jumio | Signaux de risque

Atténuation des risques tout au long du cycle de vie du client

Pour de nombreuses entreprises, la vérification de l'identité nécessite plus qu'une simple vérification de la pièce d'identité. Les signaux de risque avancés de Jumio offrent une assurance supplémentaire et une confiance que vos clients sont bien ceux qu'ils prétendent être - et qu'ils ne présentent pas de risque inutile pour votre entreprise - lors de l'ouverture de compte et à chaque fois qu'ils reviennent sur votre plateforme.

Le hub de données complet de Jumio donne accès à plus de 500 sources de données pour confirmer les informations personnellement identifiables (PII) de vos clients et évaluer leur risque. Un score de risque composite facilite l'obtention d'une réponse oui/non et permet de prendre automatiquement des décisions dans vos flux de travail.

Voici quelques-uns des principaux services de gestion des risques que Jumio propose :

Vérification de l'identité mondiale

Passez le nom, l'adresse, le numéro de téléphone et l'e-mail de l'utilisateur dans un réseau de bases de données d'identité mondiale pour obtenir l'assurance qu'ils appartiennent à cette personne et pour évaluer le risque global de la personne. Ce service détermine la validité de chaque point de données - tel que la vérification que l'e-mail appartient réellement à cette personne - et détermine le risque en fonction du comportement, tel que l'attribution d'un risque plus élevé si le téléphone est associé à de nombreuses adresses IP. Après avoir évalué tous ces facteurs, le service renvoie une seule note de risque pour la personne, que vous pouvez ensuite utiliser dans vos règles pour déclencher des procédures KYC plus strictes au besoin.

Ce service est particulièrement utile comme vérification légère lors de l'ouverture de compte pour déterminer si des vérifications supplémentaires sont nécessaires, ou pour la surveillance continue des risques de vos clients existants.

Vérification de l'adresse IP géographique

Vérifiez le risque et la réputation de l'adresse IP de l'utilisateur et déterminez l'emplacement de son fournisseur de services Internet (ISP).

Ce service est particulièrement utile pour arrêter le parcours de l'utilisateur avant même qu'il ne commence s'il tente de cacher sa véritable localisation ou si son adresse IP a une vitesse anormalement élevée pouvant être attribuée à un bot.

Vérification de l'appareil

Évaluez le risque de l'appareil de l'utilisateur grâce à des indicateurs tels que l'historique étendu de l'appareil, les anomalies de l'empreinte digitale, les modèles d'utilisation et les émulateurs. Découvrez si un fraudeur utilise une émulation GPS, le rootage de l'appareil, des VPN ou des proxies pour masquer son emplacement à haut risque et tromper votre flux d'identification en ligne.

Comme ce service s'exécute en arrière-plan avant que l'utilisateur n'ait saisi des informations, il constitue une excellente vérification sans friction à exécuter dès le début du parcours d'ouverture de compte ou de transaction numérique.

Vérification de l'adresse e-mail

Évaluez le risque d'une adresse e-mail en évaluant sa vélocité, son ancienneté, les détails du domaine, le pays, l'historique de fraude et d'autres détails.

Ce service renvoie des informations détaillées sur l'adresse e-mail afin que vous puissiez prendre une décision éclairée.

Vérification du numéro de téléphone

Déterminez le risque et la réputation d'un numéro de téléphone. Ce service examine les modèles d'utilisation (y compris le trafic vocal), la vélocité d'utilisation et les attributs des données téléphoniques tels que le type de téléphone et les informations sur l'opérateur. Il vérifie également le numéro auprès du Global Phone Data Consortium pour l'historique de fraude, évalue le comportement de messagerie et identifie s'il se trouve dans une plage de numéros de téléphone qui sont vus à plusieurs reprises sur un ou plusieurs services web, ce qui pourrait indiquer qu'un profil numérique est partagé.

Le service renvoie une note de risque et des données supplémentaires pouvant guider votre flux de travail, telles que la nécessité pour les utilisateurs dont les numéros de téléphone sont bloqués d'entrer un numéro non bloqué.

Vérifications d'adresse

Validez et corroborez les adresses avec des sources tierces indépendantes. Déterminez si l'adresse extraite d'une pièce d'identité délivrée par le gouvernement existe dans le monde réel, et voyez si la personne vérifiée habite réellement à l'adresse figurant sur sa pièce d'identité. Jumio vérifie l'adresse auprès de plusieurs sources de données de confiance (par exemple, USPS, Royal Mail) pour formater correctement l'adresse, s'assurer qu'elle existe dans une juridiction donnée, et vérifier que la personne y habite.

Ce service est utile pour se conformer aux réglementations régionales qui exigent de valider les adresses et d'établir la preuve de la résidence en utilisant des sources publiques indépendantes.

Vérifications dans les bases de données gouvernementales

Vérifiez que les données fournies par l'utilisateur ou extraites de la carte d'identité correspondent aux données détenues par la juridiction qui a délivré le document légal.

Ce service vérifie les bases de données gouvernementales dans le monde entier.

Vérification du numéro de sécurité sociale

Vérifiez que le nom et l'adresse (et éventuellement la date de naissance et le numéro de téléphone) correspondent au numéro de sécurité sociale en consultant des bases de données telles que l'Administration de la sécurité sociale, l'USPS, les agences de crédit et d'autres sources exclusives.

Ce service est utile comme vérification légère pour les utilisateurs américains.

Quels signaux de risque ai-je besoin ?

Toutes les entreprises peuvent bénéficier de la vérification de la réputation de l'appareil avant même que l'utilisateur n'entre son nom, ce qui vous permet de rediriger les utilisateurs suspects vers des flux de travail plus rigoureux tout en simplifiant l'expérience pour vos clients légitimes. Vous pouvez également effectuer une vérification d'identité mondiale pour filtrer les identités suspectes avant d'effectuer des vérifications plus strictes. Vous pouvez vérifier l'adresse IP de l'utilisateur pour empêcher les utilisateurs dans des emplacements interdits d'accéder à votre plateforme. De même, si vous permettez aux clients de transférer de l'argent entre eux, vous pourriez déterminer si la transaction a lieu dans un emplacement à haut risque qui nécessiterait des vérifications KYC ou LCB/FT plus strictes. Et pour une surveillance encore plus approfondie, vous pouvez effectuer une vérification de l'adresse, du numéro de téléphone et de l'e-mail ainsi que des vérifications dans les bases de données gouvernementales lors de l'ouverture de compte et effectuer périodiquement des vérifications d'identité sur les clients existants. Jumio facilite le choix des signaux de risque qui répondent à vos besoins commerciaux spécifiques et à votre tolérance au risque.