

Authentification biométrique et prévention, Engagement client omnicanal

Comment la biométrie peut tenir les fraudeurs à distance

[Brett Beranek](#) | Vice President & General Manager, Security & Biometrics

30 Avril 2020



Avec le passage massif au travail à domicile, les entreprises doivent prendre conscience de l'évolution des menaces et des fraudeurs qui cherchent à tirer profit de ce changement sociétal. Grâce aux solutions biométriques, les entreprises peuvent tenir les mauvais acteurs à distance, s'assurer que leurs connexions avec leurs clients sont sûres et sécurisées et permettre à leurs organisations de s'adapter rapidement aux nouvelles menaces.

Avec le passage massif au travail à domicile, les entreprises doivent prendre conscience de l'évolution des menaces et des fraudeurs qui cherchent à tirer profit de ce changement sociétal. Grâce aux solutions biométriques, les entreprises peuvent tenir les mauvais acteurs à distance, s'assurer que leurs connexions avec leurs clients sont sûres et sécurisées et permettre à leurs organisations de s'adapter rapidement aux nouvelles menaces.

La pandémie ne ralentit pas les fraudeurs. Au contraire, ceux-ci profitent souvent de l'immense changement qui accompagne un tel événement pour intensifier leurs activités. Avec le récent passage à un monde de travail à domicile, on observe une augmentation significative des attaques frauduleuses contre les centres d'appels : les fraudeurs testent leur vulnérabilité soit en attaquant directement les agents travaillant à domicile, soit en se faisant passer pour d'autres agents. Cette méthode leur permet d'évaluer les faiblesses pouvant leur permettre de commettre des fraudes.

Pour tenir les cybercriminels à distance et assurer la sécurité de leurs opérations et de leurs clients, les organisations du secteur public et privé doivent s'équiper d'outils permettant de réduire au minimum les perturbations causées par la fraude. Les organisations qui ont déployé la biométrie trouvent la technologie incroyablement utile dans cet effort car elle permet d'identifier les fraudeurs, plutôt que de s'appuyer sur des méthodes plus traditionnelles axées sur des modèles transactionnels suspects établis.

Il existe des applications de la biométrie permettant de résoudre certains des défis nouveaux et plus complexes auxquels les organisations sont confrontées aujourd'hui :

La protection des expériences des clients et des agents : alors que les centres de contact s'efforcent de faire face à l'afflux de demandes de renseignements généré par la pandémie, une interaction trop lente et stressante peut facilement frustrer l'ensemble des interlocuteurs. L'authentification biométrique peut jouer un rôle crucial non seulement en accélérant les résolutions et en libérant le temps de l'agent, mais aussi en garantissant que les niveaux de frustration sont maintenus à un minimum en ne créant aucune friction inutile entre le client et l'agent. La biométrie peut éliminer la nécessité de tout processus d'identification et de vérification manifeste et soulager les agents de première ligne, réduisant ainsi les risques d'erreur lors d'un appel.

Lutter contre les nouvelles tentatives de fraude : de nombreuses organisations, dont les institutions financières, les compagnies d'assurance, les fournisseurs télécom et les services publics en contact avec les citoyens, constatent une augmentation massive du volume d'appels en raison de la fermeture de certains sites. Et, dans certains cas, elles constatent une augmentation exponentielle des demandes de renseignements et des transactions sur les canaux numériques. Face à cette augmentation, il est très difficile d'attendre des agents du service clientèle qu'ils fassent la distinction entre les fraudeurs et les véritables clients tout en essayant de répondre à leurs besoins. Après tout, le rôle des agents du service clientèle est de se concentrer sur la clientèle. Par ailleurs les agents font face à une pression accrue en raison du manque de supervision et de support qu'entraîne le travail à domicile, il devient plus facile pour les fraudeurs de les manipuler. La biométrie s'avère être un outil précieux pour identifier automatiquement les appels frauduleux, ce qui permet de réduire la pression exercée sur les agents de première ligne et de les protéger contre l'ingénierie sociale.

Elle permet aux agents de travailler de chez eux en toute sécurité sans faire de compromis : permettre aux agents de travailler à distance s'accompagne d'une série de défis, notamment dans le cas où ils utilisent leurs ordinateurs et téléphones mobiles personnels. Ce passage rapide au travail à distance a créé d'innombrables opportunités pour les fraudeurs, car les systèmes habituels protégeant les installations des centres de contact ne sont plus présents. La biométrie offre un vaste potentiel pour améliorer les contrôles de sécurité interne dans ces situations en vérifiant l'identité des agents et en empêchant les fraudeurs de s'emparer de leurs comptes. L'authentification biométrique permet également aux organisations d'afficher moins d'informations personnelles sur leurs clients aux agents, ce qui réduit par conséquent les risques de fraude professionnelle dans un contexte de travail à distance où l'absence de supervision directe représente une opportunité pour les fraudeurs travaillant au sein des organisations.

Aujourd'hui plus que jamais, les centres de contact sécurisés sont une nécessité pour les organisations afin d'interagir avec les clients. Pour en savoir plus sur ce que nous faisons pour aider nos clients à rester en sécurité, cliquez [ici](#).

Tags:



About Brett Beranek

Brett Beranek est responsable de la sécurité et de la biométrie chez Nuance. Avant de rejoindre Nuance, il a occupé, au cours des dix dernières années, divers postes de développement commercial et de marketing dans le domaine des logiciels de sécurité B2B. Brett Beranek possède une vaste expérience des technologies biométriques, notamment en tant qu'associé fondateur de Viion Systems, une start-up spécialisée dans le développement de solutions logicielles de reconnaissance faciale pour le marché des entreprises. Brett Beranek a également une expérience approfondie d'un large éventail d'autres technologies de sécurité, y compris la biométrie des empreintes digitales, l'analyse vidéo pour l'espace de sécurité physique et la technologie de reconnaissance des plaques d'immatriculation. Il est titulaire d'un Bachelor of Commerce, Information Systems Major, de l'université McGill, ainsi qu'un certificat de marketing exécutif de la Sloan School of Management du Massachusetts Institute of Technology.



[View all posts by Brett Beranek](#)