Online-Betrug immer einen Schritt voraus

PayPal Open

Betrug ist auf dem Vormarsch

Betrug kann bei jeder Interaktion zwischen einem Unternehmen und Kund:innen eine Bedrohung darstellen.

- **Vor einer Transaktion** – wenn Kund:innen ihre Daten teilen, um Konten zu erstellen.
- **Während einer Transaktion** – wenn Zahlungen verarbeitet werden.
- **Nach einer Transaktion** – wenn Kund:innen die Gebühren anfechten.

Die Betrugsbekämpfung muss jedoch nicht mit der Kundenzufriedenheit kollidieren. PayPal bietet eine einzige Plattform für eine umfassende Zahlungsabwicklung, globale Skalierbarkeit und profitables Geschäftswachstum. Die richtigen Tools können Ihnen dabei helfen, Ihr Unternehmen effizient zu führen, die Autorisierungsraten zu erhöhen, die Kosten zu senken und Betrugsfälle zu reduzieren.

In diesem E -Book erfahren Sie, wie Sie dabei am besten vorgehen.

Voraussichtlich werden die E-Commerce-Umsätze bis 2028 fast

$8 Billionen

US-Dollar erreichen[1]

[1] Statista, April 2025, „Global retail e-commerce sales 2022-2028."

Digitale Kanäle sind inzwischen für

52 %

aller Verluste durch Betrug verantwortlich und übertreffen damit erstmals den physischen Betrug.[2]

Betrüger:innen nutzen KI, um sich weiterzu-entwickeln und zu expandieren

Durch KI und soziale Medien ist Betrug für jeden einfach geworden.

Betrug kann teuer sein – sowohl kurz - als auch langfristig:

- Wenn ein Unternehmen regelmäßig das Ziel von Bertrüger:innen wird, könnte ein Kartenanbieter es als riskantes Unternehmen einstufen und Strafen auferlegen. Ein Zahlungsdienstleister könnte sich auch weigern, die Transaktionen dieses Unternehmens zu bearbeiten.
- Der Ruf eines Unternehmens kann darunter leiden. Eine einzige schlechte Erfahrung kann Kund:innen dazu verlassen, dem Unternehmen für immer den Rücken zuzukehren. Potenzielle Kund:innen könnten auch von schlechten Bewertungen oder negativer Mundpropaganda abgeschreckt werden.
- Die Zeit, die für die Betrugsbekämpfung aufgewendet wird, kann Unternehmen dann dafür fehlen, sich auf ihre Kernkompetenzen zu konzentrieren und im Wettbewerb zu bestehen.

[2] Forrester, Februar 2024, „LexisNexis® True Cost of Fraud™ Study – EMEA."

94%

der deutschen Kund:innen gaben an, dass sie beim Onlinekauf eine frühzeitige Betrugsbekämpfung schätzen.[3]

Seien Sie offen für Geschäfte. Aber bleiben Sie geschlossen für Betrüger:innen.

Ihr Unternehmen muss sich nicht zwischen effizienter Zahlungsabwicklung und Betrugsbekämpfung entscheiden. Eine wachstumsfreundliche Betrugsprävention kann Ihnen dabei helfen, Betrug zu bekämpfen und gleichzeitig zu wachsen.

Arbeiten Sie mit einem Zahlungsdienstleister zusammen, um Hilfe bei der Betrugsbekämpfung zu erhalten

Ein Zahlungsdienstleister mit globalen Tools zur Betrugsbekämpfung, wie PayPal, kann Ihrem Unternehmen dabei helfen, böswillige Akteure offline und online abzuwehren. Diese Tools arbeiten zusammen, um betrügerische Transaktionen zu markieren, ohne dass die Kauferfahrung guter Kund:innen darunter leidet.

Wählen Sie Lösungen zur Betrugsbekämpfung auf mehreren Ebenen

Mehrschichtige Betrugsbekämpfungslösungen werden durch umfangreiche Datenbestände unterstützt. Diese können Händlern dabei helfen, Betrug über den gesamten Transaktionszyklus hinweg zu identifizieren und sich davor zu schützen. Wenn Unternehmen in mehrschichtige Lösungen, die in die Cybersicherheit und den Online-Kundendienst integriert sind, investieren, können sie Betrugsverluste verringern.

[3] IDC, im Auftrag von PayPal. Verbraucherumfrage unter insgesamt 8.000 Verbraucher:innen in Großbritannien, Irland, Spanien, den Niederlanden, Frankreich, Schweden, Deutschland und Italien (1.000 Verbraucher:innen aus jedem Markt) im Zeitraum von Dezember 2024 bis Januar 2025. Grundlage N = 1.000.

Erhöhen Sie die Autorisierungsraten. Reduzieren Sie Kosten. Verringern Sie Betrug.

Neue, strenge Compliance- und Regulierungsanforderungen helfen Händlern, ihre Kund:innen vor zunehmendem Betrug zu schützen. Der Authentifizierungsprozess hat sich über die einmalige Passwortabfrage hinaus weiterentwickelt – hin zu breiteren Identitäts- und Authentifizierungslösungen.

Tools, mit denen Unternehmen Informationen sicher und auf dem neuesten Stand halten können:

Kontoaktualisierungstools

Kreditkartenkonten bleiben auch mit abgelaufenen Karten aktiv. Betrüger:innen können diese Karten nutzen, um auf Finanzinformationen zuzugreifen oder betrügerische Transaktionen durchzuführen. Tools zur Kontoaktualisierung können sensible Karteninformationen, z. B. Nummern, Ablaufdaten und Kontenstatus, sicher verwalten und automatisch aktualisieren. Das kann das Betrugsrisiko eines Unternehmens senken.

Netzwerk-Tokenisierung

Die Tokenisierung des Netzwerks ersetzt die Primary Account Number (primäre Kontonummer, PAN) einer Debit- oder Kreditkarte durch einen unternehmensspezifischen Token. Danach wird ein einmaliges Kryptogramm für jede einzelne Transaktion mit diesem Unternehmen generiert. Netzwerktoken können Händler:innen dabei helfen, Betrug zu bekämpfen, indem sie einen sicheren Zahlungsweg bereitstellen.

Compliance-Tools

Hochentwickelte Authentifizierungstools, wie 3D Secure (3DS), können Händler:innen dabei helfen, die Vorschriften einzuhalten sowie Betrüger:innen fernzuhalten – und gleichzeitig positive Erfahrungen für gute Kund:innen zu ermöglichen. Unternehmen können 3DS aufrufen, um die Authentifizierung für bestimmte Anwendungsfälle und Regionen anzupassen. Dies kann Händlern dabei helfen, Betrüger zu erkennen und abzuschrecken.

KI und ML können falsche Positive um bis zu

86 %

reduzieren.[4]

Entscheiden Sie smarter – mit Risikointelligenz

Schützen Sie Ihr Unternehmen mit KI vor entstehenden Bedrohungen

KI und Machine Learning (ML) Tools können sich anpassen, um Betrugsmuster in Echtzeit aufzudecken. So können Unternehmen Betrug aufdecken, selbst wenn sich die Betrüger:innen weiterentwickeln.

Diese Tools können ein Profil über sich ständig ändernde Kaufmuster erstellen, womit die die Händler:in dann riskante Kund:innen und Transaktionen in Echtzeit erkennen können. Außerdem lassen sich so die Autorisierungsraten guter Kund:innen erhöhen.

Reduzieren Sie Betrug mit dynamischem Routing

Mit einer dynamischen Routingstrategie können Unternehmen Zahlungen über verschiedene Zahlungsdienstleister basierend auf ihren vorbestimmten Regeln routen.

Einige dynamische Routingsysteme können eine erweiterte Betrugserkennung beinhalten. Diese identifiziert betrügerische Transaktionen und hilft Händler:innen, gegen diese in Echtzeit vorzugehen.

[4] Legit Security, März 2024, „Using AI to Reduce False Positives in Secrets Scanners."

Seien Sie Betrug einen Schritt voraus

Reduzieren Sie Rückbuchungen

Unternehmen können Rückbuchungen im Voraus reduzieren, indem sie mit Zahlungsdienstleistern zusammenarbeiten, die einen Schutz vor Rückbuchungen anbieten. Ein Rückbuchungsschutz, der durch maschinelles Lernen unterstützt wird, kann Unternehmen dabei helfen, zu entscheiden, ob Transaktionen genehmigt oder wegen potenziellem Betrug abgelehnt werden sollen.

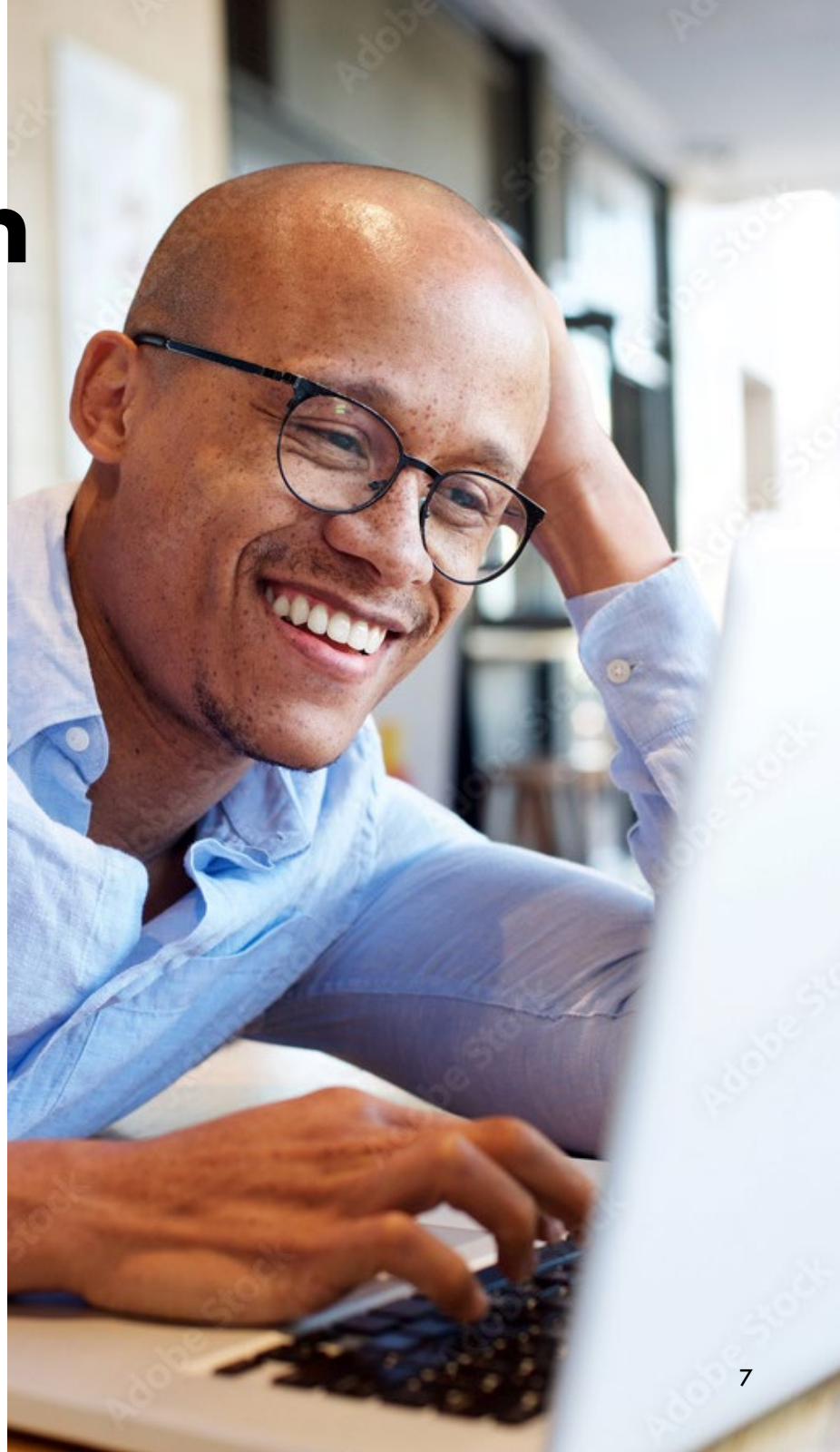
Ein Rückbuchungsschutz kann Unternehmen auch bei Folgendem helfen:

- Steigerung der Conversion und des Umsatzes aus guten Transaktionen.
- Schutz vor potenziell betrügerischen Transaktionen.
- Verringerung von Rückbuchungen, die zu höheren Bearbeitungsgebühren führen können.
- Reduzierung von falschen Ablehnungen oder von Ablehnungen legitimer Käufe.
- Vermeidung von unangenehmen Gesprächen mit Kund:innen.

Automatisches Rückbuchungsmanagement

Zahlungsdienstleister, die Tools anbieten, die den Prozess zur Beilegung von Streitigkeiten automatisieren, können Händler:innen dabei helfen, Streitigkeiten automatisch zu bekämpfen:

- Die Automatisierung von Streitfällen ermöglicht es einem Unternehmen, in großem Umfang auf Rückbuchungen zu reagieren. Ein Zahlungsdienstleister kann Antworten auf Streitfälle im Namen des Händler:ins automatisch erstellen und übermitteln.
- Der Rückbuchungsschutz hilft Ihnen dabei, die Rate Ihrer erfolgreichen Antworten auf Rückbuchungen zu erhöhen, und verschafft Ihnen Erkenntnisse, mit denen zukünftige Rückbuchungen vermieden werden können.



PayPal hilft Kiva, die Transaktionsprüfungsrate um 200 % zu senken

Die Aufgabe

Erhöhen Sie die Produktivität mit einer erweiterten Betrugslösung
Kiva, eine gemeinnützige Crowdfunding-Organisation, hatte ein kompliziertes Verfahren zur Betrugsbekämpfung. Jeden Monat mussten Tausende von Transaktionen manuell überprüft werden, einschließlich vieler falscher Positiver. Kiva wollte das Betrugsmanagement automatisieren, um sich mehr auf seine Mission konzentrieren zu können.

Die Lösung

Kiva integrierte den erweiterten Betrugsschutz von PayPal[5]
Kiva entschied sich für die adaptive Machine-Learning-Lösung von PayPal, die Organisationen dabei hilft, sich vor Betrug und dessen finanziellen Kosten zu schützen.

Der Effekt

Der erweiterte Betrugsschutz hilft bei der Reduzierung von Überprüfungen, optimiert die Produktivität und bietet maßgeschneiderte Analysen
Kiva verzeichnet nun 200 % weniger Transaktionen, die überprüft werden müssen. Der erweiterte Betrugsschutz bietet Berechnungen und Analysen, denen Kiva vertraut. Das gibt Kiva Vertrauen in die Effektivität des Tools gegenüber manueller Entscheidungsfindung.[6]

Lesen Sie die Fallstudie von Kiva und erfahren Sie, wie die Non-Profit-Organisation die manuelle Überprüfung von Transaktionen mithilfe von PayPal reduziert hat.

[5] Für das Tool zum Betrugsschutz gelten bestimmte Bedingungen und Ausschlüsse. Betrugsschutz ist für Konten verfügbar, die für erweiterte Kredit- und Debitkartenzahlungen angemeldet sind. Siehe Bedingungen.
[6] Die Daten stammen von Kiva; Vergleich des dritten Quartals 2023 mit dem dritten Quartal 2020. Diese Ergebnisse sind möglicherweise nicht typisch und können je nach Branche wesentlich variieren.

Checkliste

- ✔ Arbeiten Sie mit einem Zahlungsdienstleister wie PayPal und helfen Sie Ihrem Unternehmen dabei, Betrug zu bekämpfen.
- ✔ Wählen Sie mehrschichtige Betrugslösungen über die gesamte Transaktion hinweg.
- ✔ Optimieren Sie die Authentifizierung, um die Kundentransaktionen bestmöglich zu schützen.
- ✔ Nutzen Sie KI und schützen Sie Ihr Unternehmen vor sich entwickelnden Bedrohungen.
- ✔ Verwenden Sie smarte Routing-Systeme, um Betrug in Echtzeit zu reduzieren.
- ✔ Nutzen Sie den ML-gestützten Schutz, um Rückbuchungen proaktiv zu reduzieren.

Mit einem jährlichen Gesamtzahlungsvolumen von 1,68 Billionen US-Dollar[7] kann PayPal Einblicke und Lösungen bieten, die Ihrem Unternehmen helfen, Betrug ohne Reibungsverluste zu bewältigen.

Das Vertriebsteam von PayPal beantwortet gern Ihre Fragen.

Mehr erfahren

PayPal Open

[7] PayPal-Erträge des GJ 2024, basierend auf internen PayPal-Daten.