neustar
A TransUnion® Company

Four Challenges to Phone Channel Authentication

And how to overcome them for good.

Table of Contents

Executive Summary

As if there weren't enough complexity in identifying and authenticating callers, four challenges threaten to introduce more chaos into the phone channel. Call spoofing tools abound. Call virtualization services, the greater threat, offer criminals legitimacy and anonymity. Meanwhile, callers change contact information regularly, without giving you notice, and then expect to be recognized immediately. Lastly, possible solutions have to provide complete coverage of the network. In all, these challenges undermine the use of phones and their numbers as a way of identifying and authenticating callers.

Two types of technologies promise to bring back trust to phone numbers. One approach inspects phones and calls within the carrier network. The other analyzes carrier-provided header data to estimate call legitimacy. This document compares the merits of each approach in addressing modern call centers' needs.

How your call center became a target

Thirty years ago, identifying callers was simple, fast and accurate. When a call connected to a call center the caller's correct phone number was presented. Always. The global phone network was a closed system. Callers' numbers could never be manipulated. The number could be matched to an account record to determine the caller's identity with confidence.

That confidence has become skepticism with the arrival of several new technologies. When the global phone network connected to the internet in 1998, anyone could hide behind a virtual and anonymously provisioned phone number. When open-source telecommunications switches became available in 2003, criminals could easily hack phone signaling data to impersonate customers and take over their accounts: "spoofing." In response, call centers implemented basic spoof-detection solutions and knowledge-based authentication (KBA), two countermeasures incapable of keeping up with the challenges described in this report.

Aite labeled the phone channel "the fraud enablement channel" for good reason.[1] Fraudsters know that the call center is a major weakness in enterprise security and a comparatively easy shortcut to account takeover. This paper explores four reasons for that weakness – spoofing, virtualization, gaps in customer data, and coverage – and compares the efficacy of both solutions in addressing these challenges.

Before we can explore the four challenges to call center authentication, let's define the processes by which call centers may attempt to authenticate their callers.

Since 2003 criminals have been able to hack phone signaling data to impersonate customers.

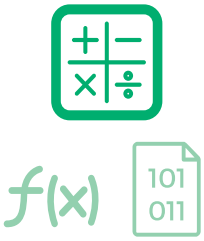
Two approaches to caller authentication

Both inspection and estimation start with data provided as a header by the call center's carrier when a call is connected. The header signaling data contains the calling phone's Automatic Number Identification (ANI), routing information, media type and billing details. Telephone calls carried through the internet use the Session Initiation Protocol (SIP), which explains the synonymous term 'SIP data.'

SIP data offers limited utility for determining phone call legitimacy. Since the telephone network connected to the internet, anyone can hide behind virtual numbers, or "spoof" the ANI and all of the signaling data delivered with a call. It's unreliable for detecting and stopping criminals from attempting account takeover or other fraud.

1 | ESTIMATION USING CALL HEADER DATA ANALYSIS

These solutions analyze call header data to estimate the likelihood that a calling phone's claimed ANI is an authentic and unique match to the ANI associated with a customer's account. Solutions operating outside of the phone network rely heavily on SIP header data for this estimation. In particular, many of these systems are dependent on a richer form of SIP data that has been 'enhanced' with additional data provided by a call center's carrier. Enhanced SIP data remains vulnerable to manipulation, just like standard SIP data. What's more, only a few of the 4,000+ carriers in North America offer enhanced SIP data, severely limiting this approach's coverage.



2 | INSPECTION USING TRUSTID TELEPHONE NETWORK FORENSICS

An inspection approach goes beyond signaling data by directly examining a call within the phone network. This examination looks at the source of a call down to the physical address of a landline call or the SIM card of a mobile phone. This approach confirms that the call is not virtualized, anonymous, hacked, or otherwise altered.

These two approaches—rooted in radically different technologies—yield vastly distinct results when confronting the current challenges to phone channel authentication.

Four challenges to phone channel authentication

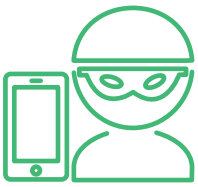
Spoofed Calls

When the internet connected to the phone network, people gained the ability to fake phone numbers. Criminals quickly realized that they could intentionally present a different ANI than their calling phone's assigned ANI in the call's SIP data. By spoofing a legitimate customer's ANI, criminals could impersonate the customer over a phone call. If the criminal could answer basic security questions —mother's maiden name, last four digits of social security number, etc.—they could take over the victim's accounts.

(For the purposes of this paper, we'll include hacked calls in this category. This is where the origination, routing or signaling data is edited by the caller.)

Today, fraudulent callers are now the minority of spoofed calls. Virtual receptionist services and other common telecommunications platforms help honest people to hide their real phone numbers. There are many legitimate uses for this practice. For example, doctors calling patients from their cell phones will often display their office numbers.

Other groups with legitimate uses of spoofing include: celebrities, domestic abuse shelters, businesses, schools, law-enforcement, online-daters, online-sellers, etc.



Best Practices for Spoof Detection

- **Call analysis should not depend on signaling data.** It can be manipulated by criminals.
- **No spoofed call should ever receive an authentication token.** The authenticity of the caller has been obfuscated.
- **Segment spoofed calls based on other data.** Separating high-risk spoofed calls from low-risk spoofed calls helps to minimize false positives and allows for more appropriate scrutiny of lower-risk calls.

Efficacy for Detecting Spoofed Calls

Estimation using call header data analysis

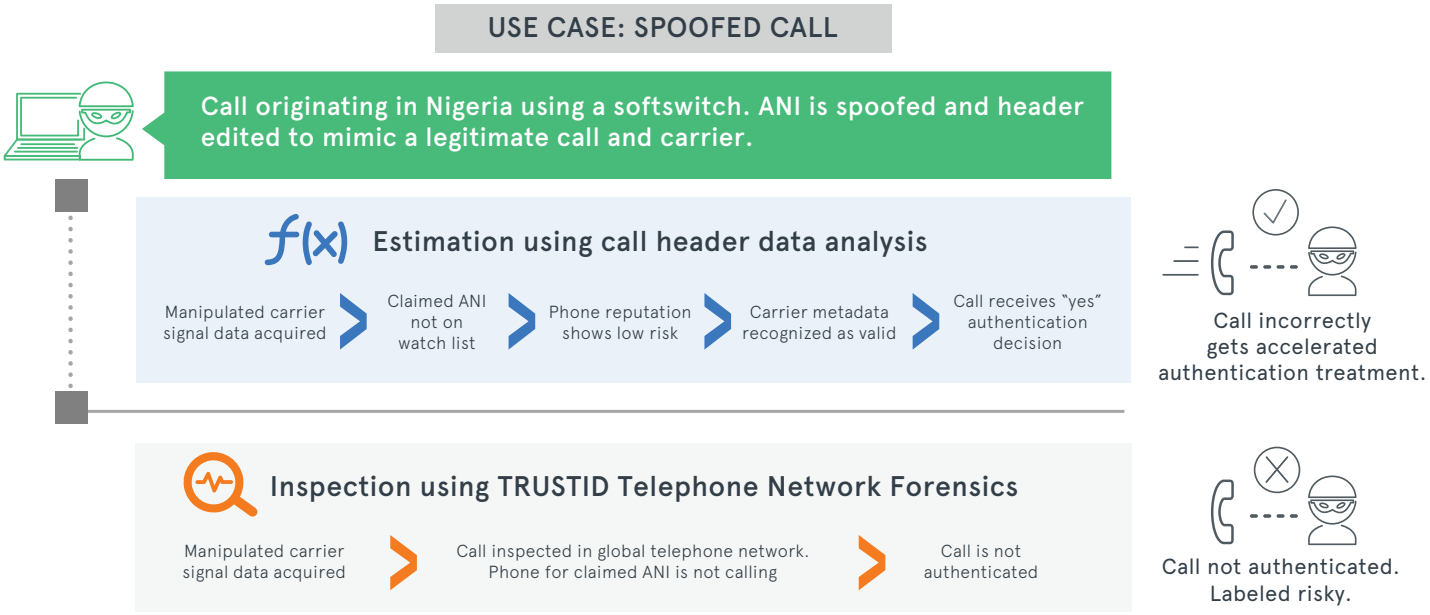
Estimation approaches have some value for the detection of spoofed calls. If there's a structural flaw in the call's data, then the call is likely to be spoofed and thus ineligible for an authentication token. This may be adequate for call centers that handle low-risk business and aren't subject to authentication regulations, compliance obligations or sensitive business requirements.

However, spoofed calls aren't high risk by default. Estimation solutions operating outside of the phone network may mark spoofed calls as risky, in spite of their many legitimate uses. In the context of a high-risk call center, the increase in false positives will bring with it a commensurate increase in costs from the fraud department and complaints from customers. What's more, sophisticated criminals can repeatedly beat any call estimation system that only searches for anomalies in signaling data.

Inspection using TRUSTID Telephone Network Forensics

By their nature, spoofed calls inherently cannot deceive an inspection process based on TRUSTID telephone network forensics. Inspection of a spoofed call will reveal that the calling device is different from the device claimed in the signaling data. That's because a direct inspection of a call reveals its true routing, in real-time, end-to-end from the caller to the call center.

In addition, data from TRUSTID telephone network forensics can inform a risk-scoring solution. Spoofed calls from non-authenticated callers can be segmented by risk to help distinguish very risky spoofed calls from those that are more likely to be legitimate. With this approach, moderate-trust callers would receive a simpler authentication challenge and faster service. Only lower-trust callers would go to the fraud team for more rigorous, and costly, examination.



Minimizing False Positives

Call-risk-detection services that rely exclusively on call header data will flag some legitimate calls as risky. That's because some legitimate calls present anomalies in their signaling data. Tools that look for these anomalies will incorrectly identify these callers as risky. This results in additional investigation and treatment of false positive calls. These mistakes undermine the caller's experience, add to average handle time and distract fraud teams from calls presenting true risk signals.

In contrast, a telephone network forensic technology reduces or eliminates false positives. By directly inspecting calls and accurately identifying those coming from confirmed phones (even if the signaling data is anomalous), fraud teams can focus their efforts. Instead of looking for fraudsters in a large 'haystack' of all inbound calls, they only have to look in a much smaller haybale of non-authenticated calls.

Only inspection of a call can accurately determine if it is spoofed.

Virtualized Calls

Virtualization is the legitimate practice of providing phone numbers that can be used by multiple devices. This is the value proposition behind web-based calling services (e.g., Skype and Vonage), Google Project Fi (routed through T-mobile or U.S. Cellular), or a business PBX. They allow a home computer, work laptop, cell phone and even a shared computer in a hotel's business center to access a virtual account and make anonymous and untraceable phone calls.

They're also the biggest threat vector to call centers today. The call is authentic, unique and legitimate. Its signaling data and call certificates are correct and will pass by technology designed to detect spoofing attempts through errors in enhanced SIP data.

It's much easier for criminals to reach a call center with a virtual service than to go through the effort of engineering a spoofed call that can beat spoof-detection tools.

Virtualization frees criminals from the need to imitate specific callers' numbers. They simply need to reach an agent from a number that appears to be legitimate but isn't tied to a customer's record. When they connect, they have a chance to socially engineer the agent into granting control over a customer's account.

Best Practices for Defending Against Malicious Virtualized Calls

- **Identify all virtualized calls** and ensure they are not provided an authentication token.
- **Separate virtualized calls from other VoIP calls processed by carriers** (such as Comcast) that can be tied to a physical address and granted an authentication token.
- **Use other risk and phone reputation data** to stratify virtualized calls and guide subsequent authentication treatments.

Virtualization frees criminals from the need to imitate specific callers' numbers.

Types of Virtualized Calls

Apps

- **Burner** ("We reroute calls coming to your Burner and send them to your cell phone so your personal number stays private.")
- **Sideline** ("Add a second number to your smartphone. Keep your personal number private.")
- **Hushed (**"Get a custom, disposable number in over 40 countries. Manage multiple numbers from a single app.")
- **Textfree** ("Since 2009, Textfree has been the best way to turn any Wi-Fi enabled device into a phone for free calling and SMS.")

Anonymously provisioned

- Prepaid cell phones are available at convenience stores complete with anonymously provisioned ANIs. The phones are never linked to a human user. Criminals buy dozens of these phones at a time. The calls they make are real.

Skype

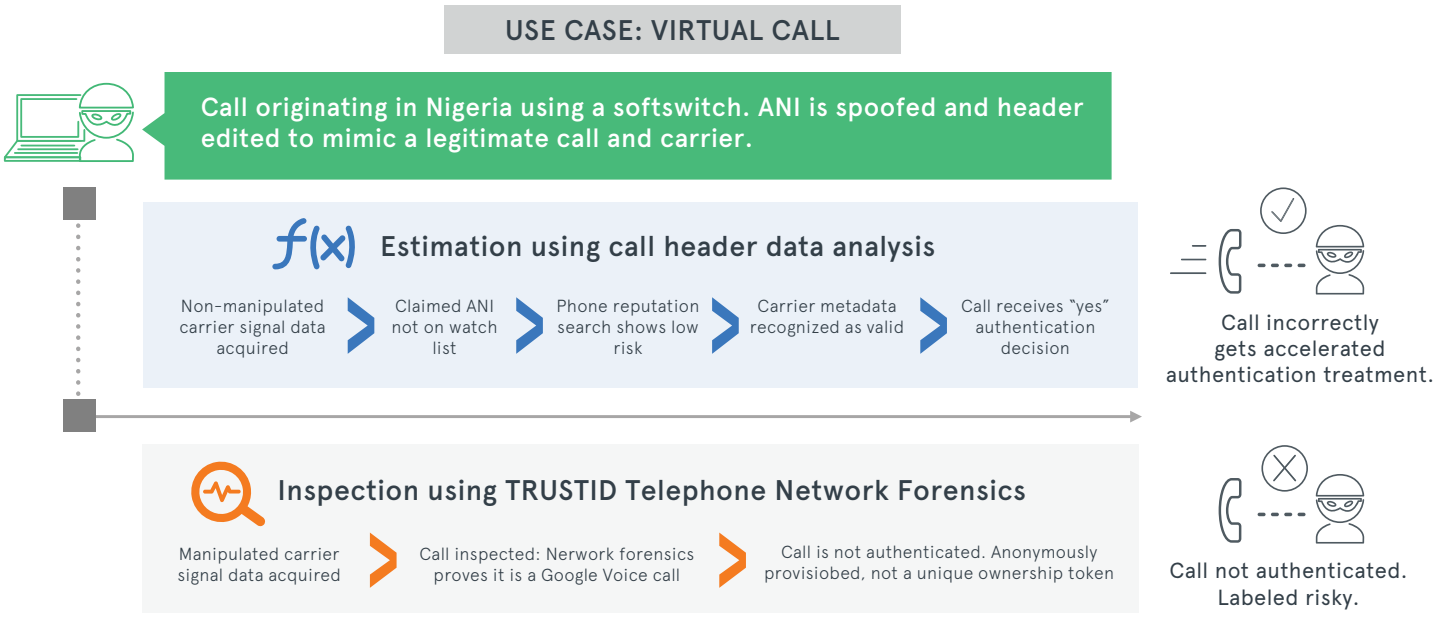
- ("You can use Skype on whatever works best for you - on your phone or computer or a TV with Skype on it.")

Google

- **Voice** ("Google Voice gives you a free phone number for calling, text messaging, and voicemail. It works on smartphones and computers, and syncs across your devices so you can use the app while on the go or at home.")
- **Project Fi** ("puts you on the best available network between Wi-Fi and three 4G LTE networks.")

Low-cost Services

- **MagicJack** ("make and receive calls using your computer or regular telephone. No additional telephone service is required.")
- **SIP.US** ("If your company uses automated dialing for telemarketing, unlike most other SIP service providers, SIP.US can connect you with upstream carriers who welcome this type of traffic.")
- **VoipStunt** ("When you use the free VoipStunt software, you can call regular phones in various popular destinations for free.")
- **TextNow** ("Send messages and make calls on your computer or tablet, then access them from your phone while on the go.")



Efficacy for Detecting Virtualized Calls

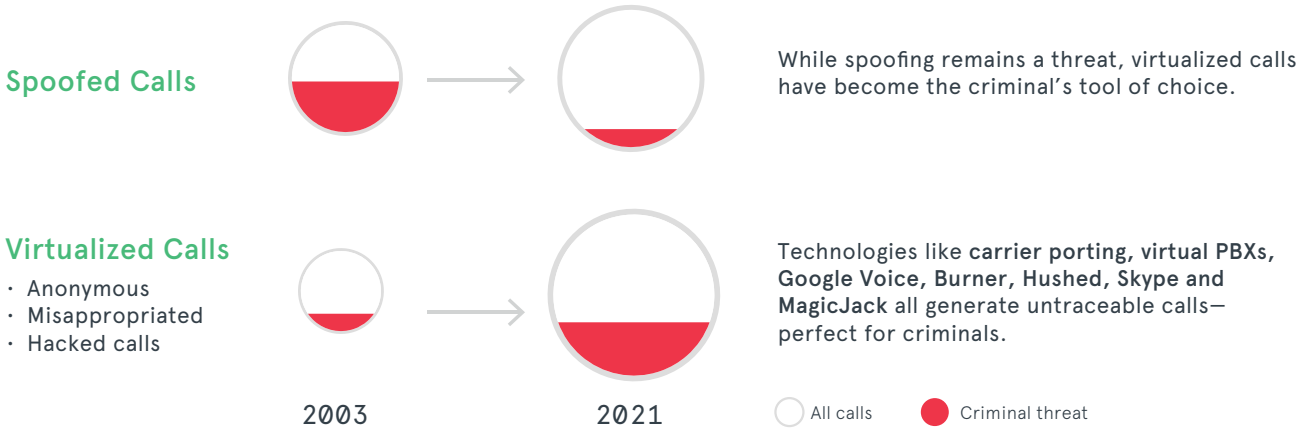
Estimation using call header data analysis

Because virtualized calls are legitimate, estimation solutions based on call header data can't determine if a call originated from a cellular device with a unique SIM card, or from an anonymous VoIP service such as Google Voice. Criminals thrive on this ambiguity. They're allowed to advance to the call center and attempt to socially engineer an agent.

Inspection using TRUSTID Telephone Network Forensics

Because network forensics operates inside the phone network, auditing devices and calls end-to-end in real time with an inspection and confirmation process, it recognizes virtualized calls instantly. Without a unique connection between a physical device and a claimed phone number, virtualized calls will never receive an ownership authentication token from a network forensics authentication process.

HOW CHALLENGES TO CALL CENTER AUTHENTICATION HAVE CHANGED



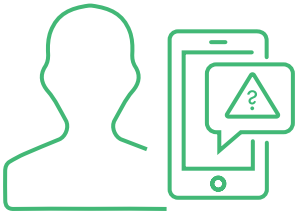
Today, criminals prefer to attempt account takeover through virtual call services.

Calls From Unknown Phone Numbers

On average, between five and fifteen percent of a company's CRM data becomes out-of-sync within a month, and 60 percent of a CRM is inaccurate within only two years.[2] With over 35 million phone number changes every year in the U.S. alone, it's becoming more common for consumers to call in on unfamiliar phone numbers. Will they proactively update your organization with their new phone number? Probably not. Will they expect the prompt recognition and service that a good customer deserves? Absolutely.

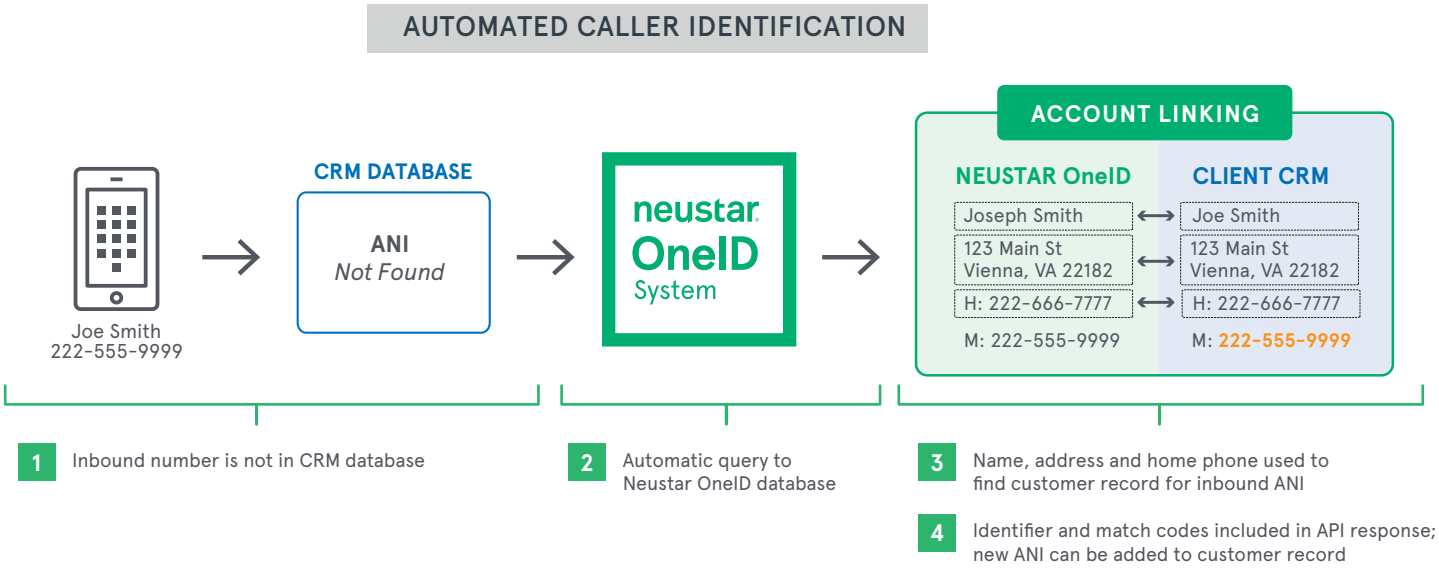
Even if you can inspect and confirm the legitimacy of the phone and the call, you still have to identify the caller. How will you do so? With KBA questions? That negates all of the potential value from implementing an authentication technology based on telephone network forensics.

A successful inbound authentication solution must have the ability to match a claimed identifier to an account. Identification is an essential complement to authentication, and should occur in the same timeframe. You can't have one without the other, and yet most authentication solutions neglect to identify callers entirely.



Best Practices for Calls From Unknown Numbers

- Identify the caller concurrently with authentication.



While checking the call's authenticity, Neustar Inbound Authentication increases CRM match rate.

Efficacy for Calls From Unknown Numbers

Estimation using call header data analysis

These solutions only examine data about a phone number. They have no way of recognizing when a caller from an unrecognized phone number is the actual consumer associated with an account. Consequently, contact center agents have to waste time confirming the caller's identity.

Inspection using Neustar Inbound Authentication

Authoritative data from the Neustar OneID® database about a calling phone number is used to identify callers' accounts, while TRUSTID technology inspects the calls in real-time, before they're answered. In most cases, by the time callers hear "Hello," their authenticity and identity is already established.

What is the Neustar OneID database?

The Neustar OneID system is built on a framework of authoritative data sources—such as government, telecom, billing, utilities, and financial—whose operations depend on having up-to-date identity records.

This includes unparalleled coverage of wireless, VoIP, and nonpublic numbers, unique insight into billions of call transactions, and management of over 90 percent of U.S. caller ID. With 11 billion daily updates to consumer data, the Neustar OneID system proactively gives the most accurate, up-to-date contact information — empowering organizations with the right information, right now to accurately and confidently identify their customers' phone numbers to mitigate risk and improve operational efficiencies.

Coverage

The final challenge to call center authentication is one of access. For solutions to the first three challenges to succeed, they need complete access to the entire volume of calls approaching the call center. If they can only evaluate a fraction of the calls, then they're already behind.

Efficacy for Accessing Calls

Estimation using call header data analysis

Most estimation services rely on enhanced SIP data from carriers to make their call-risk estimates. Only a portion of carriers provide these 'enhanced' data. If the call center's carrier only provides standard SIP data, then a probabilistic modeling service dependent on enhanced SIP data won't have enough information for analysis. Therefore, only a small fraction of incoming calls are eligible for analysis.

Inspection using TRUSTID Telephone Network Forensics

The combination of its patented network forensic technology and extensive carrier infrastructure allows TRUSTID's technology to inspect phone calls without any legal or technical dependence on other carriers. The solution works for all carriers, with all phone types, without the need for customer consent. It's 100 percent coverage, 100 percent of the time.

Conclusion

Let's finish with a quick summary of how TRUSTID telephone network forensics and probabilistic modeling perform against the challenges to phone channel authentication.

TRUSTID telephone network forensics is the best solution on the market for authentication in the phone channel. It's an inviolable confirmation that the phone call is unique and in the network, not spoofed, virtualized or misappropriated. It's the best choice for efficiency, security and customer authentication. So, why isn't your call center using it?

CHALLENGE	INSPECTION USING NEUSTAR INBOUND AUTHENTICATION	ESTIMATION USING CALL HEADER DATA ANALYSIS
Spoofing	 Detects both amateur ANI spoofing and sophisticated criminal ring spoofing and hacking	 Detects some basic ANI spoofing, but not advanced spoofing where signaling data has been manipulated
Virtualization	 Detects all risk vectors	Misses the threats
Unrecognized Phone Numbers	 Consults most up-to-date database available	Not designed for the task
Coverage	 All North American carriers and lines	 Limited coverage due to dependence on carrier data

LEARN MORE For more information, call **1-855-898-0036 x4**, email **risk@team.neustar**, or visit **www.risk.neustar**.

1. Aite Group, "Contact Centers: The Fraud Enablement Channel"
2. Neustar, "The Marketer's Identity Crisis"

About Neustar.

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.

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.

www.home.neustar

WP-FRC-289715-02.06.2022