What's next

Enterprise

Mitigating risk of unemployment fraud with AI and biometrics

Unemployment fraud in the US topped $36 billion in 2020 as fraudsters leveraged the chaos of COVID-19 to intercept billions of dollars in relief and stimulus funds. Now, labor departments 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.

Simon Marchand

Posted April 16, 2021

The business of fraud is booming. Identity theft cases doubled in 2020, according to the U.S. Federal Trade Commission. Another study from December 2020 found that 47% of adults in the U.S. have experienced identity theft in the past two years, losing $712.4 billion in 2020—and those are just the reported numbers. We can assume that many more people simply haven't discovered their theft yet or haven't reported it.

This is a particularly acute problem as fraudsters continue to exploit the chaos created by the COVID-19 pandemic; a quarter of American adults say they or someone in their household were laid off or lost a job because of the coronavirus outbreak, jumping to 47% of those with lower incomes. As Congress released new relief and stimulus funds, the application process was, in some cases, streamlined to reduce burden on agencies and get money into the hands of citizens in desperate need. Fraudsters were quick to take advantage, filing thousands of unemployment claims in people's names and stealing at least $63 billion. As we're only now in the midst of tax season, these scams are only just coming to light, and people may no longer be able to access the money they urgently need to pay bills and rent.

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 of all sizes are taking note, dedicating larger budgets for these efforts and asking what else they can do to protect 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 center dozens of times, purporting to be different people each time in order to file fraudulent benefits claim. If the scammer has these citizens' identity details (social security number, address, and so on—easily obtainable on the dark web), they go undetected and steal thousands of dollars from the government. But if you've integrated a biometrics solution into your contact center, you'll recognize the fraudster in seconds and alert the contact center agent in real-time. Meanwhile, your fraud teams will be analyzing 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 get access to their benefits more quickly and stopping fraudsters in their tracks.

Interested in learning more? Read about Nuance’s security and biometrics solutions or book time today with Simon Marchand, CFE, C.Adm., to discuss your agency’s specific challenges and how you can use technology like biometrics to solve them.

Tags: Artificial Intelligence, biometrics, Security and Biometrics

More Information

Better unemployment fraud prevention, all around
Meet with Nuance’s Chief Fraud Prevention Officer for a consultation, personalized to your needs.
Learn more

About Simon Marchand

Simon Marchand is Nuance’s chief fraud prevention officer for security and biometrics. Certified Fraud Examiner, Simon has extensive expertise in fraud prevention, detection and management - as well as in authentication and identity - in both the banking and telecom industries, with more than 10 years of experience in the field. Prior to Nuance, Simon held key fraud prevention positions at Montreal-based Laurentian Bank, at Bell Canada, and at Québec’s Order of Chartered Administrators, where he managed its professional inspection program. As chief fraud prevention officer, he works closely with Nuance clients to design biometric-based fraud prevention and authentication strategies that disrupt criminals while reducing effort and friction for legitimate customers. He regularly shares his expertise in various conferences and with associations around the world and he speaks on the risks of fraud and the ethical use of biometrics in the media.

View all posts by Simon Marchand