



Insight

## Allianz Coffee Guide to: Voice Biometrics

Broking business is busier than ever, and staying on top of the latest insurance and risk management buzzwords can sometimes fall by the wayside. So, harking back to the coffee shop origins of insurance, Allianz is offering a series of short and snappy insights that pull on our commercial expertise. A perfect way to catch up on what's hot!

**On this week's agenda: Voice biometrics. We hope the following comes in handy next time you're awaiting a cappuccino in your local coffee house and a fellow coffee customer turns to you and says...**

***Coffee Customer: I'm locked out of my banking again! I can never remember all these account IDs, passwords, secret questions, PINs... it's just too much.***

**You:** Some banks let you verify your identity with speaker recognition now – it's called voice biometrics. You'd still have to answer a question or provide a password as an extra layer of security, but it's still at least one less thing to remember as your 'voiceprint' can be used to provide an element of authentication to a call centre operator or an app.

***Coffee Customer: My 'voiceprint'? What's that?***

**You:** It's basically a visual representation of the sounds you make when you speak – it looks a bit like a graph and its proper name is 'sound spectrogram'. There'll be different shapes and colours or shades for each sound and because every voice is unique, each person's sound spectrogram, or voiceprint, will be distinctive.

***Coffee Customer: I didn't think every voice could be unique... What if I get a cold?***

**You:** Your voice has dozens of traits that can be analysed from a voiceprint and they're all separately affected by things like the size of your vocal chords, shape of your mouth, speed, pronunciation and emphasis. If you've got a sore throat, it will most likely still figure out who you are by picking up on your behavioural traits and physical aspects that won't be so affected.

***Coffee Customer: Okay, but is it really that secure? What if someone records my voice and uses it to trick the bank?***

**You:** Modern voice biometrics technology won't be fooled by a recording – the sound will be coming from a speaker instead of your mouth so it won't be exactly the same. Plus, they'd still need to know the answer to a question that, ideally, only you can answer. Think of your voice as being a bit like a three-dimensional barcode. There's dozens of possible variations for each of the dozens of physical and behavioural traits that your speech is made up of, plus the voice needs to be saying the right thing. That would be a lot harder to figure out than an eight character password!

**At this point, your drink will be served and you can smile modestly knowing that your coffee catch up went well.**



### Insurance implications at a glance:

- Voice biometrics has the potential to simplify identity verification processes while making things a lot harder for fraudsters.
- Unlike passwords and secret questions, voices can't be changed if the data is stolen and used to impersonate someone with voice spoofing technology. Even with additional forms of verification, many IT security professionals are nervous of voice biometrics for this reason.
- The technology behind voice biometrics is already very good at detecting when a voice isn't coming from its true owner's mouth, but there have still been instances where people have been able to trick the system.