WHITE PAPER

2021 STATE OF CALL CENTER AUTHENTICATION

How a Year of Disruption Reshaped Inbound Call Center Leaders' Approach to Fraud Prevention, Customer Experience, and Operational Efficiency.

neustar®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Inbound contact center leaders stepped up in the last year to adapt to an increasingly complex call center environment. Personnel management went virtual due to social distancing mandates. Capacity from offshore partners paused for extended periods of time. Meanwhile, inbound call volumes, the complexity of callers' matters, and callers' anxiety increased. Fraudsters' calls poured in to take advantage of the disruption and high emotion. These factors are reflected in the respondents' answers to the 2021 State of Call Center Authentication survey.

More respondents cited the call center as enabling account takeover (ATO) fraud in 2020 than in prior years. Contact center fraud increased for 40 percent of respondents' firms. Sixty-four percent of respondents from financial services organizations expressed concern over fraud originating in the contact center.

Respondents' preference for agent-led authentication fell 57 percent, down to the lowest point since this survey began in 2018. Over 80 percent of respondents prefer completing most of the authentication process before callers reach agents. This timing would minimize the potential for fraudsters to socially engineer agents into granting account access by mistake.

More fraudsters are using call spoofing and virtualization services. Over half of respondents saw more fraudulent activity associated with these vectors. Unfortunately, 90 percent of respondents' firms are not prepared to take advantage of the STIR/SHAKEN framework, which can help enterprise inbound contact centers to detect spoofed calls.

Respondents defined strong, clear priorities for their fraud-detection technologies. Over three-quarters of respondents valued each of the following capabilities: minimizing false positives (79 percent), leveraging consortium data to identify attacks (78 percent), alerting on a first-time attack without dependence of consortium data (76 percent), and providing a risk signal before a call is answered (73 percent).

These preferences align with respondents' desire for inbound caller authentication to complete with minimal agent involvement, and support balancing fraud prevention with customer experience and operational efficiency.

1 MORE FRAUD COMES THROUGH THE CALL CENTER

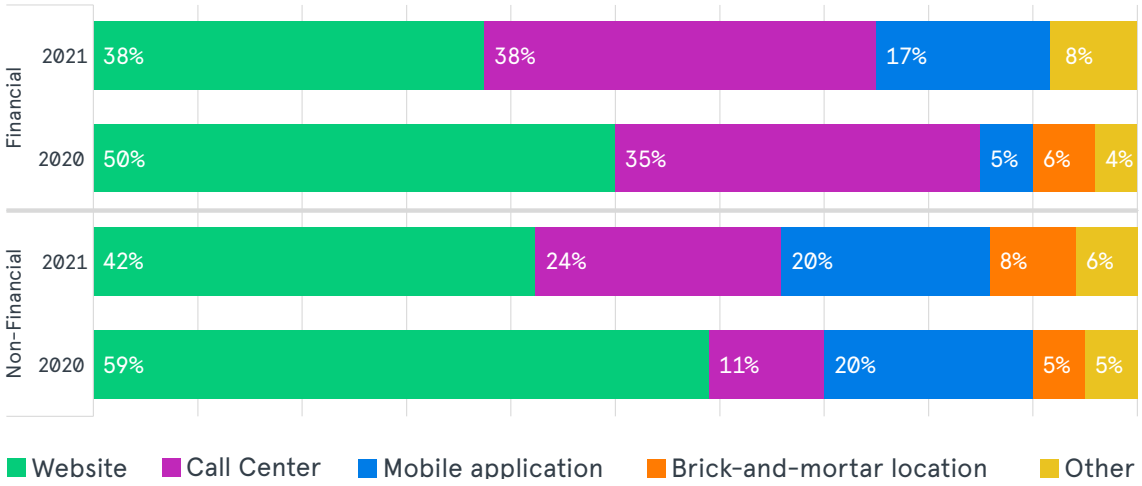
More respondents cited the call center as enabling ATO fraud in 2020 than in prior years. Financial institutions attributed ATO fraud equally to website and call center channels, a change from 2020 when websites took greater blame. Twice as many non-financial respondents reported ATO fraud in the call center than in 2020.

Fraudsters gravitate to the phone channel because the primary line of defense—call center agents asking challenge questions—is highly vulnerable to social engineering. It is easier for fraudsters to find answers to challenge questions and then socially engineer a human agent into granting access to a consumer account than it is to hack IT infrastructure backed by a dedicated security team. The increased inbound call volume in 2020—combined with heightened caller anxiety, sympathetic agents working from home, and related disruptions—would have helped fraudsters to socially engineer call center agents.

Forty percent of respondents saw more contact center fraud in 2020 than in years prior. Sixty-four percent of respondents from financial services organizations are somewhat or very concerned over fraud originating in the contact center. In February 2020, shortly before the COVID-19 pandemic gripped the U.S., almost one quarter of respondents to the 2020 State of Call Center Authentication survey preferred authentication to take place during an agent conversation. That protocol increased call centers' risk of account takeover fraud and may help to explain respondents' experiences reported in this year's survey.

Fraudsters often start in the contact center, and then move on to digital channels. Once a fraudster takes over a victim's account via the phone channel, the fraudster may change an online password or phone number associated with that account. These changes allow the fraudster to take over a victim's online accounts. The number of respondents reporting an increase in contact center fraud in 2020 may very well underrepresent the reality; it takes considerable root-cause analysis for an organization to attribute the eventual fraud loss in the digital channel to an ATO via phone call.

In which communication channel do you think most account takeovers start?



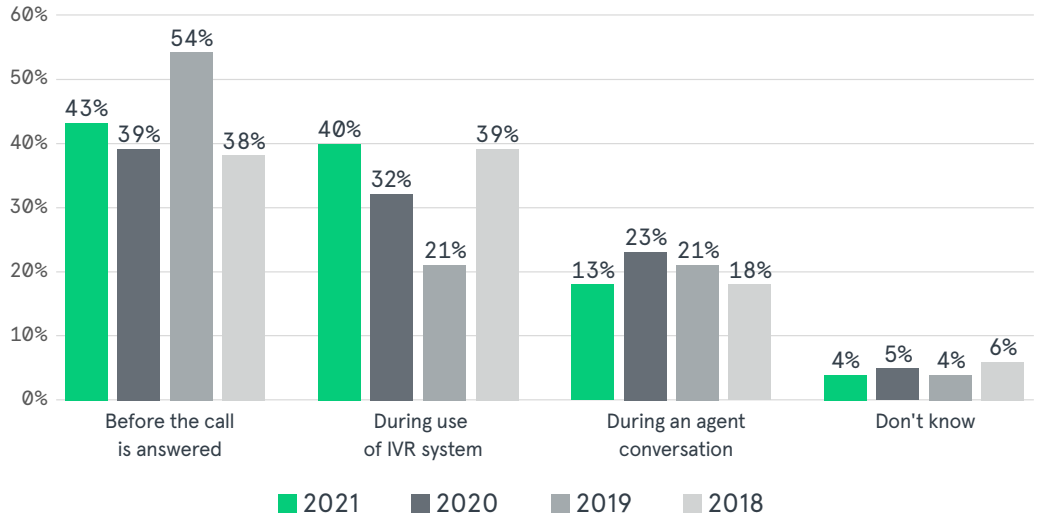
2 KEEP AGENTS OUT OF AUTHENTICATION

Respondents overwhelmingly want to keep agents out of the authentication process, with 83 percent preferring to complete authentication pre-answer or while a caller engages with an interactive voice response (IVR) system. Preference for agent-led authentication fell 57 percent, down to the lowest point since this survey began in 2018. Agent-led authentication relies on asking challenge questions—knowledge-based authentication (KBA)—an approach that increases call centers' risk of fraud loss, customer attrition, and operational waste.[1]

Minimizing agent involvement in authentication mitigates these risks. Fraudsters have less opportunity to socially engineer agents into granting illicit access to customer accounts. Customers receive better service by addressing their matters without an initial interrogation of their identity. Average handle time decreases between 20 and 70 seconds.

Nearly 70 percent of respondents like the idea of matching callers to their accounts using callers' phone numbers, which is possible only if contact centers trust the authenticity of the calling number.[2] Authenticated callers' accounts may pre-populate on agent screens for faster, more personal service.

At what time in the customer journey would you prefer to complete authentication?



1 Neustar, 10 Reasons Why Knowledge-based Authentication Threatens Contact Centers (Find a brief summary of KBA's shortcomings in the glossary.)
2 Neustar, How COVID-19 has Reshaped Inbound Authentication

3 FRAUDSTERS ATTACK ON MULTIPLE FRONTS

Fifty-eight percent of respondents reported an increase in the use of call spoofing to impersonate customers. Fifty percent observed an increase of fraudsters using virtual call services to launch anonymous attacks. To prevent account takeover fraud, organizations must be able to detect both fraud methods in the call center.

Criminals can manipulate the call signaling ("SIP") data that many spoof detection approaches rely upon. By iterating on different access points and editing signaling data, criminals can find a combination that is, as far as a spoof detection solution is concerned, indistinguishable from an actual call. Web applications and mobile apps make this functionality even more accessible to fraudsters.

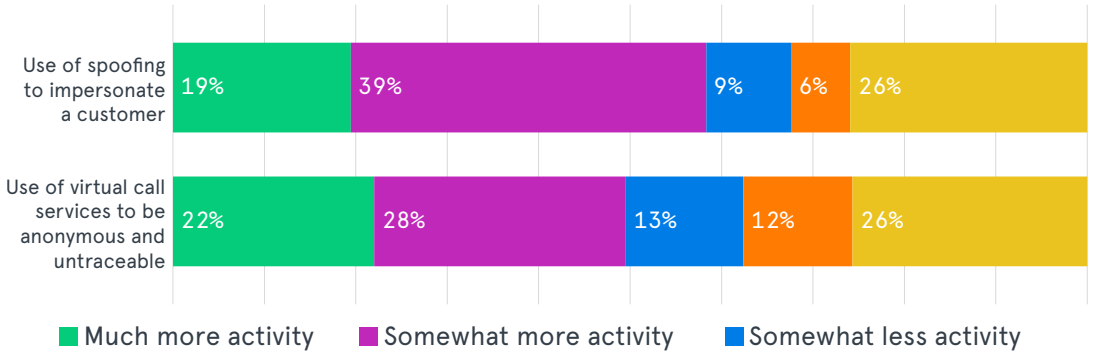
Because some fraudsters will always be able to bypass spoof detection solutions, contact centers often treat all of their inbound call volume with caution. This prevents contact centers from achieving the full value of identifying legitimate calls and limits the degree to which they can ease their authentication protocol for trusted callers.

Assessments of call signaling data do nothing to combat fraud originating through virtual call services, such as Google Voice, Pinger, or Text Now. As far as fraud detection services are concerned, these calls are authentic, legitimate, and unique. Virtual calls represent approximately two percent of all call volume today, according to Neustar internal data.

It is much easier for criminals to reach a call center with a virtual service than to engineer a call that can beat spoof detection tools. Virtual calls' signaling data and call certificates are "correct" and will pass by technology designed to detect errors in SIP data. In fact, even the best SIP data provides no information to distinguish calls placed via virtual apps from VoIP calls tied to a physical device, such as a cable modem.

With a virtual call service, criminals can call from anywhere in the world with little risk of getting caught. To succeed, fraudsters first reach an agent from a legitimate number unrelated to a customer's record. When they connect, they have an excellent chance to socially engineer the agent into granting access to a customer's account.

How has the threat posed by the following criminal tactics changed in the past 12 months?



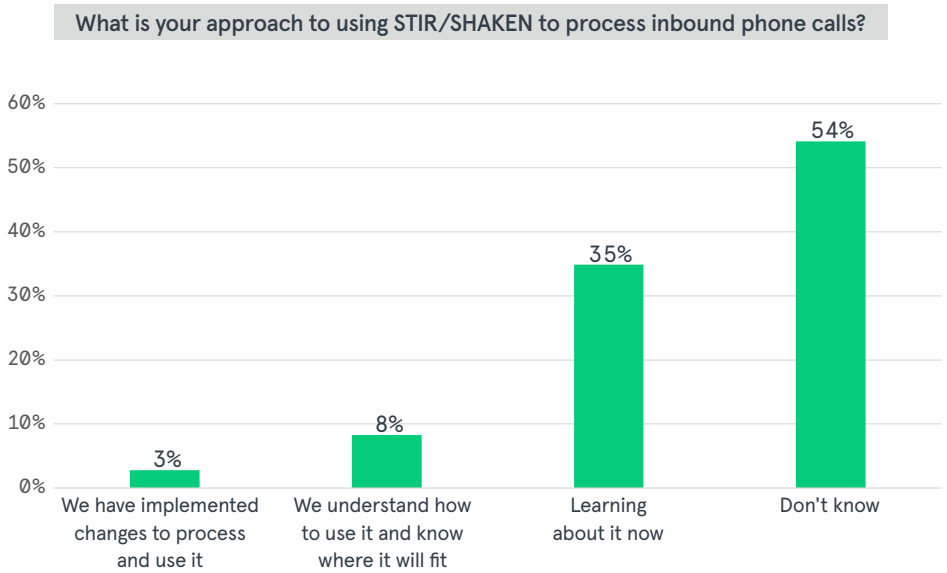
4 90% OF INBOUND CALL CENTERS ARE NOT PREPARED FOR STIR/SHAKEN

When the STIR/SHAKEN[3] standard goes into full production on June 30, 2021, it will begin to help consumers determine the legitimacy of calls that reach their phones. At that time, enterprise contact center analytics platforms can begin incorporating valuable information from STIR/SHAKEN to help identify spoofed calls.

Most enterprises have been working with their telephone carrier to ensure their outbound calls get delivered as STIR/SHAKEN goes into effect. However, the same is not true for enterprises processing inbound phone calls. Almost nine-in-ten respondents say that their inbound call center analytics are not prepared to ingest STIR/SHAKEN data.

Enterprises should deploy STIR/SHAKEN in a way that supports both their inbound and outbound businesses. STIR/SHAKEN will make it easier for inbound call centers to identify callers that are not spoofing customer phone numbers. More attention can be focused on calls that do not receive strong STIR/SHAKEN attestations.

As STIR/SHAKEN makes it more difficult to spoof calls, fraudsters are likely to adopt virtual call services to launch their attacks. Because these services place legitimate phone calls, they will receive high-quality attestations from the carrier that originates the calls.



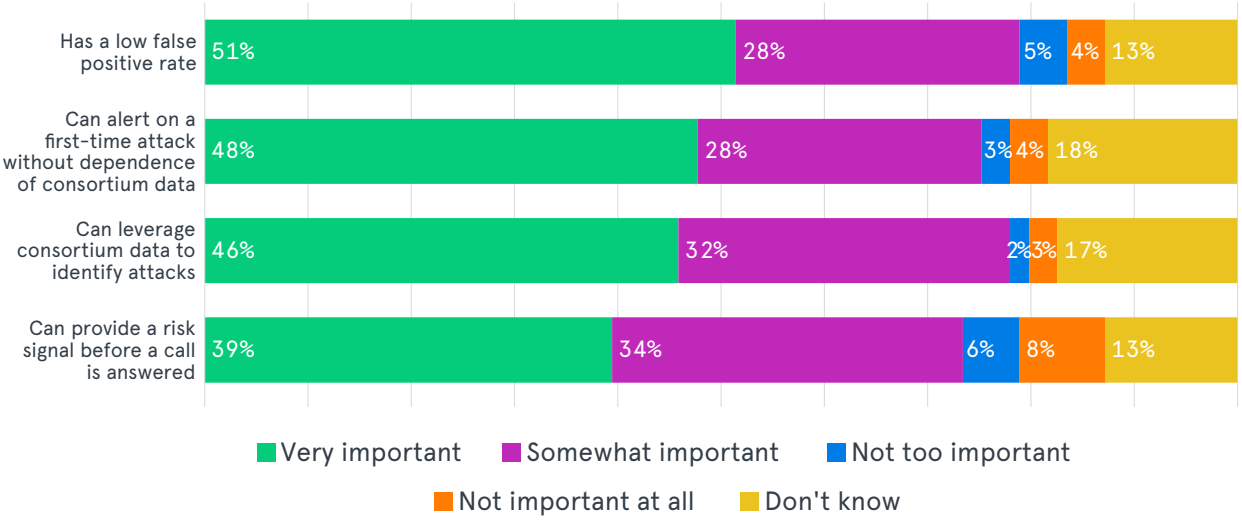
3 Neustar, STIR/SHAKEN Resource Hub
4 Neustar, How to Evaluate STIR/SHAKEN Attestations
5 Neustar, Not All Greens Are Created Equal

5 RESPONDENTS PRIORITIZE FRAUD PREVENTION CAPABILITIES

Respondents shared strong expectations for fraud detection technologies in the inbound call center. Over three-quarters of respondents indicated that each of the following benefits was "somewhat" or "very" important:

- **Minimizes false positives** – Flagging customers as suspicious (i.e., false positives) impacts the operations and fraud teams. False positives often require more authentication, which degrades the customer experience and increases average handle time. These innocent calls sap the fraud team's resources intended for genuinely suspicious callers. Reducing false positives helps call centers to focus fraud prevention resources more effectively, while also improving the customer experience.
- **Can leverage consortium data to identify attacks** – Different organizations using the same fraud prevention technology may share anonymized intelligence about the calls into their respective call centers. This shortens the time to detect emerging fraud tactics and reduce false positives.
- **Can alert on a first-time attack without dependence of consortium data** – To circumvent the protections of the consortium model, sophisticated fraudsters cycle devices, phone numbers, callers, and call scripts. A single successful fraud incident can yield a healthy return, justifying the cost of more sophisticated evasion tactics. The ability to detect attacks from unfamiliar sources and devices closes a costly loophole in many call centers' defenses.
- **Can provide a risk signal before a call is answered** – A pre-answer signal enables call centers to route suspicious calls to agents who have had more fraud prevention training. This approach reduces fraud risk and false positives, thereby improving the customer experience and the average handle time of frontline agents.

In considering new technologies for fraud dection, how important is each of the following to your organization?



CONCLUSION

Inbound call center leaders have emerged from a tumultuous year with valuable new lessons and approaches. The industry will use these lessons to hone best practices for keeping ahead of fraudsters' tactics, meeting customer expectations, and driving operational efficiency.

The findings in this report indicate that inbound caller authentication could undergo substantial change in 2021. The conditions for this change have been maturing since this survey began in 2018: the weaponization of customers' personally identifying information (PII), the increasing sophistication of account takeover attacks beginning in the phone channel, and consumers' rising expectations for safe and easy connections.

As the inbound call center industry moves into the next phase, Neustar expects that organizations will continue to revisit and revise their fraud prevention approaches to enable efficient, frictionless customer connections.

WHY NEUSTAR?

With 11 billion daily updates to consumer data, continuously corroborated from over 200 authoritative sources, Neustar provides the most accurate, up-to-date, and complete identity information possible. Powered by TRUSTID® technology, the most powerful ownership authentication forensic technology in the market, Neustar Inbound Authentication creates a Trusted Caller Flow™ that minimizes knowledge-based authentication, reduces IVR-to-agent transfers, and allows agents to move quickly into problem-solving mode. By diverting trusted callers into their own flow, fraud-fighting staff and tools can focus on the remaining, smaller pool of questionable callers.

Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100.

LEARN MORE

Mitigate fraud risk, improve operational efficiency, and delight consumers with Neustar Inbound Authentication.

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

APPENDIX A: GLOSSARY

Pre-answer authentication

A real-time forensic analysis within the telephone network[6] that validates that the calling and called numbers are engaged in a call, and further validates that the signal data from the call is consistent with known patterns. This process completes before callers hear "Hello."

Voice-biometrics ('voice-bio') authentication

Requires callers' permission to obtain, store, and use a reference voice print for comparison in future calls. On subsequent calls after enrollment, a caller's live voice sample can be compared to the reference voice print for authentication.

The three factors of authentication

- **Knowledge** - Asking callers questions about personal information. When used as the sole factor of authentication, both subtypes, described next, are insecure due to the flood of data breaches and proliferation of information available on social media. Traditional KBA uses challenge questions the caller configures when she opens her account. "Out of wallet" KBA challenges callers with dynamic questions drawn from credit bureau or demographic data. KBA takes between 30 and 90 seconds, increasing average handle time (AHT) without adding value, and forcing callers to submit to identity interrogation before receiving service.
- **Inherence** – Using physiological or behavioral identifiers (e.g., fingerprint, retina scan, typing rhythm, or, for the purposes of the phone channel, the caller's voice and intonation) to generate an authentication token.
- **Ownership** – Using a physical item unique to the individual – such as a credit card, a house key, or a phone – as an authentication token.

Multi-factor authentication

Using two or three factors of authentication in concert to confirm a caller's claimed identity and grant access to the caller's account.

Call spoofing

Intentionally presenting a different ANI than the calling phone's assigned ANI in order to impersonate a customer over a phone call. Once the primary vehicle for phone channel fraud, spoofing is now easy to detect.[7]

Virtualized calls

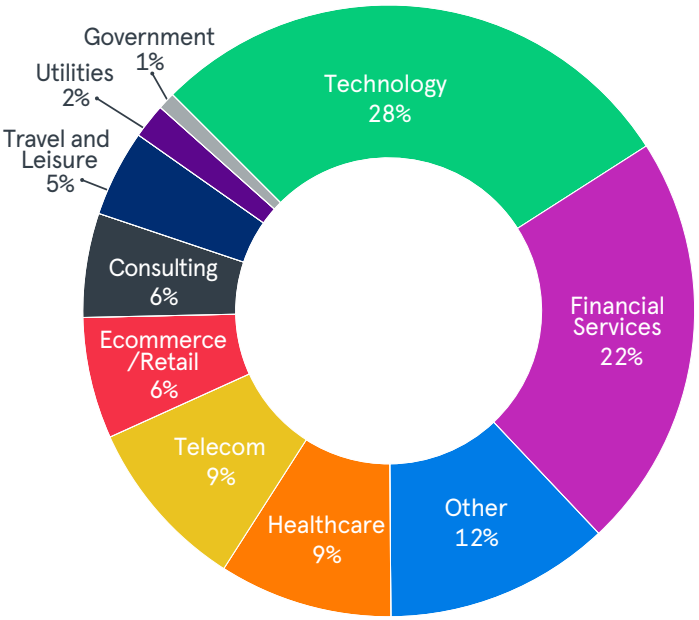
Technology that provisions phone numbers that can be used by multiple devices. Virtualized calling services allow a home computer, work laptop, cell phone, and even a shared computer in a hotel's business center to access a virtual account and make anonymous and untraceable calls.

6 Neustar, Telephone Network Forensics: The Technology for Phone Ownership Authentication
7 Neustar, Call Center Authentication: Four Challenges in the Phone Channel

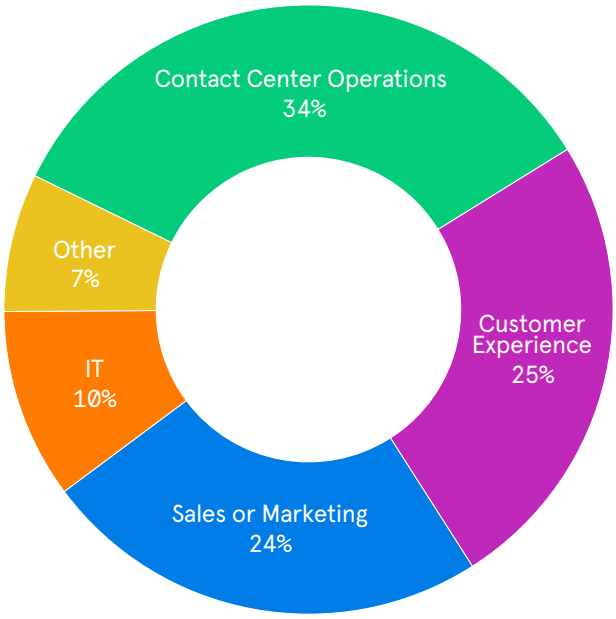
APPENDIX B: METHODOLOGY

Neustar conducted an online survey in March, 2021. The 109 respondents work primarily in contact center operations, customer experience, sales, marketing, or information technology. The primary markets represented by respondents were technology and financial services. Respondents were offered a small monetary incentive as a thank you for time spent on the survey.

Survey Respondents



Respondent Roles



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, and Security 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 at www.home.neustar.

WP-FRC-302800-06.11.2021