Stop Fraudsters Before They Reach Your IVR or Agents

By Adam Russell, Neustar

Fraudsters' increasingly sophisticated tactics compel enterprise contact centers to invest in fraud-prevention solutions that assess risk before callers engage with human agents. The resulting risk assessment ideally improves contact centers' security posture and ability to treat each caller according to their trustworthiness.

However, most fraud-prevention solutions require some degree of engagement with the caller to assess risk. The delay can result in millions of dollars in fraud and loss of customer lifetime value.

IVRs are Highly Vulnerable

Callers may freely explore contact centers' automated interactive voice response (IVR) systems during their trust assessment, which can take up to 45 seconds. Over thousands of calls, that IVR access substantially increases risk of account takeover (ATO) fraud.

"Fraudsters don't mind calling repetitively until they are successful in impersonating a legitimate customer," writes[1] Aite Group Senior Analyst Shirley Inscoe. "The purpose of each call is to obtain an additional data element that can lead to success on the next attempt. This behavior has been demonstrated over and over, and makes contact centers especially vulnerable to organized, targeted attacks... Detecting accounts via the IVR enables fraudsters to focus their attacks against the [financial institutions] owning them; data leaked through the IVR helps fraudsters refine attacks to make them more effective."

One-third of the financial services fraud executives whom Inscoe surveyed did not know whether fraud was occurring in their institutions' IVRs. Another 37 percent had seen evidence of such activity.

Fraudsters have ready access to the tools and knowledge necessary to program a bot to navigate an IVR, either by touchtone or voice. Touchtone automation is so accessible that the iOS and Android smartphone platforms allow users to "program" their phones to navigate the IVR tree behind a phone number. Tutorials, and even automated services, offer voice bots so convincing that they can deceive humans. The prerequisite mapping of an IVR tree, even manually, is unlikely to raise suspicions.

1 Aite Group, "Improved Customer Experience, Reduced Fraud and Cost: Contact Center Solutions"

Once an IVR tree has been mapped, a bot can complete reconnaissance in very little time, even if it were programmed to behave at human speed to evade anomaly detection. Scaled up with a robodialer, such an operation would be able to acquire sensitive information for thousands of accounts. The years-long plague of illicit robocalls shows that fraudsters can evade basic phone-number blocklisting capabilities.

Enterprise contact centers incur undue risk by granting IVR access to non-authenticated callers. Fraud losses can quickly reach millions of dollars. At least 40 percent of victims of financial account takeover move one or more accounts to another financial institution. The fraud manager responsible for such dismal results may end up in an unexpected job search.

At the heart of these issues is post-answer authentication, which significantly increases the risk of fraud. "The engagement models of service have changed," states Javelin Strategy & Research, "yet security in contact centers is, for the most part, stuck in the 1990s." This begs the question: how well prepared are inbound call centers to distinguish fraudsters from customers over the long term?

Authenticate Inbound Callers Pre-Answer Using Their Phones

A trust assessment that completes before the caller hears "hello" essentially eliminates the vulnerabilities described above.

Unique, physical devices—mobile phones and residential cable and landlines—can help to significantly expedite this process for 70 to 75 percent of inbound call volume.

Confirming the calling phone's authenticity and matching the calling number to the reference phone number on file allows the contact center to identify and deterministically authenticate callers—similar to the way credit cards facilitate cashless transactions. Deterministically authenticated callers may receive faster service and higher-risk self-serve options, such as account transfers, contact information updates, and password/PIN resets.

Callers should not receive a deterministic authentication token if they use a different type of calling device, such as a call-spoofing or -virtualization service. Fraudsters rely on these services to evade conventional call-tracing measures.

To distinguish customers from possible fraud threats, other call signals inform a probabilistic pre-answer risk assessment, such as calling history, call routing, and line type. Insights from these assessments help to stratify non-authenticated callers into "trust levels" and refocus valuable fraud-fighting resources. Only risky callers receive stepped-up authentication or the full focus of the fraud department. This reduces the search for "a fraud needle in a haystack" into a more efficient search in a much smaller population.

False positives approach zero because deterministically authenticated callers never enter a fraud review queue. The fraud department focuses its resources on the fewer remaining, potentially risky callers. The results of each non-authenticated caller's probabilistic risk assessment may be analyzed in conjunction with other fraud signals to distinguish fraudsters from customers with even greater accuracy and speed.

However, unlike a post-answer authentication approach, which requires fraud feedback to ward off future attacks from the same source, device-based authentication doesn't require a past fraud incident before flagging a risky caller. Detecting and preventing "first-time attacks" reduces fraud loss, while also providing an important signal for other fraud tools' future reference.

Completing a trust assessment before callers hear "hello" enables contact centers to mitigate risks with greater speed and security than strategies that require caller engagement. Stratifying callers by trust level reduces false positives sent to the fraud department and shrinks the pool of callers that merit closer scrutiny. Shortening the trust assessment experience for trustworthy callers and offering more valuable self-serve options improves customer satisfaction and reduces average handle time.[2] Contact centers that invest in pre-answer inbound authentication to prevent fraud also invest in happier and more loyal customers.

2 Aite Group

**This article was originally published on BAI in May 2021.*