WHITE PAPER

2020 STATE OF CALL CENTER AUTHENTICATION

How Changes to Authentication Will Improve Customer Experience, Operational Efficiency, and Fraud-Fighting Ability.

neustar®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Caller identity remains a central concern for call center leaders tasked with improving customer experience, operational efficiency, and fraud-fighting ability. Trusted callers must be served quickly to maximize operational efficiency. High-risk calls must be flagged quickly to focus costly fraud-fighting resources.

The market is shifting in response to these imperatives. Awareness of pre-answer phone call analysis rose 22% this year, placing the approach on par with traditional knowledge-based authentication (KBA). That may have been driven in part by the preference for authentication to complete before callers hear "hello;" just 23% of respondents are content to leave authentication to an agent conversation, which is costly and risky.

Agents' susceptibility to social engineering continues to attract account takeover (A.T.O.) attacks. For a second year, more respondents from the financial services industry (35%) recognized the phone channel as a threat vector for A.T.O. than respondents from other industries (11%). However, web sites were the most problematic channel for respondents, a sign that new phone channel authentication technologies may be having a positive impact.

The reverberations of that positive impact may have contributed to respondents' overwhelming optimism (77%) that they can successfully balance customer experience with fraud prevention, and their overall satisfaction (59%) with their current authentication methods.

However, respondents are clear-eyed on where their fraud risk comes from; 70% of respondents saw 'somewhat' or 'much more' threat activity as coming from virtualized call services. These easy-to-use services free criminals to bypass spoof-detection tools and focus on socially engineering agents with consumers' personal information acquired on the dark web and social media.

Knowledge-based authentication (KBA) remains well entrenched, despite how easily criminals can acquire consumers' personal information. 54% of respondents are 'somewhat' or 'very' confident in KBA's ability to accurately authenticate inbound callers. This flies in the face of respondents' high expectations for authentication technologies, such as supporting seamless customer experience (96% marked as important), improving fraud detection (96%), and reducing operating costs (92%). Will inbound call center operations attain these and other desired technology benefits or hold on to KBA?

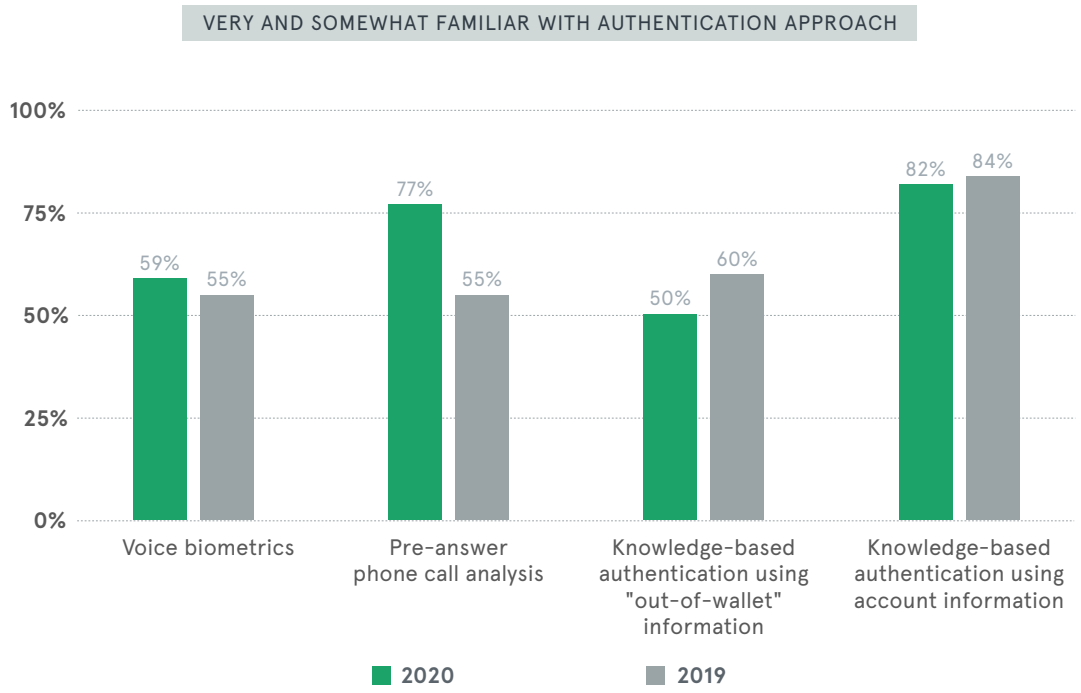
The answer, a compromise, may lie in the movement toward multi-factor authentication (MFA). Just 23% of respondents didn't know their organizations' MFA strategy this year, the lowest percentile since we started this survey in 2018. 34% of respondents plan to supplement KBA with another factor of authentication, while 27% plan to replace it altogether. Just 17% of respondents have no plans to move beyond KBA.

How does your call center's authentication strategy compare to those of others?

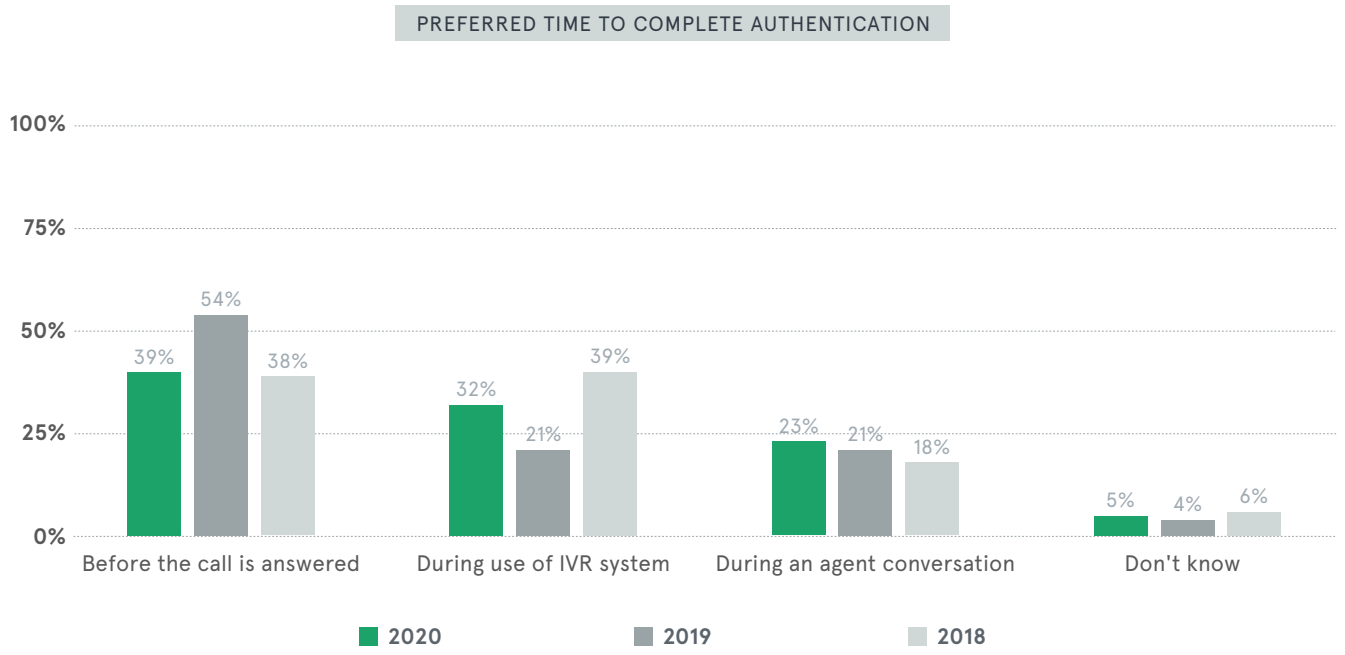
Keep reading to find out.

1 PRE-ANSWER AUTHENTICATION GROWS IN AWARENESS AND PREFERENCE

Awareness of pre-answer phone call analysis leapt 22% in the last year, placing the approach on par with traditional KBA. For the first time, two tiers of call center authentication have emerged: the leaders (pre-answer analysis and traditional KBA) and the laggards (voice biometrics and 'out of wallet' KBA). The increase in familiarity with pre-answer authentication may have to do with public endorsements from some leading institutions: Bank of America, UBS, and USAA.



Despite receiving its share of endorsements, voice biometrics did not enjoy the same increase in awareness. This discrepancy may be due to respondents' preference for authentication to conclude as soon as possible, either before the caller hears 'hello' or during use of the IVR. Empowering agents for prompt problem solving, not identity interrogation, best supports customer experience and operational efficiency.

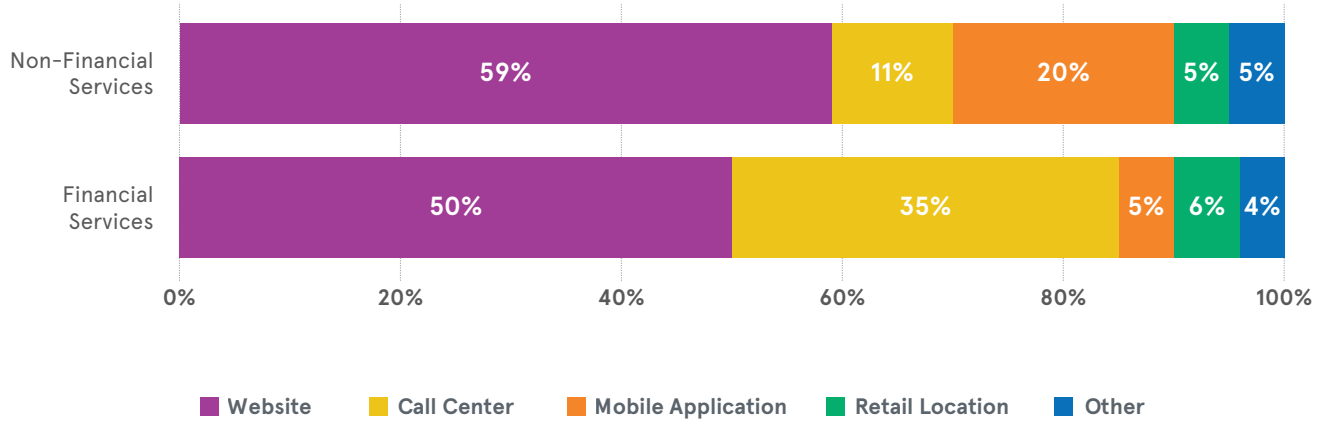


2 CALL CENTERS CONTINUE TO ATTRACT ACCOUNT TAKEOVER ATTACKS

Criminals seek to exploit the weakest point in organizations' defenses. In 2020, criminals saw more potential in websites than in call centers. That may be because call centers implementing new caller authentication technologies to supplement the weaknesses of KBA (Insight #6) were more capable of repelling A.T.O. attempts. Criminals that find call centers more difficult to 'attack' will direct their efforts to more promising channels. As in 2019, respondents from the financial services industry perceived more risk of A.T.O. from the phone channel than respondents from other industries.

Account takeovers tend to show up in the online channel, but most fraudsters initiate their efforts by socially engineering call center agents to reset passwords for online accounts. It's easier to trick a human than to hack IT infrastructure backed by a dedicated security team. Aite warned of this vector in 2016. Javelin Advisory services reiterated the warning in 2019.

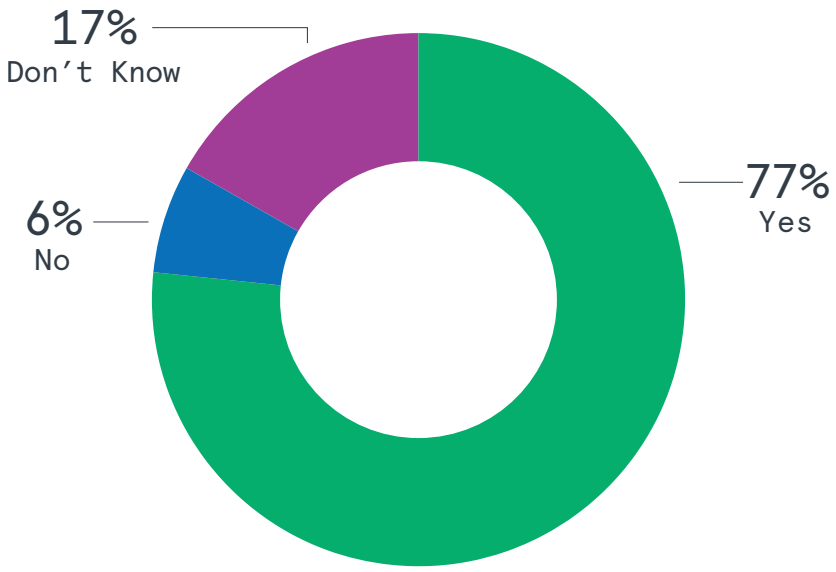
CHANNELS FOR FRADULENT ACCOUNT TAKEOVERS

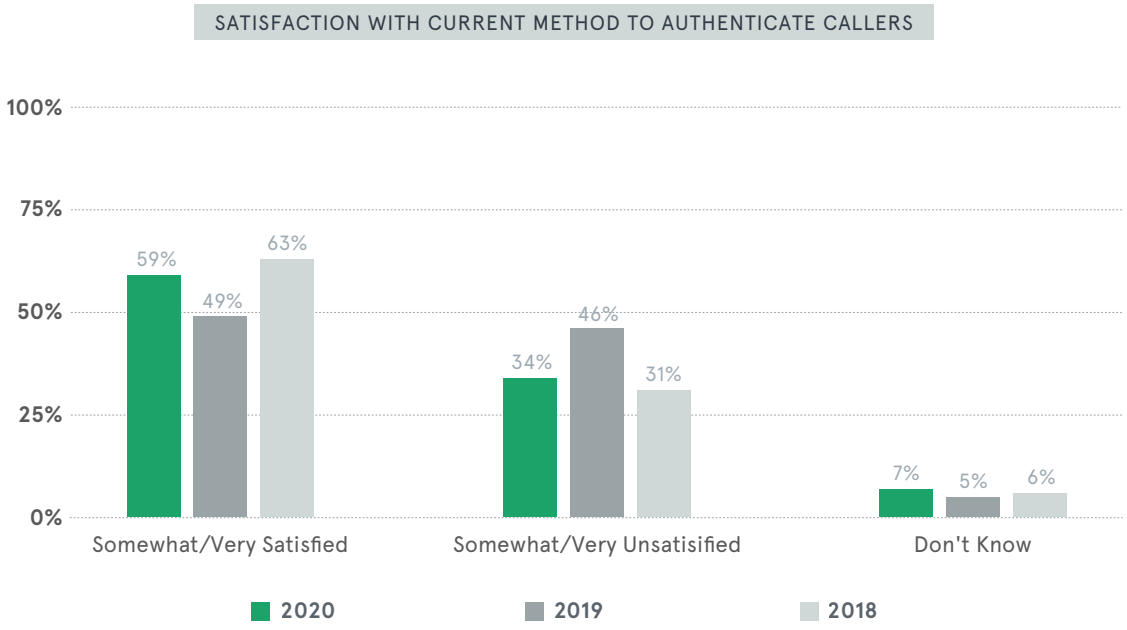


3 OPTIMISM IN BALANCING CUSTOMER EXPERIENCE AND FRAUD PREVENTION

Respondents were overwhelmingly confident that they would be able to prevent A.T.O.s without obstructing the customer experience. This aligned with respondents' increasing awareness of pre-answer call analysis (Insight #1), the change in perception of A.T.O. risk over the phone channel (Insight #2), plans to implement multi-factor authentication (Insight #6), and increasing satisfaction with current caller authentication methods. As the market put more trust in new authentication technologies, a proxy for satisfaction (next page), respondents had more reason to feel optimistic about balancing customer experience with fraud-prevention efforts.

DO YOU BELIEVE IT IS POSSIBLE TO PREVENT A.T.O.S WITHOUT OBSTRUCTING THE CUSTOMER EXPERIENCE?





This insight aligns with a finding that appeared in a Forrester Consulting study commissioned by Neustar ("Mitigate Fraud And Consumer Friction With Integrated [Identity Verification]," February, 2019). Nearly 70% of that study's respondents said that reducing or preventing fraud was a high or top priority for investment, if not one of the highest. In addition, firms that were actively expanding their identity verification capabilities on multiple fronts were "more likely to take many types of customer expectations into account when making decisions about fraud strategy, including security and privacy concerns. This type of customer obsession is what businesses need to remain competitive in the age of the customer."

4 VIRTUAL CALLING SURPASSES SPOOFING AS TOP A.T.O. VECTOR OVER THE PHONE

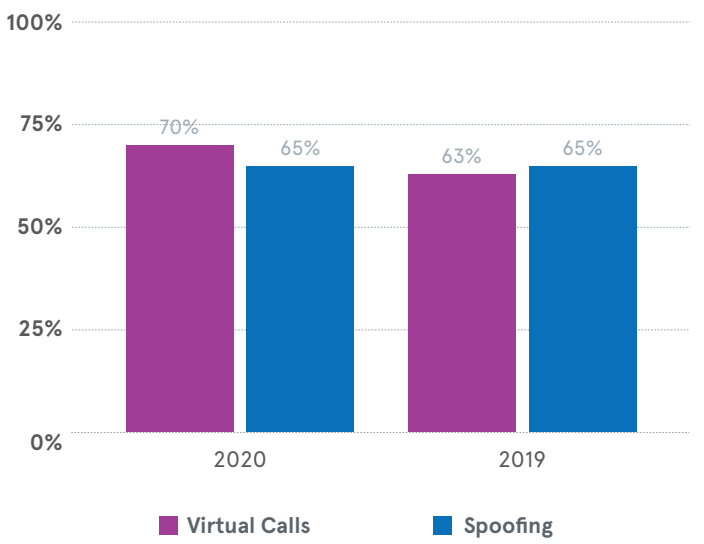
Virtual calls were recognized as the biggest A.T.O. threat. 70% of respondents saw 'somewhat' or 'much more' threat activity toward the call center as coming from virtualized call services.

It's little wonder that virtual calls are recognized as a threat, considering how easy it is to perpetrate A.T.O. with this method. Fraudsters create a free email account and then register it with a virtualized calling service that requires only an email account to activate. No other steps are needed; criminals can now make legitimate calls that will slip by spoof-detection technologies.

Virtualization frees criminals from the need to imitate specific callers' numbers. They just have to reach an agent from a legitimate number that's unrelated to a customer's record. When they connect, they have an excellent chance of socially engineering the agent into granting control over a customer's account. The threat of virtualized call fraud is pervasive. Fraud feedback data from Neustar's customers show as many as 80% of A.T.O. attempts between September, 2019 and February, 2020 were made with virtual calling services.

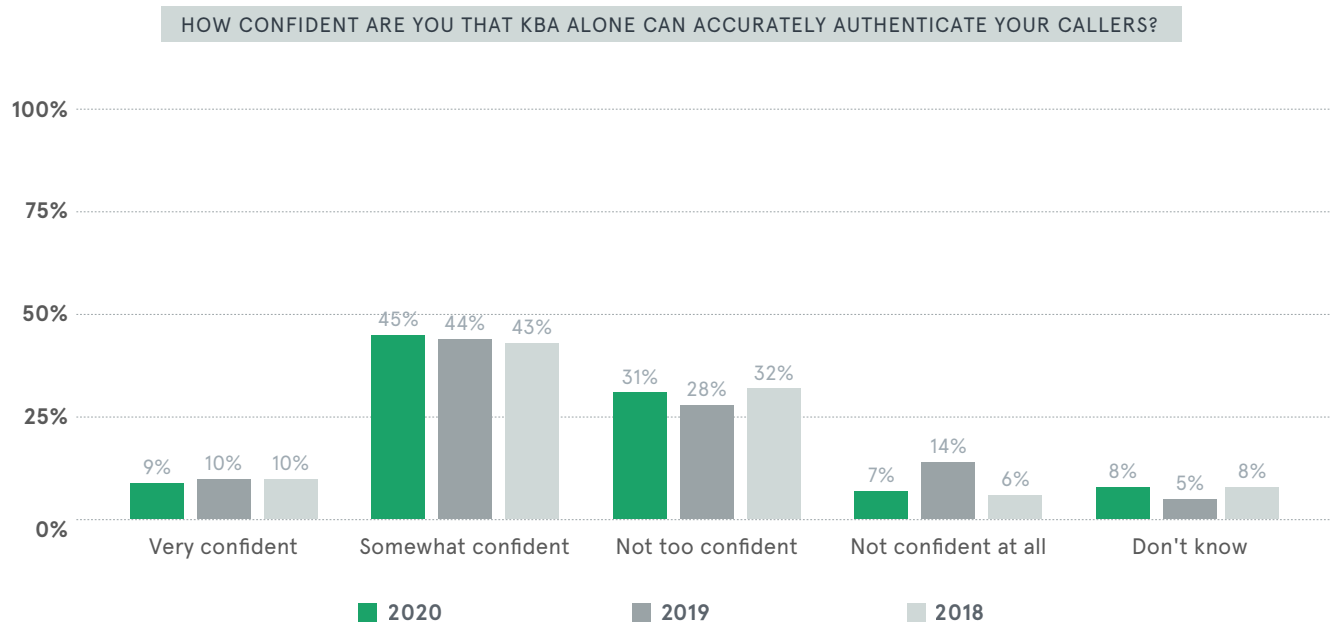
To prevent fraud from exploding through this vector, call centers will have to arm their agents with tools that determine each calling device's uniqueness, authenticity, physicality, and risk of fraud.

THREAT WHERE THERE IS SOMEWHAT AND MUCH MORE ACTIVITY



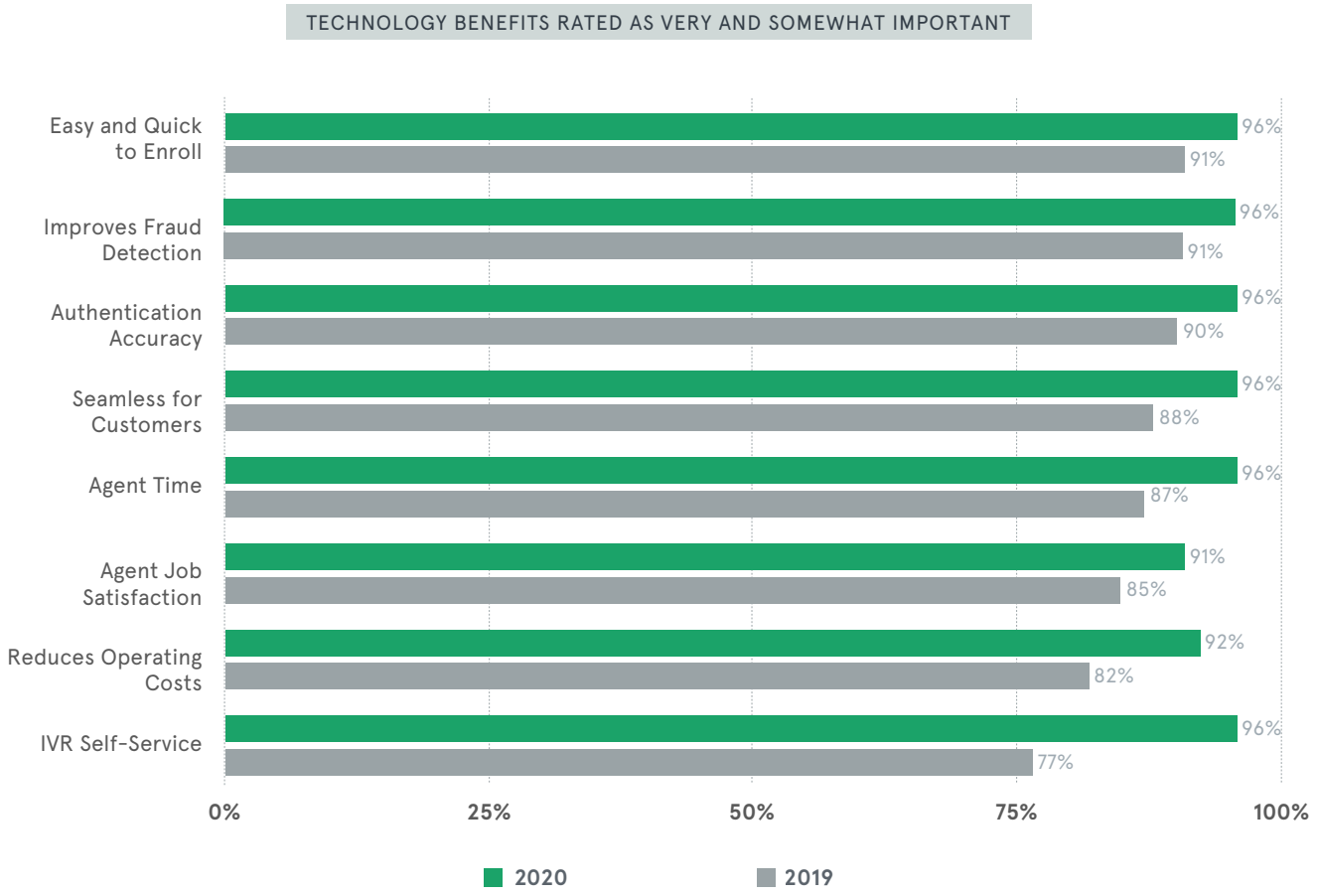
5 DISCONNECT OPENS BETWEEN STATED PRIORITIES AND ENTRENCHED PREFERENCE FOR KBA

Respondents held on to confidence in KBA, which aligns with a finding from Forrester's study: "92% of the fraud management decision makers we surveyed said that [KBA] is somewhat or very effective at reducing ID theft and fraud; 90% said the same about validation of static identifiers against data bureaus. However, after prominent credit bureau breaches of the past few years, we've entered an era in which credit data and KBA should be regarded as highly suspect forms of IDV because this information can be socially engineered or purchased by fraudsters via dark web marketplaces."



Misplaced confidence in KBA partly explains why customer accounts are still vulnerable to A.T.O. over the phone channel (Insight #4), and why respondents' expectations for new technologies rose. All benefits listed in the survey were ranked as 'very' or 'somewhat' important. KBA fails to deliver many of these benefits[1]: it hampers fraud detection, worsens authentication accuracy, degrades customer experience, squanders agent time, frustrates agents, balloons operating expenses, and keeps call centers from offering higher-value IVR self-service options[2].

Inbound call center operations must make a choice: attain the desired technology benefits or hold on to KBA. Perhaps industries will choose in 2020. While 54% of respondents said they were 'somewhat' or 'very' confident in KBA, their stated plans (Insight #6) showed otherwise; just 17% of respondents plan to stick with 'pure KBA' for the year ahead.



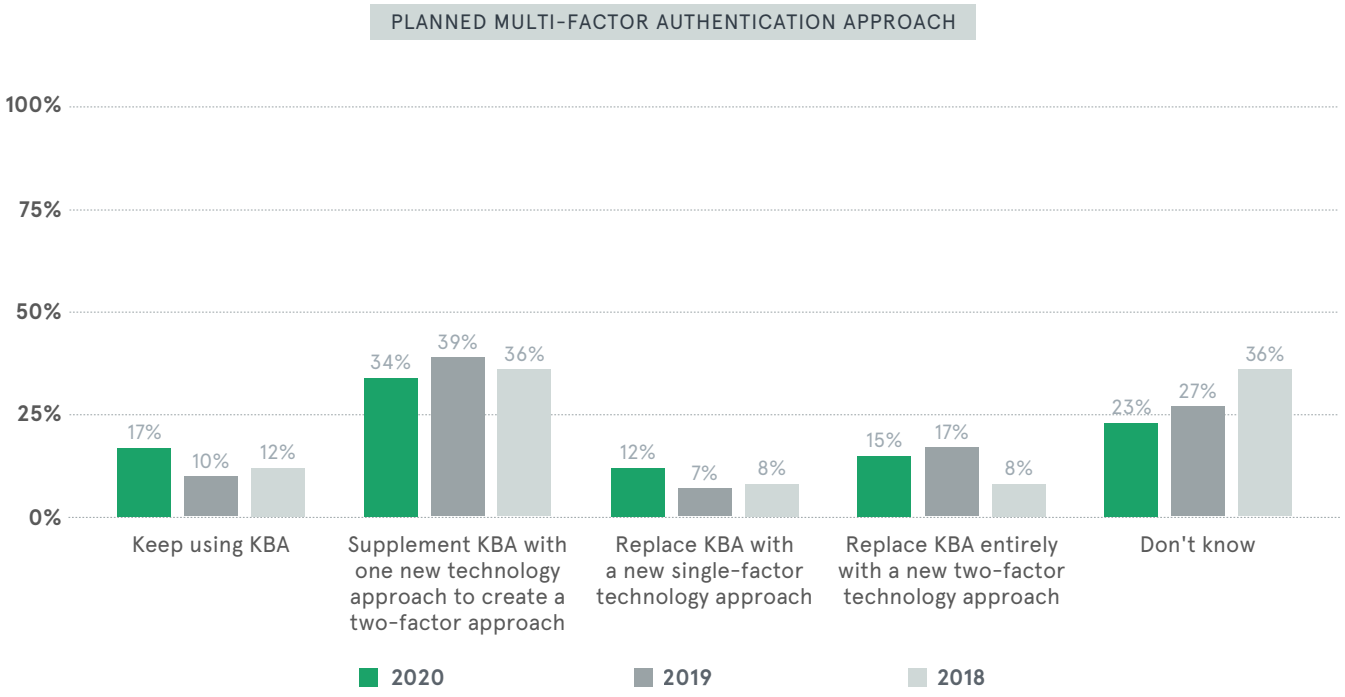
[1]Read "Ten Reasons Why Knowledge-based Authentication Threatens the Modern Contact Center" https://www.home.neustar/resources/whitepapers/knowledge-based-authentication-threatens-contact-centers
[2]Read "The Trusted Caller Flow Solution" https://www.home.neustar/resources/whitepapers/contact-center-efficiency-the-trusted-caller-flow

6 PLANS TO MOVE TO MULTI-FACTOR AUTHENTICATION ACCELERATE

The number of respondents unsure of their MFA approach dropped to 23%, the lowest since this survey started in 2018. Increased momentum toward multi-factor authentication over the phone channel corresponds to what the survey respondents reported:

- encountering more A.T.O. attempts on websites than on the phone channel. (Insight #2)
- sustaining optimism that they can prevent A.T.O.s without degrading customer experience (Insight #3)
- changing satisfaction levels with caller authentication (Insight #5)
- extending the lifespan of KBA (Insight #6)

Respondents planned to supplement KBA, rather than replace it altogether.[3] In order for multi-factor authentication to deliver on respondents' expectations (Insight #5), the second factor should not just reduce fraud, but also improve customer experience and operational efficiency.



[3]See how USAA improved operational efficiency, customer experience, and fraud-fighting capacity by enhancing its inbound caller authentication posture. https://www.home.neustar/resources/webinar/contact-center-authentication-fraudsters-love

CONCLUSION

Call centers have largely relied on using personal information known about customers to validate callers' identities. The amount of personal information available in social media and through data breaches enables fraudsters to operate with a high degree of impunity. This has compelled call centers to subject all callers to more friction during authentication, which degrades customer experience and operational efficiency. Now that multi-factor authentication options are gaining adoption, Neustar expects that organizations will revisit and revise their approach to maintaining privacy while protecting customer relationships in the year ahead.

In 2020, Neustar predicts[4]:

1. **The weaponization of customers' personal information will spur an awakening in the call center**
2. **Callers will continue to demand less friction in the phone channel**
3. **Use of KBA will decrease—albeit slowly, given its associated poor customer experience, inefficiency, and lack of security**
4. **Consumers will begin to perceive KBA as a misuse of their personal information**

[4]Read "Five Fraud And Caller Authentication Predictions for 2020" https://www.home.neustar/blog/five-fraud-and-caller-authentication-predictions-for-2020

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, increases IVR containment, 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

Delight your consumers, improve operational efficiency, and mitigate fraud risk with Neustar Inbound Authentication.

For more information, visit **www.inbound.neustar**, contact us at **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[5] 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 calls are answered.

Voice-biometrics ('voice-bio') authentication

Requires up to a seven-minute caller-enrollment process to obtain a reference voice print and gain permission to use the caller's recorded voice for comparison in future calls. After enrollment, when calls are made by the customer, a 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 below, 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 unknown questions drawn from credit bureau or demographic data.
- **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 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.[6]

Virtualized calls

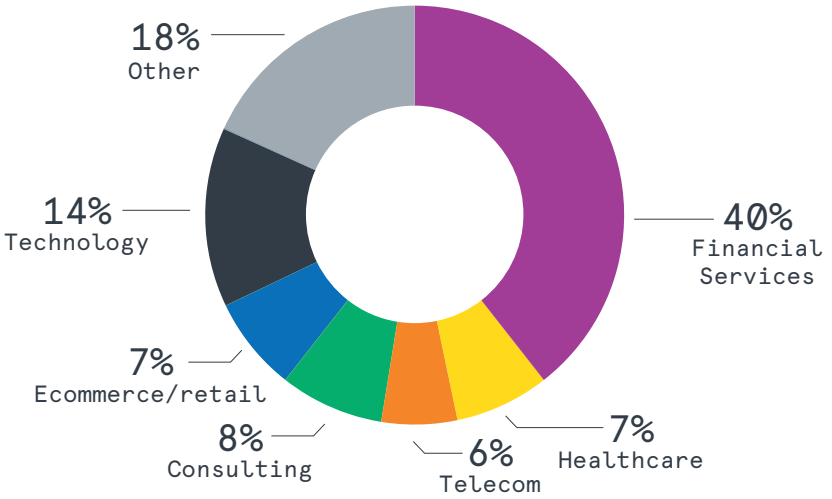
The legitimate practice of providing phone numbers that can be used by multiple devices. Virtualized calling services allow a home computer, work laptop, cell phone, and even a shared computer in a hotel's business center to access a virtual account and make anonymous and untraceable calls.

[5]Read "Telephone Network Forensics - The Technology for Phone Ownership Authentication" https://www.home.neustar/resources/whitepapers/telephone-network-forensics
[6]Read "Call Center Authentication: Four Challenges in the Phone Channel" https://www.home.neustar/resources/whitepapers/four-challenges-in-phone-authentication-and-identification

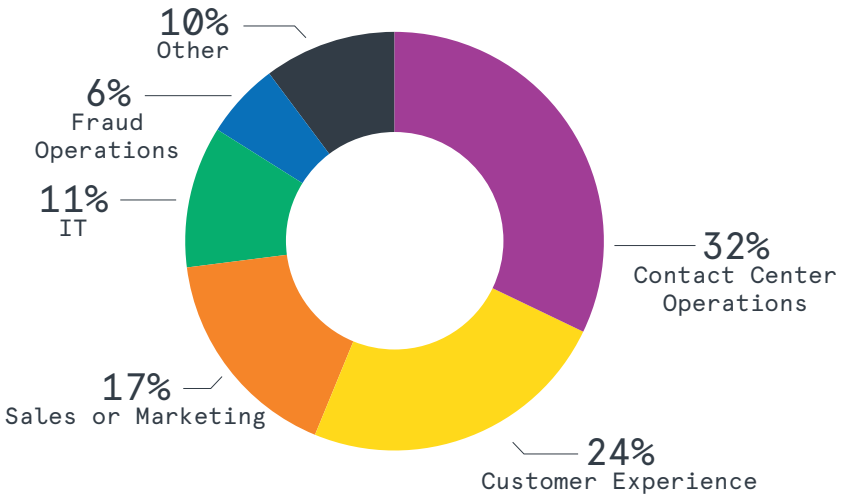
APPENDIX B: METHODOLOGY

Neustar collaborated with Contact Center Week to conduct this online survey in February, 2020. The 137 participants work in contact center operations, customer experience, sales, marketing, information technology, and fraud operations. The primary markets represented by respondents were financial services and technology. Respondents were offered a small monetary incentive as a thank you for time spent on the survey.

SURVEY RESPONDENTS BY MARKET 2020



SURVEY RESPONDENTS BY ROLE 2020



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.**

WP-FRC-224796-05.05.2020