NUANCE | WHAT'S NEXT BLOG

Autentification biométrique et prévention, Engagement client omnicanal

« Cela ne me concerne pas » – Pourquoi l'authentification est-elle importante pour les consommateurs.

Brett Beranek | Vice President & General Manager, Security & Biometrics

4 Mars 2021

L'équilibre entre faire en sorte que les clients se sentent à l'aise et en sécurité pour faire des transactions avec leur banques et leur introduire de nouveaux éléments de friction est ténu. La prise de conscience des consommateurs quant aux risques existants en ligne a pris une dimension particulièrement significative ces dernières années, les articles d'attaques de phishing et des arnaques en ligne paraissant régulièrement dans la presse. Cependant, nombreux sont les consommateurs qui ne font pas le lien entre ce qu'ils lisent et leurs actes en ligne. Les institutions financières pourraient dès lors considérer comme un véritable atout la mise en œuvre d'un processus de sécurité où le consommateur est conscient de qui se passe sans que cela ne crée de l'agacement additionnel pour eux. Tirer parti de la biométrie est un moyen d'y parvenir.

Comme si 2020 ne nous avait pas assez épargné, en Europe, la date limite pour la mise en œuvre de la DSP2 et du volet authentification forte client (SCA) des RTS (Regulatory Technical Standards) était au 31 Décembre 2020. Cette règlementation impacte le consommateur dans la manière d'accéder à leurs informations financières que ce soit en agence ou en ligne ou lors d'achats de biens et services en ligne, mais il n'est pas clair que l'industrie soit complètement prête.

Ce qui est clair c'est que ce sera un changement important pour nombre de consommateurs et que l'évangélisation de ces derniers autours de l'authentification forte a été inconsistante. Au mieux, quand les consommateurs se sont connectés à leur compte, ils ont été avertis de changements à venir et on leur a demandé pour certains des informations de contact comme l'email et de vérifier que leur numéro de téléphone était bien à jour. Toutefois, **au fur et à mesure que les banques ont introduit ces modifications, les clients ont été surpris et parfois frustrés de voir qu'il n'était plus possible d'effectuer des opérations aussi aisément qu'auparavant.**

Comme bien des choses, tant que ça ne leur arrive pas, les personnes pensent que la violation de leurs informations n'aura pas réellement d'impact sur leur vie et qu'elles sont en « sécurité ». Mais quand elles sont impactées, il existe un réflexe de surcompensation se traduisant par une minimisation des informations qui sont partagées et en ajoutant des niveaux additionnels d'authentification à leurs comptes.

Quelle que soit l'extrémité à laquelle se situent les consommateurs, à la fin de 2020, les clients en Europe vont devoir s'habituer à ces étapes supplémentaires qui vont leur être demandées, au regard de l'implémentation de l'authentification forte client. Cela signifie que plus le processus pourra être rendu simple, plus l'interaction aura des chances d'aboutir.

L'usage de la biométrie telles que les empreintes digitales, la rétine, la voix, la reconnaissance faciale démontre les multiples manières de l'implémenter. Le fait est qu'une étude récente réalisée par Mercator[iii], montrant que 41% des possesseurs de smartphone utilisent la biométrie pour s'authentifier sur leur téléphone et il est prévu que cette valeur grimpe jusqu'à 66% en 2024, indique que les gens ont de plus en plus confiance dans la biométrie et que l'usage sera probablement croissant du fait que ces informations sont stockés côté serveur, permettant d'offrir à cette fonctionnalité d'être mise a disposition sur de multiples canaux et appareils, qu'ils soient mobiles, ordinateurs, télévisions ou des objets connectés.

Avoir une vue complète du client est critique pour l'industrie bancaire. Etant donné que la biométrie peut être intégrée au travers de n'importe quel canal, que ce soit en agence, au téléphone, sur mobile ou en ligne et qu'elle apporte une expérience client fluide et sans friction, cela permet d'appliquer une sécurité au niveau du client et non pas au niveau de l'interaction ou au niveau de ses équipements. Ayant la capacité de centraliser les données biométriques, elles ont également la capacité d'utiliser des données bien plus riches pour prendre des décisions plus exactes tout en protégeant leurs clients des risques de fraudes et en minimisant la friction de leur expérience.

La simplicité de la biométrie de ne pas avoir besoin de se souvenir de mot de passe, ni de répondre à des questions de sécurité, ni d'avoir d'appareils supplémentaires sur soi et le fait que 2 éléments sont nécessaires parmi lesquelles la nécessité que la personne elle-même soit présente, signifie que le consommateur ressent que la sécurité est prise aux sérieux et que la donnée est plus complexe à compromettre et à répliquer. En complément, pour les procédés qui sont gérés de manière centralisée, peuvent être d'autant plus fluides qu'une analyse en profondeur permet de déployer une sécurité plus précise et que l'utilisateur peut être reconnu sur de multiples appareils même ceux qui ne sont pas les leurs lorsqu'ils sont en agence.

Parvenir à trouver un moyen d'authentifier le consommateur qui minimise la disruption de leur quotidien, aussi bien que la possibilité de pouvoir réinitialiser le procédé si un facteur d'authentification change, deviendra un élément différentiateur pour ceux qui ont besoin d'authentifier les clients, telles que les institutions financières et les émetteurs de cartes. Ceci a été confirmé par la manière dont les comportements des consommateurs et des fraudeurs évoluent et que les solutions omnicanales peuvent fournir une expérience fluide qui feront suite à ces changements.

Aujourd'hui, les institutions financières rapportent une augmentation de 250% des transactions digitales et Mckinsey estime que dans une « nouvelle norme » du COVID, la part des besoins basiques bancaires gérées en agences pourrait tomber jusqu'à 5%. Dans ce nouveau monde, **le besoin des banques de s'assurer qu'elles interagissent avec le véritable client en deviendra d'autant plus fort mais bien plus difficile au regard de la nature distancielle de cette interaction.**

Les conditions de crises créent de nouveaux risques pour les établissements financiers du fait que la fraude prend de l'essor. **Un établissement financier avec lequel nous travaillons a observé une augmentation de 400% dans les tentatives de fraude pendant la pandémie et pour de nombreux canaux digitaux s'appuyant sur d'anciennes méthodes d'authentification (Code PIN et mots de passes), notamment pour ceux déjà bien établis, cette augmentation peut devenir très perturbante.** La manière d'authentifier les clients dans les canaux digitaux n'a pas évolué, tout particulièrement en comparaison avec les centres d'appels. Dans ces derniers, il n'y a pas d'appareil pour l'authentification, au lieu de cela, l'authentification doit être résolue avec une approche côté serveur, ce qui ouvre la porte à la biométrie de remplacer complètement l'authentification basée sur la connaissance. Là encore, cela permet au client d'effectuer le processus d'authentification avec une disruption minimale de son expérience mais elle procure le sentiment que la sécurité est au cœur de l'interaction. Ainsi, **l'expérience des centres d'appels doit être étendu à d'autres canaux digitaux et avec la sécurité des données et la précision de l'authentification comme fondamentaux.**

L'adoption de la biométrie est un facteur clé pour répondre à des besoins de sécurité, tout en augmentant l'engagement client, notamment avec le monde digital qui ne cesse de s'étendre. Pour les banques, cette capacité va permettre aux clients de s'engager sans friction avec leurs banques tout en sentant que leurs informations et leurs interactions seront sécurisées.

Tags:

More Information

Voir maintenant

Ne manquez pas cet entretien avec Enrique Tellado, PDG d'EVO Banco, et Pedro Serrahima, directeur de l'expérience client chez Telefónica Espagne. Ils vous parleront de leur expérience et des résultats de la mise en œuvre de Voice ID chez EVO et d'un système de détection de l'âge chez Telefónica. Deux projets d'envergure basés sur la biométrie vocale et l'IA au service de l'expérience client et de la prévention de la fraude.

Learn more

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