NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

Mitigating the risk of unemployment fraud with AI and biometrics

Nuance Communications

3 June 2021

Across Europe and the UK, fraudsters have leveraged the chaos of COVID-19 to intercept billions in relief and stimulus funds. Now, governments and banks are asking: How can we prevent this fraud and protect our citizens? A growing number are turning to intelligent solutions powered by AI and biometrics to proactively detect and prevent unemployment fraud while continuing to make sure legitimate claimants get their benefits.

The business of fraud was already booming. When the European Commission shared the results of an EU-wide "scams and fraud" survey in January 2020, the report revealed that the majority (56%) of Europeans had experienced fraud in the previous two years.

Then came COVID-19. The widespread economic disruption caused by the pandemic created many new opportunities for fraudsters—especially in terms of unemployment fraud.

The crisis saw the EU labour market shrink dramatically, with a record 5.5 million jobs lost across the bloc in the second quarter of the year. But as governments rushed to release new relief and stimulus funds—from Spain's ETRE, to the UK's "furlough" scheme—the application process was, in some cases, streamlined to reduce administrative burdens and get money into the hands of citizens in need.

Professional fraudsters were quick to take advantage, filing unemployment and business relief claims in other people's and companies' names. In France, criminals stole €1.7 million in payments intended to support struggling businesses. In Germany, fraudsters took at least €31.5 million from a single provincial government. And in the UK, it's been estimated that up to £3.5 billion in COVID-related support may have

been claimed fraudulently or paid out in error.

This is just one way in which the COVID-19 pandemic has accelerated the need to rethink how we approach authentication and fraud prevention. And government agencies across Europe—and in the UK—are taking note, dedicating larger budgets for these efforts and asking what else they can do to protect themselves and their citizens.

One answer is AI-based biometrics, which can authenticate citizens and catch fraudsters quickly and securely during phone and digital interactions. Compared to security questions or phone validation, biometrics are faster and more accurate at authenticating and catching fraudsters because they focus on the actual person—that is, verifying people based on who they are, rather than something they know or something they have. Even better is to layer biometrics with other features like environment detection (verifying the device, network, channel and location) and anti-spoofing (preventing ANI spoofing and detecting synthetic speech or audio playbacks).

Consider an example: A scammer calls into your contact centre dozens of times, purporting to be different people each time in order to file fraudulent benefits claims. If the scammer has these citizens' identity details (often easily obtainable on the dark web), they can go undetected and steal thousands in government support.

But if you've integrated a biometrics solution into your contact centre, you'll recognise the fraudster in seconds and alert the contact centre agent in real-time. Meanwhile, your fraud teams will be analysing historical call recordings to identify where the same voice appears multiple times across a number of calls. They'll then be able to add that voice to your watchlist, so that the fraudster is immediately detected the next time they call, as well as gather high-quality evidence to build a case for prosecution.

Adapting to the new realities of fraud is essential as we navigate the tail end of the pandemic and beyond. Amidst the transition to our "new normal" throughout 2021, government agencies need to take proactive steps to protect their citizens. Smart investments in next-gen technologies like AI and biometrics can help streamline and protect every citizen interaction, helping citizens access their benefits more quickly and stopping fraudsters in their tracks.

Interested in learning more? Read about Nuance's security and biometrics solutions or book a time with me to discuss your agency's specific challenges, and how you can use technology like biometrics to solve them.

Tags: COVID-19, Government, Citizen experiences