Commercial feature

# Pandemic is a perfect storm for voice fraud

Criminals are exploiting the coronavirus pandemic to commit lucrative phone fraud, but help is at hand

With the loss of the high street in lockdown and the subsequent boom in online retail, banking and financial services, with everyone working from home, call volumes to customer service staff have spiked. The coronavirus outbreak saw businesses then scale their phone-based operations, while shifting call centre and customer-facing staff to work remotely. In the process voice fraud has soared.

Contact centre crime has already rocketed by 350 per cent in the past five years. Every year $14 billion is lost to phone fraud across the globe. Every minute of every day there are hundreds of voice channel attacks worldwide, with many consumers pointing the finger at the company they're dealing with when an attack occurs on their account. It's bad for brand reputation and the bottom line.

"Voice-based syst ems and call centres have traditionally been vulnerable to security threats and fraud. Many phone systems still are and these vulnerabilities have been exacerbated by the pandemic. Right now, there's an arms race going on with criminals using the COVID-19 crisis in highly creative ways to commit sophisticated attacks via phone," explains Mark Horne, chief marketing officer at Pindrop, a global pioneer in voice security and authentication.

"One client saw calls go up tenfold. But their capacity to cope plummeted with the closure of their call centres. Fraudsters then subjected stressed customer service staff working from home to coronavirus-themed requests that required immediate action, many to transfer money to distressed loved ones. It's created the perfect storm, especially for financial services."

Out of all those who dial in to contact centres, only 0.1 per cent are fraudulent, finding them is therefore difficult. Criminals use interactive voice response, or IVR, the self-service systems that most companies now use to verify accounts and test whether passwords work. They are able to deploy spoof telephone numbers and customer data purchased from the dark web to impersonate valid account holders.

"Sixty per cent of online fraud can be tracked back to reconnaissance work that criminals do via the IVR. Once they've breached the system, they're able to commit the attack by withdrawing funds, resetting passwords or updating contact information while on the phone to an agent or online. But there's now technology that can identify an illegitimate caller," says Horne, whose company works with Lloyds Bank Group, other top banks, insurers and etailers such as the Very Group (formally Shop Direct) in the UK.

"Education is huge part of this; consumers who use the same password for their Netflix, email and bank account are open season for attacks. Time and again we try to inform people about this. However, the battle's ongoing. It doesn't help that fraudsters now use deepfake audio to commit fraud. It is a worrying trend."

> **We can catch fraud in real time, while the criminal is on the line**

Authenticating more callers using software is now a significant trend. Artificial intelligence (AI) and machine-learning are being increasingly used to analyse calls to contact centres in a bid to counteract fraud and improve the customer experience.

"Our AI engines can process thousands of factors from an individual call, including voice, location, device type, number history, behaviour and call details. Additionally, we have one of the world's largest databases of known fraudsters. So we can catch 80 per cent of criminals even before they commit the crime," says Horne. So far, Pindrop has processed more than 1.2 billion calls and detected 1.5 million fraud attacks.

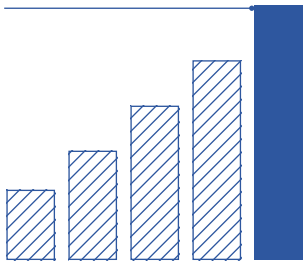
"We can catch fraud in real time, while the criminal is on the line; machine-learning algorithms operate on calls via the cloud analysing the call data. If a call centre representative looks at the risk score and it's in the red, they pass it on to a fraud team or decline the transaction immediately. At Pindrop we can now shine a spotlight on fraudulent activity in banking, insurance, etail and many more sectors before it becomes an issue. The more calls we analyse, the better we're getting at detecting fraud. It's a game-changer," Horne concludes.

**Check out why voice fraud matters at pindrop.com**

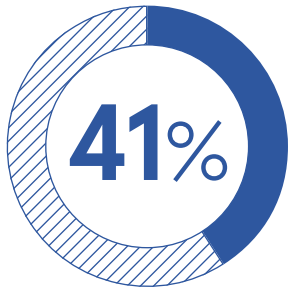
pindrop

**$14bn**
lost to phone fraud globally each year

**350%**



increase in contact centre fraud in last five years




of customers blame the brand for fraud happening

COUNTERFEITING

# Protecting the real deal

Imitation may be the sincerest form of flattery, but counterfeit fashion products are costing the real deal in both reputation and revenue; new technology might be an answer

Josh Sims

These are tough times for the fashion industry and boom times for counterfeiters. Once fakes were sold on street corners. Now the underground has gone overground, with technology providing a global platform for elusive traders. A study by analytics firm Ghost Data this spring suggests that nearly 20 per cent of all posts about fashion products on Instagram, for example, feature counterfeits.

"Online has meant that access to fashion counterfeits has exploded. There are so many ways for counterfeiters to sell this stuff and the challenge is to get these channels to adopt better practices," says Bruce Foucart, deputy director of the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy. "Are they responding? Well, yes and no."

Pressure is applied, he says, but it still typically falls back to expectations that fashion brands should be doing more to stop counterfeiters in the first place. So, if technology is providing counterfeiters with a route to market, can tech also counter counterfeiting? Holographic bubbles, radio-frequency identification chips, smart tags, blockchain – so-called check tech – are exploring every angle.

"The market for technological solutions to counterfeiting is

> **Unfortunately for fashion, copying a pharmaceutical is not easy, while copying a pair of Nikes is not so hard**