprint and U.S. Cellular mobile networks; or a business-grade phone system) today pose the greatest account takeover threat.

[1] American Bankers Association, 5 Nov. 2019, https://www.aba.com/about-us/press-room/press-releases/survey-bank-customers-preference-for-digital-channels-continues-to-grow
[2] Upwork, 5 Mar. 2019, https://www.upwork.com/press/2019/03/05/third-annual-future-workforce-report/
[3] Consumer Sentinel Network Data Book 2019. Federal Trade Commission, 2020, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf
[4] 2019 State of Call Center Authentication. Neustar, 2019, https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/risk/neustar-2019-state-of-call-center-authentication-survey.pdf?_ga=2.233951902.1419243714.1584268400-1880278485.1582567561

Virtualized calls are inherently anonymous and much more difficult to identify compared with a spoofed call given that the signaling data and call certificates are correct. This has made virtualized calls the threat vector of choice for many of today's fraudsters.[4]

SIM swapping

For today's customers, most of whom own a mobile phone, there are several distressing scenarios that could play out should their SIM card fall into the wrong hands.

A fraudster might steal a phone to swap out the SIM card and place it into their own phone. Alternately, they may call a customer's cell phone service provider and claim the phone was lost or damaged. They then ask the provider to activate a new SIM card connected to a customer's phone number on a new phone. Unfortunately, it's a phone the fraudster owns. Either way, the fraudster now has control of the customer's cell phone number.

Once a fraudster has control of a customer's cell phone, they can receive any codes or password resets sent to that phone via call or text for any of the customer's accounts. This means they could log into accounts — like bank accounts — that use text messages as a form of multi-factor authentication (MFA).[5]

Unfortunately, fraudsters are extremely nimble and can rapidly shift tactics to exploit vulnerabilities. Therefore, it is essential that financial institutions stay abreast of market trends, collaborate to combat fraud rings, and partner with a leading identity resolution provider who can accurately diagnosis the threat and help develop an effective fraud-prevention strategy.

Understanding the threats can better position your financial institution in the fight against fraud.

[4] 2019 State of Call Center Authentication. Neustar, 2019, https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/risk/neustar-2019-state-of-call-center-authentication-survey.pdf?_ga=2.233951902.1419243714.1584268400-1880278485.1582567561

[5] Puig , Alvaro. SIM Swap Scams: How to Protect Yourself. Federal Trade Commission, 23 Oct. 2019, www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself

2 DELIVER A FRICTIONLESS EXPERIENCE

Your customers don't want to be interrogated. That's why an essential part of the customer experience is ensuring that your authentication methods are as frictionless as possible. Failure to do so places your financial institution at risk of losing valuable clientele.

Underscoring this point, a Neustar/Forrester Consulting survey of 204 respondents with decision-making responsibility for fraud management, authentication, and customer experience (CX) found that many struggle to maintain high-quality customer experience throughout authentication. More specifically, 62 percent of respondents said they're challenged by low customer satisfaction and/or an end-user experience process that is too complicated, resulting in poor customer experience.[6]

In today's digital environment, authenticating customers behind the device to reduce false positives and separate legitimate customers from fraudsters — without undue friction — is no doubt a delicate balancing act. And it's a challenge that has not gone unnoticed among financial institutions.

According to a 2018 Neustar/American Banker survey of more than 500 executives at banks, credit unions and nonbank lenders, roughly 62 percent of respondents said reducing customer inconvenience is a high priority when thinking about bolstering fraud protection. Furthermore, only 22 percent of executives expressed high confidence that their fraud prevention routines provided them visibility into the device linked to an identity and the reputation of the device. And just 19 percent were highly confident that their anti-fraud system could connect customers' online identity to authoritative offline identity information.[7]

"They want to be able to appropriately apply friction in the right places but not have false positive rates go through the roof, negative customer experiences, and so forth. So that balancing act between the two becomes the rub for my banking clients," said Adam Russell, Vice President – Financial Services and Healthcare at Neustar.[8]

Much of the concern resides in the fact that many financial institutions are still relying heavily on MFA (which is easily defeated by identity thieves who

[6] Mitigate Fraud And Consumer Friction With Integrated IDV. Neustar and Forrester Consulting, 2019, https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/fraud/neustar-mitigate-fraud-and-consumer-friction-with-integrated-idv.pdf?_ga=2.196121132.1419243714.1584268400-1880278485.1582567561
[7] Neustar, 27 Sept. 2018, https://www.home.neustar/about-us/news-room/press-releases/2018/AmericanBankerFraud
[8] Russell, Adam, phone interview, March 3, 2020

hijack customer phone numbers via SIM swapping) and knowledge-based authentication (KBA).

KBA — which seeks to prove the identity of a caller through knowledge of personal information (e.g., mother's maiden name, account number, pet's name, etc.) — is not only costly and time-intensive, but customers loathe it. And for good reason. Customers can find it extremely frustrating and cumbersome to try and keep secret questions straight.

"Each of us are having to prove that we're not the fraudster versus the other way around. That is the friction or the dissatisfier for the consumers," Russell said. [9]

Plus, KBA fails to stop fraud. Thanks to the rise in data breaches, criminals can purchase PII (e.g., Social Security numbers, bank account numbers and driver's license numbers, etc.) on the dark web, or even collect the right answers using social media.

"Knowledge-based authentication really is no longer an effective method for multi-factor authentication, which everybody should be doing and most people are. Most of our clients know that [KBA] is not effective but very few have moved fully away from it. ... It's a known issue and it's something that people really do need to move away from. The less interaction, the more passive the data the better it is going to be, and the more unspoofable it is the better that is going to be," Russell said.[10]

In today's digital environment, authenticating customers behind the device to reduce false positives and separate legitimate customers from fraudsters — without undue friction — is no doubt a delicate balancing act.

[9,10] Russell, Adam, phone interview, March 3, 2020

3 LEVERAGE IDENTITY, DEVICE ATTRIBUTES

How can financial institutions effectively provide legitimate customers the frictionless digital experience they deserve without exposing the business to fraud? By taking a multilayered approach that involves bridging the gap between device identity and physical identity.

What does this mean? Linking multiple data points from multiple sources, like combining a Social Security number with an IP address or cookie data, to reduce false positives and quickly separate legitimate consumers from fraudsters.

Has this cell phone recently been activated? Is it a burner phone? Has the name-to-phone relationship on the mobile network recently undergone changes? Is it from a reputable phone company? Has it recently been SIM swapped? The answers to such questions arm financial institutions with the intelligence needed to determine whether to proceed with a transaction or flag it for additional verification.

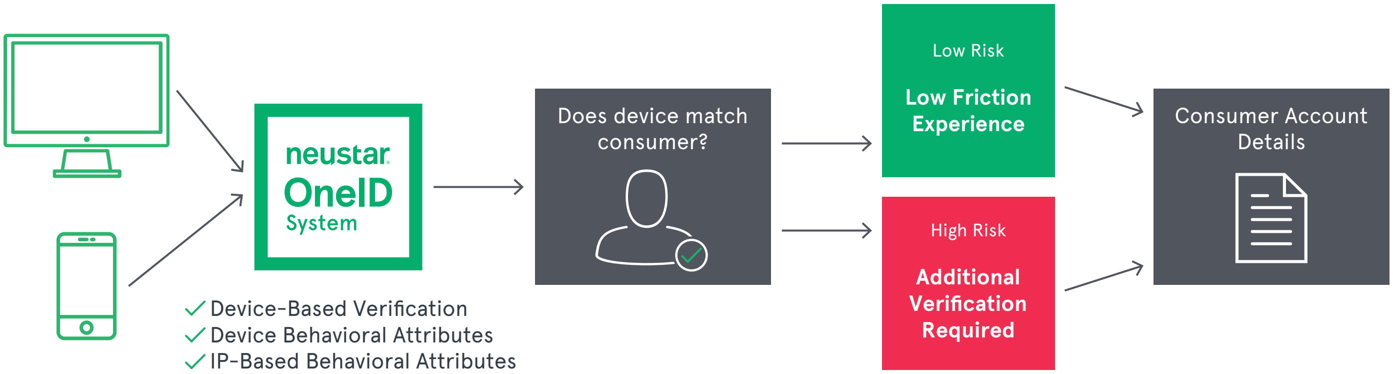
“These additional details are really useful in understanding how much trust you can bestow upon that relationship between a phone and other aspects of a physical identity,” said Sam Jackson, Director of Product Management, Fraud Detection and Prevention at Neustar.[11]

Leveraging identity and device attributes to quickly identify and let through the legitimate low-risk customers also leads to greater customer satisfaction.

Consider, for instance, a solution like Neustar’s Digital Identity Risk. Using a host of digital elements — including IP, browsing, phone activity, and connections to digital footprints to person or household — Neustar can help financial institutions reduce false positives by corroborating the digital information against authoritative offline consumer data.

[11] Jackson, Sam, phone interview, March 10, 2020

AUTHENTICATING DIGITAL CHANNELS TO IMPROVE CUSTOMER EXPERIENCE


neustar
OneID
System
✓ Device-Based Verification
✓ Device Behavioral Attributes
✓ IP-Based Behavioral Attributes
Does device match consumer?
Low Risk
Low Friction Experience
High Risk
Additional Verification Required
Consumer Account Details

How it works:

1. A customer navigates a financial institution's website using their phone, tablet, or laptop.
2. Neustar automatically compares the customer's submitted PII to device-based observations, corroborating device information with offline identity.
3. Neustar provides the financial institution with the intelligence needed to either proceed with the transaction or flag it for additional verification.

This is just one example of the products available in Neustar's broad portfolio of risk, security, marketing, communications, and customer intelligence solutions.

It should also be noted that, with more than 90 percent of caller ID data and updated device data on more than 500 million phones through relationships with mobile network operators, Neustar has access to a wide variety of device data. This includes if a SIM card is tied to a customer's phone or if a phone number has been forwarded. Neustar can use that data, along with offline and online data, to help ensure that financial institutions can confidently authenticate customers.[12]

"We're able to basically identify whether or not an individual, whose provided information like name, address and phone number, is historically associated with a particular device or IP address about 65 percent of the time. We also have a lot of different signals around anomalies, bot networks, proxies, things that could signal some level of elevated risk," said Jackson. "By bringing all of these probabilistic signals together, in conjunction with machine learning, we can actually do the identity proofing process in a way in which almost no fraud gets through, and there's also no additional friction for the end user."[13]

[12] McKay, Bob. Neustar, 20 Nov. 2018, https://www.home.neustar/blog/reducing-friction-fraud-false-positives
[13] Jackson, Sam, phone interview, March 10, 2020

CONCLUSION

In today's digital-first environment, customers don't just desire a frictionless experience — they expect it. Unfortunately, rigorous identification standards too often result in undue friction. For financial institutions, this could result in lower customer satisfaction and, ultimately, a loss of revenue.

By better understanding the threats, eliminating undue friction, and leveraging solutions to help bridge the gap between device identity and physical identity, financial institutions can break the mold.

The good news: You don't have to go it alone. Turn to a leading identity resolution provider, like Neustar, today to set your business on the path to improved operational efficiency, greater customer loyalty, and reduced risk.

LEARN MORE

For more information, visit **www.risk.neustar**, contact us at **1-855-898-0036 x4**, or email **risk@team.neustar**.

ABOUT NEUSTAR

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, Security and Registry that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections here: **www.home.neustar.**