neustar
A TransUnion® Company

Knowledge-based Authentication Threat

Ten Reasons Why Knowledge-based Authentication Threatens the Modern Contact Center

Table of Contents

Executive Summary

Enterprise contact centers most popular authentication strategy is outdated and broken.

Knowledge-based authentication (KBA) seeks to prove the identity of a caller through knowledge of personal information ("Account number, PIN, and mother's maiden name, please.").

Over reliance on this method now represents a material risk to contact centers and their relationships with callers.

KBA is costly and time-intensive – especially when seconds count for average handle time (AHT) – and is a huge frustration for the customer. Callers do not like the 'identity interrogation.' It's a waste of money for contact centers. Finally, criminals have no problem circumventing KBA and committing fraud.

Regulatory bodies are calling for more advanced authentication. Management wants "frictionless authentication." Customer satisfaction, security, profitability and brand reputation are at risk. Brands need to move in a new direction quickly.

This paper details 10 reasons why KBA is unfit for modern contact centers, ranging from excess costs to poor customer experience to weak security. It concludes with an overview of a solution that reduces operating costs, delivers exceptional customer care, and improves fraud-fighting ROI: pre-answer authentication.

The death of knowledge-based authentication.

For years, KBA has been the cornerstone of authenticating customers over the phone channel.

The majority of contact centers still rely on KBA as the primary authentication tool for their broad spectrum of callers – from premiere accounts all the way down to fraudsters.

Today's phone channel security questions – the usual personally identifiable information (PII) as well as more elaborate "out of wallet" questions such as previous home addresses or amount of last mortgage payment – attempt to validate the caller's identity. However, this fraud-fighting strategy drives up costs, undermines customer service, and fails to stop criminals.

Once the star of customer authentication, KBA no longer predicts identity. Data breaches such as Equifax's[1], Yahoo!'s[2], and River City Media's[3] have exposed millions of consumers' PII, including answers to KBA questions. Fraudsters have little trouble acquiring[4] callers' PII on the dark web and perpetrating[5] sophisticated account takeover.

Let's explore in detail 10 ways that KBA fails modern contact centers and their callers

Ten Reasons Why KBA Threatens The Modern Contact Center

1 INCREASES AVERAGE HANDLE TIME

In 2016, "86% of calls were reported to be authenticated by agents. On average, it takes 32 seconds to go through knowledge-based authentication for a low-risk interaction. Using these statistics, the overall cost of agent-handled security and identification checking has been estimated at $8 billion per year."[6]

Assuming that a typical agent call costs $1.00/minute, shortening caller identification by 20 seconds would save about $0.35 per typical call. The savings would be greater for high-risk calls where authentication can take up to 120 seconds.

30–90 seconds

Delay KBA adds to typical and high-risk calls, respectively

2 REDUCES IVR CONTAINMENT

By the time your customers call your contact centers, they're frustrated. They want to resolve their problem quickly and get on with their day. If they have trouble authenticating, they're likely to become even more frustrated and to request a transfer to a live agent.

That frustration incurs two costs: one's immediate and tangible (below), the other is slower and insidious (see "#7 - Frustrates agents and leads to turnover").

A typical agent call costs $1.00/minute. IVRs cost $0.10/minute. Therefore, an average four-minute call transferred from IVR to an agent costs an extra $3.60 per call. Every 1,000 transferred calls per day costs $3,600 per day or more than $1.3 million per year.

$8B/year

Estimated overall cost of agent-handled security and identification checking in 2017[6]

3 EXACERBATES CALLERS' FRUSTRATION

The phone channel has entered a new era. The emotional response callers have during and after phone interactions has become a significant variable for brands' competitive advantage. If they are dissatisfied they will complain on social media and review sites, causing long-lasting brand damage. The ability to service customers' needs represents a significant competitive differentiator and driver of growth.[7]

When callers have a problem they can't resolve themselves – account lockout or answering a fraud alert, for example – they're stressed by the time they speak with an agent. They don't want to answer knowledge-based authentication questions. They want help.

Brands that understand this shift and alter their business processes to improve the customer experience and ensure consumer safety will gain a hard-won competitive advantage that can improve top- and bottom-line performance, and build trust and brand loyalty.

In spite of this opportunity, contact centers continue to grill callers with personal questions at the onset of a call — before they can clarify their needs. This makes the telephone channel an unpleasant experience, threatens the goodwill of customers, and squanders agents' best chance at establishing rapport and selling additional products and services.

4 MISSES MODERN SELF-SERVICE EXPECTATIONS

The Internet has revolutionized the way customers interact with brands. It has simplified customer support and opened new ways to maintain accounts, make purchases, and perform other transactions.

Where technology once favored companies it now empowers customers. They expect their experiences over the phone channel to be as smooth as their online communications. Unfortunately, contact centers' standard treatment of callers misses consumer expectations by a wide margin.

Why don't contact centers offer more self-service options in their IVRs (e.g. money transfers, PIN resets, and even international travel notifications)? Fear of fraud and account takeover.

Contact centers have constrained the actions that can be completed in their IVRs because fraudsters have been so successful at repeatedly beating weak knowledge-based authentication with callers' PII acquired on the darkweb. If callers want to conduct higher-risk business such as money transfers, credit card replacements or address changes they must transfer to an agent.

Customers expect their experiences over the phone channel to be as smooth as their online communications. Unfortunately, contact centers' standard treatment of callers misses consumer expectations by a wide margin.

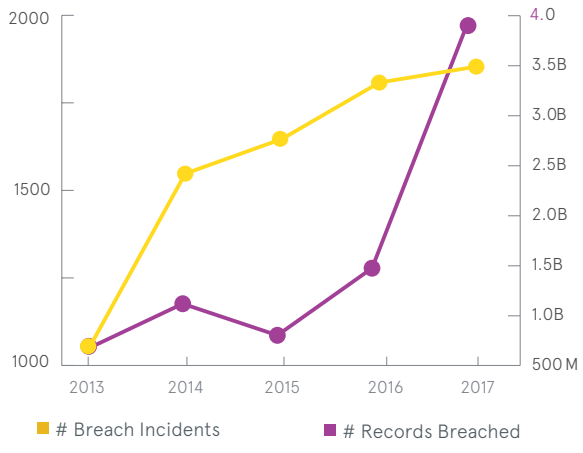
5 FAILS TO STOP FRAUDSTERS

Fraudsters have been pursuing callers' PII since KBA became the primary means of authentication. Once criminals can answer KBA questions correctly they can socially engineer your agents, commit fraud in your contact center, and leave you to make costly amends with irate, vocal customers.

It all begins with your callers' PII. Due to the spate of data breaches in recent years (see graphic to the right), fraudsters can easily buy PII on the black market and reconstruct your callers' identities.

Even if your organization is doing everything right to protect callers' PII, it won't matter. Hackers have breached your callers' PII stored by other organizations. They're selling it to fraudsters targeting your contact center. KBA won't stop them.

2017 GLOBAL CONTACT CENTER SURVEY[8]



6 ENCOURAGES DATA BREACHES

The value of PII has made large databases of consumer information irresistible to hackers. Breaches such as Equifax's and Anthem Insurance's show that any organization is susceptible, and that attackers have become more sophisticated.

Full credit reports[9] and electronic health records[10] fetch more on the black market than stolen credit card numbers. This is due in part to the fact that consumers' PII underpins KBA in many contact centers.

Hackers will only steal PII for as long as fraudsters will buy it. The moment KBA becomes obsolete our PII will lose its value on the black market.

30x

Digital identities reconstructed from data breaches fetch significantly more on the dark web than a U.S. credit card number

7 FRUSTRATES AGENTS AND LEADS TO TURNOVER

In mid-2017, the mean annual rate of contact center agent attrition in the US was 30%.[11] One contributing factor to agents' stress levels: knowledge-based authentication. Frustrated callers don't want to be interrogated, they want to resolve their problems quickly.

However, by complying with KBA protocol, agents provoke and incur callers' frustration hundreds of times every day. ("You should know who I am! I've been a loyal customer for the last 10 years! It's the 21st century for goodness sake!")

This deteriorates agents' job satisfaction and drives up turnover. With the expense of replacing contact center agents ranging from $5,000-$8,000, this hidden cost of KBA represents a significant, silent drain on the contact center's bottom line.

Conversely, your callers benefit when agents can begin problem solving faster. Happier agents make better brand representatives and are less likely to quit. The more senior agents become the more effectively they can help callers with complex problems.

100x/day

By complying with KBA protocol, agents provoke callers' frustration 100's times every day

8 DOES NOT MEET COMPLIANCE REGULATIONS

In a June 2011 report[12], the Federal Financial Institutions Examination Council (FFIEC) stated[13] that: "institutions should no longer consider such basic challenge questions [like mother's maiden name], as a primary control, to be an effective risk mitigation technique."

In June 2017, the National Institute of Standards and Technology (NIST) expressly stated that "Knowledge based authentication, where the claimant is prompted to answer questions that can be confirmed from public databases, also does not constitute an acceptable secret for e-authentication."

All contact centers using KBA should take note, not just regulated institutions. If contact centers connected to more lucrative organizations become more difficult for fraudsters to compromise, those fraudsters will look for easier targets. They will likely look first to contact centers that still rely on KBA.

9 WON'T STOP INSIDER FRAUD

The Wells Fargo scandal of 2016 showed that KBA provides no protection from internal abuse. Without customers' permission, thousands of employees submitted applications for more than 500,000 consumer credit card accounts and 1,500,000 million deposit accounts.

The bank's reliance on KBA made the debacle possible. The delinquent employees had enough access to consumers' PII to open the accounts.

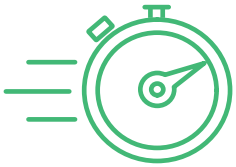
If Wells Fargo had followed guidelines on multi-factor authentication across all channels, there would have been substantially less fraud.

KBA made possible the Wells Fargo scandal of 2016

10 WASTES FRAUD-FIGHTING RESOURCES

Today, all callers are greeted with suspicion. Why? Due to phone spoofing, social engineering, and all the data breaches, fraudsters call in well prepared to answer KBA questions. Most contact centers struggle to identify the few fraudsters that attempt to hide among the large volume of legitimate callers.

As a result, the fraud department wastes most of its time sifting through a large subset of legitimate callers to find a few fraudsters, the proverbial "needles in the haystack." This adds expense and friction, requires expensive personnel, and inconveniences customers caught as false positives.



10 sec.

Time required for multi-factor authentication when using a pre-answer authentication token

KBA aggravates the potential for human error. Once contact center agents are tricked or intimidated by callers, or they simply become tired, they may stray from KBA protocol and enable fraud.

Conclusion

KBA drives up costs, alienates callers, and fails to stop criminals. If you're spending money to interrogate callers, and you still aren't sure if your agents are speaking with customers or criminals, it's time to reevaluate your business processes.

Instead of KBA, implement pre-answer authentication. Before a call is even answered, verify that it's coming from a trustworthy phone and tag it as valid.

A pre-answer authentication token reduces time spent for multi-factor authentication to less than 10 seconds. That's a significant improvement in efficiency, customer experience, and security over the current industry standard: using multiple KBA questions.

As a result callers will resolve their issues 20-80 seconds faster with less frustration, more self-service options and better security. By eliminating your primary reliance on KBA, fraudsters will be left out in the cold.

The first steps are simple: recognize that KBA represents an outsized liability in the modern contact center, and commit to using pre-answer authentication. Doing so will bring an immediate, indelible benefit to your contact center and your callers.

Begin authentication before answering the call.

To learn more visit:

www.trustid.com

Ten reasons why knowledge-based authentication threatens the modern contact center:

1. Increases Average Handle Time
2. Reduces IVR containment
3. Exacerbates callers' frustration
4. Misses modern self-service expectations
5. Fails to stop fraudsters
6. Encourages data breaches
7. Frustrates agents and leads to turnover
8. Does not meet compliance regulations
9. Won't stop insider fraud
10. Wastes fraud-fighting resource

1 Goldman, D. (2017, September). Equifax hack: What's the worst that can happen? Retrieved November 1, 2017 from http://money.cnn.com/2017/09/11/technology/equifax-identity-theft/index.html

2 Newman, L. (2017, October). Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts. Retrieved November 1, 2017 from https://www.wired.com/story/yahoo-breach-three-billion-accounts/

3 Vanian, J. (2017, March). Major Spammer Accidentally Leaks Data on a Billion People. Retrieved November 15, 2017 from http://fortune.com/2017/03/06/spammer-leaks-data/

4 Kitten, T. (2015, June). Breached PII: Why KBA Has to Go. Retrieved November 1, 2017 from http://www.bankinfosecurity.com/blogs/breached-pii-kba-has-to-go-p-1900

5 Popper, N. (2017, August). Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency. Retrieved November 1, 2017 from https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html

6 Contact Babel: The US Contact Center Decision-Makers' Guide (2017). Retrieved October 12, 2017 from http://www.contactbabel.com/pdfs/july16/US-CC-DMG-2017.pdf

7 Deloitte: 2017 Global Contact Center Survey. (2017). Retrieved October 12, 2017 from https://www2.deloitte.com/us/en/pages/operations/articles/global-contact-center-survey.html

8 Figures for 2017 have been annualized based on reports from the first half of the year.

9 Goldman. Equifax hack.

10 Humer, C. & Finkle, J. (2014, September). Your medical record is worth more to hackers than your credit card. Retrieved January 16, 2018 from https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

11 Contact Babel. US Decision-Makers' Guide (2017).

12 Federal Financial Institutions Examination Council. (2011, June). Retrieved January 16, 2018 from https://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf

13 National Institute of Standards and Technology. (2017, June). Retrieved January 16, 2018 from https://pages.nist.gov/800-63-3/sp800-63b.html

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-371770-01.11.2022