NUANCE

La difficulté avec laquelle les expériences d'authentification des clients sont ressenties dans l'ensemble de votre établissement de services financiers.

Et ce que vous pouvez y faire, en tant que responsable de l'expérience client.

eBook
Repenser l'authentification client

Perdez-vous le sommeil à cause du problème de l'authentification des clients ?

Vous n'êtes pas le seul.

Si vous êtes responsable de l'expérience client dans votre entreprise, il est probable que votre processus d'authentification des clients vous procure quelques insomnies.

Après tout, la manière dont un établissement de services financiers vérifie l'identité des clients est essentielle pour leur expérience de la marque. Et si ces interactions s'avèrent trop douloureuses, les clients peuvent rapidement se diriger vers une autre institution.

Mais vous n'êtes pas le seul concerné. Les processus d'authentification traditionnels, basés sur les connaissances et sur des jetons et susceptibles de nuire à l'expérience client, sont aussi une source de gros soucis pour le centre de contact de votre entreprise et les responsables de la prévention des fraudes.

Dans les pages suivantes, nous verrons comment tant de vos problèmes résultent d'une même cause profonde.

Nous expliquerons aussi pourquoi il est intéressant de réunir tout le monde pour repenser votre stratégie d'identité et de vérification (ID&V), y compris les avantages dont vous pourriez tous bénéficier en optant pour un processus d'authentification plus simple et plus sécurisé, basé sur la biométrie vocale.

96 %

des clients deviennent moins fidèles à la suite d'interactions de service qui nécessitent beaucoup d'efforts.

Gartner[1]

1 Rapport Gartner, via ID R&D, Biometrics to the Rescue.

La pyramide des problèmes liés à l'authentification

Chaque fois qu'un client oublie son mot de passe, ou s'aperçoit que son compte a été usurpé par un fraudeur, la douleur qu'il ressent se répercute sur l'ensemble de votre entreprise.

77 %

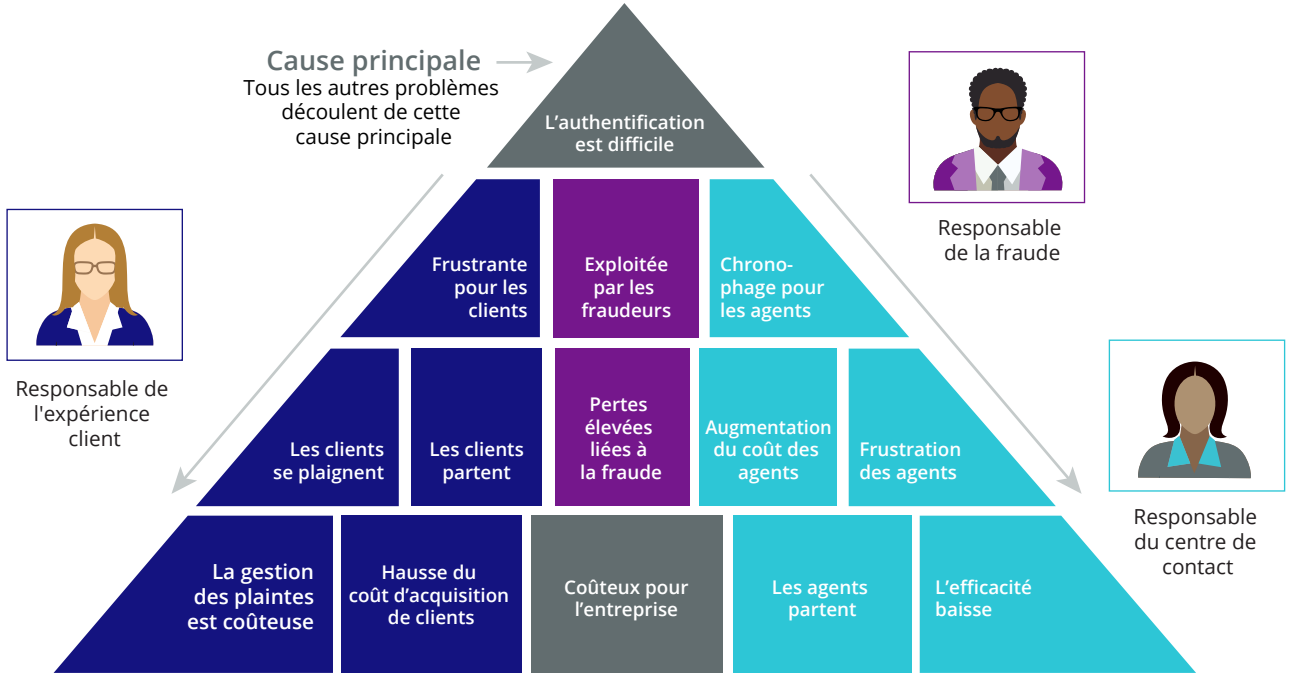
des clients veulent changer de fournisseur de services apres une seule interaction frustrante avec un agent.[2]

Répercussions négatives pour vous

Les expériences d'authentification lentes et difficiles frustrent vos clients. Elles génèrent des plaintes – aujourd'hui souvent exposées publiquement sur les réseaux sociaux – et votre entreprise doit consacrer du temps et des ressources à y répondre avec la sensibilité et la vitesse qui s'imposent.

Pire encore, la frustration d'un client peut les inciter à quitter votre marque définitivement. PwC explique qu'une seule interaction frustrante avec un agent suffit à inciter 77% des clients à changer de fournisseur de services.[2]

Pour ajouter de la difficulté à la difficulté, les nouveaux clients sont plus difficiles à attirer lorsque d'autres marques peuvent les tenter en leur proposant des expériences d'authentification plus simples, basées sur des technologies plus modernes. La concurrence dans ce domaine est de plus en plus farouche : 96% des entreprises considèrent désormais la vérification d'identité comme un élément de différenciation concurrentiel.[3]



2 Enquête PwC 2017 « Experience is Everything », Recherche terminée en 2018.
3 IDology 7th Annual Fraud Report, octobre 2019.

Répercussions négatives pour les responsables de la prévention de la fraude

La douleur de vos processus d'authentification est ressentie tout aussi vivement par votre équipe de prévention de la fraude.

L'authentification basée sur la connaissance demande à des êtres humains, vos agents, d'agir comme des gardiens. Même un agent expérimenté peut être victime d'ingénierie sociale de la part d'un fraudeur expérimenté, ce qui peut permettre au criminel d'accéder au compte d'un client ou à des informations personnelles qu'il pourra utiliser lors d'attaques ultérieures.

Toutefois, bon nombre de criminels n'ont pas à tromper vos agents pour les convaincre de révéler des informations sensibles. Ils les ont déjà achetées sur le Dark Web.

Même s'ils ne disposent pas du mot de passe d'un client, il y a de grandes chances qu'ils parviennent à le déchiffrer. Une analyse récente portant sur >1 milliard d'identifiants usurpés, dont 168 919 919 mots de passe, a permis de découvrir que 42% d'entre eux étaient vulnérables aux attaques rapides par dictionnaire. Et 1 mot de passe sur 142 était « 123456 ».[4]

15
milliards

de combinaisons nom d'utilisateur-mot de passe de compte sont à vendre en ligne, y compris des combinaisons donnant accès à des comptes bancaires.[5]

L'authentification basée sur des jetons, par exemple, par l'envoi d'un code au téléphone d'un client, présente également des problèmes. Un fraudeur disposant un accès au compte mobile de votre client n'a qu'à échanger son numéro contre celui d'une autre carte SIM pour porter son attaque.

Le problème de fond est le suivant : les technologies d'authentification actuelles sont trop faciles à exploiter, ce qui aboutit à des coûts élevés de prévention des fraudes et à des pertes importantes.

4 Rapport ZDNet sur une analyse portant sur >1 milliard d'identifiants usurpés, dont 168 919 919 mots de passe, juillet 2020.
5 Étude Digital Shadows rapportée par ZDNet, juillet 2020.

Répercussions négatives pour les responsables des centres de contact

Poser des questions d'authentification basées sur les connaissances demande du temps – pour certaines entreprises, entre deux et sept minutes.[6] Cela donne aux agents des centres de contact le sentiment d'être des interrogateurs et ils redoutent les conséquences auxquelles ils s'exposeraient en ne repérant pas un criminel.

Cela a pour conséquence de prolonger le temps de gestion moyen et de générer le mécontentement et l'angoisse chez les agents. Ce qui, comme vous pouvez l'imaginer, est la dernière chose que souhaite voir quiconque est chargé de diriger un centre de contact efficace et productif.

La durée de chaque conversation avec un client réduit l'efficacité de l'agent et augmente les coûts de personnel. D'autre part, la perte de moral des agents accentue le taux de renouvellement. Outre les coûts d'acquisition supplémentaires des agents de votre centre de contact, vous vous retrouvez avec des agents moins expérimentés et cela entraîne aussi finalement un impact sur l'expérience de vos clients.

Alors qu'un nombre croissant d'interactions avec les clients se déroulent en ligne, les responsables de centres de contact ont également besoin d'un moyen plus efficace d'authentier les clients entre les canaux ; 65% des responsables de la lutte anti-fraude déclarent que les attaques frauduleuses numériques engendrent des coûts, des pressions liées au volume, voire les deux, dans le centre de contact.[7]

La douleur financière pour votre entreprise (une excellente raison de résoudre une bonne fois pour toutes ce problème)

Par conséquent, pour résumer, un processus d'authentification douloureux génère :

— Des coûts liés aux plaintes des clients

— Des coûts d'acquisition de clients

— Des coûts de prévention de la fraude

— Des pertes liées à la fraude (et des préjudices pour la réputation)

— Des coûts opérationnels pour le centre de contact

— Des coûts de recrutement d'agents

En termes simples, ce problème est extrêmement coûteux pour votre entreprise dans son ensemble.

Voici la bonne nouvelle : en tant que responsable de l'expérience client, vous êtes parfaitement placé pour prendre l'initiative du changement et générer des bénéfices qui seront ressentis par l'ensemble de votre institution de services financiers.

6 Cadre temporel basé sur des conversations avec des clients de Nuance.
7 Market Trends in Digital Fraud Mitigation report, Aitë Group.
8 Étude Nemertes réalisée en avril 2020.

26%

Les entreprises qui maintiennent le remplacement de leurs agents à <15% constatent une amélioration de 26% des notes attribuées par les clients.[7]

Pourquoi de nombreuses marques adoptent-elles l'authentification biométrique ?

Le problème fondamental des processus d'authentification traditionnels est facile à comprendre : ils identifient les personnes en fonction de ce qu'elles savent, ou de ce qu'elles possèdent, au lieu de les identifier en fonction de qui elles sont.

L'authentification biométrique s'attaque de front à ce problème. Elle utilise des caractéristiques uniques à vos clients : leurs empreintes digitales, leur visage, la manière dont ils tiennent leur périphérique, leur façon de taper, le son de leur voix – pour confirmer leur identité.

Grâce à sa simplicité d'utilisation et à son degré de précision extrêmement élevé, la biométrie vocale constitue une solution de plus en plus populaire pour les institutions de services financiers de premier plan.

Une fois qu'un client a enregistré son « empreinte vocale » pour la marque, son identité peut être vérifiée automatiquement en quelques secondes, qu'il parle à un agent humain ou à un SVI. Le client n'a pas à mémoriser un mot de passe ni à demander un code unique. L'agent n'a pas à jouer les inquisiteurs. Tous deux peuvent se concentrer sur la tâche à exécuter.

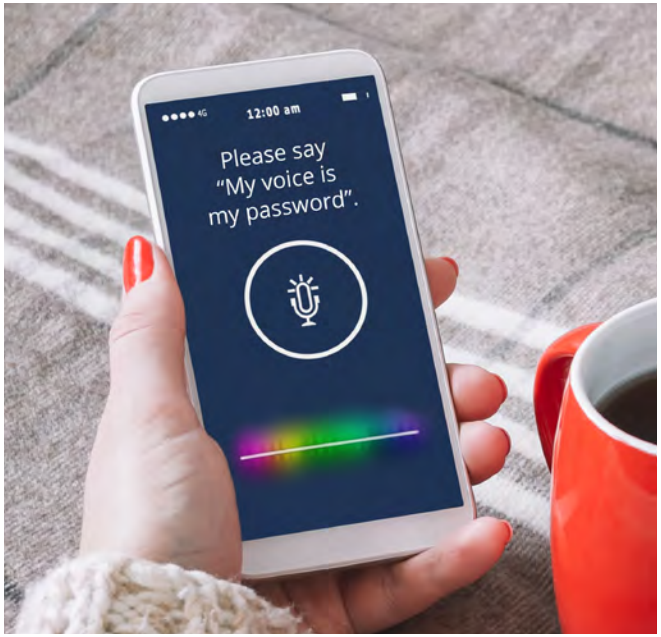
Mieux encore, vous pouvez utiliser la biométrie vocale pour identifier de façon proactive des criminels connus en comparant leur voix à une liste de surveillance d'empreintes vocales.

De même qu'un processus d'authentification lent et faible provoque des douleurs dans l'ensemble d'une entreprise, la rapidité et la sécurité de la biométrie vocale permettent de libérer une cascade de bénéfices très étendus.

9 Entretien avec le Responsable de la Fraude mondiale et de l'Innovation dans la production d'identifiants chez Experian, février 2020.

81 %

des consommateurs considèrent la biométrie comme une forme plus sûre de vérification de l'identité.[9]



Les avantages pour vous : une meilleure expérience client

Les solutions d'authentification vocale peuvent être « actives » ou « passives ». Si elles sont actives, votre client est invité à prononcer une phrase simple pour vérifier son identité. Si elles sont passives, la solution écoute le début de leur conversation avec votre SVI ou votre agent, authentifiant le client entièrement en arrière-plan. Dans un cas comme dans l'autre, il s'agit d'une expérience rapide, facile et sécurisée.

L'authentification vocale vous permet d'accueillir plus d'appels dans votre SVI, écourtant le temps d'attente des clients. Lorsqu'un client a besoin de parler à un agent, l'interaction est plus simple, plus efficace et moins maladroite ; votre client n'a pas à s'efforcer de mémoriser un mot de passe et votre agent peut se détendre et se concentrer sur l'aide à lui apporter, sachant qu'ils sont protégés contre l'ingénierie sociale.

De plus, le niveau de sécurité supérieur offert par l'authentification vocale permet aux marques d'étendre la plage des actions qu'un client peut effectuer sans recourir à un agent humain. Pour une institution de services financiers, un choix populaire consiste à prendre en charge certaines transactions à risque plus élevé, comme la configuration d'un nouveau bénéficiaire.

Amélioration des expériences grâce à la biométrie vocale chez Barclays

— Amélioration de la satisfaction des clients comme des agents

— 93% des clients ont obtenu une note de 9 ou 10 (sur 10) pour l'ID&V

— 90% de réduction des plaintes

CSAT & ASAT

« L'utilisation de la technologie de biométrie vocale Nuance a fait partie intégrante de notre mission visant à proposer une expérience client d'excellence. Les résultats en termes de satisfaction des clients et des employés parlent d'eux-mêmes. Nous sommes impatients de collaborer avec Nuance à l'avenir pour utiliser la biométrie vocale afin d'authentifier davantage de processus ».

— Anne Grim
Responsable de l'Expérience client mondiale
Barclays Wealth and Investment Management

Les avantages pour votre centre de contact : un temps moyen de traitement (AHT) réduit, des clients plus satisfaits

Une authentification plus rapide et plus robuste n’est pas seulement gagnante pour vos clients : elle est aussi gagnante pour votre centre de contact.

Comparées à l’authentification basée sur les connaissances, les solutions d’authentification vocale réduisent l’AHT de 53 secondes en moyenne , et souvent d’une minute ou plus. Mieux encore, dans la mesure où la réussite de l’authentification ne dépend plus de la mémoire de vos clients, les échecs d’authentification de clients authentiques sont plus rares et vous perdez moins de temps à gérer ces cas.

Cette amélioration de l’efficacité du centre de contact va de pair avec une réduction du renouvellement des agents.

Comme nous l’avons vu, l’authentification vocale réduit la charge sur les clients et les protège des critiques. Cela leur permet de se concentrer sur l’aide réelle au client – augmentant la satisfaction professionnelle des agents et réduisant le risque de les voir quitter leur poste. D’où une diminution du temps et de l’argent consacrés à l’embauche et à la formation de nouveaux agents. Et lorsqu’il faudra embaucher un nouvel agent, sa formation à la conduite de conversations conformes avec les clients devient plus rapide et plus simple que jamais.

Réduction de l’AHT dans le monde entier grâce à la biométrie vocale

Client de biométrie vocale Nuance	Réduction rapportée de l'AHT
Australian Tax Office	48 secondes
Banco Santander	42 secondes
Eastern Bank	60 secondes
Royal Bank of Canada	43 secondes

10 Réduction moyenne de l’AHT calculée en fonction des résultats rapportés par des clients de Nuance.

Prévention de la fraude grâce à la biométrie vocale chez NatWest Group

17 millions

d’appels protégés par an

+2 500

appels frauduleux détectés

>300 %

de retour sur investissement (ROI) dès la première année

Les avantages pour votre équipe de prévention des fraudes : réduction des pertes et prévention active

Avec l’authentification basée sur la biométrie vocale, les criminels ne peuvent plus utiliser des noms d’utilisateur et des mots de passe volés pour lancer une attaque efficace et ont moins d’opportunités d’obtenir de telles informations de vos agents grâce à l’ingénierie sociale.

Ajoutez à cela l’aptitude de la technologie à identifier les fraudeurs connus, et à signaler plus efficacement les appels suspects de robots, et l’impact sur les pertes liées à la fraude et sur la prévention peut être considérable.

Le système de biométrie vocale de la banque HSBC UK (Voice ID) a évité 608 millions de £ de pertes liées à des tentatives de fraude en moins de deux ans. La banque compte aujourd’hui plus de trois millions de clients du Royaume-Uni dans son système, qui procède à environ neuf millions de vérifications par an.[11, 12]

11 https://www.about.hsbc.co.uk/news-and-media/hsbc-voiceid-attempted-fraud (accès le 8 février 2021).
12 https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-launches-new-voice-driven-technology (accès le 24 mars 2021).

« Le ROI de l’outil est probablement nettement supérieur à 300 %, de sorte qu’en tant que rendement lié au déploiement d’une technologie, il s’est avéré très impressionnant ».

— Jason Costain
Responsable de la stratégie de lutte contre la fraude et de la gestion des relations NatWest Group (anciennement Royal Bank of Scotland Group)

Les avantages pour la réputation de l'ensemble de votre entreprise

L'introduction de l'authentification vocale, ou de toute autre technologie permettant d'améliorer la détection et la prévention des fraudes, renforce la réputation de votre institution de services financiers, témoignant clairement de l'engagement de votre marque à protéger ses clients.

Dans le même temps, cela permet de vous protéger contre le préjudice pour la réputation que peuvent engendrer les attaques criminelles réussies.

88%

des consommateurs déclarent que leur perception d'une entreprise est améliorée lorsque celle-ci investit dans l'expérience client, à savoir la sécurité.[13]

13 Rapport Experian 2020 sur les Identités mondiales et la fraude.

Il est temps de repenser l'authentification.

Ensemble.

Lorsque l'authentification est douloureuse pour vos clients et agents, elle est douloureuse pour votre entreprise. La biométrie vocale peut vous aider, en particulier lorsqu'elle est intégrée à une solution multi-facteurs qui fournit une vue unifiée de l'authentification – et des tentatives de fraude – sur l'ensemble des canaux d'engagement.

En tant que responsable de l'expérience client, vous êtes idéalement placé pour mettre en relation vos collègues de la prévention des fraudes et votre centre de contact afin d'initier une transformation qui aidera finalement chacun d'entre vous à atteindre ses objectifs.

Mais vous n'avez pas à agir seul. Nuance est à vos côtés pour vous aider, tout comme nous avons déjà aidé tant de marques de services financiers.

EN SAVOIR PLUS

Découvrez les solutions d'authentification biométrique et de prévention des fraudes de Nuance sur notre site Web.

Vous apprendrez pourquoi Opus Research nous a désignés « leader induscutable du marché » au cours de son enquête Intelligent Authentication and Voice Biometrics Intelliview en 2020.

À propos de Nuance Communications, Inc.

Nuance Communications (Nuance) est précurseur et leader dans le domaine des technologies innovantes d'intelligence artificielle conversationnelle et d'intelligence ambiante. Partenaire de confiance de 77 % des établissements hospitaliers américains et de 85 % des entreprises du Fortune 100, Nuance crée des solutions intuitives qui amplifient l'intelligence humaine.

ENT_4323_01_EB_FR, 6 Sept 2021