A DEEPER LOOK AT AUTHENTICATION AND FRAUD PREVENTION

"Start by thinking of things like account number and social security number as identity only; these are not paths to authentication or verification in today's data-compromised world."

Contact Center Pipeline

A DEEPER LOOK AT AUTHENTICATION AND FRAUD PREVENTION

Use a multi-layered approach that cuts across people, process and technology.

BY Lori Bocklund, Strategic Contact

Optimizing authentication and preventing fraud are "hot topics" in the industry. I had the pleasure of facilitating a panel on the topic at the ICMI Contact Center Demo in September, joined by two major vendors in this space—Patrick Cox, CEO of TRUSTID, and Vijay Balasubramaniyan, CEO and CTO of Pindrop. Both companies leverage network capabilities to assess call integrity and validity while improving the customer experience. And while the two compete for business, they exist side-by-side in some implementations.

This article highlights key learnings from these discussions as well as project work we have been doing to tackle this ubiquitous challenge.

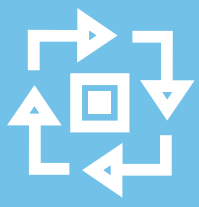
Key Takeaway

I'm going to start with the key message that anyone exploring the topic should know. **You *must* use a layered approach.** There is no silver bullet to improve authentication and prevent fraud. Moreover, the layers cut across people, process and technology. They may leverage any of the following types of authentication: Knowledge (what you know), Possession (what you have), and Inherence (who you are).

Knowledge-based authentication (KBA), has been the approach for most centers until now; however, it is terribly flawed and vulnerable. "KBA has to go away," according to the panelists since so much information has been compromised and can be obtained through the "dark web" and "social engineering." In case these are unfamiliar terms to you, let me share my reaction to seeing and hearing about them: It is scary to know there is a parallel marketplace to our much loved and used "World Wide Web" where thieves who steal information repackage and sell it to other nefarious individuals to pursue their evil tasks. And there are wicked people who specialize in extracting information and are increasingly calling your very helpful customer service representatives (and perhaps your customers!) because the other channels (including web, mobile and face-to-face) have become more difficult to penetrate.

Even if the "dark web" and "social engineering" weren't threats, Vijay from Pindrop admonishes us not to outsource authentication to customers by asking a bunch of questions. That approach results in long handle times and frustration for representatives and customers. Moreover, it's not a sure-fire way to authenticate, much less prevent fraud. Patrick

People, Process and Technology Combine for Success



The challenges of authentication and fraud prevention know no boundaries for size or other demographics. Clearly not all centers can afford the latest technology, yet the "multi-layered" mantra means you can start now even without big budgets or project teams. Use existing technology like CTI and CRM well—pop screens (and warnings!)—guide people through authentication workflows, capture structured and unstructured information about suspicious contacts, and pass information with transferred calls. Define and deploy well-structured processes and reinforce them through quality monitoring and coaching and development. Conduct analysis of IVR data, other channels, contact handling and end-to-end/cross-departmental activity.

All of this requires the proper resources that can help optimize processes and use of technology on an ongoing basis. A model we like is a Business Analyst who understands the technology, the workflows, and the authentication and fraud challenges. That individual can join forces with those who handle the online and mobile app to leverage these tools for authentication and seamless channel crossing, and work closely with the fraud/risk management team to tackle the challenges and hopefully stay one step ahead of the bad guys.

says TRUSTID sets a goal of getting 90% of customers into a "trusted flow" and applying more rigor to the remaining 10%. Both companies offer solutions that don't require enrollment and can add value in identifying the first-time caller.

So with all these problems with knowledge, multi-factor authentication (MFA) is the better approach, and the push is on for possession (e.g., ANI/caller ID, phone device) and inherence (e.g., biometrics). TRUSTID calls the phone an "ownership identity token" as the characteristics of the number (ANI) and carrier information that both companies examine provide possession-based authentication. Going further into fraud detection, Pindrop can look at the characteristics of the sound, which they label "phoneprinting™." While it takes a little time to evaluate, this approach can offer insights even when ANI doesn't. A further step evaluates the voice print, matching it to your very own "blacklist" database of recognized fraudsters. Pindrop also has a "consortium of bad guys" and can enable assessments of the phone print against a shared database, offering a broader view in the fight against evil!

These front-end tools enable a center to then perform a *risk-based* level of authentication with the representatives. Using the indicators from the network services, the reps can make informed decisions and proceed based on transaction type, account type, amounts involved or other factors.

Where Does the Technology Fit?

So if this all sounds intriguing, the question remains of whether it is a fit for your center. Both vendors target financial services as early adopters, with a high percentage of the big banks, insurers and credit card companies on board. But authentication and fraud prevention applies to all vertical markets, and the vendors have delivered solutions in healthcare, retail, travel, telecom, government and more. Both vendors see greater value in these solutions when an IVR front-ends the calls and plays a role in authentication and self-service, increasing success rates.

The next question is size, and up until now these solutions have been the realm of big centers with hundreds of agents and millions of calls annually. But again, the problem is not exclusive to these demographics. So the vendors are moving downstream by partnering with value-added resellers (VARs) that can deliver the capabilities as part of a broader solution. **THE SIDEBAR** shares more about how centers of all sizes can make headway.

I asked the panelists who the buyer is since we see others beyond the contact center engaged in solving the problem. They indicated it is typically the center because of the great value to their operation—specifically, lower handle time can have a big impact on labor costs. Most centers take something like 30 seconds to identify someone; that time can be way longer for suspicious situations or high risk scenarios. We've seen the "slippery slope" as risks increase where centers start to apply the most rigorous (and therefore longest, and most painful) authentication process to *all* callers. That worst-case scenario makes for a strong business case to put these technologies in place while also making great strides in improving the customer experience. As an added bonus, the fraud risk and costs go down, too!

The line of business with profit and loss responsibility (i.e., the ones that absorb fraud losses) should be part of the decision processes, along with teams variously labeled Fraud, Risk Management or Compliance. They benefit by reducing the number, and cost, of fraud investigations.

The bottom line is these tools can have a strong, tangible business case because of the cost of authentication and fraud. If you need data to make the case in your company, check out the resources the two vendors offer on their websites.

Not Fun Facts!

- FROM PINDROP: Fraudulent calls per legitimate call: 1 in 937 as of 2016 (and rising fast!)
- FROM TRUSTID: 100% of Identity Fraud occurs after Weak Authentication

Take a Deeper Dive to Build a Strategy

If you face challenges related to authentication and fraud, your "call to action" is to build and execute a strategy *now*, before you incur unnecessary costs and put innocent customers through the ringer.

Start by thinking of things like account number and social security number as *identity* only; these are not paths to authentication or verification in today's data-compromised world. They are vulnerable to theft and not enough to authenticate and trust that customers are who they say they are. Similarly, date of birth, mother's maiden name, address and other "knowledge" are relatively easy for fraudsters to secure. And all those other questions about phone passwords (that are often forgotten), recent activities and favorites just make everyone want to scream. Accept these realities as you build a strategy that is customer-friendly and protects your company at the same time.

Your strategy should address various activities that might raise a flag. For example, companies experiencing fraud can have many calls to the IVR, or see very long calls. Pindrop uses phrases like "identity compiling" and "using IVR for reconnaissance" to describe how bad guys are gathering information. Repeat callers may also fish around with multiple agents to get info, because the bad guys know agents want to help customers! The vendors refer to "velocity" from a given number, showing lots of calls coming in from a single ANI or Caller ID. They also see omnichannel fraud with bad guys trying different paths into an account, so tracking across channels including online, mobile and chat is pretty important, too.

Internal transfers are another tactic. As Patrick of TRUSTID says that you should never use an internal number as a "token" (i.e., indicator of valid call). Fraudsters try to get to individuals in other departments (e.g., IT, HR) and then say, "I'm sorry, I am in the wrong place, please transfer me to the call center…" You need to shut down this alternate path and capture the contact record of the attempt.

All this data about contact history needs to

go somewhere. It should be integrated into a CRM (or similar) application to track all contacts and note suspicious activity. Ideally, the various applications (e.g., IVR, network service, desktop tracking) should feed information into a common system through standard APIs (application programming interfaces), and agents should have ready access to it, ideally through structured data, not just notes. The best systems will use business rules that look at this data to route suspicious callers to the appropriate staff and pop clear warning signs at agent desktops.

As another defense, any kind of change in contact information should trigger follow up with the customer. For example, a change of address, phone or email triggers communication to both the old and new address. Use of more timely communications can help engage the customer more quickly and stop a fraudulent scenario from developing.

We can't forget new customers. They can pose a different challenge as there is not contact history or records to match. As noted above, the phone number and carrier information is still useful in indicating the caller is legitimate (e.g., the phone number is engaged, the SIM card is valid), even when they can't be matched in a customer database.

While the focus of these efforts tends to be on inbound calls, outbound calls play a role, too. Some centers need to make outbound calls, and others turn inbound into outbound to address risk concerns or long queues. They may call customers at the number on file when concerned about large value or high-risk transactions. The bad news is that this does not guarantee success, as bad guys have ways to divert calls. Moreover, legitimate customers receiving such calls may be suspicious and not want to provide authenticating information. Rather, they want to authenticate the caller! So your best bet is to make inbound work well.

All these scenarios point to the importance of building a strategy with the right kinds of technology, as well as people and process changes (SEE THE SIDEBAR). As an example, a recent project identified 10 "quick-hit" opportunities that don't require a big project or investment. The vendors on my panel emphasized that many companies conduct a Proof of Value (PoV). This term is different from a proof of concept as it focuses not on whether the technology works, but whether it can deliver enough value to justify the cost. They stand by statements that it will decrease AHT and fraud, and thus deliver a strong return on investment. With cloud solution options, such an endeavor is relatively easy and low cost to set up, and you can turn it off if you don't reap adequate benefits.

Proactively Pursue Optimized Authentication and Fraud Prevention

The vendors' research and market data shows that this problem is growing and expensive. The problem will also continue to evolve, so companies must adapt to the latest tactics fraudsters try. Engaging a specialist that lives in this world is probably the strongest defense a center can have.

Don't wait until you have a bad situation with fraud, or long handle times and frustrated customers and representatives. Proactively pursue a plan to optimize your authentication and fraud prevention.

Lori Bocklund is Founder and President of Strategic Contact. (lori@strategiccontact.com)

CONNECT WITH PIPELINE

 @SusanHash • @CCPipeline

 youtube.com/ccPipeline

 linkd.in/17M5rKM

About Contact Center Pipeline

Contact Center Pipeline is a monthly instructional journal focused on driving business success through effective contact center direction and decisions. Each issue contains informative articles, case studies, best practices, research and coverage of trends that impact the customer experience. Our writers and contributors are well-known industry experts with a unique understanding of how to optimize resources and maximize the value the organization provides to its customers.

To learn more, visit: www.contactcenterpipeline.com

 Download complete issues, articles, white papers, and more at http://bit.ly/14bq01k

PIPELINE PUBLISHING GROUP, INC. PO Box 3467, Annapolis, MD 21403 • (443) 909-6951 • info@contactcenterpipeline.com