jumio | Liveness-Erkennung

Verhindern Sie Betrug von Anfang an

Der ideale Zeitpunkt, Betrug zu verhindern, ist während des Onboarding Prozesses. Dies ist auch die beste Zeit für Identitätsfälschung. Die von Ihnen gewählte biometrische Identity Lösung muss über robuste Anti-Manipulations-Maßnahmen verfügen. Manche behaupten, das zu tun. Andere können es beweisen.

Die NIST-konforme Lebenderkennung Jumios schützt Ihr Ökosystem nachweislich vor manipulativen Angriffen und anderen Arten von Identitätsbetrug, indem sie sicherstellt, dass die beim Onboarding erfassten Bilder einen echten Menschen darstellen und nicht durch Manipulation entstanden sind.

Hochmoderne Technologie

Die Technologie von Jumio zur Erkennung von Liveness wird ständig weiterentwickelt, um neuen Bedrohungen immer einen Schritt voraus zu sein. Wir verwenden branchenführende, patentierte Techniken, um Spoofs wie Video- und Kamera-Injection-Angriffe zu erkennen. Unsere Lösung hat die Tests des NIST/NVLAP-akkreditierten Labors iBeta für ISO-Angriffserkennung bestanden, die gemäß dem ISO/IEC 30107-3-Standard und im Einklang mit dem ISO/IEC 30107-1-Rahmen durchgeführt wurden.

Vorteile

Betrüger erkennen und abschrecken

Sich überzeugen, dass Ihre Benutzer echte Menschen sind

Verwandeln Sie Besucher schneller in Kunden mit einem nahtlosen Erlebnis über Mobilgeräte oder

Wie Lebenderkennung zu Ihrer Identitätsprüfung passt

1. Ausweisprüfung

Ist das Ausweisdokument (ID) authentisch und gültig?

2. Selfie + Liveness Prüfung

Ist die Person, die den Ausweis besitzt, dieselbe auf dem Ausweisfoto abgebildete Person? Ist sie während der Transaktion physisch anwesend?

3. Risikobasierte Entscheidung

Jumio berechnet das Betrugsrisiko und genehmigt oder lehnt die Identitäts-Transaktion innerhalb von Sekunden auf Grundlage Ihrer vordefinierten Risikotoleranzen ab.

jumio

Erfahren Sie mehr unter **jumio.com/de**