stripe

Überblick zum Thema Online-Betrug

Einleitung

Dieser Bericht bietet einen umfassenden Überblick über den Stand der Dinge beim Phänomen des Online-Betrugs. Wir haben in einem Zeitraum von zwei Jahren Milliarden von versuchten Zahlungen auf Stripe analysiert und gemeinsam mit Milltown Partners (in Zusammenarbeit mit Focaldata) mehr als 2.500 führende Unternehmensvertreter/innen aus neun Ländern (Australien, Kanada, Frankreich, Deutschland, Japan, Niederlande, Singapur, Vereinigtes Königreich und USA) befragt.

Durch die Kombination unserer Stripe-Analyse mit diesen Umfrageergebnissen können wir die größten Betrugstrends des vergangenen Jahres ermitteln. 2020 gab es beispielsweise einen Anstieg bei angefochtenen Zahlungen im Zusammenhang mit Produkten. Insbesondere Unternehmen mit wiederkehrenden Umsätzen sorgen sich um die finanziellen Auswirkungen von Betrug. Wir gehen auch darauf ein, wie Sie diesen Betrugstrends erfolgreich begegnen können. Der gesamte Bericht enthält Tipps auf der Grundlage der von uns ermittelten Daten. Am Berichtsende stehen vier die gesamte Thematik betreffende Best Practices auf Basis unserer Vorhersagen zur zukünftigen Entwicklung des Betrugsgeschehens.

Dieser Bericht ist in vier Abschnitte unterteilt:

- Warum steigen die Betrugsfälle?
- Wie unterscheidet sich das Phänomen des Betrugs je nach Region und Unternehmensgröße?
- Welche geschäftlichen Auswirkungen hat Betrug?
- Unsere Prognosen in Sachen Betrug

Zusammenfassung

- Unserer Umfrage zufolge sagen 64 % der Unternehmensverantwortlichen weltweit, dass seit Beginn der Pandemie die Betrugsbekämpfung im Unternehmen schwieriger geworden ist. Unserer Einschätzung nach liegt das zum Teil an der wachsenden Zahl von Betrugsarten und am Betrugsvolumen insgesamt.
- Zu Beginn der Pandemie stieg die Zahl der angefochtenen Zahlungen im Zusammenhang mit Produkten vorübergehend um 156 % an, etwa mit Fällen wie „Produkt nicht erhalten“ oder „Produkt nicht annehmbar“. Wir gehen davon aus, dass viele Kund/innen Rückbuchungen einforderten, weil es den Verkäufer/innen aufgrund von Unterbrechungen der Lieferkette wochen- oder sogar monatelang nicht möglich war, Bestellungen abzuwickeln.
- Außerdem beobachteten wir bei versuchten Kartentest-Angriffen einen Anstieg von 40 %. In der Pandemie wurden Tausende neue E-Commerce-Unternehmen gegründet. Unserer Auffassung nach hat dieses Wachstum betrügerischen Akteur/innen neue Chancen eröffnet.
- Weltweit stellten Unternehmen einen Anstieg von Betrugsfällen fest. Besonders vielen Betrugsangriffen waren – und sind – jedoch Unternehmen in Lateinamerika ausgesetzt. Im Vergleich zu Unternehmen in Nordamerika hatten Unternehmen aus Lateinamerika eine um 97 % erhöhte Betrugsrate. Im Vergleich zu Unternehmen im Asien-Pazifik-Raum war die Betrugsrate sogar um 222 % höher. Dies lässt sich auf eine Vielzahl regionsspezifischer Faktoren zurückführen, wie etwa eine lokale Zahlungsinfrastruktur.
- Am häufigsten von Betrug betroffen waren Unternehmen mit wiederkehrenden Umsätzen, insbesondere B2C-Unternehmen. Mehr als 75 % der Anbieter von B2C-Abonnements berichteten, dass im vergangenen Jahr die Menge der manuellen Prüfungen zugenommen hat und dass sie zusätzliche Ressourcen in die Betrugsbekämpfung stecken mussten. Wir glauben, dass die Produkte von diesen Unternehmen mit direktem Kundenkontakt aufgrund höherer Markenbekanntheit einfacher weiterverkauft werden können. Daher geraten sie eher in das Visier von betrügerischen Akteur/innen.
- Die geschäftlichen Auswirkungen von Betrug gehen über finanzielle Verluste hinaus. Unserer Stripe-Analyse zufolge steigt mit der Zahl der verhinderten Betrugsversuche auch die Wahrscheinlichkeit, dass legitime Abbuchungen geblockt werden. Dadurch sinken die Konversionsraten von Zahlungen. Um die Zahl der falsch positiven Ergebnisse zu reduzieren, können Unternehmen markierte Zahlungen manuell prüfen. Jedoch bedeutet dies zusätzlichen Betriebsaufwand.
- Wir rechnen damit, dass sich Unternehmen auf die folgenden vier Weisen an diese Trends anpassen: 1) Interventionen wie 3DS werden eine größere Rolle spielen. 2) Mit umfangreicheren Datenquellen können Unternehmen schneller genauere Entscheidungen treffen. 3) Aussteller und Unternehmen werden stärker zusammenarbeiten, um die Abläufe bei angefochtenen Zahlungen zu optimieren und die Zahl falscher Ablehnungen zu reduzieren. 4) Die Zahlungspräferenzen der Verbraucher/-innen werden sich weiter verändern, wodurch sich auch die Betrugslandschaft verändert.

Warum steigen die Betrugsfälle?

Die COVID-19-Pandemie hat zu einem historischen Wachstum im E-Commerce geführt. Unternehmen, die Stripe nutzten, wickelten 2021 Zahlungen in Höhe von mehr als 640 Milliarden $ ab – ein Anstieg von 60 % gegenüber dem Vorjahr. Diese Zahlungen stammten aus einer schnell wachsenden Gruppe von Unternehmen: 1.400 neue Unternehmen gingen im letzten Jahr täglich eine Partnerschaft mit Stripe ein. Das Wachstum – insbesondere bei neuen Unternehmen – schuf neue Gelegenheiten für betrügerische Akteur/innen.

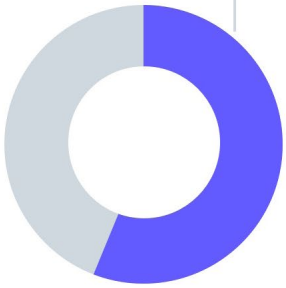
Viele Unternehmer/innen hatten als Neulinge weder die Instrumente noch die Ressourcen, um mit Betrug richtig umzugehen. Oder aber sie legten mehr Wert auf den Aufbau ihres Unternehmens und auf ein möglichst schnelles Erreichen der Gewinnzone statt auf eine Strategie zur Betrugsprävention. Diese Herausforderungen galten jedoch nicht nur für neue Unternehmen. Auch für etablierte Unternehmen gestaltete sich die Betrugsvorbeugung schwieriger, weil die Komplexität oder auch die schiere Zahl der Fälle im Vergleich zu Zeiten vor der Pandemie gestiegen war.

Gleichzeitig werden die Tricks der betrügerischen Akteur/innen immer ausgeklügelter. Sie entwickeln neue Methoden, um die Unternehmen anzugreifen. Häufig organisieren sie sich in Gruppen mit anderen betrügerischen Akteur/innen und tauschen ihre „Best Practices“ untereinander aus.

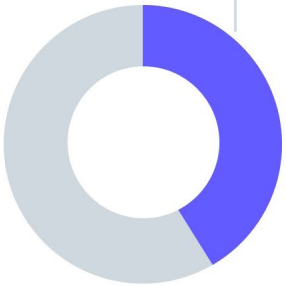
> “ Der Umfang des Zahlungsbetrugs ist in dem Maße gestiegen, in dem die Zahl der Käufer/innen in unseren Online-Stores gestiegen ist. Nicht alle Transaktionen können manuell geprüft werden. Daher konzentrieren wir uns auf eine kleine Auswahl, weil es nicht genügend Ressourcen gibt.
>
> - Betrugsexperte bei einem E-Commerce-Anbieter aus Singapur

64 % der Befragten geben an, dass seit der Coronapandemie **die Betrugsprävention im Unternehmen schwieriger geworden ist**

Unter denjenigen, die angeben, dass die Betrugsbekämpfung schwieriger geworden ist, fielen folgende Aussagen:



56 % geben an, dass ihr Unternehmen **komplexeren Betrugsarten** als vor der Pandemie ausgesetzt ist



41 % geben an, dass ihr Unternehmen **einem höheren Betrugsumfang** als vor der Pandemie ausgesetzt ist

Insbesondere bei angefochtenen Zahlungen in Bezug auf Produkte und bei Kartentest-Angriffen gab es einen Anstieg:

Die Zahl der angefochtenen Zahlungen im Zusammenhang mit Produkten hat sich von 2019 auf 2020 verdoppelt

Unsere Stripe-Analyse fand heraus, dass von März bis Mai 2020 die Wahrscheinlichkeit, dass es zu angefochtenen Zahlungen mit nicht mit Betrug zusammenhängenden Ursachencodes wie „Produkt nicht erhalten“ oder „Produkt nicht annehmbar“ kommt, doppelt so hoch war wie noch 2019. Wir gehen davon aus, dass viele Kund/innen mehr Rückbuchungen einforderten, weil es den Verkäufer/-innen aufgrund von Unterbrechungen der Lieferkette wochen- oder sogar monatelang nicht möglich war, Bestellungen abzuwickeln.

In Lateinamerika war die Anfechtungsquote in Bezug auf Produkte auf den ersten Blick am geringsten, aber unserer Auffassung liegt dies am Verhalten der Aussteller. In Mexiko ist die Wahrscheinlichkeit einer Anfechtung ohne Angabe eines Ursachencodes siebenmal so hoch wie bei allen Ländern zusammen. In Brasilien ist die Wahrscheinlichkeit, dass angefochtene Zahlungen als Betrug gemeldet werden, 50 % höher.

Best Practices zur Vermeidung von angefochtenen Zahlungen im Zusammenhang mit Produkten:

- ☐ Legen Sie eine klare, transparente und angemessene Rückgaberichtlinie fest. Bestimmen Sie beispielsweise, dass die Rückgabefrist nicht am Tag des Warenversands, sondern am Tag des Wareneingangs beim Kunden bzw. bei der Kundin beginnt.
- ☐ Fügen Sie Ihren Firmennamen direkt in die Beschreibung für die Kreditkarte ein.
- ☐ Legen Sie einen förmlichen Prozess für Anfechtungen fest.
- ☐ Benachrichtigen Sie die Kund/innen, bevor Sie deren Zahlung verarbeiten. Sorgen Sie als Anbieter von Abonnements dafür, dass die Kund/innen vor dem Fälligkeitstermin mindestens eine Zahlungserinnerung erhalten.
- ☐ Fordern Sie bei E-Commerce-Unternehmen bei der Auslieferung der Bestellung eine Kundenunterschrift an.

Von versuchten Kartentest-Angriffen waren 40 % mehr Unternehmen betroffen

Zu Kartentests kommt es, wenn jemand versucht herauszufinden, ob gestohlene Karteninformationen noch aktiv sind und daher für Einkäufe genutzt werden können. Betrügerische Akteur/innen kaufen hierfür zum Beispiel gestohlene Kreditkarteninformationen und versuchen anschließend zu ermitteln, ob diese Karten noch funktionieren, indem sie mit diesen Karten Einkäufe tätigen.

Im ersten Pandemiejahr schnellte der Anteil der Unternehmen, die versuchten Kartentest-Angriffen ausgesetzt waren, um 40 % in die Höhe. Dieser Trend war bei neuen Unternehmen ebenso festzustellen wie bei etablierten Firmen. Der Anteil neuer Unternehmen unter den Firmen mit Kartentest, die sich innerhalb der letzten 90 Tage bei Stripe angemeldet hatten, war jedoch größer als gewöhnlich.

Kartentest-Angriffe können sich in verschiedener Weise negativ auf Unternehmen auswirken. Der Einfluss von Transaktionen aufgrund eines Kartentest-Angriffs kann zu höheren Kosten für die Zahlungsabwicklung und Ausfallrisiken führen. Die Website reagiert unter Umständen nicht mehr, wenn ein Unternehmen den Anstieg beim Datenverkehr nicht bewältigen kann. Darüber hinaus schädigen erfolgreiche Kartentest-Angriffe das weltweite Finanzsystem. Die Wahrscheinlichkeit steigt, dass Unternehmen Zahlungen über gestohlene Karten abwickeln, was letztlich zu mehr Anfechtungen führt. Aufgrund des Risikos für das Finanzsystem können Unternehmen von Ausstellern und Kartennetzwerken bestraft werden, wenn sie Kartentest-Angriffe zulassen.

> Eine separate Stripe-Analyse vom November 2021 ergab, dass Wohltätigkeitsorganisationen von Kartentest-Angriffen besonders betroffen sind: 11 % aller von uns beobachteten Kartentest-Angriffe richteten sich an Wohltätigkeitsorganisationen. Warum? Viele Wohltätigkeitsorganisationen lassen auch die Überweisung sehr kleiner Spendenbeträge wie 1,00 oder 5,00 $ durch Spender/innen (in diesem Fall betrügerische Akteur/innen) zu. Kleine Transaktionen werden von dem/der tatsächlichen Karteninhaber/in auf dem Auszug schneller übersehen. Außerdem sind die Betrugspräventionsteams in Wohltätigkeitsorganisationen in der Regel kleiner und mit weniger Ressourcen zum Blocken von Transaktionen ausgestattet. Den Wohltätigkeitsorganisationen (und allen Unternehmen, die Opfer von Kartentest-Angriffen werden,) entgehen nicht nur die Gelder, sondern sie müssen auch noch Strafen an die Banken zahlen, weil sie derartige Angriffe nicht verhindert haben.

Best Practices zur Vermeidung von Kartentest-Angriffen:

- [ ] Optimieren Sie die Integration in den Systemen Ihres Zahlungsdienstleisters. Viele Zahlungsdienstleister stellen verschiedene Kontrollen zur Abmilderung von Kartentest-Angriffen bereit, aber der Erfolg dieser Kontrollen hängt von der Qualität der Integration und den Signalen, die Sie an den Anbieter senden, ab. Im Allgemeinen gilt: Je mehr Daten die Integration bereitstellt, desto erfolgreicher kann die Vorbeugung gegen Kartentest-Angriffe sein.
- [ ] Schützen Sie Ihre API-Schlüssel. Ihr geheimer API-Schlüssel kann für API-Aufrufe für Ihr Konto (z. B. für Zahlungen oder Rückerstattungen) verwendet werden. Behandeln Sie Ihren geheimen API-Schlüssel wie andere Passwörter auch und gewähren Sie nur denjenigen Zugriff darauf, die ihn wirklich benötigen.

- [ ] Aktivieren Sie CAPTCHA in Ihrem Bezahlvorgang, um zwischen legitimen Kund/innen und Kartentest-Bots unterscheiden zu können.
- [ ] Steuern Sie durch Ratenbegrenzungen die Menge des ein- und ausgehenden Datenverkehrs. Wenn Kartentester/innen zum Beispiel Karten validieren, indem sie sie neuen Kund/innen zuweisen, können Sie die Zahl der Neukund/innen, die an einem Tag über eine einzelne IP-Adresse registriert wird, beschränken.
- [ ] Erwägen Sie, von Kund/innen zu verlangen, sich bei ihrem Konto anzumelden, um eine Zahlung vorzunehmen.

Wie unterscheidet sich das Phänomen des Betrugs je nach Region, Land und Unternehmensgröße?

Die Bedeutung des Kampfs gegen den Betrug ist universell: 90 % der von uns befragten Unternehmensverantwortlichen halten die Vorbeugung vor E-Commerce-Betrug für wichtig. Es gibt jedoch je nach Branche und Standort der Unternehmen gewisse Unterschiede im Hinblick auf die Betrugsaktivitäten. Daraus ergibt sich ein komplexes Bild.

Betrug je nach Region und Land

Stripe hat die meisten Daten zum Zahlungsvolumen für Unternehmen in Nordamerika, daher werden wir in der Analyse dieses Abschnitts Nordamerika als Basis für andere Regionen verwenden.

Alle Online-Unternehmen müssen sich mit dem Thema Betrug beschäftigen. Unsere Stripe-Analyse hat jedoch ergeben, dass Unternehmen in Lateinamerika von steigenden Betrugsraten besonders betroffen sind.

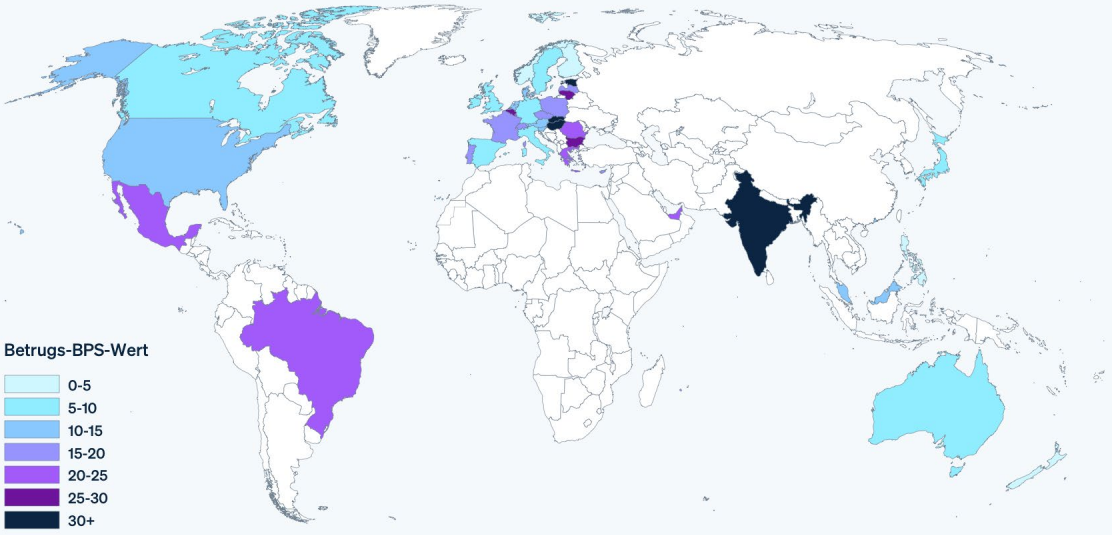
Unsere Daten haben gezeigt, dass während unseres Studienzeitraums weltweit die meisten Kartenbetrugsfälle in Lateinamerika stattfanden: 97 % höher als in Nordamerika und 222 % höher als im Asien-Pazifik-Raum. Lokale Zahlungsinfrastruktur und der seltenere Einsatz von Kreditkarten führen dazu, dass die von den Banken eingesetzten Betrugspräventionsmodelle dort schwächer sind als in anderen Regionen. Die Regeln bevorzugen Karteninhaber/innen bei Anfechtungen, wodurch Unternehmen besonders anfällig für Betrug sind. Neben diesen lokalen Faktoren verlagert sich der Markt immer mehr in den Online-Bereich (wir verzeichneten 2021 in Lateinamerika einen Anstieg der neuen Unternehmen bei Stripe um 518 %), wodurch die betrügerischen Akteur/innen noch mehr Angriffsmöglichkeiten erhalten.

Unternehmen in Europa, dem Nahen Osten und Afrika verzeichneten erheblich geringere Betrugsraten als Nordamerika. Das ist vermutlich das Ergebnis der Regelungen zur starken Kundenauthentifizierung (SCA), die Unternehmen in ihren Bezahlvorgang integrieren müssen.

Es gab außerdem erhebliche Unterschiede zwischen den Ländern. In Frankreich lag die Betrugsquote beispielsweise nahezu doppelt so hoch wie in Deutschland, wohingegen Singapur nur etwa die Hälfte der Quote des gesamten asiatisch-pazifischen Raums aufwies. Diese unterschiedlich hohe Betrugsquote in den Ländern kann globalen Unternehmen die Betrugsbekämpfung noch mehr erschweren. Aus diesem Grund gibt es für das Betrugsmanagement keine Universallösung.

Betrugsraten auf Landesebene mit Radar

Radar hilft Unternehmen mithilfe von maschinellem Lernen bei dem Erkennen und Verhindern von Betrug.



Empfehlungen:

Wenn Sie über die Kapazität und Bandbreite verfügen, empfehlen wir die Analyse des Verhaltens Ihrer Kund/innen sowie von Markttrends und der Regelungen in den Ländern, in denen Sie tätig sind. So können Sie besser einschätzen, welche Betrugsangriffe und -vektoren bei Ihnen besonders wahrscheinlich sind. In großen Unternehmen kann diese Komplexität jedoch schnell nicht mehr zu bewältigen sein. Daher ist ein intelligentes und automatisiertes Betrugspräventions-Tool so wichtig.

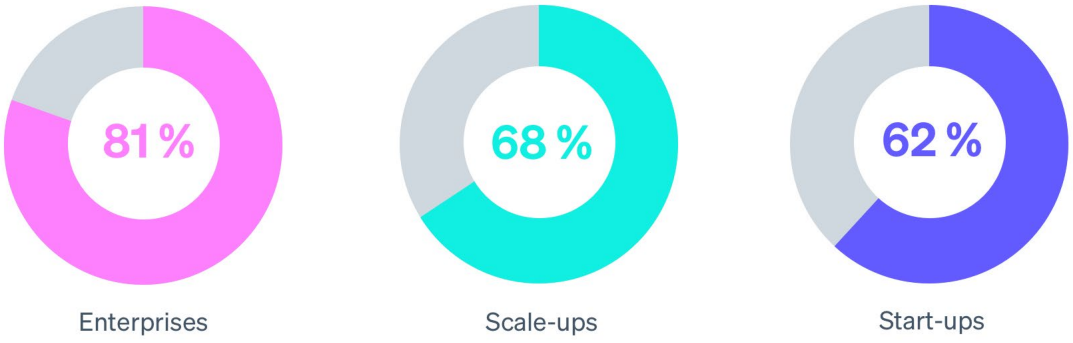
Betrugsrisiko abhängig von Unternehmensgröße und Geschäftsmodell

Unternehmensverantwortliche fassen das Betrugsrisiko oft unterschiedlich auf – je nachdem, wie groß das Unternehmen ist und welches Geschäftsmodell es verfolgt. Aus unserer Umfrage ging beispielsweise hervor, dass die Betrugsprävention wichtiger wird, je größer das Unternehmen ist. Außerdem ist es wenig überraschend, dass große Unternehmen mehr Ressourcen in eine Strategie zur Betrugsprävention stecken können als kleinere Unternehmen. Ressourcen allein verhindern jedoch noch keinen Betrug. Gemäß unserer Umfrage stieg mit großen Betrugspräventionsteams

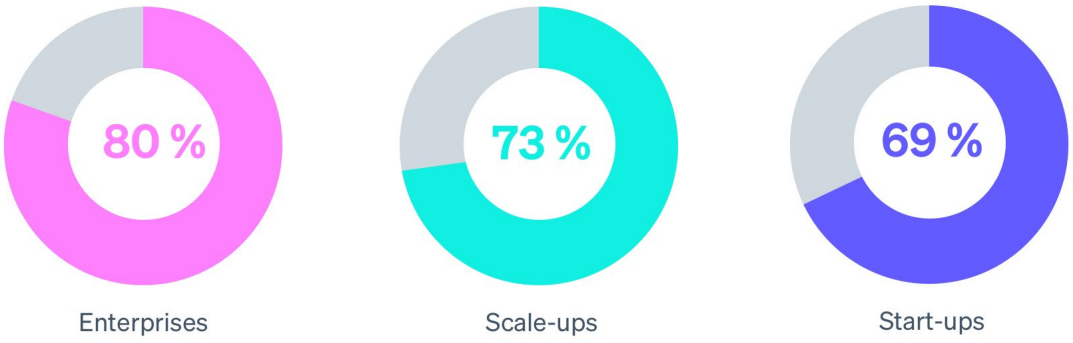
die Wahrscheinlichkeit betrieblicher Herausforderungen bei der Betrugsvorbeugung und der Aufdeckung größerer Verluste aufgrund von Betrug.

Diese Trends weisen eventuell auf Chancen für kleinere Unternehmen hin: Wachsende Unternehmen entscheiden sich vielleicht jetzt, solange sie klein sind, für eine ausführliche Betrugspräventionsstrategie, um dem Problem voraus zu sein. Zeit und Ressourcen zur Betrugsbekämpfung bereitzustellen, geht jedoch eventuell zulasten des geschäftlichen Wachstums. Daher müssen kleinere Unternehmen Kompromisse sorgfältig abwägen.

Die Führungskräfte von größeren Unternehmen betrachten E-Commerce-Betrug eher als sehr wichtiges Thema



Die Führungskräfte von größeren Unternehmen stimmen eher der Aussage zu, dass sie von einem im Vergleich zum Vorjahr höheren Ressourcenaufwand für die Betrugsprävention ausgehen



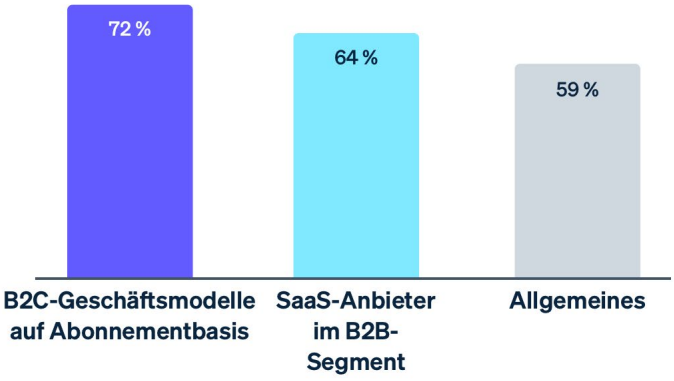
Enterprise: Unternehmen mit einem Jahresumsatz von mehr als 60 Millionen $.
Scale-up: Unternehmen mit einem Jahresumsatz zwischen 2 und 60 Millionen $.
Start-up: Unternehmen mit einem Jahresumsatz von weniger als 2 Millionen $.

Wir haben auch unsere Umfrageergebnisse auf der Grundlage des Geschäftsmodells analysiert und die Unternehmen in folgende Kategorien unterteilt:

- Software-as-a-Service (SaaS)
- B2C-Abonnements
- Marktplätze und Plattformen
- E-Commerce

Unserer Beobachtung nach machten sich Unternehmen mit wiederkehrenden Umsätzen am meisten Gedanken über die finanziellen Auswirkungen von Betrug. Im Vergleich zu den anderen von uns in der Umfrage behandelten Geschäftsmodellen zeigten sich die für die Betrugsprävention Verantwortlichen bei Unternehmen mit wiederkehrenden Umsätzen besonders besorgt über mögliche Betrugsverluste. Außerdem ging ein größerer Teil davon aus, 2021 einen höheren Prozentsatz des Umsatzes durch Betrug verloren zu haben als zu Zeiten vor der Pandemie. Diese Bedenken könnten ein Resultat des Geschäftsmodells sein: Da sie Umsätze in regelmäßigen Abständen generieren (etwa monatlich oder vierteljährlich) und im vergangenen Jahr steigende Betrugsraten festgestellt haben, gehen sie davon aus, dass sich der Trend bei wachsendem Geschäftsvolumen fortsetzt.

Bei Unternehmen mit wiederkehrenden Umsätzen ist die Wahrscheinlichkeit höher, dass sie 2022 höhere Verluste durch Betrug befürchten als 2021



Insbesondere Anbieter von B2C-Abonnements hatten erheblich mit der betrieblichen Belastung durch Betrug zu kämpfen. Bei ihnen war die Wahrscheinlichkeit von mehr gemeldeten manuellen Prüfungen im Jahr 2021, von einer Stärkung der Ressourcen zur Betrugsbekämpfung und von deswegen verschobenen Investitionen bzw. Expansionsplänen höher.

Wir gehen davon aus, dass B2C-Unternehmen mehr mit Betrug zu tun hatten, weil es sich hierbei mit größerer Wahrscheinlichkeit um Haushaltsmarken handelt. Das heißt, die betrügerischen Akteur/innen können gestohlene Waren und Dienstleistungen (wie zum Beispiel der Kauf eines digitalen Abonnements über eine gestohlene Kreditkarte, das dann zu einem niedrigeren Preis wieder verkauft wird) einfacher weiterverkaufen.

Welche geschäftlichen Auswirkungen hat Betrug?

Betrug verursacht hohe Kosten. 59 % der Befragten erwarten, dass ihr Unternehmen in diesem Jahr mehr Umsatz durch Betrug verliert als letztes Jahr.

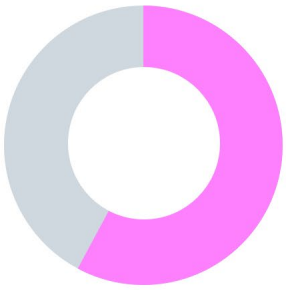
Unternehmen verlieren durch Anfechtungen aufgrund von Betrug Geld und versuchen daher, diesem Betrug vorzubeugen. Wenn Ihr Unternehmen zum Beispiel eine Anfechtung verliert, ist nicht nur der ursprüngliche Transaktionsbetrag fällig. Betrug führt oft zu Rückbuchungsgebühren, die die Bank für eine Rücknahme der Kartenzahlung erhebt, und zu höheren Netzwerkkosten aufgrund der Anfechtungen.

Wie wir in unserer Umfrage herausgefunden haben, geht es bei den geschäftlichen Auswirkungen von Betrug aber gar nicht nur um finanzielle Verluste. Viele Unternehmen müssen ihre Expertenteams für die Betrugsaufdeckung personell aufstocken oder Produkt- bzw. Technikressourcen auf das operative Management umschichten. Dadurch kommen wertvolle Ressourcen nicht mehr dem zentralen Produkt zugute.

Die geschäftlichen Auswirkungen von Betrug gehen über bloße finanzielle Verluste hinaus

72 %

der Führungskräfte weltweit mussten **zur Betrugsbekämpfung Produkt- oder Technikressourcen umschichten**



58 %

der Führungskräfte weltweit mussten **aufgrund von Betrug Expansions- oder Investitionspläne verschieben**

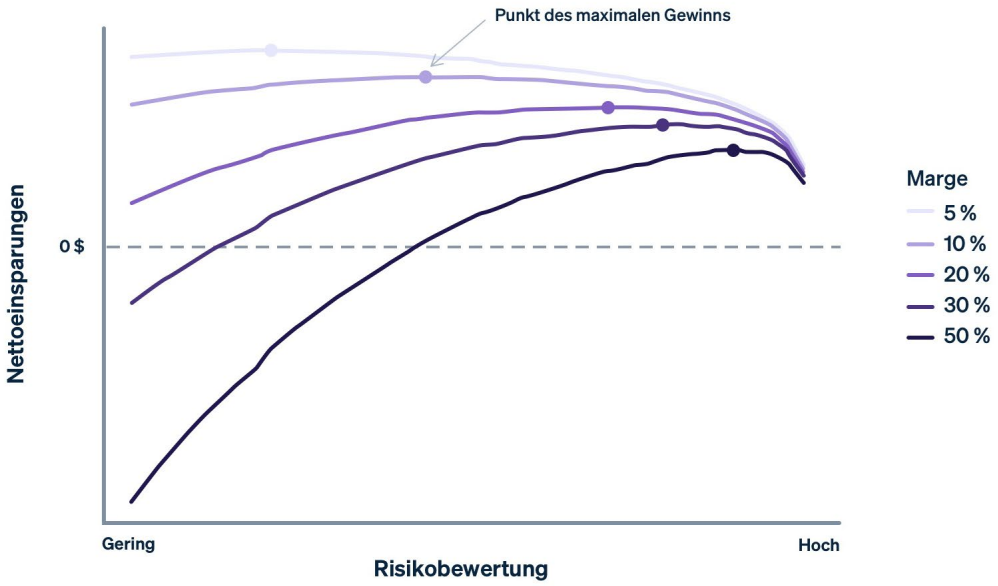
Geringere Zahlungskonversionsraten

In unserer Stripe-Analyse stellten wir fest, dass mit der Zahl der verhinderten Betrugsversuche auch die Wahrscheinlichkeit steigt, dass legitime Abbuchungen geblockt werden.

Zu falsch positiven Ergebnissen bzw. falsch abgelehnten Zahlungen kommt es, wenn ein/e legitime/-r Kunde/Kundin daran gehindert wird, einen Einkauf zu tätigen. Falsch abgelehnte Zahlungen wirken sich negativ auf den Bruttogewinn und auf den Ruf des Unternehmens aus. **33 % der Verbraucher/-innen** geben an, dass sie nicht mehr bei Unternehmen kaufen wollen, bei denen es zu einer falsch abgelehnten Zahlung gekommen ist.

> Selbst ein einzelner Fall von Betrug kann erhebliche Probleme bereiten und durch zusätzliche Sicherheitsprüfungen dazu führen, dass uns legitime Käufer/innen entgehen.
>
> - Betrugsexperte bei einem kanadischen SaaS-Unternehmen

Es ist ein permanentes Abwägen zwischen dem Vermeiden von Anfechtungen einerseits und der verringerten Anzahl legitimer, geblockter Kund/innen andererseits. Wenn Sie mehr Betrug vermeiden, steigt der Anteil der geblockten, legitimen Kund/innen. Andererseits führt die Reduzierung der fälschlicherweise geblockten Kund/innen häufig dazu, dass die Wahrscheinlichkeit nicht erkannter Betrugsversuche steigt. Wie die Abwägung konkret ausfällt, hängt auch von Ihrer Lösung zur Betrugsbekämpfung ab: Sie müssen diese Abwägung immer selbst vornehmen, wenn Sie mit einer statischen Lösung arbeiten und nicht kontinuierlich Ressourcen in deren Verbesserung investieren.



Risikobewertung ist der Schwellenwert, ab dem Transaktionen mithilfe von Radar geblockt werden (gemäß Standardeinstellungen werden Transaktionen gestoppt, wenn die Risikobewertung über einem Wert von 75 liegt).

Nettoeinsparungen ist die Differenz aus den gesamten durch Betrugsprävention abgewendeten Kosten abzüglich der entgangenen Gewinne aus eigentlich legitimen Transaktionen.

Punkt des maximalen Gewinns ist der Punkt, an dem ein Unternehmen den Höchstwert bei den Nettoeinsparungen erreicht und damit die optimale Abwägung zwischen dem Blocken betrügerischer und legitimer Transaktionen erzielt.

Interpretation des Diagramms: Je höher der Risikoschwellenwert auf der x-Achse, desto größer ist die Wahrscheinlichkeit, dass eine Transaktion betrügerisch ist. Je höher der Risikoschwellenwert, desto weniger Transaktionen blocken Sie. Wenn Sie mehr Transaktionen blocken, steigen die Nettoeinsparungen durch Betrug. Gleichzeitig steigt jedoch die Wahrscheinlichkeit, dass Sie auch legitime Transaktionen blocken.

Das Abwägen zwischen der Betrugsvermeidung und dem Blocken legitimer Transaktionen basiert auf der Marge pro Transaktion. So gilt zum Beispiel: Bei Transaktionen mit hoher Marge (50 %) – der dunkelblaue Graph im Diagramm – ist die Wahrscheinlichkeit höher, dass die Unternehmen mehr Transaktionen zulassen und einen höheren Risikoschwellenwert haben, weil jede einzelne legitime Transaktion sehr viel wertvoller ist (als z. B. bei Transaktionen mit geringerer Marge).

Andererseits wird das Abwägen erleichtert, wenn sich die Modelle der Betrugsbekämpfungslösung fortwährend anhand von Betrugsvektoren anpassen und verändern.

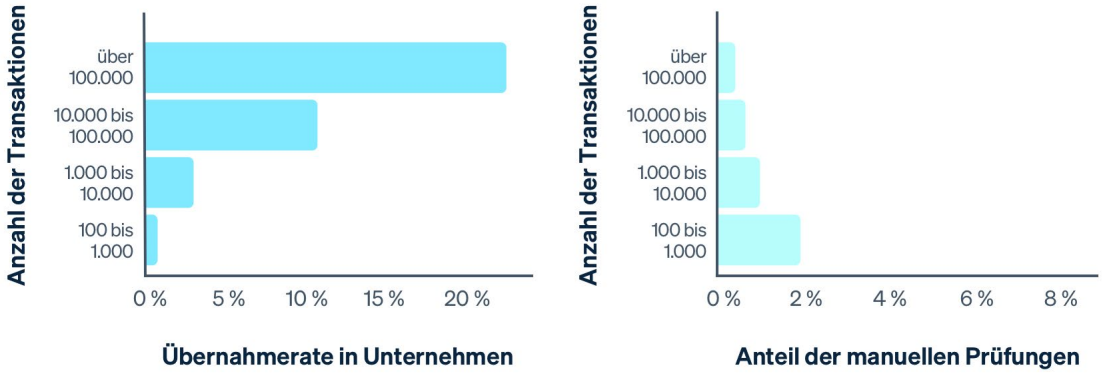
Bei der Abwägung zwischen der Vermeidung von Anfechtungen und dem Blocken legitimer Zahlungen können Unternehmen einen Schwellenwert angeben, ab dem Zahlungen geblockt werden sollen, damit der Gewinn möglichst wenig beeinträchtigt wird. Der Punkt des maximalen Gewinns befindet sich dort, wo die Differenz zwischen den vermiedenen Betrugskosten und dem geblockten, legitimen Gewinn am größten ist.

Unternehmen müssen Entscheidungen auf der Grundlage ihrer Margen, ihres Wachstumsprofils und anderer Faktoren abwägen. Wenn die Margen eines Unternehmens klein sind, wie etwa bei Online-Lebensmittelhändlern, müssen die Kosten einer betrügerischen Transaktion den Hunderten legitimen Transaktionen gegenübergestellt werden. In dieser Konstellation ist jedes falsch negative Ergebnis sehr kostspielig. Unternehmen mit diesem Profil sind unter Umständen geneigt, ein sehr weites Netz zur Bekämpfung potenziellen Betrugs zu spannen. Für Unternehmen mit hohen Margen – wie etwa SaaS-Anbieter – gilt das Gegenteil. Der entgangene Gewinn aus geblockten, legitimen Kundentransaktionen ist eventuell höher als die Kosten, die durch mehr Betrug anfallen. Allerdings können Unternehmen die Betrugsraten nur bis zu einem gewissen Punkt optimieren. Wenn Betrug ein bestimmtes Niveau erreicht, verlangen Kartennetzwerke Gebühren und Strafzahlungen.

Betriebsaufwand

Um die Zahl der falsch positiven Ergebnisse zu reduzieren, können Unternehmen markierte Zahlungen manuell daraufhin prüfen, ob sie wirklich betrügerisch sind. Das ist ziemlich arbeitsintensiv. Unternehmen benötigen ein Team aus Betrugsanalyst/innen, um das Risiko auf der Grundlage verschiedener Faktoren wie Transaktionsdetails und Kundenhistorie zu beurteilen.

> “ Es ist wirklich frustrierend, weil ich dafür woanders Ressourcen abziehen muss. Denn sonst müsste ich befürchten, dass die Situation außer Kontrolle gerät.
>
> - Betrugsexperte bei einem australischen SaaS-Unternehmen



Der Anteil der aktiven und berechtigten Stripe-Unternehmen, die manuelle Prüfungen vornehmen (Unternehmensübernahmerate) und der durchschnittliche Anteil der manuell geprüften Transaktionen (manuelle Prüfrate) nach der Anzahl der Transaktionen im vergangenen Jahr (die aufgeführten Zahlen sind die Obergrenzen der Gruppen)

Wir haben herausgefunden, dass größere Unternehmen eher manuelle Prüfungen vornehmen, aber je größer die Unternehmen sind, desto kleiner ist der Anteil der tatsächlich geprüften Transaktionen. So führten mehr als 20 % der Unternehmen mit mehr als 100.000 Transaktionen im vergangenen Jahr manuelle Prüfungen durch, jedoch wurden dabei weniger als 1 % der gesamten Transaktionen geprüft. Große Unternehmen hätten ausreichend Ressourcen zur manuellen Prüfung von Transaktionen zur Verfügung, sparen sich diesen Aufwand aber für Transaktionen größeren Umfangs auf.

Empfehlungen zur Reduzierung des Betriebsaufwands:

- ☐ Bei kleineren Unternehmen ohne eigene Expertenteams für die Betrugsaufdeckung kann eine Lösung mit Rückbuchungsgarantie, bei der ein Drittanbieter die Übernahme der Rückbuchungskosten garantiert, besonders hilfreich sein.
- ☐ Bei mittleren bis großen E-Commerce-Unternehmen kann eine Lösung mit maschinellem Lernen dazu beitragen, Betrug im großen Stil zu bekämpfen, ohne dass zusätzliche Technikressourcen benötigt werden.
- ☐ Große Unternehmen setzen häufig eine Reihe punktueller Lösungen (wie etwa Tools für CAPTCHA oder das Scannen von Karten) in Kombination mit Betrugserkennungssoftware oder als Input für ihre eigenen Betrugsbekämpfungsmodelle ein.

Unsere Prognosen in Sachen Betrug

Betrug entwickelt sich mit der Zeit weiter. 2021 war da keine Ausnahme. Im vergangenen Jahr wurden die Betrugsmaschen, denen Online-Unternehmen ausgesetzt waren, immer ausgeklügelter. Dieser Bericht beschäftigt sich mit einer Reihe von Herausforderungen, aber was bedeutet das für Ihr Unternehmen? Wir glauben, dass Unternehmen sich auf vier Weisen an die aktuelle Betrugslandschaft anpassen sollten:

1. Interventionen, wie 3DS, spielen eine größere Rolle

Durch Interventionen können Sie mit höherer Zuverlässigkeit verdächtige Transaktionen korrekt einschätzen und dann blocken oder zulassen. Hierfür stellen Sie den Kund/innen eine „Aufgabe“, indem Sie beispielsweise um die Eingabe eines per SMS versendeten einmaligen Codes bitten.

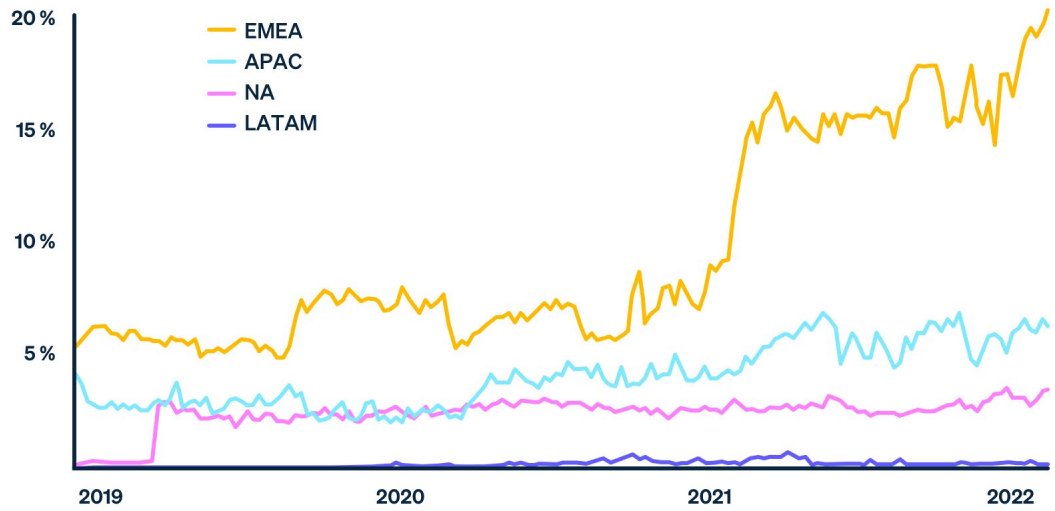
Interventionen können unter anderem die folgenden Formen annehmen:

- Bei **3DS** müssen die Kund/innen zur Durchführung einer Zahlung eine Zwei-Faktor-Authentifizierung durchlaufen. Dies ist die Hauptmethode zur Kartenauthentifizierung nach Maßgabe der Anforderungen der **starken Kundenauthentifizierung** (SCA) in Europa und ein zentraler Mechanismus zur Anforderung von SCA-**Ausnahmen**.
- **Überprüfungen der Identität**, wie zum Beispiel das Scannen eines Personalausweises oder eines anderen behördlichen Dokuments zur Feststellung der Identität.

- Karten-Scans zur Prüfung, ob der/die Kunde/Kundin die physische Karte zum Zeitpunkt der Transaktion in seinem/ihrem Besitz hat.
- CAPTCHA-Tools, mit denen Website-Besucher/innen aufgefordert werden, einfache Rätsel zu lösen, etwa eine Reihe von Zahlen und Buchstaben in einem verzerrten Bild zu erkennen.

Interventionen haben bereits an Popularität gewonnen. Wir haben die Aktivität einer bestimmten Intervention – 3DS – bei Stripe-Unternehmen im Jahr 2021 analysiert und dabei festgestellt, dass die Übernahme von 3DS auf breiter Front, aber besonders stark außerhalb von Nordamerika, gestiegen ist. Wie erwartet ist es unter europäischen Unternehmen zum größten Anstieg bei der 3DS-Übernahme gekommen (aufgrund von SCA-Anforderungen, die in nahezu allen europäischen Ländern im vergangenen Jahr vollständig in Kraft getreten sind). SCA-ähnliche Regelungen werden auch außerhalb Europas immer beliebter. In Indien verläuft das Wachstum dabei besonders schnell.

3DS-Abdeckung von Zahlungen nach Region im Laufe der Zeit



In einem Experiment fand Stripe heraus, dass eine Absenkung des Schwellenwerts, bei dem 3DS ausgelöst wird, zu einem Rückgang der Anfechtungsquote bei Betrug um 74 % führte. Darüber hinaus bleiben bei 3DS im Vergleich zur kompletten Zahlungssperre die meisten Zahlungen erfolgreich (67 % auf allen Risikoebenen und 5 % bei erhöhtem Risikoniveau). Die 3DS-Leistung ist jedoch abhängig vom jeweiligen Aussteller.

Für die Zukunft rechnen wir mit einem Anstieg der Interventionen. Unternehmen wenden Interventionen auf einen größeren Teil ihres Transaktionsvolumens an und setzen unterschiedlichere Arten von Interventionen ein – insbesondere diejenigen, mit denen sich die Probleme beim Bezahlvorgang reduzieren lassen.

Tipps für den Einsatz von Interventionen:

- ☐ Setzen Sie bei Transaktionen, die Sie aktuell blocken, stattdessen auf Interventionen, um für mehr Konversionen zu sorgen und legitime Zahlungen nicht zu stoppen.

- [ ] Interventionen können das Kundenerlebnis beeinträchtigen, was sich negativ auf die Konversion auswirken kann. Sie sollten sorgfältig optimieren und testen, wie Sie Interventionen auslösen können, ohne dass dies negative Folgen für legitime Kund/innen hat.
- [ ] Die einzelnen Interventionen weisen unterschiedliche Bestehensquoten auf und haben unterschiedliche Auswirkungen auf die Reduzierung von Betrug. Sicherheitsschlüssel sind beispielsweise äußerst effektiv bei der Bekämpfung von betrügerischen Akteur/innen, können aber auch die Konversion ganz erheblich beeinträchtigen. Entscheiden Sie sich auf Grundlage des Risikos der Handlung Ihres/Ihrer Kunden/Kundin und Ihrer eigenen Toleranz in puncto Risiko/Konversion für die richtige Intervention.
- [ ] Führen Sie dort Interventionen ein, wo sie von der Nutzerlogik her am sinnvollsten sind, z. B. das Scannen einer Karte, wenn ein/e Kunde/Kundin Kartenangaben macht.

2. Vielfältigere Datenquellen helfen Unternehmen, schneller genauere Entscheidungen zu treffen

Das Betrugsmanagement war bislang ein hochgradig manueller Prozess, für den ein Analystenteam jede einzelne Transaktion prüfen musste. Heutzutage setzen die meisten Unternehmen neben bedarfsweisen manuellen Prüfungen unterschiedliche Abstufungen von Modellen und Automatisierungen auf der Basis von maschinellem Lernen ein, um Betrug im großen Maßstab zu bekämpfen. Diese hybride Herangehensweise ist stark von der Branche und vom Geschäftsmodell abhängig. Modellen mit maschinellem Lernen kann beigebracht werden, legitime Transaktionen von potenziell betrügerischen zu unterscheiden. Einige können sich sogar selbst trainieren und sind dadurch skalierbarer und effizienter.

Modelle mit maschinellem Lernen galten einmal als Top-Technologie zur Betrugsbekämpfung, heute sind sie aber praktisch der Mindeststandard. Funktionen für maschinelles Lernen reichen nicht mehr aus, um die sich immer weiter entwickelnden Betrugsrisiken in Schach zu halten. Die Befragten in unserer Umfrage bestätigen: Mehr als die Hälfte der Befragten, deren Prüfprozess im Wesentlichen automatisiert ist, geben an, dass sich Betrug in Art und Umfang so schnell entwickelt, dass ihr Unternehmen nicht mithalten kann.

> “ Die Möglichkeiten für Finanzbetrug sind mit der Zeit vielfältiger und komplexer geworden. Wir müssen uns immer wieder an neue Betrugsmuster und -möglichkeiten anpassen.
>
> - Betrugsexperte bei einem deutschen Unternehmen für professionelle Dienstleistungen

Wir sind der Auffassung, dass umfangreichere Daten zur besseren Versorgung von Modellen im Mittelpunkt der nächsten Evolutionsphase des Betrugsmanagements stehen werden. Die Tools und Technologien zur Erfassung dieser Informationen stehen bereits zur Verfügung, sind aber oft in isolierten und untereinander kaum kompatiblen Systemen untergebracht. So haben viele Unternehmen zum Beispiel separate Instrumente zur Identitätsprüfung und für biometrische Daten.

In Zukunft können Unternehmen nach unseren Prognosen Technologie und Integrationen besser zur Konsolidierung dieser Informationen an einem zentralen Ort nutzen. Dieser ganzheitliche Ansatz stärkt die Effizienz von Betrugsmodellen.

Durch die Betrachtung von relevanten Daten in den verschiedenen Phasen der Nutzung durch die Kund/innen können Unternehmen ein neues Niveau bei der Genauigkeit der Betrugserkennung erreichen – einschließlich Verhaltens-, biometrischen und ergänzenden Daten von Drittanbietern in Bezug auf Telefonnummern, E-Mail-Adressen, dem ungenutzten Reservoir an Ausstellerdaten und sogar zu sozialen Netzwerken.

Dieses Datenniveau ist für die Optimierung von Betrugsmodellen sehr hilfreich. Die Unternehmen müssen jedoch bei der Erfassung und Speicherung dieser Informationen sehr vorsichtig agieren, damit sie weltweit geltende Gesetze zu Datensicherheit und Datenschutz einhalten.

3. Aussteller und Unternehmen sorgen gemeinsam für eine bessere Abwicklung von Anfechtungen und für weniger falsch abgelehnte Zahlungen

Wenn ein/e Kunde/Kundin etwas auf Ihrer Website kauft, übermittelt Ihr Zahlungsdienstleister die Transaktionsdaten über ein Kartennetzwerk wie Visa, Mastercard oder China UnionPay als Zahlungsaufforderung an die Ausgabebank (Kundenbank). Die Ausgabebank, etwa Chase, Citi und Barclays trifft letztlich die Entscheidung darüber, ob innerhalb der **Autorisierungsphase** Transaktionen genehmigt oder abgelehnt werden. Die Bank berechnet das Betrugsrisiko auf der Grundlage von einer sehr begrenzten Menge an Signalen, die sie während der Autorisierung erhält.

Die Unternehmen wiederum verfügen über umfassende Kunden- und Transaktionsdaten, wie etwa die E-Mail- und die Rechnungsadresse der Kund/innen. Diese Daten mit denen des Ausstellers zu kombinieren, kann zu einem höheren Anteil genehmigter Transaktionen beitragen.

Verbesserte Autorisierungs- und Betrugsraten sind für beide Seiten von Vorteil – die ausstellende Bank kann die Betrugsverluste reduzieren, Betriebskosten senken und das Transaktionsvolumen steigern, indem sie die Anzahl der Kundenanfragen zu falsch abgelehnten Zahlungen reduziert. Gleichzeitig profitieren Unternehmen von höheren Zahlungskonversionsraten und einer besseren Kundenbindung. Die meisten Unternehmen geben diese Daten jedoch immer noch nicht an die Aussteller weiter. Die dadurch entstehende Asymmetrie bei den Informationen trägt dazu bei, dass sich die falsch abgelehnten Zahlungen im Jahr 2021 auf einen Betrag von **443 Mrd. $** summierten.

Inzwischen beobachten wir, dass Aussteller in den Aufbau moderner Autorisierungs-APIs wie der **Enhanced Decisioning Data API** von Capital One und in die **Enhanced Authorization API von Amex** investieren. Großen Unternehmen, bei denen jeder zusätzliche Prozentpunkt bei den Autorisierungen Millionen von Dollar ausmacht, ist die Bedeutung von Datenpartnerschaften bewusst. Daher beginnen die Unternehmen damit, in die Integrationslösungen der Aussteller zu investieren. Bei Millionen anderen Unternehmen, die nicht die technische Kapazität haben oder denen das enorme

Zahlungsvolumen fehlt, mit dem sich die maßgeschneiderten Integrationen rechtfertigen ließen, klafft hier jedoch eine Lücke. Bei diesen Unternehmen gehen wir davon aus, dass Finanzpartner wie Stripe und andere Zahlungsdienstleister dabei helfen, diesen Austausch über ihre Größe und über die integrierten Partnerschaften mit den Ausstellern zu erleichtern.

4. Die Präferenzen der Verbraucher/innen werden sich weiterhin verändern, wodurch sich auch die Betrugslandschaft verändert

Zahlungsmethoden wie **Jetzt kaufen, später bezahlen**, Digital Wallets und Kryptokarten ohne aufgedruckte Nummer (wie zum Beispiel die **Gemini-Kreditkarte**) gewinnen an Bedeutung. Insbesondere werden mehr Services nach dem Konzept „Jetzt kaufen, später bezahlen“ nachgefragt: **Mehr als die Hälfte der US-Kund/innen** nutzen einen „Jetzt kaufen, später bezahlen“-Service. In **Indien** und dem **Vereinigten Königreich** war dies die Zahlungsmethode mit dem schnellsten Wachstum im Jahr 2020.

Alle für Online-Transaktionen verwendeten Zahlungsmethoden sind mit einem gewissen Betrugsrisiko behaftet. Das gilt auch für kartenlose Methoden. So ist das Risiko eines Transaktionsbetrugs bei Zahlungsmethoden wie „Jetzt kaufen, später zahlen“ zwar geringer, aber dafür ist die Gefahr eines Betrugs beim Anlegen eines neuen Kontos bzw. bei Kontoübernahmen größer. Im ersten Fall erstellen betrügerische Akteur/innen neue Identitäten zum Eröffnen betrügerischer Konten, was eventuell durch schlecht geschützte Onboarding-Abläufe erleichtert wird. Im zweiten Fall verschafft sich ein unbefugter Dritter Zugriff auf die Zugangsdaten für ein Kundenkonto und tätigt mit diesen Zahlungsinformationen betrügerische Einkäufe.

Unternehmen können diese Risiken jedoch in den Griff bekommen, indem sie sich zu einem früheren Zeitpunkt im Lebenszyklus der Kund/innen auf Strategien zur Betrugsprävention konzentrieren. Statt die Transaktion selbst in den Mittelpunkt zu stellen, haben Unternehmen zu einem früheren Zeitpunkt die Möglichkeit, nach betrügerischen Aktivitäten zu suchen, also bevor der/die Kunde/Kundin (bzw. der/die betrügerische Akteur/in) überhaupt etwas kauft. Unternehmen könnten beispielsweise die Identität des/der Kunden/Kundin beim Onboarding überprüfen, nach doppelten Konten suchen und Maßnahmen zur Verifizierung der Identität (etwa Zwei-Faktor-Authentifizierung) bei der Anmeldung vorschreiben.

So kann Stripe Sie unterstützen

Stripe ist ein vollständig integriertes Paket an Zahlungsprodukten, das Zahlungen für den Online- und den klassischen Einzelhandel, für Abonnementanbieter, Softwareplattformen und Marktplätze und vergleichbare Lösungen ermöglicht. Stripe schützt vor Betrug und dient zur Identitätsprüfung. Millionen Unternehmen setzen es zu folgenden Zwecken ein:

Optimierung des Bezahlvorgangs

- **Mehr relevante Informationen beim Bezahlvorgang erfassen:** Indem Sie die Kund/innen auffordern, weitere relevante Informationen beim Bezahlvorgang anzugeben, können Sie deren Legitimation besser prüfen. Erfassen Sie zum Beispiel den Namen und die E-Mail-Adresse des/der Kunden/Kundin. Diese zusätzlichen Informationen können an Stripe Radar weitergeleitet werden. Dies führt zu einer besseren Betrugserkennung auf Basis von maschinellem Lernen und versorgt Sie mit mehr Beweisen bei potenziellen Anfechtungen.
- **Weitere Zahlungsmethoden erkunden:** Mit dem richtigen Satz an Zahlungsmethoden erhalten die Kund/innen mehr Flexibilität und das Betrugsrisiko wird reduziert. Bei Digital Wallets wie Apple Pay oder Google Pay sind zusätzliche Kundenverifizierungen, wie z. B. biometrische Daten, SMS oder Passcode, für den Abschluss von Zahlungen erforderlich. Das trägt zum Rückgang der Anfechtungsquote bei. Ebenso ist es bei den meisten Banklastschriften, bei denen Gelder direkt vom Bankkonto eines/einer Kunden/Kundin abgebucht werden, notwendig, dass die Kund/innen einem Mandat zustimmen oder die Kontoinhaberschaft überprüft wird. So gibt es eine zusätzliche Sicherheitsebene und die Wahrscheinlichkeit von Anfechtungen sinkt.

Betrugsvorbeugung im Bezahlvorgang

- **Betrugserkennung mit maschinellem Lernen nutzen:** Die regelbasierte Betrugserkennung, die nach der Logik „auf Ereignis x folgt Handlung y“ funktioniert, wurde nicht für moderne Internetunternehmen entwickelt und kann zu einem Umsatzverlust führen. Stripe Radar ist mit adaptivem maschinellem Lernen ausgestattet. Algorithmen werten jede Transaktion aus und weisen eine Risikobewertung zu. Auf der Basis des Betrugsrisikos werden die Transaktionen dann entweder geblockt oder zugelassen. Die Radar-Algorithmen passen sich schnell an wechselnde Betrugsmuster und Ihr Unternehmen an.
- **Betrug verhindern und Autorisierung durch Ausstellerpartnerschaften stärken:** Die Partnerschaften von Stripe mit den Ausstellern dienen zum Austausch ausgewählter Risikodaten (falls möglich), damit die Aussteller betrügerische Transaktionen blocken und legitime genehmigen können. Die Integration mit Ausstellern schafft Mehrwert für sowohl Karteninhaber/innen als auch für das Unternehmen: Kund/innen fühlen sich beim Einkaufen sicherer und Unternehmen können mehr Transaktionen genehmigen, ohne einen Anstieg von Anfechtungen aufgrund von Betrug zu verzeichnen.
- **Zwei-Faktor-Authentifizierung dynamisch anwenden:** Stripe Checkout ist mit den europäischen SCA-Anforderungen kompatibel und setzt die Authentifizierung (z. B. 3DS) dynamisch um, wenn die Bank des/der Karteninhabers/Karteninhaberin dies erfordert oder wenn es einen Betrugsverdacht gibt. Stripe Checkout unterstützt außerdem die einfachste Methode der PCI-Validierung mit einem vorausgefüllten SAQ A und löst CAPTCHAs nur aus, wenn wir den Verdacht eines Kartentest-Angriffs haben, um Betrug zu vermeiden.

Betrugsmanagement im Team

- **Individuelle Regeln für Betrug festlegen:** Mit Radar for Fraud Teams können Sie individuelle Regeln für das Management eingehender Zahlungen festlegen und damit alle von Ihnen als verdächtig erachteten Zahlungen blocken oder prüfen lassen. Sie könnten zum Beispiel den für die Auslösung manueller Prüfungen erforderlichen Risikowert absenken oder große Bestellungen von Neukund/innen prüfen. Radar for Fraud Teams ermöglicht auch Risikoeinblicke in bestimmte Zahlungen. So erhalten Sie einen Überblick über die wichtigsten Faktoren, die zu einer hohen Risikobewertung führen. Mit diesen Informationen können Sie zusätzliche und zielgerichtetere Regeln erstellen.
- **Hochrisikozahlungen manuell prüfen:** Radar for Fraud Teams umfasst einen zusätzlichen Prüfprozess, bei dem Sie bestimmte Zahlungen zur Prüfung markieren können. Diese Zahlungen werden jedoch verarbeitet und die Kreditkarte wird belastet. Radar for Fraud Teams wird häufig von größeren Organisationen genutzt. Unabhängig von der Größe des Unternehmens ist jedoch die Möglichkeit hilfreich, Zahlungen manuell prüfen zu können. Allerdings finden vor allem kleinere Unternehmen manuelle Prüfungen hilfreich. Eine manuelle Prüfung von verdächtigen Zahlungen kann Ihnen dabei helfen, punktgenauere Maßnahmen zu ergreifen, bevor es zu einer potenziellen Anfechtung kommt. Wenn Sie sich beispielsweise beim Prüfen einer Zahlung unsicher sind, können Sie den/die Kunden/Kundin telefonisch oder per E-Mail kontaktieren. Oder Sie können den Betrag zurückerstatten, wenn Sie den Verdacht haben, dass eine Zahlung betrügerisch zustande gekommen ist.

Zusätzliche Tipps zur Betrugsprävention

- **Tiefere Einblicke in Betrugstrends gewinnen:** Stripe Sigma ermöglicht eine schnelle Analyse der Stripe-Daten über vorab definierte oder benutzerdefinierte SQL-Abfragen im Stripe-Dashboard. Hier finden Sie Antworten auf Ihre komplexen geschäftlichen Fragen, angefangen bei der Frage, warum Kund/innen Zahlungen anfechten, bis hin zu Statistiken darüber, wie viel Prozent der Anfechtungen Sie widersprechen. Sie können auch über Stripe Data Pipeline aktuelle Stripe-Daten an Ihr Data Warehouse bei Snowflake oder Amazon Redshift senden. Dies bietet Ihnen die Möglichkeit, Ihre Stripe-Risikobewertungen mit anderen Betrugsdaten zu vergleichen und umfangreichere Betrugsberichte zu erstellen.
- **Weltweite Kund/innen verifizieren:** Mit Stripe Identity verifizieren Sie die Identität neuer Nutzer-innen nahtlos. So können Sie die Zahl der Betrugsversuche reduzieren und legitime Kund/innen erfahren nur minimale Reibungsverluste.
- **Konversion optimieren und Umsatz steigern:** Die Stripe-Verifizierung des Kartenbilds hilft dabei, die Zahl der fälschlicherweise geblockten Transaktionen zu reduzieren. Statt potenziell hoch riskante Transaktionen zu blocken, erhalten die Nutzer/innen die Gelegenheit nachzuweisen, dass sie die Karte tatsächlich besitzen, indem sie die Karte scannen (neue Funktion ab 2022).

Weitere Informationen darüber, wie Stripe Radar Ihrem Unternehmen bei der Betrugsbekämpfung hilft, erhalten Sie, indem Sie unser Sales-Team kontaktieren oder wenn Sie ein Konto erstellen.

Weitere Quellen

Hier finden Sie weitere Quellen, die Ihnen dabei helfen, mit Betrug umzugehen und Ihr Unternehmen zu schützen:

- Einführung in Online-Zahlungen
- Best Practices für die Betrugsprävention
- Einführung: Maschinelles Lernen in der Betrugsbekämpfung
- Radar for Fraud Teams: Das Regel-Einmaleins
- Über Stripe Radar
- Über Radar for Fraud Teams

Methodik

Stripe hat zwischen 2019 und 2021 Milliarden Zahlungsversuche von Millionen Unternehmen analysiert. Bei diesen Zahlungen und Unternehmen haben wir Anfechtungen und deren Begründungen, Prognosen von unseren auf maschinellem Lernen basierenden Modellen, die 3DS-Nutzung und die manuelle Prüfaktivität der Unternehmen genauer untersucht. Zur Ermittlung von Betrugsraten haben wir Länder, in denen 2021 weniger als 10.000 Zahlungen abgewickelt worden, aus der Analyse ausgeschossen, da sich auf dieser Transaktionsmenge keine verlässlichen Betrugsraten berechnen ließen.

Im Frühjahr 2022 hat Stripe gemeinsam mit Milltown Partners (in Zusammenarbeit mit ihrem Datenanbieter Focaldata) mehr als 2.500 führende Unternehmensvertreter/innen aus neun Ländern weltweit (Australien, Kanada, Frankreich, Deutschland, Japan, Niederlande, Singapur, Vereinigtes Königreich und USA) befragt. Die Unternehmen machten nach eigenen Angaben mindestens 10 % ihres Umsatzes mit Online-Verkäufen.