AWARE

BOOTH
N°C36

Au-delà de l'authentification : La validation biométrique de l'identité en combat contre la fraude à sa fondation

David Benini, Vice-président marketing produit, Aware, Inc.

Certaine forme de vol d'identité est au cœur de la plupart des fraudes à motivation financière. Une prolifération des informations personnelles identifiables (PII) sur les réseaux sociaux est facilement accessible aux fraudeurs, tandis que l'anonymat du commerce et la communication sur Internet leur donne une grande couverture pour l'usurpation d'identité qui est de plus en plus commis par les organisations criminelles sophistiquées opérant au-delà de la portée des lois dépassées qui ne traitent pas de tels crimes. En plus la fraude d'identité synthétique, basée sur la création habile d'identités fictives, qui utilise des éléments volées est la forme prédominante de fraude d'identité, contre laquelle les systèmes de gestion d'identité doivent être rendus résilients.

La biométrie était principalement l'affaire des gouvernements depuis de nombreuses années. Aujourd'hui, les capteurs biométriques sont omniprésents et des millions de personnes utilisent la biométrie plusieurs fois par jour pour l'authentification. Il est maintenant difficile de se souvenir d'une époque où l'association de la biométrie et de la criminalité était réflexive ; une notion que la collecte de mes empreintes digitales - et encore moins une photo « Mugshot » - représente l'accusation et la méfiance inhérente. Il s'agit d'un changement dans la façon dont les consommateurs perçoivent la biométrie. La photo d'identité est devenue un selfie. Et l'association n'est pas avec le crime, mais avec la haute technologie, de commodité et de futurisme. Nous comprenons mieux, aussi, les risques qui se cachent dans le domaine numérique ; nous comprenons à quel point notre identité numérique peut être puissante, et ce qui peut arriver si nous ne la protégeons pas.

Et après ? La technologie biométrique utilisée par les gouvernements pour rechercher des bases de données criminelles et des listes de surveillance peut également être très utile pour les entreprises commerciales qui essaient de dénicher des fraudeurs qui tentent d'ouvrir de nouveaux comptes à des fins infâmes. La biométrie fait rapidement son chemin dans le courant dominant. Plus visiblement, nous voyons des capteurs d'empreintes digitales intégrés dans les téléphones intelligents comme un mode plus pratique d'accès sécurisé à un appareil pour son propriétaire. Ces dispositifs permettent de plus en plus l'utilisation de la biométrie vers des modèles de paiement mobile plus sécurisés qui visent à éviter les pièges de sécurité des cartes de crédit. La fonctionnalité d'authentification biométrique fournie dans la version récente de Microsoft Windows 10 peut être utilisée pour sécuriser l'accès aux systèmes externes et aux sites Web, en prenant en charge les modalités d'empreintes digitales, de visage et d'iris.

La fraude à l'identité et ses crimes dérivés coûtent des centaines de milliards de dollars chaque années aux banques, détaillants, fournisseurs de soins de santé, gouvernements et, en fin de compte, aux consommateurs et aux contribuables du monde entiers, et ce chiffre continue de croître.

L'utilisation de la biométrie augmente parce que nos empreintes digitales, nos visages, nos iris et nos voix ont des propriétés vraiment spéciales qui en font un obstacle efficace pour les fraudeurs qui tentent de nous imiter subrepticement. C'est la valeur de l'authentification biométrique pour l'utilisateur final. Mais du point de vue bancaire, d'une agence gouvernementale ou de toute autre organisation visant à réduire largement son exposition à la fraude d'identité, une approche plus universelle est nécessaire pour avoir un large impact. Voici pourquoi :

1. Une grande partie de la fraude d'identité est commise en utilisant des identités «synthétiques» qui ne sont pas volées mais créées. L'authentification biométrique ou la vérification seule ne permet pas de résoudre ce type de fraude.

2. La vérification biométrique ne vérifie pas l'authenticité des données d'identité ; seulement que la personne qui vérifie est la même qui a enregistré les données. Cela signifie que la vérification biométrique sur un appareil aide à empêcher un fraudeur d'utiliser un appareil volé pour réclamer faussement l'identité du propriétaire, mais ne l'empêche pas d'établir des comptes avec des informations frauduleuses.

3. La pénétration des smartphones est en croissance rapide, mais elle n'est encore que de l'ordre de 36% dans le monde (GSMA Intelligence, 2015). Dans les endroits où beaucoup de gens n'utilisent toujours pas les smartphones, d'autres mécanismes sont nécessaires pour prévenir la fraude d'identité plus universellement.

4. L'authentification sur les smartphones est spécifique à l'appareil et contrainte à fonctionner telle que mise en œuvre par les fournisseurs d'appareil, le système d'exploitation et les applications.

Fondamentalement, il existe de nombreux modes de fraude d'identité qui ne peuvent pas être résolus par l'amélioration du mot de passe. Plus que « quelque chose que nous sommes », la biométrie nous permet de nous lier de façon permanente à l'information numérique ; une capacité puissante qui nous permet non seulement d'authentifier biométriquement, mais aussi de dédupliquer biométriquement; c'est-à-dire, pour déterminer par la recherche biométrique si quelqu'un tente subrepticement d'établir une fausse identité. Autrement dit, la vérification d'identité avec la recherche biométrique permet d'assurer l'intégrité de nos données d'identité : une identité représente chaque personne, chaque personne a une seule identité et les données d'identité associées à une donnée biométrique peuvent être fiables.

Une preuve d'identité robuste exige que l'inscrit présente des documents d'identité et des informations en personne dans le cadre d'une demande ou d'un processus d'intégration. Le processus peut également utiliser des sources de données publiques et privées. Une inscription biométrique et une recherche effectuée dans le cadre de ce processus constituent un « double contrôle » très fiable pour s'assurer que le demandeur n'est pas déjà enregistré dans le système, peut-être avec des informations d'identité différentes. Si, lors de l'inscription, une recherche biométrique établit une correspondance avec une identité et des informations différentes de celles qui sont revendiquées, l'enquête se poursuivra pour une bonne raison.

Une fois qu'une vérification de doublons est effectuée, une inscription biométrique lie numériquement l'enregistrement unique de confiance de l'enrôlé à eux physiquement à travers leur biométrie. Ces données biométriques peuvent ensuite être utilisées perpétuellement pour empêcher de futures tentatives de fausse représentation de leurs informations d'identité par un fraudeur. Le processus établit également un haut niveau de confiance dans l'authenticité des données d'identité associées à la biométrie inscrite, ce qui les rend plus utiles pour de futures authentifications biométriques. Tandis que la vérification d'identité biométrique nécessite des efforts supplémentaires pour vérifier l'intégrité des données d'identité et détecter les doublons, elle constitue un autre obstacle très efficace à la fraude.

CONCLUSION

La validation biométrique d'identité apparaîtra comme une approche clé de prévention de la fraude d'identité ; un moyen de valider l'intégrité de l'information d'identité au moment de la collecte. Il complètera l'authentification biométrique, permettant un plus haut degré de confiance dans la validité et l'unicité de l'identité revendiquée.