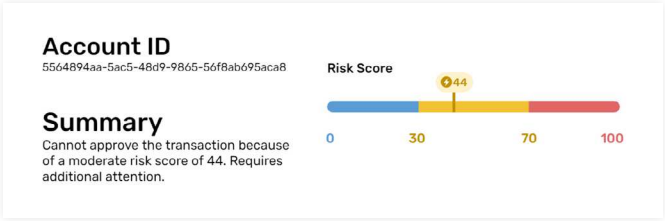
jumio | **Risikosignale**

Minderung kundenbezogener Risiken während des gesamten Lebenszyklus

Für viele Unternehmen erfordert der Identitätsnachweis mehr als nur die Überprüfung einer Identität. Die fortschrittlichen Risikosignale von Jumio bieten zusätzliche Sicherheit und Vertrauen, dass Ihre Kunden legitim sind und Ihr Unternehmen während des Onboardings und jedes Mal, wenn sie auf Ihre Plattform zurückkehren, nicht bedrohen.

Das umfassende Datenzentrum von Jumio bietet Zugriff auf über 500 Datenquellen, um die personenbezogenen Daten Ihrer Kunden zu bestätigen und ihr Risiko zu bewerten. Eine zusammengesetzte Risikobewertung macht es einfach, eine Ja/Nein-Antwort zu erhalten und Entscheidungen in Ihren Arbeitsabläufen automatisch zu treffen.

Im Folgenden sind einige der wichtigsten Risk Signals aufgeführt, die Jumio anbietet.



Device Risk

Bewerten Sie das Risiko des Geräts des Benutzers, indem Sie dessen IP-Adresse, Betriebssystem und Alter ermitteln. Finden Sie heraus, ob ein Betrüger GPS-Emulation, Geräte-Rooting, VPNs oder Proxys verwendet, um seinen risikoreichen Standort zu verschleiern und Ihr Online-Identifizierungssystem zu täuschen.

Da dieser Dienst im Hintergrund ausgeführt wird, bevor der Benutzer Informationen eingegeben hat, ist er eine hervorragende, reibungslose Überprüfung, die ganz am Anfang der Onboarding-Reise oder digitalen Transaktion ausgeführt werden kann.

Telefonrisiko

Bestimmen Sie das Risiko und den Ruf einer Telefonnummer. Dieser Dienst untersucht Nutzungsmuster (einschließlich Sprachverkehr), Nutzungsgeschwindigkeit und Device-Merkmale wie Telefontyp und Netzbetreiberinformationen. Es vergleicht die Nummer auch mit dem Global Phone Data Consortium auf Betrugsgeschichte, wertet das Nachricht-Verhalten aus und identifiziert, ob es sich um eine Reihe von Telefonnummern handelt, die wiederholt auf einem oder mehreren Webdiensten angezeigt werden, was darauf hindeuten könnte, dass ein digitales Profil geteilt wird.

Der Dienst gibt eine Risikobewertung und zusätzliche Daten zurück, die Ihren Arbeitsablauf leiten können, z. B. die Anforderung, dass Benutzer mit gesperrten Telefonnummern aufgefordert werden, eine nicht gesperrte Nummer einzugeben.

E-Mail-Verifizierung

Bewerten Sie das Risiko einer E-Mail-Adresse, indem Sie Geschwindigkeit, Alter, Domänenangaben, Land, Betrugsgeschichte und andere Einzelheiten auswerten.

Dieser Dienst gibt detaillierte Informationen über die E-Mail-Adresse zurück, damit Sie eine fundierte Entscheidung treffen können.

eKYC-ID-Datenbanken

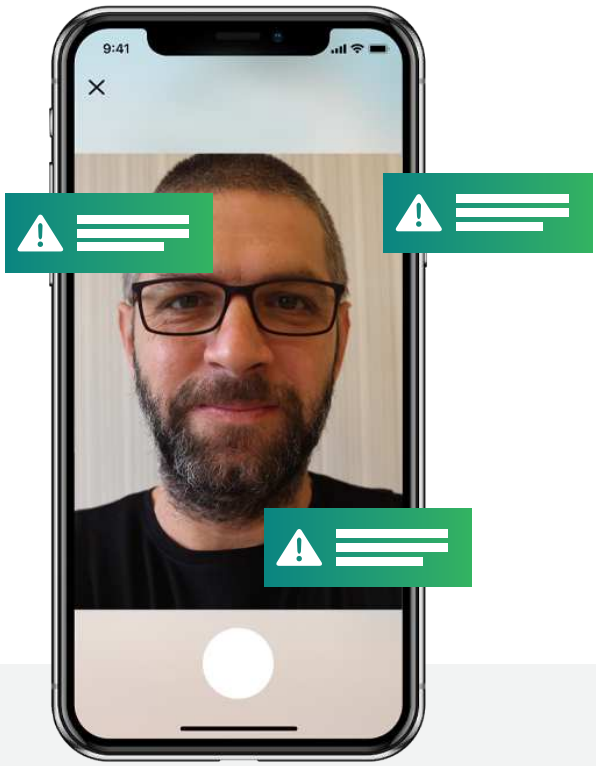
Geben Sie den Namen, die Adresse, die Telefonnummer und die E-Mail-Adresse des Benutzers in ein Netzwerk globaler Identitätsdatenbanken ein, um sicherzustellen, dass sie dieser Person gehören und um das Gesamtrisiko der Person einzuschätzen. Dieser Dienst bestimmt die Gültigkeit jedes Datenpunkts – wie z. B. die Überprüfung, ob die E-Mail tatsächlich dieser Person gehört – und bestimmt das Risiko basierend auf dem Verhalten, z. B. die Zuweisung eines höheren Risikos, wenn das Telefon mit vielen IP-Adressen verknüpft ist. Nach der Bewertung all dieser Faktoren gibt der Dienst eine einzelne Risikobewertung für die Person zurück, die Sie dann in Ihren Regeln verwenden können, um bei Bedarf strengere KYC-Verfahren auszulösen.

Dieser Dienst ist bei der laufenden Risikoüberwachung Ihrer aktuellen Kunden besonders nützlich.

Adressdienste

Validieren und bestätigen Sie Adressen mithilfe von unabhängigen Drittquellen. Stellen Sie fest, ob die aus einem amtlichen Ausweis extrahierte Adresse in der Wirklichkeit besteht und prüfen Sie, ob die zu verifizierende Person tatsächlich an der Adresse auf ihrem Ausweis lebt. Jumio vergleicht die Adresse mit einer Reihe vertrauenswürdiger Datenquellen (z. B. USPS, Royal Mail), um sie richtig zu formatieren und sicherzustellen, dass die Adresse in einer bestimmten Gerichtsbarkeit besteht.

Dieser Dienst ist nützlich, um regionale Vorschriften einzuhalten, die von Ihnen verlangen, Adressen zu validieren und eine Meldebestätigung mithilfe unabhängiger öffentlicher Quellen festzustellen.



Welche Risikosignale brauche ich?

Alle Unternehmen können davon profitieren, ein Gerät zu überprüfen, bevor der Benutzer überhaupt seinen Namen eingibt, sodass Sie verdächtige Benutzer auf strengere Arbeitsabläufe umleiten und gleichzeitig die Erfahrung für Ihre guten Kunden optimieren. Wenn Sie es Kunden ermöglichen, Geld untereinander zu überweisen, können Sie feststellen, ob die Transaktion an einem Ort mit hohem Risiko stattfindet, der strengere KYC- oder GwG-Prüfungen erfordern würde. Und für noch genauere Ergebnisse können Sie während des Onboardings eine Adress-, Telefon- und E-Mail-Überprüfung und regelmäßig eKYC-Datenbankprüfungen bei bestehenden Kunden durchführen. Jumio erleichtert die Auswahl der Risikosignale, die Ihren spezifischen Geschäftsanforderungen und Ihrer Risikotoleranz entsprechen.