TRUSTID
A Neustar Company

SURVEY

2019 State of Call Center Authentication

As criminals' tools and tactics shift, call center leaders become clearer about how they'll fight back while preserving customer experience.

Executive Summary

As criminals continue to exploit the call center to take over customers' accounts, TRUSTID's second annual survey on call center authentication describes business leaders' maturing attitudes about fighting back. It all revolves around authenticating callers. If criminals can pass through that defensive measure, then they can take over consumers' accounts. This year, 51% of respondents from the financial services industry, and 32% of all respondents, recognized the phone channel as the primary source of account takeover (ATO) attacks. As more personally identifying information (PII) becomes available on the dark web, and organizations further fortify their cyberdefenses, we expect ATO attacks over the phone channel to become more common in the year ahead as fraudsters increasingly recognize it as the weakest link in an organization's attack surface.

The means by which ATO attempts take place is also shifting. Respondents recognized 'much more' criminal activity coming through virtualized calls (40%) than spoofed calls (32%) in the past year. With spoofing easier than ever to detect, we expect that gap to grow. Since virtualized calls (e.g., Skype or Google Project Fi routed through a carrier) breeze through most spoof-detection methods, this is the vector to watch in 2019.

Despite this shifting threat landscape, and the concurrent pressure to deliver the best customer experience possible, 76% of call center leaders felt that they could prevent ATO without obstructing their customers' experience. At the same time, our data also suggest that they are eager for change. 46% of call center leaders were 'very' or 'somewhat' dissatisfied with their current caller authentication method(s), a 50% increase since 2018.

51% **Financial services respondents that see phone channel as top threat for ATOs**

46% **Respondents are unhappy with current authentication method**

40% **Criminal activity is coming through virtualized calls than spoofed calls (32%)**

76% **Call center leaders feel they can prevent ATO without obstructing their customers' experience**

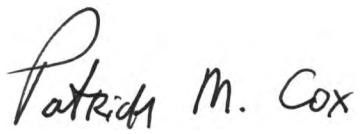
That dissatisfaction may be driven by respondents' dramatic shift in expectations for caller authentication. 54% of respondents prefer authentication to complete before the call is answered; over twice as many as those who either prefer authentication with an agent or in the IVR system. That clarity has trickled into respondents' priorities for a new approach. Emerging authentication solutions must provide easy enrollment to callers, increased fraud detection, and improved accuracy – all without hindering the customer experience.

We can't presume to know exactly what the right solution will look like, but we can be sure that it will be some flavor of multi-factor authentication (MFA). Since our 2018 survey, the percentage of respondents that did not know their organization's plans for MFA dropped from 36% to 27%, indicating more organizations are formalizing plans to abandon dependence on a single-factor knowledge-based authentication (KBA) approach. What's more, the percentage of respondents planning to replace KBA with an MFA approach based on new technologies more than doubled from 8% to 17%.

54% **Respondents prefer authentication to complete before the call is answered.**

2X **Respondents planning to replace KBA with an MFA-based approach doubled from 8% to 17%.**

What could this all mean for the year ahead at your call center? Keep reading for our interpretation.



Neustar vice president and general manager of TRUSTID

Insight #1

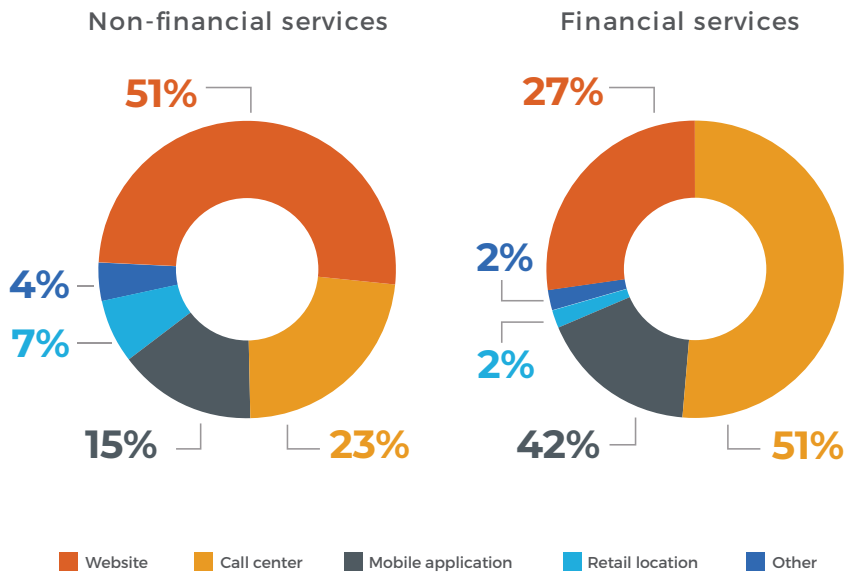
Call centers are now the vector of choice for criminal attacks

That's according to 51% of respondents from the financial services industry. This acknowledgement continues a trend described by Aite Group's 2016 report[1] "Call centers: The Fraud Enablement Channel." The report—based on interviews with 25 executives at 18 of the 40 largest financial institutions in the United States—found that "contact center fraud has continued to grow substantially at many U.S. financial institutions in recent years. Armed with a wealth of data from breaches, organized fraud rings are probing [financial institutions] and using social engineering tactics to add to the information they already have to take over customer accounts. Fraudsters tend to look for the point of least resistance, and often that is the contact center." This helps explain why our respondents from the financial services industry tended to perceive the phone channel as a greater threat than the web channel, as compared to respondents from other industries.

Several industry experts at the recent Money 20/20 USA conference—including Jim Hickman, Assistant Vice President of Financial Crimes Operations at USAA, and Tom Poole, Senior Vice President for Digital Payments and Identity at Capital One—agreed that most fraud starts in the call center. They said that account takeovers tend to show up in the online channel, but the majority of fraudsters initiate their efforts by socially engineering call center agents in order to reset passwords for online accounts.[2]

The reason is simple: Attempting to socially engineer a call center agent is easier and cheaper than planning and launching an intrusion against a hardened target online with a small attack surface. It's easier to trick a human than to hack IT infrastructure backed by a dedicated security team.

Channel for fraudulent account take overs



Fraudsters know that many call centers still rely on KBA to protect customers' accounts. As personally identifying information (PII) has become free and plentiful[3], fraudsters can answer KBA questions correctly and take over customers' accounts.

Insight #2

Virtualized calls pose the greatest account takeover threat

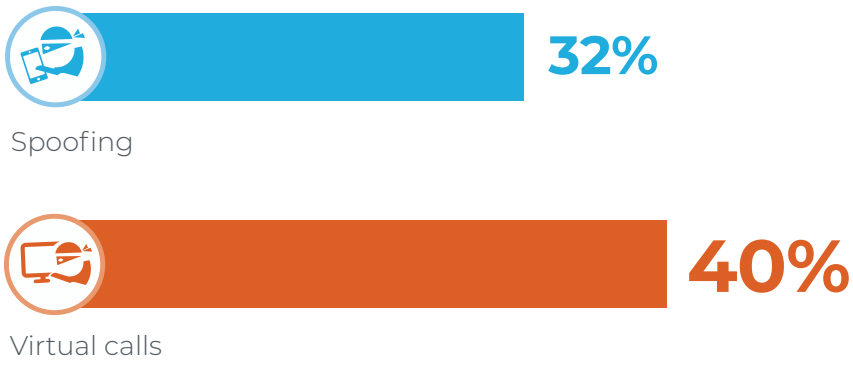
Across all industries, respondents recognized virtual calls as the primary vector through which they saw 'much more' criminal activity, marking a substantial shift away from spoofing.

Spoofing customer phone numbers—once a popular criminal tactic—is falling out of favor. That's because spoofed calls are easier to detect. If there's a structural flaw in a call's signaling data, then the call is likely to be spoofed. Today, there are more spoof-detection solutions on the market than ever before. Criminals are turning to a more effective alternative: call virtualization.

Virtualization (e.g., web-based calling services (Skype), Google Project Fi (routed through T-Mobile or U.S. Cellular), or a business PBX) is the biggest threat vector to call centers today. The calls are authentic, unique and legitimate. Their signaling data and call certificates are correct and will pass by technology designed to detect spoofing attempts.

Virtualization frees criminals from the need to imitate specific callers' numbers. They just have to reach an agent from a number that is legitimate but 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. To prevent fraud from exploding through this vector, call centers will have to arm their agents with tools that identify calls with more nuanced risk factors, such as those made through virtualized call services.

Attack vectors with 'much more' activity in last 12 months



Insight #3

Customer experience and fraud prevention expected to improve in tandem

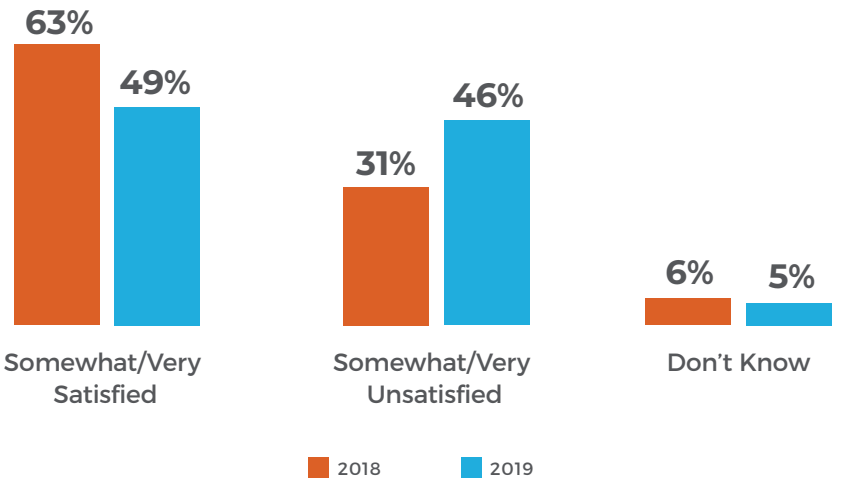
In this year's survey, 50% more respondents expressed dissatisfaction with their current authentication approaches as compared to a year ago: 46% vs. 31%. (68% of those in financial services were 'somewhat' or 'very' unsatisfied.) Since single-factor knowledge-based authentication (KBA) was the dominant authentication approach in last year's study[4], we conclude that respondents' dissatisfaction has to do with that approach.

This fits with IDology's Sixth Annual Fraud Report[5], which found that "Balancing consumer friction with fraud prevention has taken the first place of the challenges companies are facing for fraud prevention, surpassing shifting tactics being used by fraudsters, which until this year was the dilemma of greatest concern."

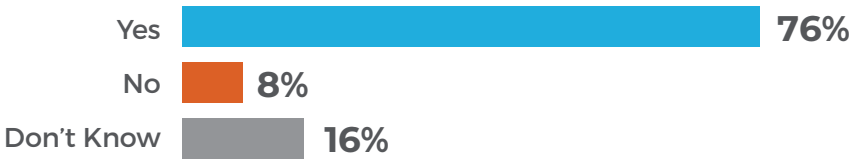
Despite sharply rising dissatisfaction, 76% of call center leaders in this year's State of Call Center Authentication survey remain optimistic that they can prevent account takeover without obstructing the customer experience.

The combination of respondents' dissatisfaction with the status quo and their optimism for a better future points to an imminent shift in the market's choice of authentication method and timing.

Satisfaction with current method to authenticate callers



Respondents who believe it's possible to prevent ATOs without obstructing the customer experience



Insight #4

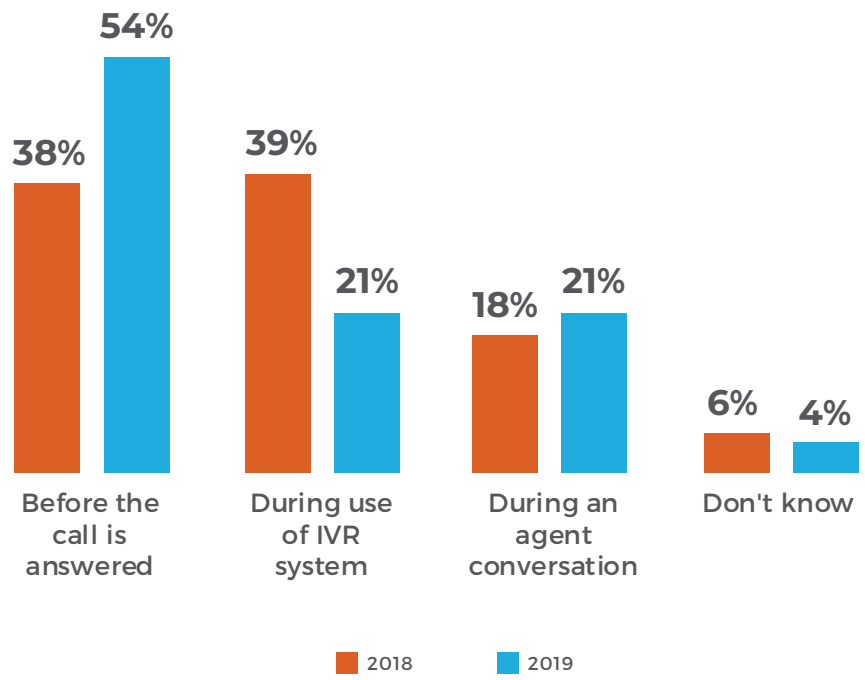
Pre-answer authentication emerges as preferred choice

What will close the gap between respondents' dissatisfaction with their current authentication approach, and fulfill their optimism for a solution that will prevent fraud without obstructing the customer experience? The answer may lie in the growing interest in pre-answer authentication approaches to speed the authentication process – with respondents increasingly recognizing speed as essential to delivering the best customer experience possible.

Over twice as many respondents now want authentication to complete before the call is answered, a dramatic shift from last year's survey.

This switch likely reflects respondents' growing understanding of pre-answer authentication options. It may also have contributed to the optimism mentioned above.

Preferred time to complete authentication



Insight #5

Easy customer enrollment tops requirements for second year in a row

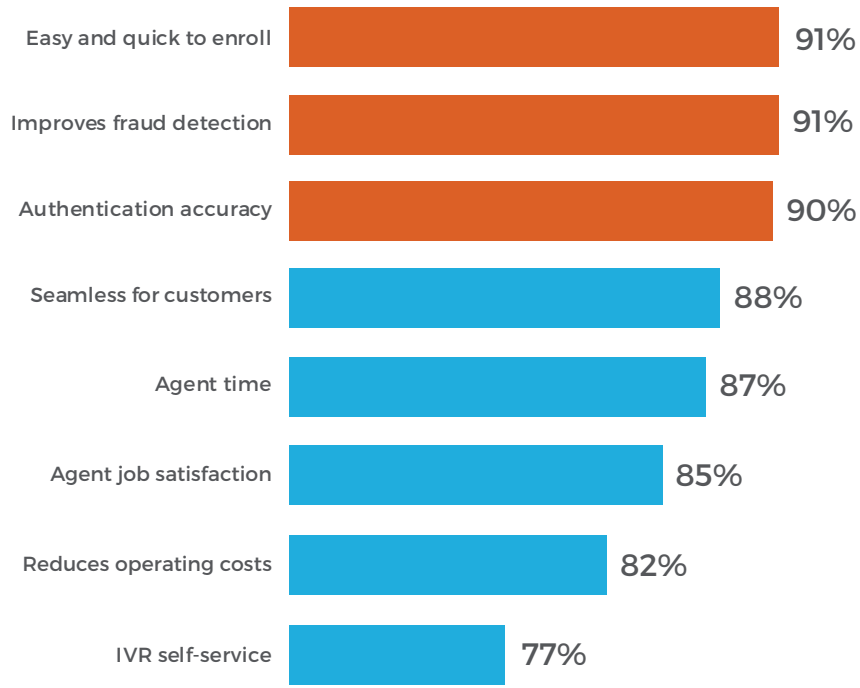
The growing awareness of new authentication technologies appears to have heightened respondents' expectations. Where last year respondents' priorities were mixed, this year three clear front-runners emerged:

Easy user enrollment: For a second year, this topped respondents' priorities. The consistency reflects a simple but essential truth: if callers refuse to enroll in a new authentication approach—due to privacy concerns, impatience, lack of technical savvy, or otherwise—then the technology can't deliver any benefit. We believe this priority drove insight #4. Solutions that authenticate callers in a pre-answer time frame inherently improve the enrollment process. Better yet, some solutions eliminate completely the enrollment process and its inherent friction.

Improve fraud detection: Also consistent with last year's survey, 91% of respondents rated improved fraud prevention as a high priority. When call centers can trust that their good customers are authenticated accurately, they can apply all of their fraud-fighting resources to the remaining pool of unauthenticated callers, a small subset of call volume.[6]

Authentication accuracy: That brings us to the third most important requirement. In an environment where the status-quo, KBA, has failed, respondents will only consider new technologies that can be trusted to authenticate legitimate callers and no one else. Accurate authentication of legitimate callers also reduces the number of false positives; fewer good callers get flagged for fraud investigation.

Technology benefits rated as 'very' and 'somewhat' important



Insight #6

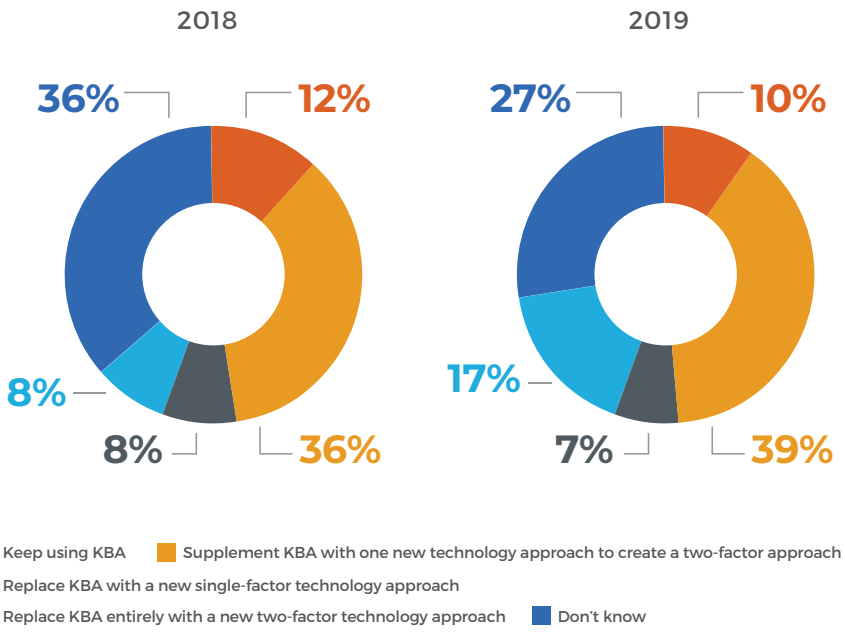
Plans for true multi-factor authentication double

While most respondents still plan to supplement KBA with an additional factor to achieve a multi-factor authentication (MFA) solution—consistent with our 2018 survey—we noticed two noteworthy trends:

1. **The percentage of respondents that did not know their organization's plans for MFA dropped from 36% to 27%**, indicating more organizations are formalizing plans to reduce their dependence on a single-factor KBA approach. They're smart to do so, as this dependency frustrates callers and leaves the call center vulnerable to fraudsters equipped with callers' PII.[7]

2. **The percentage of respondents planning to replace KBA with an MFA approach based on new technologies more than doubled from 8% to 17%.** This likely reflects growing awareness of practical vendor solutions in biometric and ownership-factor authentication. It also coincides with a key recommendation from a commissioned study[8] conducted by Forrester Consulting on behalf of Neustar: "Initial identity verification at onboarding and repeated routine and step-up authentication are all part of establishing a context for a secure transaction. Password-based authentication is just one pillar of login: for step-up authentication, consider using device fingerprints, phone number reputation, and other browser attributes."

Multi-factor authentication approach



As more breached personal information enables more account takeover through the phone channel in the year ahead, we **expect more call center leaders to advocate for a completely new multi-factor authentication strategy.**

1. Call centers: The Fraud Enablement Channel, Aite Group, April 2016. Retrieved February 27, 2019 from https://www.aitegroup.com/report/contact-centers-fraud-enablement-channel
2. TRUSTID 2018 Learnings on Customer Authentication, TRUSTID, Inc., December 2018. Retrieved February 27, 2019 from https://www.trustid.com/wp-content/uploads/2019/03/2018-Learnings-Report.pdf
3. Hackers Are Passing Around A Megaleak Of 2.2 Billion Records, WIRED, January 2019. Retrieved February 27, 2019 from https://www.wired.com/story/collection-leak-usernames-passwords-billions/
4. 2018 State of Call Center Authentication, TRUSTID Inc., 2018. Retrieved February 27, 2019 from https://www.trustid.com/content/report-2018-state-of-call-center-authentication-survey/
5. IDology Sixth Annual Fraud Report Reveals Lowering Customer Friction Is Now #1 Challenge To Fraud Prevention, IDology.com, October, 2018. Retrieved February 27, 2019 from https://www.idology.com/blog/idology-sixth-annual-fraud-report-reveals-lowering-customer-friction-is-now-1-challenge-to-fraud-prevention/
6. The Trusted Caller Flow™ Solution, TRUSTID, Inc., 2018. Retrieved February 27, 2019 from https://www.trustid.com/wp-content/uploads/2019/03/2019_Trusted-Caller-Flows-Solution.pdf
7. Ten Reasons Why Knowledge-Based Authentication Threatens the Modern Call Center, TRUSTID, Inc., 2018. Retrieved February 27, 2019 from https://www.trustid.com/wp-content/uploads/2019/03/2019_the-KBA-Threat.pdf
8. Mitigate Fraud And Consumer Friction With Integrated IDV, a commissioned study conducted by Forrester Consulting on behalf of Neustar, February 2019. Retrieved March 11, 2019 from https://www.risk.neustar/resources/whitepapers/integrated-idv-mitigate-fraud-and-consumer-friction

Conclusions

Call centers become the vector of choice for criminal attacks

Pre-answer authentication emerges as preferred choice

Virtualized calls pose the greatest account takeover threat

Easy customer enrollment remains top requirement

Customer experience and fraud prevention expected to improve in tandem

Plans for true multi-factor authentication double

Appendix A:
Definitions

Pre-answer authentication
A real-time forensic analysis within the telephone network 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 ('voicebio') 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. Static KBA uses challenge questions the caller configures when she opens her account. Dynamic KBA challenges callers with unknown questions drawn from credit bureau or demographic data. When used as the sole factor of authentication, both subtypes are insecure due to the flood of data breaches and proliferation of information available on social media.
- **Inherence** - Using physiological or behavioral identifiers (e.g. fingerprint, retina scan, typing rhythm, or, for the purposes of the phone channel, the caller's vocal tract and intonation) to generate an authentication token.
- **Ownership** - Using a physical item unique to the individual – such as 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.

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.

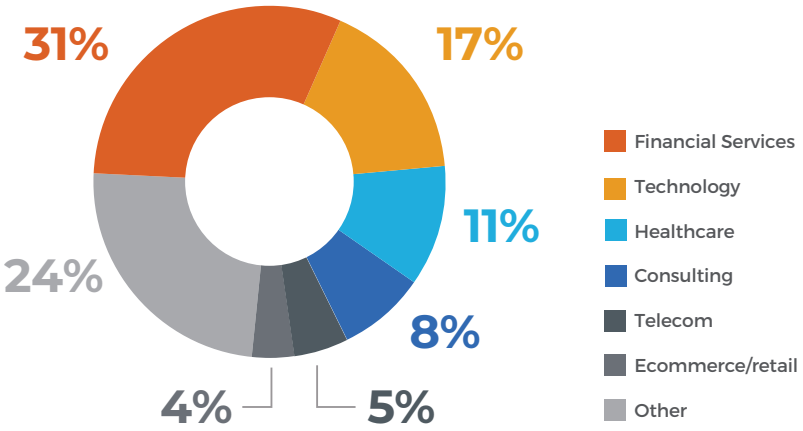
Appendix B:

Survey Respondents

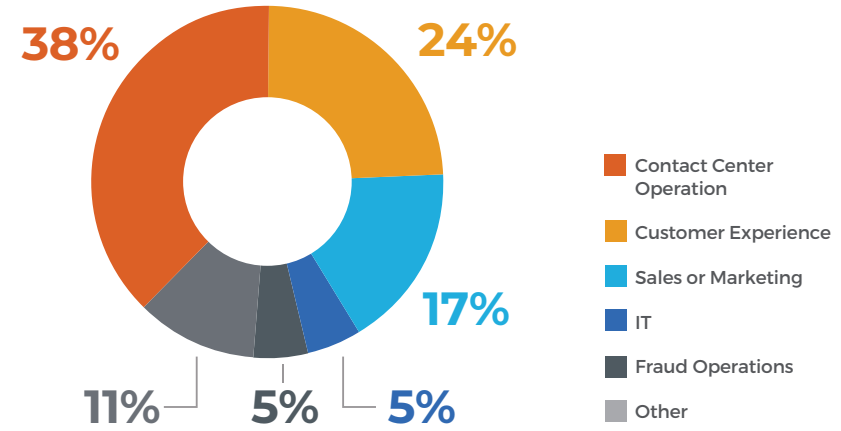
TRUSTID collaborated with Contact Center Week to conduct this survey in January and February of 2019. 134 survey responses were collected online and at the CCW-Winter conference in Nashville, TN. Survey participants included contact center managers, customer experience leaders, IT professionals and fraud managers.

The primary markets represented by respondents were financial services, healthcare, telecommunications and technology firms. Respondents were offered a small monetary incentive as a thank you for time spent on the survey.

Survey respondents by market



Survey respondents by role



About TRUSTID, a Neustar Company

Acquired by Neustar in January 2019, TRUSTID is a leading provider of caller authentication, identity and risk solutions. TRUSTID works with financial institutions and other enterprises to authenticate callers using a caller's phone as an ownership-based authentication token that puts trusted callers into the fast lane, before their calls are even answered, while assessing the risk of others. TRUSTID's inbound caller engagement solutions with Neustar's market leading outbound, phone-centric risk solutions help clients reduce contact center operating costs, improve the customer experience and increase the efficiency of fraud-fighting efforts.

More information is available at https://www.trustid.com

Discover how TRUSTID helps:

Enhance operational efficiency

Improve customer satisfaction

Increase fraud-fighting ROI

About Neustar

Neustar, Inc. is a leading global information services provider driving the connected world forward with responsible identity resolution. As a company built on a foundation of Privacy by Design, Neustar is depended upon by the world's largest corporations to help grow, guard and guide their businesses with the most complete understanding of how to connect people, places and things. Neustar's unique, accurate and real-time identity system, continuously corroborated from billions of transactions, empowers critical decisions across our clients' enterprise needs.

More information is available at www.home.neustar