DSP 2 et Authentification forte du client.

Améliorer la sécurité des paiements électroniques grâce à l'authentification biométrique.

NUANCE

Pour faciliter la mise en conformité avec le nouveau cadre réglementaire applicable aux paiements dans l'Union européenne, Nuance fournit des solutions biométriques de pointe conçues pour aider les prestataires de services financiers à sécuriser les transactions en garantissant une expérience client sans points de friction.

Deuxième directive sur les services de paiement

La deuxième directive sur les services de paiement (« **DSP 2** »)[1] s'inscrit dans une tendance mondiale en matière de réglementation bancaire visant à favoriser la sécurité, l'innovation et la concurrence. La DSP 2 est entrée en vigueur le 13 janvier 2018, avec une première extension de délai au 14 septembre 2019, suivie d'une deuxième au 31 décembre 2020. Ce report a été autorisé par l'Autorité bancaire européenne (ABE) afin de faciliter la mise en conformité de tous les opérateurs concernés. La DSP 2 vise à moderniser les services de paiement européens dans l'intérêt des consommateurs et des entreprises. Elle permet ainsi aux entreprises de rester en phase avec un marché en rapide évolution, de renforcer la protection des consommateurs contre la fraude et de redéfinir les responsabilités dans l'écosystème des paiements.

Selon Valdis Dombrovskis[2], *« Cet acte législatif constitue une nouvelle étape dans la création d'un marché unique numérique dans l'UE. Il encouragera le développement de systèmes de paiement en ligne et mobiles innovants, ce qui stimulera l'économie et la croissance. »*

La nouvelle directive européenne vise à la fois à prendre en compte les changements technologiques et à promouvoir l'innovation numérique en facilitant l'entrée sur le marché de nouveaux types de prestataires de services de paiement. Elle vise également à favoriser davantage de transparence sur les transactions, à renforcer la protection des consommateurs et à améliorer la sécurité des paiements.

DSP 2 : principaux changements

- Garantit l'égalité de traitement des différents prestataires de services de paiement en permettant à de nouveaux prestataires tiers d'accéder à l'écosystème des paiements.
- Inclut davantage de types de transactions, par exemple des transactions dans de nouvelles zones géographiques et monnaies (autres que l'euro et celles des États membres).
- Réglemente de nouveaux services de paiement, autres que les paiements par cartes de crédit et les transferts entre comptes bancaires, notamment les services d'initiation de paiement et d'information sur les comptes.
- Renforce les exigences de sécurité, avec notamment l'authentification forte du client (en anglais Strong Customer Authentication, SCA) et de nouvelles mesures de protection des consommateurs.
- Introduit des contrôles en cas de paiement non autorisé et la responsabilité du prestataire de service de paiement. En cas d'opération non autorisée, le prestataire de service de paiement du payeur devra rembourser immédiatement le montant de la transaction non autorisée.

1. Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur
2. Vice-président chargé de la stabilité financière, des services financiers et de l'union des marchés des capitaux

En quoi la DSP 2 est-elle si différente ?

OPEN BANKING

La DSP 2 sera un catalyseur essentiel dans la révolution qui fera de l'« Open Banking » une réalité. Les nouveaux services d'initiation de paiement et d'information sur les comptes fourniront l'occasion à de nouveaux acteurs de perturber les règles concernant les paiements dans l'Union européenne. Ces changements constituent à la fois un défi (en raison du risque de désintermédiation) et une opportunité (en raison de l'expertise et de l'infrastructure dont disposent les établissements financiers).

PROTECTION DES CONSOMMATEURS

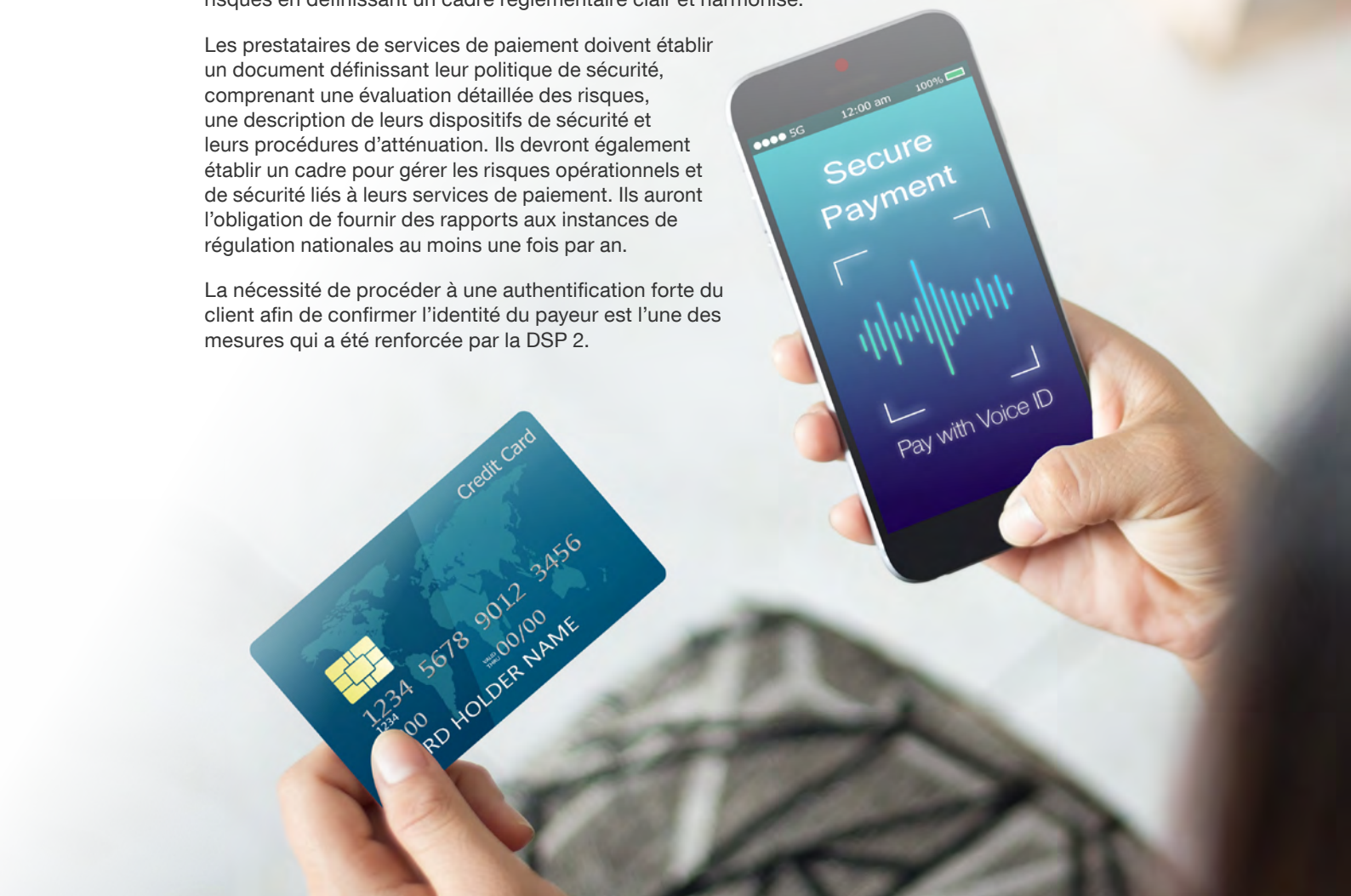
Plus de transparence sur les coûts et une meilleure protection contre les frais permettront de mieux protéger les consommateurs. En réponse à l'augmentation de la cybercriminalité et de la fraude en ligne, la DSP 2 poursuit la tendance en faveur du renforcement de la sécurité des paiements. L'organisme bancaire ou de services financiers est responsable des paiements non autorisés, à moins qu'il ne soit en mesure de démontrer que l'opération a été dûment authentifiée et qu'aucune défaillance technique n'est survenue.

SÉCURITÉ DES PAIEMENTS

Les risques de sécurité liés aux paiements électroniques ont augmenté ces dernières années, notamment en raison de la complexité technique accrue, de l'augmentation constante du volume des paiements électroniques et du développement de nouveaux types de services de paiement. Selon la DSP 2, la responsabilité des risques de sécurité revient aux prestataires de services de paiement. La DSP 2 vise à limiter ces risques en définissant un cadre réglementaire clair et harmonisé.

Les prestataires de services de paiement doivent établir un document définissant leur politique de sécurité, comprenant une évaluation détaillée des risques, une description de leurs dispositifs de sécurité et leurs procédures d'atténuation. Ils devront également établir un cadre pour gérer les risques opérationnels et de sécurité liés à leurs services de paiement. Ils auront l'obligation de fournir des rapports aux instances de régulation nationales au moins une fois par an.

La nécessité de procéder à une authentification forte du client afin de confirmer l'identité du payeur est l'une des mesures qui a été renforcée par la DSP 2.



Authentification forte du client (SCA)

L'authentification forte du client, un nouveau règlement européen qui vise à réduire la fraude et à renforcer la sécurité des paiements en ligne, est l'un des principaux piliers de la DSP 2.

À compter de la date d'entrée en vigueur de la SCA (31 décembre 2020)[3], au moins deux facteurs dans les trois catégories ci-dessous devront être utilisés pour le traitement des paiements.

Connaissance

Quelque chose que seul l'utilisateur **connaît** (PIN, mot de passe, etc.)

Possession

Quelque chose que seul l'utilisateur **possède** (carte de crédit, token RSA, etc.)

Inhérence

Quelque chose que l'utilisateur **est** (reconnaissance vocale ou faciale, biométrie comportementale...)

Les prestataires de services de paiement doivent respecter les exigences relatives à l'authentification forte du client chaque fois qu'un client accède à son compte de paiement en ligne, initie une opération de paiement électronique ou exécute « une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse ».

De plus, certaines opérations de paiement à distance, notamment les paiements sur Internet et sur smartphone, devront permettre d'« établir un lien dynamique » avec un montant et un bénéficiaire spécifiques, générant un code d'authentification unique. Grâce à ce lien dynamique, toute modification du montant ou de l'identité du bénéficiaire invalidera le code.

3. L'Autorité bancaire européenne (ABE) a autorisé un délai supplémentaire avant l'entrée en vigueur. Celle-ci sera reportée au 31 décembre 2020.

Impact de l'authentification forte du client sur les services financiers

L'obligation d'appliquer la SCA concernera l'ensemble du secteur des paiements et les prestataires de services financiers en particulier. L'obligation d'authentification forte du client pour les paiements sur ordinateurs et appareils mobiles impliquera des changements de la part des prestataires de services financiers.

Pour permettre une authentification forte du client, la plupart des prestataires de services financiers ont opté pour le maintien d'un code ou PIN (mot de passe à usage unique) transmis par SMS. **Si la combinaison d'un token ou OTP (One Time Password) par SMS (élément de possession) et d'un élément de connaissance, tel qu'un mot de passe, répond d'un point de vue technique à l'exigence des deux facteurs, elle présuppose que l'appareil (la possession) du client qui reçoit l'OTP est sécurisé. C'est toutefois loin d'être le cas dans la réalité.**

L'article 22(4) des normes techniques de réglementation relatives à l'authentification forte du client et à la communication sécurisée dans le cadre de la DSP 2 stipule que « les prestataires de services de paiement doivent veiller à ce que le traitement et le routage des données de sécurité personnalisées et des codes d'authentification générés conformément au chapitre II aient lieu dans des environnements sécurisés suivant des normes sectorielles rigoureuses et largement reconnues. »

La multiplication des fraudes telles que les piratages de comptes et arnaques à la carte SIM (transferts de SIM) révèle un manque manifeste de sécurité dans les environnements cités dans l'article ci-dessus. Cela constitue une excellente raison pour les prestataires de services financiers d'abandonner le système OTP / SMS pour assurer une authentification forte du client, comme le fait de plus en plus le secteur des services financiers en Allemagne.

Des prestataires de services financiers comme Postbank, Raiffeisen Bank, Volksbank et Consorsbank ont annoncé leur intention de proscrire le système OTP / SMS en 2020, tandis que Deutsche Bank et Commerzbank suivront la même voie, ainsi que de nombreux autres certainement.

Responsabilité des prestataires de services financiers concernant la SCA

La DSP 2 représente une étape essentielle vers une meilleure protection des consommateurs en cas de perte, de vol, d'usurpation d'identité et d'exécution incorrecte. Les prestataires de services de paiement (PSP) sont désormais responsables des opérations de paiement qui n'ont pas été exécutées correctement. En conséquence, ils sont dans l'obligation de rembourser immédiatement à leurs clients le montant total de la transaction de paiement non autorisée.

Les utilisateurs des services de paiement ne sont tenus responsables qu'en cas d'acte frauduleux de leur part ou de négligence manifeste.

Ainsi, pour être en conformité avec la DSP 2, les prestataires de services financiers doivent mettre en place une solution efficace et sécurisée d'authentification forte du client pour réduire au maximum les risques d'usurpation d'identité, gagner la confiance de leurs clients et réduire les coûts liés à la fraude.

La conformité à la DSP 2 est devenue l'une des priorités numéro un des prestataires de services de paiement qui sont désormais responsables des dommages subis par leurs clients en cas de fraude.

Émergence de la biométrie

Pour mettre en place une authentification sécurisée des clients, les entreprises considèrent de plus en plus la biométrie comme une méthode d'authentification optimale qui améliore à la fois la sécurité et l'expérience client. Combinée à un élément de possession ou de connaissance, la biométrie peut vous aider à réussir une authentification forte et sécurisée à deux facteurs, sans créer de points de friction.

L'authentification biométrique, par ex. la reconnaissance faciale ou d'empreinte digitale, étant devenue courante sur les smartphones et tablettes, les utilisateurs se sont habitués à l'utiliser comme une alternative sûre et pratique aux mots de passe.

Les entreprises qui envisagent de mettre en place une authentification forte du client basée sur la biométrie doivent tenir compte des considérations suivantes :

- **Méthodes d'authentification biométrique natives et non natives :** si les méthodes d'authentification biométrique utilisées couramment sur les appareils mobiles (natives) simplifient le déploiement, il faut savoir qu'elles ne fournissent pas toutes un niveau élevé de sécurité, de précision et de protection contre les attaques. Les méthodes non natives garantissent une sécurité et une expérience plus homogènes, quel que soit le fabricant ou le modèle d'appareil. De plus, en fonction du fournisseur de solution biométrique, les méthodes non natives fournissent généralement davantage de précision et de fonctionnalités anti-usurpation.
- **Traitement biométrique côté appareil ou côté serveur :** le traitement biométrique côté appareil garantit que les données biométriques ne quittent jamais l'équipement. Ainsi, les entreprises n'ont pas à gérer l'inscription au service, le traitement et la mise en correspondance. Le traitement biométrique côté serveur permet, toutefois, d'utiliser les mêmes caractéristiques biométriques sur plusieurs canaux, par ex. l'empreinte vocale d'un client sur l'appli mobile et dans le centre d'appels d'une banque. En outre, l'inscription au service d'authentification biométrique côté serveur garantit une meilleure protection contre la fraude.
- **Choix des modalités biométriques :** les modalités passives, par ex. la biométrie comportementale, comme méthode efficace, invisible et sans friction d'authentification continue sur les canaux Web et mobiles, ont gagné en popularité. Par ailleurs, les modalités biométriques qui utilisent des capteurs intégrés à de nombreux appareils (reconnaissance faciale, vocale et d'empreinte digitale) sont également appréciées pour leur caractère familier et pratique.
- **Canaux concernés :** si la DSP 2 concerne principalement les transactions électroniques, il est important d'envisager un déploiement plus large de la biométrie qui vous permettra d'exploiter pleinement le potentiel d'une solution multicanaux englobant les canaux digitaux, le centre d'appels et les succursales physiques.

Pourquoi choisir Nuance ?

Les solutions biométriques de Nuance peuvent vous aider à répondre aux exigences de la DSP 2 et de la SCA en renforçant la sécurité des processus d'authentification et de prévention des fraudes et en améliorant dans le même temps l'expérience client et la fidélité à votre marque.

Les entreprises doivent trouver le juste équilibre entre trois objectifs :

1. Optimiser l'expérience client et maximiser la validation de transactions authentiques.
2. Minimiser les pertes liées à la fraude en détectant et en rejetant les transactions frauduleuses tout en réduisant le plus possible les faux positifs.
3. Maintenir sous contrôle les coûts opérationnels des activités de gestion de la fraude en automatisant les opérations de prévention et en réduisant la charge de travail des agents grâce à des alertes de haute qualité.

Le 21 juin 2019, l'Autorité bancaire européenne (ABE) a publié un avis validant l'utilisation de différents paramètres biométriques4 comme élément de la catégorie « inhérence », ouvrant la voie à la possibilité de mettre en place des procédures sophistiquées d'authentification forte non soumises à de possibles défaillances de sécurité dans les infrastructures de communication.

Les solutions biométriques d'authentification client et de détection des fraudes de Nuance reposent sur des algorithmes d'IA qui permettent une authentification rapide et fiable. Nuance fournit différentes modalités biométriques intégrées : haute précision, dispositifs anti-usurpation performants et détection des fraudes. De plus, un puissant moteur d'évaluation des risques permet la prise de décisions en temps réel sur la base de différents signaux de risque et de familiarité. Les solutions Nuance s'appuient sur de nombreuses années d'expérience dans le développement et la commercialisation de moteurs biométriques destinés aux entreprises, qui authentifient plus de 400 millions de clients dans le monde et sont utilisés par des centaines d'entreprises, notamment des établissements financiers internationaux de premier plan.

Nuance offre un large éventail de capacités biométriques :

Biométrie comportementale
Chaque personne interagit de manière unique avec ses appareils. Nuance Gatekeeper analyse les schémas de comportement biométriques comme la vitesse de frappe, la manière de tenir le téléphone, la pression et la surface des doigts ou encore les pauses lors de l'exécution d'une tâche. Si les comportements changent ou si le schéma comportemental correspond à celui d'un fraudeur potentiel, Nuance Gatekeeper peut augmenter le niveau de risque associé à la transaction. La biométrie comportementale est une méthode idéale pour renforcer l'authentification et réduire la fraude sur les canaux Web, mobiles et de chat, tout en étant totalement transparente pour le consommateur.

Biométrie vocale
Au sein de la biométrie, la biométrie vocale a atteint un haut niveau de maturité ces dernières années. Nuance est le leader mondial des solutions technologiques de biométrie pour le secteur financier avec plus de 500 clients et 400 millions d'empreintes vocales.

La technologie de biométrie vocale Nuance est capable de générer une empreinte vocale après analyse de centaines d'attributs et de caractéristiques physiques d'un individu (conduit vocal, langage, cavité buccale, etc.) et de ses caractéristiques vocales. Elle permet ainsi de vérifier l'identité de l'appelant avec un taux de précision supérieur à 99 %.

Cette empreinte vocale peut être utilisée pour identifier l'appelant sur un canal voix (SVI, centre d'appels) et sur les canaux digitaux (appli mobile, Web, e-mail, réseaux sociaux, etc.).

Reconnaissance faciale
La reconnaissance faciale se généralise car elle offre aux consommateurs un moyen transparent de confirmer leur identité grâce aux caméras haute résolution disponibles sur la plupart des smartphones et tablettes. Elle est aussi un élément dissuasif pour les fraudeurs car elle limite leur capacité à poursuivre leur activité criminelle face à une demande d'authentification par reconnaissance faciale.

La reconnaissance faciale est l'une des modalités proposées par Nuance Gatekeeper pour garantir une authentification sécurisée et haute précision et détecter les voix humaines.

ConversationPrint
ConversationPrint™ est une forme de biométrie comportementale totalement inédite sur le marché. Elle permet d'identifier les activités frauduleuses en temps réel à partir de termes et de schémas de langage sélectionnés ou du texte saisi pendant une interaction avec un agent humain ou un assistant virtuel sur les canaux digitaux et dans le centre d'appels. En analysant le vocabulaire, la structure des phrases, la grammaire, etc., ConversationPrint assure une authentification en continu pendant la conversation (une session de chat par ex.). Il offre aussi un moyen efficace de détecter la fraude en reconnaissant les scripts de conversation qui ressemblent aux schémas d'un fraudeur potentiel.

Nuance fournit aux entreprises des capacités biométriques multimodales renforcées par l'IA. Elles vous permettent de répondre aux exigences d'authentification forte du client tout en optimisant l'expérience client et en réduisant la fraude sur tous vos canaux d'interaction.

4. « L'inhérence peut regrouper la reconnaissance rétinienne, irienne, veineuse, faciale, vocale, des empreintes digitales et de la géométrie de la main ». Autorité bancaire européenne (21 juin 2019)

Détecteurs intelligents Nuance
Les détecteurs intelligents émettent des signaux de risque qui facilitent l'identification des fraudeurs.

Identification des voix humaines
Vérifie que l'interlocuteur est bien une personne humaine.

Identification des voix synthétiques
Détecte les voix synthétiques même avec un rendu parfait.

Identification des voix enregistrées
Détecte les fraudeurs qui utilisent un enregistrement de la voix de leur victime.

Identification géographique
Identifie le pays et la ville auxquels l'appareil est associé.

Identification du réseau
Analyse la qualité du réseau afin de détecter les changements suspects.

Identification du canal
Analyse l'ensemble de l'audio pour déterminer le type d'appareil utilisé pendant l'interaction.

Identification automatique du numéro
Analyse les métadonnées d'un appel téléphonique et détermine si l'appel entrant provient d'un client légitime.

Pourquoi Nuance ?

Nuance Communications (NASDAQ : NUAN) est une entreprise multinationale avec plus de 30 ans d'expertise dans les domaines de l'innovation, de la recherche, du développement et de la commercialisation de solutions biométriques et de technologies vocales et de compréhension du langage naturel basées sur l'intelligence artificielle (IA). Aujourd'hui, les solutions Nuance sont présentes dans la plupart des départements de service clientèle de grandes entreprises multinationales, créant de la valeur et améliorant l'expérience et la sécurité des clients.

Plus de 400 millions d'individus dans le monde valident leur identité auprès du service client grâce aux solutions de biométrie vocale Nuance. Depuis le début de l'année, plus de 8 milliards de transactions réussies basées sur la biométrie ont été réalisées, avec un seul cas signalé d'authentification frauduleuse, soit une économie annuelle de 2 milliards $ sur les coûts liés à la fraude.

Parmi nos clients qui utilisent les solutions biométriques Nuance pour l'authentification client et la prévention des fraudes figurent des entreprises leaders du secteur bancaire et des services financiers, des télécommunications, de l'assurance, de la grande distribution, de l'approvisionnement en énergie et des agences gouvernementales du monde entier. Vous trouverez ci-dessous des exemples de ces clients qui nous ont autorisés à utiliser leur logo dans nos publications :

Manulife · BARCLAYS · Royal Bank of Scotland · Crédit du Nord
HSBC · ING · TalkTalk For Everyone · BBVA · ANZ
USAA® · Telefónica · Santander · بنك أبوظبي التجاري ADCB
Australian Government Australian Taxation Office · ROGERS · Eastern Bank · VIRGINIA Credit Union
LLOYDS BANK · Vanguard · Deutsche Telekom · nab · TD

En savoir plus

Pour plus d'informations sur nos solutions biométriques et de sécurité pour l'authentification client et la prévention des fraudes cliquez ici.

Pour demander une démo d'un produit ou pour toute question, vous pouvez nous contacter directement par e-mail à l'adresse suivante : pilar.blasco@nuance.com

À propos de Nuance Communications, Inc.
Nuance réinvente la relation entre les entreprises et leurs clients à travers des solutions interactives intelligentes basées sur l'Intelligence Artificielle (IA). Notre objectif est de devenir le leader des solutions intelligentes de self-care et de service assisté pour les grandes entreprises du monde entier. Ces solutions sont basées sur des technologies différenciées : voix, biométrie vocale, assistants virtuels, chat en ligne et agents cognitifs. Elles assurent un service client homogène sur tous les canaux : SVI, applications mobiles, Web, Inbound, Outbound. Elles s'appuient sur l'expérience et le savoir-faire d'une équipe mondiale de professionnels de la conception et du développement. Nuance propose ses solutions à différentes entreprises du Fortune 2500, en direct ou par l'intermédiaire de son réseau mondial de partenaires.

NUANCE