WHITE PAPER

STOP FRAUD WITH INBOUND CALL AUTHENTICATION

neustar®
A TransUnion® Company

TABLE OF CONTENTS

HI, IT'S ME, BRIAN

Brian's a long-time customer of your community bank and has a wide-range of deposit and lending products, including checking, savings, mortgage, and investment accounts. When Brian walks into his local branch, the branch employees greet him by name and ask about his family.

Brian has a positive experience every time he sets foot in a branch.

Brian's landline phone number has been in your CRM for ages. But the CRM hasn't been updated to include Brian's mobile number. When Brian calls your call center on his cell phone, he's presented with several knowledge-based authentication (KBA) questions and instructed to enter a one-time passcode (OTM) sent through an SMS text message.

Turns out it's just Brian and not a criminal after all.

Brian's experience? Not so great. Brian wonders if your bank really knows—or values—him as a customer at all. And he's frustrated that he had to jump through hoops to prove who he was before even talking to an agent.

Opening the flood gates and letting anyone access your call center without challenging their identity just invites criminals to take over customer accounts. But what if you could let your customers like Brian without any fuss yet stop criminals in their tracks? Rather than interrogating everyone, why not stratify the risk that the call is fraudulent and take additional steps to authenticate only those calls that are riskier?

Catch the bad guys—but let the good guys through.

This research report describes how you can use inbound call authentication to provide the experience customers expect without exposing your financial institution to sophisticated fraudsters. We'll take a look at why call centers are vulnerable to fraud, common criminal tactics, and provide best practices for balancing fraud with friction so Brian, and customers like him, have a great experience no matter which channel they choose.

CATCH THE BAD GUYS—BUT LET THE GOOD GUYS THROUGH.

WHY FRAUDSTERS LOVE YOUR CALL CENTER

The death of the call center in favor of digital channels is a myth. Consumers still rely on the phone when they have complex issues or need a problem solved.

Know who else relies on your call center? Fraudsters. As opportunists, they gravitate to the most vulnerable entry point at your financial institution and today that entry point is your call center. The call center has become a lucrative channel for fraudsters to get access to or take over a legitimate customer's account or even create a brand new customer.

Call center fraud is up a dramatic 350% between 2013 and 2019 and fraud losses are up 36% in 2020 compared to 2018.[1]

The pandemic was a boom time for fraudsters. As branches closed, more customers relied on the call center. Call centers struggled to balance increased call volume and shrinking workforces. Agents struggled with outdated or obsolete technologies such as automatic number identification (ANI) without spoofing detection, KBA, and OTP.

As the volume of legitimate calls increased, so did the number of fraudulent calls.

Increased fraud, less operational efficiency, and more frustrated customers who are spending the first critical moments of their call being interrogated instead of having their issue resolved.

It's a battle of fraud versus friction.

No wonder 64% of call center leaders are concerned or very concerned about call center fraud.[2] At the same time, 65% of financial services fraud executives say that customer experience has increased in importance over the last two years.[3]

> **The engagement models of service have changed, yet security in contact centers is, for the most part, stuck in the 1990s.[4]**
>
> **– Krista Tedder, Director of Payments, Javelin Strategy & Research**

> **Even as more transactions are done online, the phone is still relevant.**
>
> **– Fernando Paredes, Senior Product Management Analyst, Neustar, a TransUnion company**

[1] https://aite-novarica.com/report/improved-customer-experience-reduced-fraud-and-cost-contact-center-solutions
[2] https://www.home.neustar/resources/whitepapers/state-of-call-center-authentication
[3] https://aite-novarica.com/report/us-identity-theft-stark-reality
[4] https://www.javelinstrategy.com/research/securing-contact-center

LESS FRAUD, LESS FRICTION: A BETTER WAY TO AUTHENTICATE IDENTITIES

Here’s a typical scenario: a fraudster, using a virtualized call platform, contacts the call center. The fraudster answers the KBA questions or intercepts the OTP sent to the victim’s phone. The fraudster then adds fake contact information to hide activity and drains the account—before the victim or the financial institution notice. The account take over is complete.

While other forms of fraud, such as account opening fraud, can happen in the call center, the predominate type of criminal activity is account takeover fraud. However, the call center is often the gateway for account opening fraud in digital channels.

The call center gives fraudsters lots of ways to accomplish fraud. For the price of a Venti Latte, a fraudster can buy a Social Security number on the dark web.[5] They can buy a child’s SSN, slowly and methodically build a credit profile, and then commit fraud.

As consumers, we’ve collectively gotten more comfortable giving out personal information or posting our birth date or dog’s name on social media. In addition, there’s a plethora of personal data available on the dark web from years of data breaches.

With easy to get personally identifiable information (PII) on the dark web and the relative ease of getting KBA and password information from social engineering, fraudsters have little difficulty in collecting ill-gotten answers to challenge questions.

Common call center authentication methods such KBA, voice recognition, and biometrics fail to address the multiple ways that fraudsters attack. In addition, traditional methods of fraud detection and prevention only make existing operational challenges worse, with stressed systems, overworked agents, longer customer wait times, longer calls, and poor customer experiences.

LET’S LOOK AT JUST FOUR OF THE REASONS FRAUDSTERS LOVE CALL CENTERS.

[5] https://atlasvpn.com/blog/your-ssn-costs-less-than-a-starbucks-coffee-on-the-dark-web

REASON 1

SPOOFING AND VIRTUAL CALLS ARE PRETTY SIMPLE TO MASTER

Fraudsters are experts at spoofing and virtual calls. In spoofing, fraudsters trick the caller ID into displaying another number. Fraudsters calling from thousands of miles away look like they are calling from a local area code or worse, look like a legitimate customer. Often spoofers use automated dialing to make thousands of calls quickly.

Once fraudsters get through to your call center, they do a very good job of manipulating call center agents into divulging personal customer details or using your IVR to do pre-fraud reconnaissance.

Virtual calls are calls placed without using a mobile phone or landline. Because the phone number is not tied to the physical device, the caller can pick a phone number in the U.S. and call from anywhere in the world. It's difficult to identify or track a caller.

Virtual call fraud is on the rise. Seven out of ten (70%) bankers saw "somewhat" or "much more" threat activity in the call center coming from virtualized call services.[6]

The challenge for financial institutions is that virtual calls are legitimate calls, and plenty of customers use services like Google Voice and Skype.

But there's plenty of less well-known virtual call platforms for fraudsters to pick from. Everyone is familiar with Zoom and Cisco WebEx, but have you ever heard of Ping or TextNow? Fraudsters, drawn to the innate ability of these platforms to be anonymous, have.

These platforms are also easy to access—all it takes to sign up is an email address to generate random phone numbers that are anonymous. With bots, fraudsters can make thousands of bogus calls quickly.

Virtual calls are great for lazy fraudsters who don't even have to engineer a spoofed call that can evade spoof-detection tools. They can reach an agent from a legitimate number and again, are very good at socially engineering the agent into granting control over a customer's account.

[6] https://www.home.neustar/resources/whitepapers/state-of-call-center-authentication

REASON 2

THE CALL CENTER IS A GREAT STARTING POINT

The call center may not be the end game, but it's a great jumping off point for cross-channel fraud. Maybe the fraudster successfully takes over a customer's account, but they don't stop there. Once they take over an account in the call center, they change the online password or phone number associated with that account so they can then completely take over the account in all channels.

Financial institutions typically write off fraud in the delivery channel in which it occurs. Account opening fraud is reported as happening in the digital channel when really the fraudster assembled all the necessary pieces through repeated calls into the call center.

As a result, financial institutions don't have an accurate picture of just how much fraud their call center enables. They may think their call center is secure when it's simply used as a ways to a means.

REASON 3

THE IVR IS THE NEW BRANCH

Criminals don't just walk into a branch with a gun and a note saying, "Give me all your money" without first doing some research. They case the joint. Criminals take the same approach to your call center. Only they case the IVR.

And it's so stealth that financial institutions don't even know it's happening.

In over 60% of fraud cases, a contact center IVR was used for pre-crime research.[7]

Just as your customers enjoy the self-service options of your IVR, fraudsters do as well. Not having to actively engage with an agent means fraudsters have plenty of time to capture the information they need to impersonate a legitimate consumer. Fraudsters use the IVR to mine data, test accounts, reset PINs, and order additional cards on an account.

Often, they use bots to streamline their information gathering using automated dialing and virtualized calls. By calling sequential phone numbers and seeing which numbers get different treatments—the IVR will treat a customer who calls into the call enter frequently differently than a first-time caller—a bot quickly maps the IVR tree and completes reconnaissance quickly.

By the time fraudsters contact an agent, they've cased the IVR and gotten everything they need to take over the account.

But many financial institutions don't monitor for fraud in the IVRs or understand that fraudsters take advantage of significant data leakage. One-third of financial institutions (33%) don't know whether fraud is occurring in their IVRs.[8]

Fraudsters play the long game. Rarely in a rush, they bide their time and will make multiple calls until they get the information they need to impersonate a legitimate customer. Each call moves them one step closer to their goal.

[7] https://aite-novarica.com/report/beating-bad-guys-safe-and-secure-voice-interactions-ivr
[8] https://aite-novarica.com/report/beating-bad-guys-safe-and-secure-voice-interactions-ivr

REASON 4

HUMANS ARE VULNERABLE

The same attributes that make for a good call center agent—a desire to help others, empathy, and problem-solving skills—make these employees vulnerable to fraudsters. Fraudsters play on agents' emotions and use them to their advantage. For example, fraudsters will use background noise such as a recording of a crying baby to illicit compassion and influence the agent to rush through the authentication process.

Keep in mind that 85% of fraud involves a human element.[9]

> **Contact centers are generally not where security professionals reside, yet it is the front door for criminal activity.**[10]
>
> **– Krista Tedder, Director of Payments, Javelin Research**[11]

> **Account takeover fraud is so commonly enabled through the contact center that it should be renamed the cross-channel-fraud-enablement channel.**[12]
>
> **– Shirley Inscoe, Senior Analyst, Aite Group**

[9] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/
[10] https://www.javelinstrategy.com/research/securing-contact-center
[11] https://www.javelinstrategy.com/coverage-area/securing-contact-center
[12] https://aite-novarica.com/report/improved-customer-experience-reduced-fraud-and-cost-contact-center-solutions

THE BENEFITS OF INBOUND CALL AUTHENTICATION

Customers like Brian don't like being interrogated when they contact your call center. Agents don't like interrogating customers. Your financial institution doesn't want to interrogate its customers.

But no one wants to let criminals steal money or identities or accounts.

It's an ongoing challenge. More than two-thirds (67%) of contact center leaders are "somewhat" or "not at all" succeeding at authentication and fraud prevention.[13]

It is possible to balance the desire to provide customers with a friction-free experience while still detecting potential fraud by using inbound call authentication that stratifies the risk that a call is fraudulent.

Inbound call authentication:

- *Provides a Better Customer Experience.* Forcing agents to spend their time authenticating instead of servicing customers not only increases call times but it degrades the customer experience. Customers now have to navigate an obstacle course and endure repetitive questioning to get authenticated. Instead of being greeted by "how are you?", customers hear, "who are you?" Those financial institutions that provide less friction see NPS scores improve 15% to 20%.[14]

- *Enables Agents to Do Their Jobs Effectively.* Customer service agents can spend less time verifying customers' identities and more time helping customers and responding to inquiries.

- *Improves Customer Retention:* Customers want a great experience but are unwilling to sacrifice security to get. And they let you know if you break that trust: 40% of victims of account takeover move one or more accounts to another financial institution.[15]

- *Reduces Operational Costs:* Neustar found that eliminating just 20 to 70 seconds of KBA challenge questions reduces costs by 45 to 90 cents per call. And an easier authentication process coupled with richer self-service options saves an average of $5.50 per call by reducing "pound outs" to agents.

[13] https://www.customercontactweekdigital.com/customer-experience/whitepapers/special-report-establishing-trust-in-inbound-callers
[14] https://www.cdn.neustar/resources/whitepapers/risk/forrester-impact-of-neustar-fraud-and-authentication-solution.pdf
[15] https://aite-novarica.com/report/us-identity-theft-stark-reality

This also enables highly-paid employees in the fraud department to focus on the 3% to 5% of non-authenticated callers.

- *Improves Onboarding:* Two-thirds (63%) of customers will abandon the onboarding process if the process is too complicated or takes too much time. And when customers use a mobile device to sign-up for a new account, the abandonment rate rises to 72%.[16]

- *Provides a Consistent Brand Experience:* Financial institutions are focused on customer experience but neglect to integrate the phone into the overall experience. You may offer a great online account opening process but if the experience deteriorates once the customer picks up the phone, tarnishing your brand suffers and you've lost an opportunity to cultivate brand loyalty.

> **It's about the customer experience and reducing false positives in so customers are not treated like criminals.**
>
> **– Adam Russell, Vice President, Identity & Risk Solutions, Neustar, a TransUnion company**

> **We interrogate our best customers.**
>
> **–Senior Vice President, Top 10 Bank**

From Call Center to Account Opening Fraud

The most common type of fraud perpetuated in the call center is account takeover fraud. But criminals take advantage of vulnerabilities to also open accounts. Here are just a few ways criminals are committing account opening fraud.

Creating Synthetic Identities: Criminals no longer rely on stealing actual identities to scam financial institutions. Instead, they create entirely fake personas by piecing together bits of personal information from legitimate people. Because there is no actual victim to report a stolen identity, accounts opened by synthetic identities often go undetected.

Committing First-Party Fraud: First-party fraud involves accounts opened by a legitimate person who has malicious intent. This person may be the actual fraudster or someone the criminal has manipulated into acting as a front for the fraud. The fraudster then uses the accounts to either launder money or commit future fraud.

Using Stolen Credentials: Criminals use stolen credentials and personal data to open accounts in the names of individuals without their knowledge. The information used to open these accounts often comes from data breaches and other data compromises. The fraudsters then add to the data through social engineering techniques such as research on social media sites and calls to call centers to extract personal information.

[16] https://www.signicat.com/blog/the-battle-to-onboard-2020-the-impact-of-covid-19-and-beyond

CAN I TRUST YOU?

All calls aren't created equal.

A virtual call is riskier than a call from a mobile device since it's impossible to link the virtual call phone number to the device. A first time call poses more risk than a call from a long-established customer. A call made from a burner phone has a higher risk profile than a call made from a landline. A call from a phone with a brand new SIM card is more likely to be fraudulent than a call from a mobile device that has used the same SIM card for three years.

So why treat all calls the same?

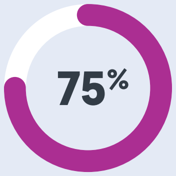
Instead shrink the pool of callers that merit closer scrutiny based on data gathered about the carrier, the type of device, and the caller who owns the device. When the ANI matches the customer phone number on file, financial institutions can be confident that a legitimate customer is calling.

In essence, the phone becomes an ownership-based authentication token.

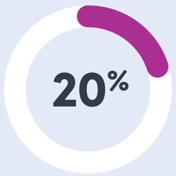
There are other data points that can stratify the risk that a call is fraudulent. While fraudsters can use spoofing to impersonate legitimate customers' telephone numbers, what they can't spoof is the type of phone, call history, call routing, cookies, or how long the owner has had the phone. A fraudster can't buy a Trak phone yesterday at Walmart and pretend it's an iPhone that was activated two years ago.

What about the 25% of calls that come into the call center from devices that are not physical or unique, such as PBX switches, burner phones, prepaid phones, public phones or phones with a recently swapped SIM card?

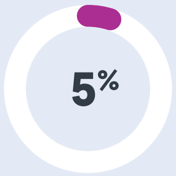
Treat Each Call by Its Trustworthiness



Highest trust: Using real-time deterministic call and device inspection, Neustar finds that these calls are legitimate, and they are routed into the fastest flow with the most self-service options.



Live inspection of the calling device isn't possible, so Neustar leverages historical results from billions of calls plus additional data about call, carriers, and network routing to assign a stratified trust rating. These callers must go through a simple authentication challenge.



Non-authenticated calls are sent for closer scrutiny to the fraud department or for authentication escalation.

[17] https://www.home.neustar/about-us/news-room/press-releases/2020/neustar-releases-2020-state-of-call-center-authentication-report

Yes, customers switch carriers and change SIM cards. While a ported or forwarded telephone number may be legitimate, a change could indicate fraud. The more recent the change, the riskier the call.

Another tool to evaluate the risk level is STIR/SHAKEN standards that use certificates to digitally sign phone calls and document call authenticity. Since June 30, 2021, telephone carriers must self-certify calls originating from their networks and assign each call an attestation rating of A, B or C.

While not a replacement for inbound caller authentication solutions, STIR/SHAKEN provides signal information that can help financial institutions identify fraudulent calls. Unfortunately, 90% of financial institutions are not prepared to take advantage of the STIR/SHAKEN framework.[17]

Establishing how much to trust a call before the caller reaches your IVR or an agent requires analyzing many fraud vectors. By adding in consumer identity data such as Social Security number and physiological or behavioral identifiers such as fingerprint or retinal scans and voice and intonation recognition, you can confidently stratify the results by trust level. Only those customers with a lower trust level—defined by the financial institution—receive additional scrutiny such as stepped up authentication or fraud department intervention.

Those customers with a high trust level experience less friction, receive few, if any, KBA questions and are even provided with more self-serve options within the IVR. Neustar has found that applying a trust level to calls reduces average handling time by 20% and IVR to agent transfers by 10%.

High trust in authenticated callers also reduces the need for KBA questions by up to 80%.

> **Judging the risk of an incoming call before it is answered has many benefits. By authenticating a caller pre-answer, it increases IVR containment and enables more services to be offered via that channel. When calls are transferred to an agent, the agent knows the call has been screened and can great the customer by name and take care of the customers' needs. The time spend asking KBA questions to interrogate customers is reduced significantly, shortening calls and improving the customer experience.**[18]
>
> **– Shirley Inscoe, Senior Analyst, Aite Group**

> **Once you put solutions in place to detect spoofing, the criminals don't go away. They just switch to another attack vector. The goal for financial institutions should be to stop all attacks, not just a particular type of attack.**
>
> **– Lance Hood, Senior Director, Authentication Solutions, Neustar, a TransUnion company**

[18] https://aite-novarica.com/report/improved-customer-experience-reduced-fraud-and-cost-contact-center-solutions

THE FUTURE OF IDENTITY AUTHENTICATION: STOP FRAUDSTERS BEFORE THEY ATTACK

Based on past experience, it's clear that fraudsters are always trying to be one step ahead of their financial institution targets. Financial institutions improved their ability to identify a spoofed call, fraudsters began using virtual call platforms. You need to prepare for every possible scenario they will face in the future.

There's no magic bullet to fraud detection and prevention. Instead, the future for financial institutions must include a layered approach to identity authentication such as device-based authentication coupled with biometrics. What is clear is that financial institutions will rely less on KBA and instead implement stronger authentications. The FFIEC even recently published guidance urging financial institutions to move away from KBA.

Fraud detection and prevention is a team sport against a common opponent. It's only by working in tandem with the other "good guys" that financial institutions can become more proactive rather than reactive to criminal activity. This includes taking a consortium approach to sharing information with other financial institutions as well as partnering and collaborating with vendors.

The objective is to shorten the time between when fraudsters attempt an attack and the attack occurs or is detected. Today, fraudsters have a long window of opportunity to commit crime. By collaborating and sharing information such as call outcomes and failed authentication results, Neustar and its financial institution clients can detect new patterns and clusters of attacks. Adapting in real time to emerging threats continually improves detection rates and reduces false positives.

TransUnion's acquisition of Neustar helps financial institutions take this holistic approach to fraud. Rather than forcing financial institutions to work with many vendors in a fragmented approach to fraud, Neustar is bringing different fraud solutions together into a single risk solution platform. Neustar separates trusted from risky callers, creating the most powerful and accurate fraud-fighting resource, while also providing a feedback loop to mitigate future false positives and negatives.

Let's give the Brian's of the world the call center experience they expect and deserve, and keep the fraudsters out.

When financial institutions don't collaborate, fraudsters win.

– Lance Hood, Senior Director, Authentication Solutions, Neustar, a TransUnion company

ABOUT TRANSUNION (NYSE: TRU)

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing an actionable picture of each person so they can be reliably represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good.®

A leading presence in more than 30 countries across five continents, TransUnion provides solutions that help create economic opportunity, great experiences, and personal empowerment for hundreds of millions of people.

http://www.transunion.com

ABOUT NEUSTAR

Neustar, a TransUnion company, is a leader in identity resolution providing the data and technology that enable trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in marketing, risk and communications that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Learn how your company can benefit from the power of trusted connections.

https://www.home.neustar