Voicing Concerns Over A New Rising Fraud

cyber security technology risk management

Summary: The rate of voice fraud has risen more than 350% from 2013 to 2017 with no signs of abating. What can you do to protect your bank from this new threat?

The human voice is interesting. For instance, singing is believed to be right hemisphere dominant, while speaking is from the left. Further, conversational speech is about 60 decibels, but the loudest scream ever recorded reached 129 decibels. Finally, the English language has about 40 distinct sounds.

Speaking of voices, you may also find it interesting that the rate of voice fraud has risen more than 350% from 2013 to 2017, according to an annual fraud report by Pindrop (voice security and authentication firm).

Banks in particular have seen voice fraud rise swiftly. Consider that from 2016 to 2017, the fraud rate in the phone channel within banks rose by 20%, and it jumped by 269% from 2014 to 2017.

Notably, fraudsters today have more cutting-edge tools at their disposal, made possible by rapid advances in machine learning and artificial intelligence. As such, fraudsters are successfully leveraging techniques like imitation, replay attack, voice modification software and voice synthesis.

While voice technology has numerous advantages for customers, it can also increase risk related to bank security. This ups the ante for banks to work even harder to keep customers and their data of all sorts safe.

Voice biometrics has already proven to be effective in stopping fraud attempts and preventing future fraud. This technology can validate a caller's identity by detecting voice patterns using more than 100 physical and behavioral factors. These include such things as pronunciation, emphasis, speed and accent. Using biometrics, a customer's identity can be verified quickly.

Because nothing is full-proof, it's a good idea to use voice biometrics alongside other means of customer authentication. For instance, one-time passwords sent to a customer's cell phone or email can be a good second verification method. This extra verification helps reduce risks and improve security.

Banks should also routinely analyze the characteristics of calls received, rather than just analyzing who the caller is. For instance, a call from an elderly customer seeking to uncharacteristically wire thousands of dollars overseas should immediately raise red flags for lots of reasons. Sure, this one is a simple example, but it also highlights the fact that banks need to have a process whereby suspicious calls of various types are routed to specially trained staff with experience in these matters. In this way, customer facing teams are better prepared to handle issues and escalate them further, as the situation warrants.

Banks should also stay current with the different ways fraudsters are gaming the system. This helps bank teams expand their own knowledge, so you can alert customers to schemes. One pattern that's becoming more prominent is where fraudsters phone individuals at random and bait them with yes-or-no questions such as "can you hear me" or "is this so-and-so?" The crooks then record their voices and use the recordings to perpetrate financial fraud.

Combatting fraud often means staying one step ahead of the bad guys and that is a never-ending task. This fight requires vigilance by banks and customers alike, as incidences of fraud increase. Voice fraud is just the latest one to add to your list.

CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your bank minimize its credit exposure, increase operational efficiency and deliver faster fraud notification. Learn more about our check imaging for Canadian cash letters.