NUANCE | WHAT'S NEXT BLOG

Autentification biométrique et prévention, Engagement client omnicanal

L'IA et à la biométrie réduisent considérablement les risques de fraude au chômage partiel

Nuance Communications

3 juin 2021

Dans plusieurs pays d'Europe, des fraudeurs ont profité du chaos ambiant dû à la Covid-19 pour s'approprier des milliards de fonds destinés à soutenir les personnes aux emplois menacés par la pandémie, ou à relancer économiquement ces pays. Les états et les banques s'interrogent : comment éviter ce type de fraude et protéger leurs citoyens ? Beaucoup adoptent des solutions intelligentes optimisées par l'IA et la biométrie pour détecter les tentatives de fraude et les bloquer de façon proactive sans perturber le reste des demandes client.

Avant 2020, le marché de la fraude était déjà florissant. Les conclusions d'une étude paneuropéenne de la Commission européenne sur les escroqueries et la fraude publiées en janvier 2020 nous apprennent que la majorité (56%) des Européens avaient été victimes d'une fraude au cours des deux années précédentes.

Puis la Covid-19 est arrivée. Les répercussions énormes de la pandémie sur l'économie ont créé de nombreuses nouvelles opportunités pour les fraudeurs, surtout en ce qui concerne les aides déployées spécialement pour endiguer la crise.

Le marché du travail dans l'UE s'est considérablement réduit, avec une perte record de 5,5 millions d'emplois dans cette zone au second trimestre en 2020. Mais dans l'empressement des états à proposer des fonds de soutien et de relance, comme le fonds ETRE en Espagne ou le système "furlough" de congé

partiellement remboursé au Royaume-Uni, la procédure de demande a parfois été rationalisée afin d'alléger la partie administrative et de transférer rapidement l'argent aux bénéficiaires.

Les professionnels de la fraude ont saisi cette occasion pour faire des demandes d'indemnisation ou d'aides sous de faux noms d'individus et de sociétés. En France, des criminels ont volé 1,7 million d'euros réservés aux entreprises en difficulté. En Allemagne, des fraudeurs ont ainsi détourné 31,5 millions d'euros auprès du gouvernement d'une seule province. Et au Royaume-Uni, on estime que 3,5 milliards de livres d'aides directement allouées à la situation créée par la Covid ont pu être réclamées indument ou versées par erreur.

C'est un autre exemple de la façon dont la pandémie de Covid-19 nous oblige à repenser notre approche de l'authentification et de la lutte contre la fraude. Les agences gouvernementales partout en Europe prennent la mesure du problème et attribuent plus de budget à ces efforts afin de mieux protéger leurs administrations et leurs citoyens.

Parmi les solutions existantes, celles de biométrie à base d'IA permettent d'authentifier les citoyens et d'identifier les fraudeurs rapidement lors d'interactions vocales et digitales. Contrairement aux questions de sécurité ou de validation « classiques » par téléphone, la biométrie permet d'authentifier les fraudeurs plus rapidement et précisément en se focalisant sur la personne, son identité véritable et non une information qu'elle connaît ou un code qu'elle pourrait avoir obtenu. Et il est aussi recommandé d'ajouter à la biométrie des fonctionnalités de détection environnementale (vérification de l'appareil, du réseau, du canal, de l'emplacement) et anti-spoofing (usurpation du numéro ANI, détection de piste audio ou de synthèse vocale).

Prenons un exemple : un escroc appelle votre centre de contact des dizaines de fois en prétendant à chaque fois être quelqu'un d'autre pour obtenir des aides indues. S'il détient des informations sur une identité quelconque (que l'on obtient souvent facilement sur le dark web), chacune de ses demandes pourra aboutir, et il pourra détourner des fonds sans être détecté.

Mais si le centre de contact intègre une solution biométrique, le fraudeur sera reconnu en l'espace de quelques secondes et l'agent prévenu en temps réel. En interne, vous pourrez analyser de précédents appels enregistrés pour vérifier si la même voix revient lors de plusieurs appels. Il suffira ensuite d'ajouter cette voix à la liste des suspects, ainsi le fraudeur sera détecté immédiatement à la prochaine occasion et vous accumulerez des preuves solides en vue de poursuites.

Même après la pandémie, il va falloir s'adapter aux nouvelles méthodes de fraude. En même temps que les administrations devront gérer leur transition vers une "nouvelle normalité" en 2021, elles vont devoir adopter des mesures proactives pour mieux protéger les citoyens. Des investissements judicieux dans les technologies de nouvelle génération, comme l'IA et la biométrie, aideront à fiabiliser les interactions avec les citoyens pour qu'ils bénéficient de leurs droits plus rapidement et à mieux détecter les fraudeurs.

Vous aimeriez en savoir plus ? Informez-vous sur les solutions biométriques et de sécurité Nuance ou réservez un entretien pour évoquer votre situation et voir comment la biométrie ou d'autres technologies pourraient vous aider.

Tags: Prévention de la fraude