TRUSTID
A Neustar Company

SURVEY

2018 State of Call Center Authentication

The decline of knowledge-based authentication accelerates as contact centers seek new ways to improve operational efficiency, customer experience, and fraud-fighting ROI.

Executive Summary

TRUSTID's first annual survey on contact center authentication reveals that knowledge-based authentication (KBA) remains the de facto authentication method, even though **40% of respondents doubt KBA's accuracy.** As data breaches continue to flood the dark web with consumers' personal information, expect that number to rise. That may be why one third of contact center leaders expressed dissatisfaction with their current authentication approach (and 50% of those in financial services).

The market appears ready to move in a new direction. While new authentication technologies operate in less than 20% of the contact centers represented, over half of the respondents are now familiar with these new approaches. They are informed and motivated for change, but first they must be convinced that the new approaches are up to the challenge.

Respondents expect a lot from the alternatives. At the top of the list is enrolling customers quickly and easily. If callers won't use a new approach, none of the other potential value will be realized. This insight also reflects a market-wide understanding of the challenges that some new approaches, such as voice-biometrics, have had in garnering customer participation. This insight favors technologies, like pre-answer authentication within the phone network, that do not rely on customer enrollment.

The market wants to make life easier for agents. 92% of respondents want new technologies to reduce agent time spent on authentication. **80% want authentication to be completed pre-answer or in the interactive voice response (IVR) portion.** New approaches must be fast and easy for callers to complete by themselves.

While 27% of respondents will have a multi-factor approach in place by the end of 2018, the majority don't have a firm schedule for implementation. Few want to replace KBA entirely. Of the respondents that have a direction in mind, **almost 6 in 10 intend to supplement KBA with one new technology to create a multi-factor solution, rather than replace KBA altogether.** New technologies that integrate with KBA easily and minimize its use will be poised for gain.

Who provided the basis for this report's insights*

127 **Contact center professionals surveyed:** most of whom work in either customer experience or operations.

60% **Respondents representing industries with mature authentication postures:** financial services, ecommerce and telecommunications.

90% **Respondents who consider authentication either 'very important' or 'somewhat important' to their customers' experience.**

*See Appendix B for more detail.

Insight #1

Knowledge-based authentication remains the default option

The overwhelming majority of respondents' contact centers continue to authenticate their callers by asking about personal information: knowledge-based authentication (KBA).

This is the status quo for several reasons:

- **Inertia:** Changing authentication methods inherently requires effort.
- **Budget:** Alternate methodologies come with implementation and training costs.
- **Familiarity:** KBA has been sufficient for decades. This is changing. Due to the spate of data breaches in recent years, fraudsters can easily buy personally identifiable information (PII) on the black market, supplemented with the proliferation of information available on social media, reconstruct callers' identities, and answer "out of wallet" challenge questions that used to be secret.

As the rest of this report shows, contact center leaders are beginning to consider options to supplement KBA for greater efficiency and customer experience. Since adoption of new technologies – such as pre-answer call analysis and voice-biometrics – has yet to pass the 20% adoption level, there's still opportunity for first-mover advantage in the market.

Authentication Approach in Use

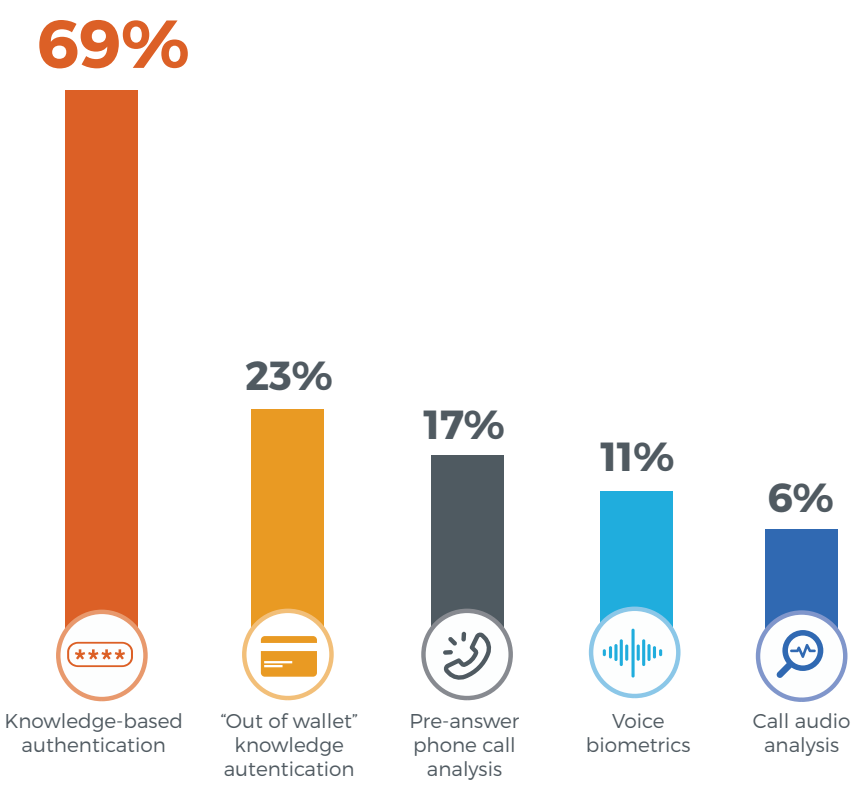


FIGURE 1. Knowledge-Based Authentication remains the status quo

Insight #2

There is widespread lack of confidence in knowledge-based authentication

Only 10% of all respondents felt very confident in KBA's ability to authenticate callers accurately. **38% of respondents expressed little to no confidence.**

Over half of financial services respondents indicated they lacked confidence in KBA. This is especially distressing, given the essential role of authentication in serving callers at financial institutions' contact centers and keeping out fraudsters.

Contact center leaders understand how easy it is for a caller to impersonate a customer. Fraudsters have been pursuing callers' PII since KBA became the primary means of authentication in contact centers, and continue to augment their efforts with every data breach and through the proliferation of social media participation.

How confident are you that knowledge-based authentication alone can accurately authenticate your customer callers?

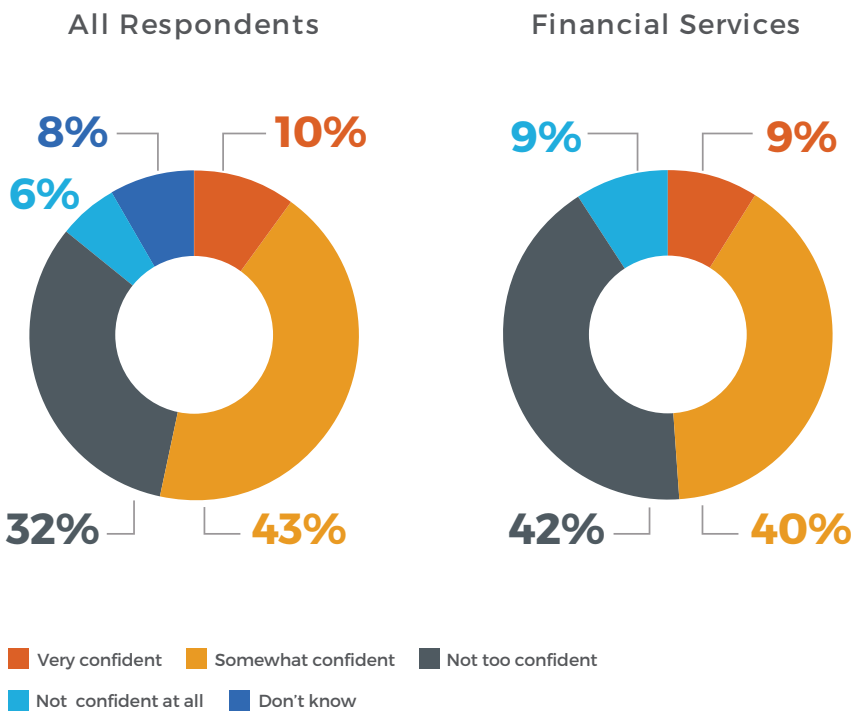


FIGURE 2. Widespread doubt in knowledge-based authentication

Insight #3

There is strong dissatisfaction with existing authentication approaches

Thirty-one percent of respondents are somewhat or very unsatisfied with their current authentication methods. The numbers are even worse in the financial services industry, with 42% noting dissatisfaction with their current methods.

Since KBA represented 92% of contact centers' authentication methods (see Figure 1), we conclude that that dissatisfaction relates directly to the use of KBA.

The reasons for this dissatisfaction boil down to three possible sources:

- **KBA lengthens agent average handle time:** It extends every call by 30 to 90 seconds (for typical and high-risk calls, respectively). Longer calls cost more, drive up staffing needs to handle call volume and squander callers' goodwill.
- **KBA degrades customer experience:** Callers expecting speedy service must endure identity-interrogation before getting help.
- **KBA gives a false sense of security:** Because fraudsters can buy customers' PII on the black market, account takeovers through the phone channel remain a persistent threat.

How satisfied are you with your current method(s) to authenticate callers?

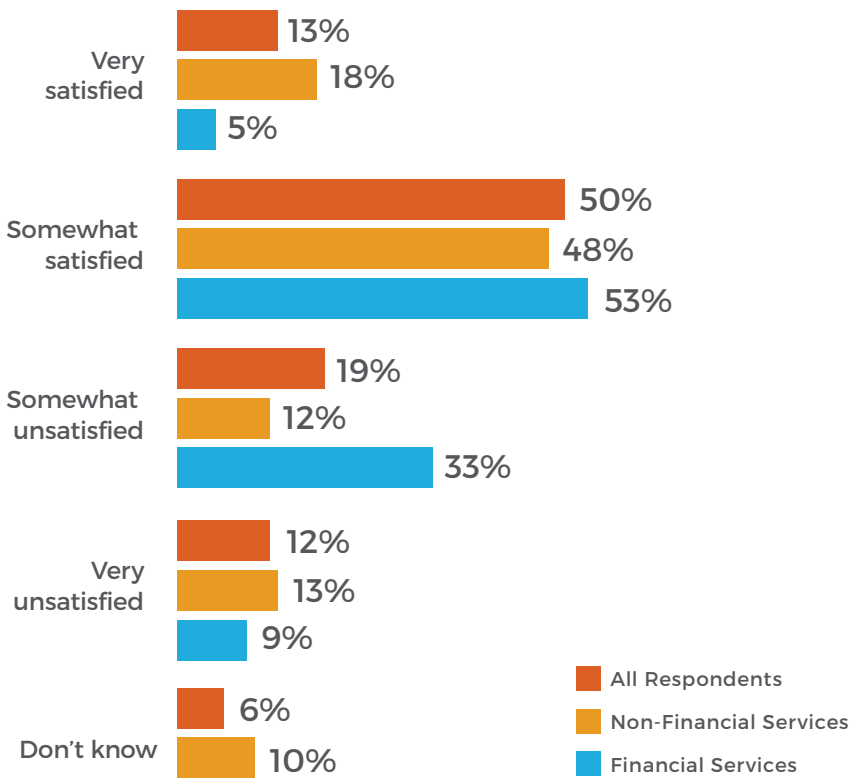


FIGURE 3. Strong dissatisfaction with knowledge-based authentication.

Insight #4

The market is poised for new technology adoption cycle

Though KBA remains the most common authentication method today, awareness of other options is growing.

Over half the respondents indicated they are 'somewhat' or 'very' familiar with both voice-biometrics and pre-answer phone call analysis.

Combined with the widespread dissatisfaction with KBA, this signals that the market is poised for a shift. For every respondent who uses an alternative to KBA, three times that many are aware of the alternatives.

Before a mass transition away from KBA is possible, the new approaches must prove that they can meet the market's needs.

How familiar are you with these approaches to call center authentication?

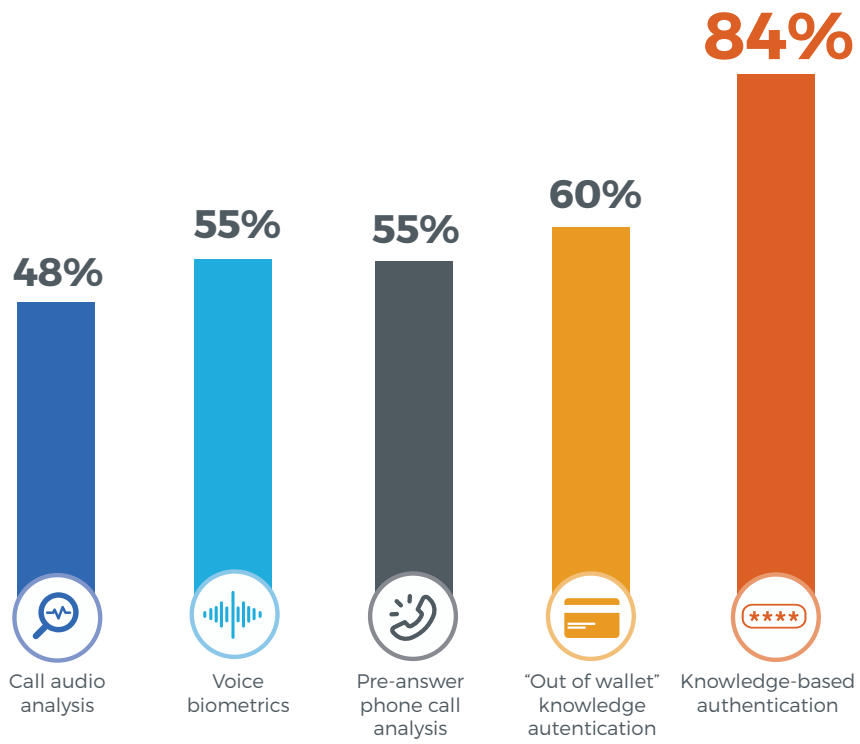


FIGURE 4. Alternatives to knowledge-based authentication gaining awareness.

Insight #5

Customer adoption and use is critical for a new technology to thrive

Respondents ranked 'quick and easy customer enrollment' as the most important criteria for emerging authentication technologies.

If callers refuse to enroll in an authentication method, then the technology does no good for either the contact center or its callers. While other attributes such as authentication accuracy and ability to reduce operating costs are also important, realizing these benefits depends on strong customer adoption.

This may explain, in part, why KBA remains the dominant authentication strategy in spite of its inherent weaknesses. With KBA, there is no need to enroll customers. Their PII is on file (making it an attractive target for hackers), and callers just need to prove that they know it.

Difficulty meeting this need may explain some of the lag in replacing KBA. With technologies that require enrollment, such as voice-biometrics, callers may be reluctant to enroll, or get frustrated during an enrollment process that can last up to seven minutes and drop out.

With regards to caller enrollment, call center leaders prefer an authentication method that wouldn't use any PII, nor require any customer involvement, and could instantly process 100% of calls upon activation. Pre-answer caller authentication is the only method currently on the market meeting all of these requirements.

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

FIGURE 5. Contact center leaders share their wishlists for a new authentication method.

Insight #6

There is a strong preference to complete authentication before agent engagement

Given that agent-based authentication often represents 20% of the cost and duration of a call, it's no surprise that removing agents from the authentication process was one of respondents' most-desired outcomes of a new authentication method.

Only 18% wanted agents involved in authentication. This is consistent with the desire for alternate technologies to reduce agent time on authentication, reduce overall call times and improve agent job satisfaction (see Figure 5).

Pre-caller authentication and voice-biometrics are the most well-known new technologies the market will consider (see Figure 4).

To perform, voice-biometrics requires a sample of the caller's voice. That is impossible to collect before the call is answered, and difficult to complete in an IVR setting.

That leaves pre-answer call analysis. Because it completes an authentication step without the caller's awareness, it requires no user enrollment, nor does it add any time to the call's duration. Pre-answer call analysis would seem poised for gain in the market.

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

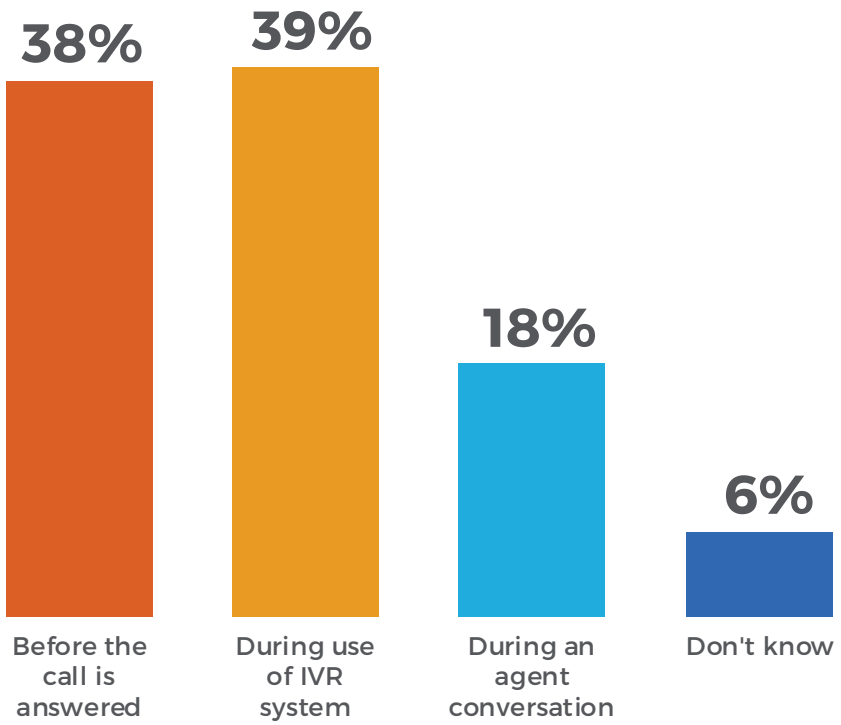


FIGURE 6. Respondents recognize the benefits of removing agents from the authentication process

Insight #7

Multi-factor: Respondents will add and improve, not rip and replace.

In spite of respondents' dissatisfaction with KBA, a significant number plan to supplement KBA with one new technology to create a two-factor solution.

This incremental direction means that new technologies will need to work well with KBA, in addition to delivering on the other criteria noted as important for emerging authentication technologies (see Figure 5).

To thread this needle, a new authentication factor should simplify the entire authentication process by reducing the number of KBA questions. Instead of agents interrogating callers with three or four complex questions, callers should be able to enter a simple data point – for example, their zip codes – in the IVR.

On the other side of the adoption curve, another significant portion of respondents didn't know how their organization planned to approach multi-factor authentication, nor knew when that might change. This may reflect the lingering lack of awareness about alternatives in the market (see Figure 4), though it's worth pointing out that this group did not believe their contact centers would keep using KBA by itself.

Which statement best describes your plans to become multi-factor authentication compliant?

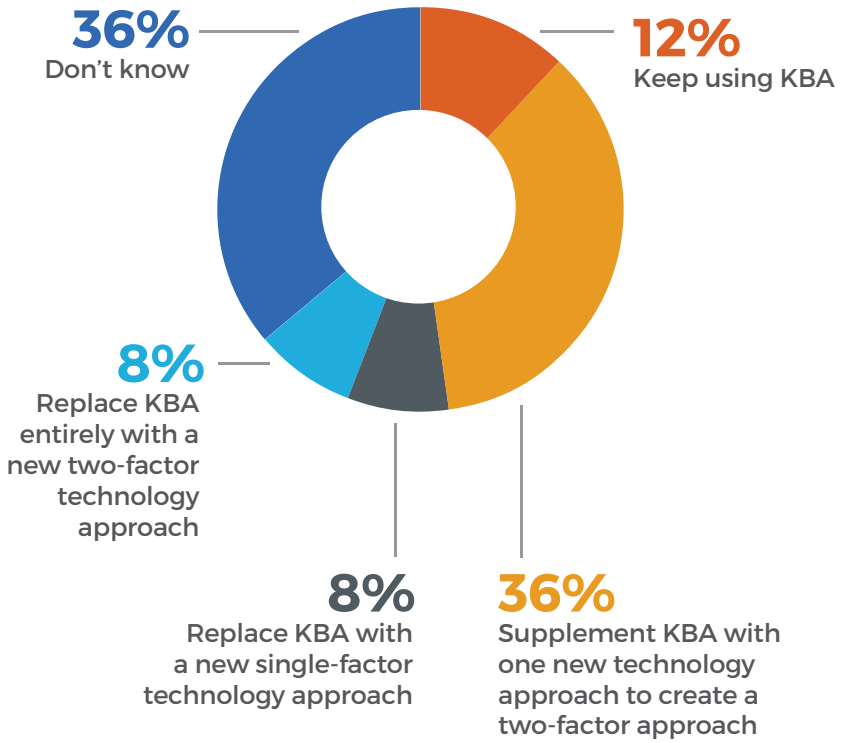


FIGURE 7. Respondents thinking about authentication plan to augment their current system.

Conclusions

KBA remains the dominant authentication approach.

Contact center leaders doubt KBA's accuracy.

There is dissatisfaction with the current state of authentication.

The market is ready to adopt new authentication technologies.

New technologies must be easy and quick for customers to adopt.

Callers should be able to authenticate before speaking with an agent.

The preferred path to multi-factor authentication will include KBA and a second complementary factor.

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 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.

Call audio analysis
Combines multiple acoustical anomalies from the call in an attempt to identify the originating device.

The three factors of authentication

- **Knowledge -** Asking callers questions about personal information. Insecure due to the flood of data breaches and proliferation of information available on social media.
  - Account-based - Asking callers to state information related to their accounts (e.g. account number, PIN, etc.)
  - Out-of-wallet - Asking callers to state information unrelated to their accounts (e.g. amount of most recent mortgage payment, mother's maiden name, etc.)
- **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.

Appendix B:

Survey Respondents

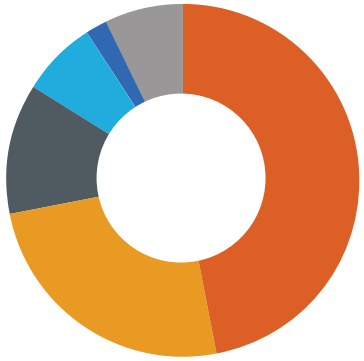
Role

Survey respondents occupy key positions in their contact centers. This distribution of respondents' roles represents a typical mix of roles involved with the purchase and use of authentication in a contact center.

- 34% Financial Services
- 16% Telecom
- 10% Consulting
- 9% Ecommerce/retail
- 9% Technology
- 22% Other

Industry

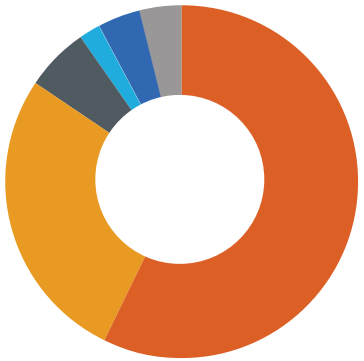
Respondents represent a range of industries. The prevalence of responses from industries like financial services, ecommerce and telecommunications ensures that the survey results are founded on opinions based on familiarity with authentication in the contact center.



- 47% Contact Center Operations
- 25% Customer Experience
- 12% Sales or Marketing
- 7% IT
- 2% Fraud Operations
- 7% Other

Authentication Importance

Over 90% of respondents consider authentication to be important to overall caller satisfaction.



- 59% Very important
- 28% Somewhat important
- 6% Not too important
- 2% Not important at all
- 1% Don't know
- 4% Do not authenticate callers

About TRUSTID's pre-answer caller authentication solution

TRUSTID identifies trusted callers before they hear "hello." Our pre-answer caller authentication draws upon a forensic analysis of each processed phone call – across the telephone network – right down to the handset of each caller in real-time.

This automatic, highly accurate approach reduces operating costs, increases customer satisfaction, and makes fraud-fighting efforts more efficient.

TRUSTID's pre-answer authentication service strongly matches the needs described by survey respondents: It requires no customer enrollment and can therefore be adopted for use on 100% of calls on the day of activation. Because it authenticates the caller pre-answer, it increases self-service in the IVR and significantly reduces the time agents and callers spend on authentication. Finally, it allows call centers to augment knowledge-based authentication to create a simple, strong two-factor solution.

Privately held and VC-backed, TRUSTID is headquartered in Portland, Oregon.

Visit TRUSTID.com to discover how TRUSTID:

Enhances operational efficiency

Improves customer satisfaction

Increases fraud-fighting ROI

Contact TRUSTID Today.

TRUSTID, Inc.
4500 Kruse Way, Ste. 350
Lake Oswego, OR 97035

(503) 715-0850
info@trustid.com
www.trustid.com

TRUSTID
A Neustar Company