PSD2: **ein Leitfaden für Käufer-Lösungen**

Ein Leitfaden für
E-Commerce Händler

Inhalt

03 **Was beinhaltet der Leitfaden?**

04 **Planung zur Durchsetzung: Der Einfluss starker Kundenauthentifizierung**

04 **Starke Kundenauthentifizierung und Friktion**

06 **Anwendung von Ausnahmen zur Friktionsminimierung**

Ausnahmeregelungen Genehmigter Kreditkartenaussteller?

Wann werden die Ausnahmeregelungen in Kraft treten?

09 **Eine Übergangsstrategie für PSD2**

Betrug minimieren

Vorbereitung auf starke Kundenauthentifizierung

12 **Betrugsmanagement unter PSD2**

12 **Aufträge, die den Rahmen sprengen**

13 **Die Zunahme von Accountübernahme-Angriffen**

15 **Die Auswirkungen von Betrug**

16 **Der Erwerb einer PSD2-Lösung**

17 **Ein gemeinsamer Ansatz von Händlern zu PSD2**

Grundlegende Übereinstimmungen

Die Entwicklung einer In-House-Lösung

Die Inanspruchnahme einer Drittlösung

21 **Fragen potentieller Anbieter**

Was beinhaltet der Leitfaden?

Als E-Commerce-Händler haben Sie sich höchstwahrscheinlich schon damit auseinandergesetzt, inwieweit die Sicherheitsmaßnahmen im Rahmen von PSD2 Ihren Online-Handel beeinflussen werden. Die Ungewissheit über die Verordnung macht dies nicht gerade leichter. Jedoch die Aufschiebung in der Durchsetzung in fast ganz Europa gibt Ihnen mehr Zeit sich auf diese neue Regulierung einzustellen.

Im Oktober 2019 wurde von der EBA eine Entscheidung getroffen, dass die starke Kundenauthentifizierung, im Englischen auch SCA von Strong Customer Authentication, am 31. Dezember 2019 in Kraft treten wird. Damit erhöht sich die Wahrscheinlichkeit, dass Banken in der gesamten Region in Bezug auf SCA einheitlich fungieren. Viele Online-Händler arbeiten jedoch noch an der Entwicklung eines umfassenden Plans, um ab dem Jahr 2020 ihre Kunden sowie ihre Einnahmen zu schützen.

Riskified hat 2000 Verbraucher, sowie 200 Online-Händler in Großbritannien, Deutschland, Frankreich und Spanien befragt um darzustellen, was wichtig für europäische Verbraucher ist und wie Händler PSD2 in ihre Online-Shops integrieren können. Die Ergebnisse dieser Umfrage geben Aufschluss darüber, wie Verbraucher, die online einkaufen wohl auf potentielle Kundenfriktion reagieren würden und dass die Implementierung beabsichtigter Maßnahmen von Seiten der Händler nicht ausreichen werden.

Dieser Leitfaden enthält Ergebnisse unserer Umfrage, wie Händler die Durchsetzung von PSD2 bewerten und wie sie sich am Besten auf diese vorbereiten können. Zudem stellen wir dar, wie Händler ihre Einnahmen unter diesen Maßnahmen sichern können. Wir haben eine Liste mit Vorschlägen zusammengestellt, die Händler berücksichtigen sollten, wenn sie eine Partnerschaft mit einem Drittanbieter in Erwägung ziehen, um Risiken zu vermeiden, die mit PSD2 in Verbindung stehen.

Planung zur Durchsetzung: Der Einfluss starker Kundenauthentifizierung

Starke Kundenauthentifizierung und Friktion

Die zentrale Befürchtung von Händlern ist es, dass es im Zusammenhang mit PSD2 und einer starken Kundenauthentifizierung zu Warenkorbabbrüchen kommen kann. Unsere Umfrage zeigt, dass über 40% aller europäischen Händler erwarten, dass sich Warenkorbabbrüche in den ersten 12-24 Monaten nach der Einführung von PSD2 häufen werden.

Im Zusammenhang mit den neuen Regulationen sind Kunden dazu verpflichtet mindestens zwei der folgenden Kriterien zu erfüllen, um einen Einkauf abschließen zu können:

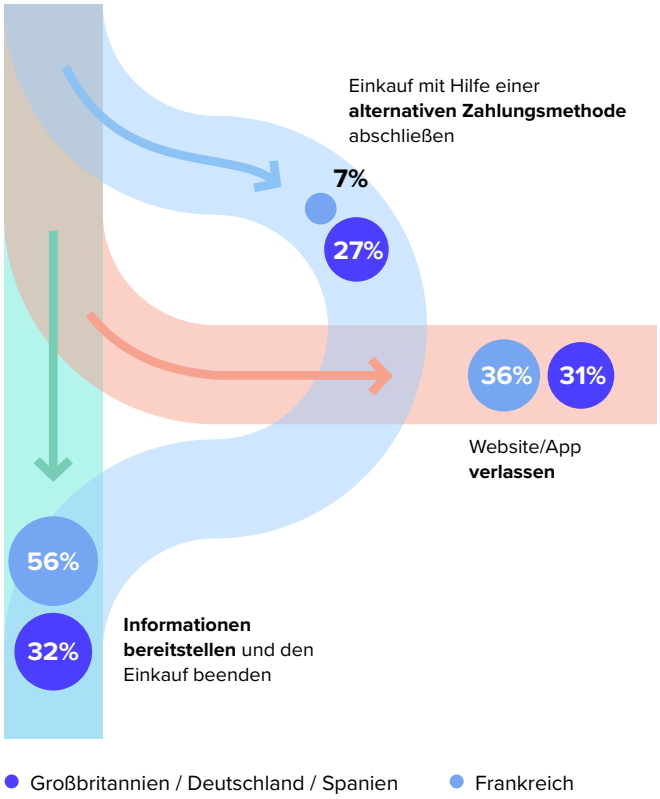
- Etwas, an das sie sich erinnern müssen (z.B. Passwort oder PIN)
- Etwas, dass sie besitzen (z.B. ihr Handy)
- Etwas, dass nur sie bereitstellen können (Fingerabdruck oder Spracherkennung)

Eine zentrale Frage war, ob Verbraucher eine Website oder App verlassen würden, wenn sie dazu aufgefordert werden würden ihre Identität zu verifizieren. Die Identität eines Kunden kann aufgrund folgender Hilfsmittel festgestellt werden: Passwort, PIN, SMS, wissensbasierte Frage, die auf dem Bildschirm erscheint oder einem Gerät, welches sich einem QR-Code bedient. Aufgrund der Antworten hat sich ergeben, dass Händler in Großbritannien, Frankreich, Spanien und Deutschland ungefähr ein Drittel an Bestellungen einbüßen werden, was auf zusätzliche Verifizierungsmaßnahmen zurückzuführen ist. 56% der französischen Verbraucher wären jedoch laut Umfrage bereit zusätzliche Informationen anzugeben. Eine Erklärung ist, das sich französische Verbraucher im Schnitt weniger alternativen Zahlungsmethoden bedienen.

Europäische Verbraucherumfrage

WENN SIE AUFGEFORDERT WERDEN WÜRDEN IM ZUGE EINES ONLINE-EINKAUFS IHRE IDENTITÄT* ZU VERIFIZIEREN, WIE WÜRDEN SIE HANDELN?

*z.B. per PIN Nummer, SMS, wissensbasierte Fragen, Personalausweis, Nachweis durch QR-Code



Anwendung von Ausnahmen zur Friktionsminimierung

Da im Zusammenhang mit starker Kundenauthentifizierung Friktion auftreten wird haben europäische Aufsichtsbehörden neun Ausnahmeregelungen festgelegt (einige davon sind im Folgenden aufgelistet), die angewendet werden können, um zu verhindern, dass Online-Bestellungen einem nachhaltigen Wettbewerbsvorteil unterliegen.

Niedriges Risiko	Transaktionen, die einen **niedrigen Wert** haben **(von 30 - 500€)** können mit Hilfe der friktionslosen Transaction Risk Analysis (TRA) geprüft werden, anstatt mit starker Kundenauthentifizierung. Die Regulation verlangt jedoch, dass **Erwerber gewisse Betrugsschwellenwerte einhalten** (im Weiteren erklärt), um diese Freistellung zu erhalten.
Niedriger Wert	Bestellungen **unter 30€** sind von starker Kundenauthentifizierung ausgenommen. Jede sechste Transaktion, die mit einer Karte erfolgt oder Einkäufe von einem Wert von über 100€ werden jedoch mit Hilfe von straker Kundenauthentifizierung überprüft.
Händler, die sich auf einer Whiteliste befinden	Karteninhaber können verlangen, dass ihr Kreditkartenaussteller **bestimmte Händler auf eine Whitelist setzt,** sodass zukünftige Einkäufe mit ihrer Karte (bei diesen Händlern) von starker Kundenauthentifizierung ausgeschlossen sind
Wiederkehrende Zahlungen	Starke Kundenauthentifizierung wird nicht angewendet, wenn wiederkehrende Zahlungen von **gleichen Geldbeträgen** von einem Kunden an einen **bestimmten Händler** festgelegt wurden, ausgenommen ist dabei die erste Transaktion
Unternehmenszahlungen	Kreditkartenaussteller können Ausnahmen bei Unternehmenszahlungen festlegen, die von einem bestimmten Unternehmen getätigt wurden. Dies gilt jedoch nicht bei Kreditprogrammen für Unternehmen.

Besonders vorteilhaft ist die Ausnahme angesichts des großen Anwendungsbereichs bei geringem Risiko. Unsere Umfrage hat ergeben, dass europäische Käufer pro Online-Kauf ungefähr 30€ - 120€ ausgeben. Die Ausnahme bei geringeren Werten hat jedoch bei den Händlern Besorgnis ausgelöst. Obwohl einige diese Ausnahmen als positiv bewerten befürchten andere, dass Betrüger in Zukunft mehrere Einkäufe von geringerem Wert tätigen werden.

Ausnahmeregelungen genehmiger Kreditkartenaussteller?

Einige Einzelhändler und Zahlungsanbieter haben Bedenken geäußert, ob Kreditkartenaussteller bereit sind Ausnahmen zu machen. Lassen Sie uns dazu einen Blick auf die Prioritäten und Interessen der Herausgeberbanken im Zusammenhang mit PSD2 werfen. Nachdem PSD2 in Kraft tritt werden Kreditkartenaussteller für Transaktionen, die eine starke Kundenauthentifizierung unterlaufen und dennoch von Betrug betroffen sind verantwortlich gemacht. Zur gleichen Zeit erhöht starke Kundenauthentifizierung Friktion. Dies wird sich bei vielen europäischen Konsumenten durch Warenkorbabbrüche und die Auswahl alternativer Zahlungsmethoden niederschlagen.

Bei einer Gewährung von Ausnahmen profitieren Kreditkartenaussteller nicht nur von der Tatsache, dass sie bei Betrug nicht haften müssen, sie profitieren auch davon, dass eine Verringerung von Kunden-Friktion ihre Zahlungsmethode fördert. Erwerber, die so viele Transaktionen wie möglich erfassen wollen, werden auf jeden Fall von den Ausnahmeregelungen profitieren.

Wann werden die Ausnahmeregelungen in Kraft treten?

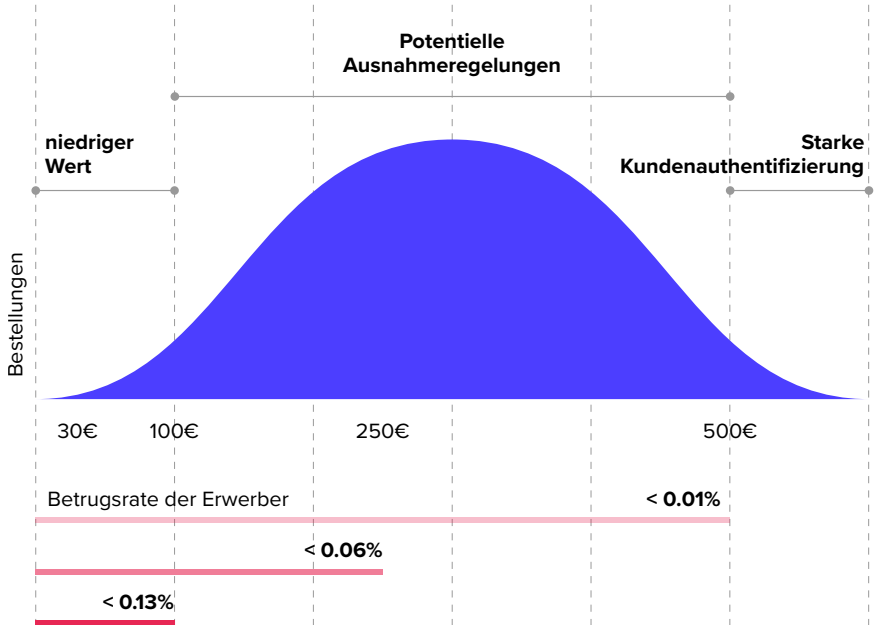
Es ist sehr gut möglich, dass die Ausnahmeregelungen erst in der letzte Hälfte des Jahres 2020 oder zu Beginn des Jahres 2021 in Kraft treten werden. Stellt sich die Frage, was europäische E-Commerce-Händler ab jetzt bis Januar 2021 unternehmen können, um Kunden-Friktion zu minimieren?

Eine Übergangsstrategie für PSD2

Betrug minimieren

Erwerber müssen den Betrugsschwellenwert der Regulierungsbehörde erfüllen, damit Kreditkartenaussteller eine Ausnahme zugunsten eines geringen Risikos erwägen.

BETRUGSSCHWELLENWERTE DER ERWERBER



Es ist Anzunehmen, dass sich die Ausnahmeregelung zu geringem Risiko unter den Erwerbern großer Beliebtheit erfreuen wird, da sie die Kunden-Friktion auf ein Minimum beschränkt und dadurch mehr Einnahmen erzielt werden können. Da die Betrugsraten der Erwerber von allen Händlern gesammelt werden, ziehen es diese vor mit Händlern zusammen zu arbeiten, die niedrige Betrugsraten aufweisen. Mit der Anwendung von PSD2 werden Händler darauf bedacht sein die Ausnahmeregelungen auszuschöpfen, um ihre Betrugsraten so niedrig wie möglich zu halten. Das wirft einige Fragen auf - wann werden Kreditkartenaussteller anfangen Bestellungen abzulehnen, die nicht mit Hilfe von 3DS überprüft wurden?

Vorbereitung auf starke Kundenauthentifizierung

Es wird erwartet, dass die meisten europäischen Länder dem neuen Zeitplan gemäß der EBA-Stellungnahme von Oktober folgen werden (d.h. Sie werden die Anwendung von PSD2 bis Januar 2021 aufschieben). Obwohl es keinen klaren Anreiz gibt könnte es jedoch sein, dass einige Banken starke Kundenauthentifizierung bereits frühzeitig einsetzen werden.

Aufgrund zusätzlicher Kunden-Friktion ist es besser Bestellungen zunächst nicht mit Hilfe von straker Kundenauthentifizierung zu überprüfen. Wenn Händler nicht in der Lage sind 3DS-Daten an Kreditkartenaussteller zu übermitteln, die starke Kundenauthentifizierung verwenden macht sich dies in einer höheren Rate an Zahlungsrückgängen bemerkbar. Werden Bezahlvorgänge nachverfolgt kann dies Aufschluss darüber geben, ob ein bestimmter Kreditkartenaussteller starke Kundenauthentifizierung verwendet. Dies hilft negative Kauferfahrungen und Umsatzverluste zu vermeiden. Daher muss sichergestellt sein, dass 3DS sofort angewendet werden kann nachdem Kreditkartenaussteller starke Kundenauthentifizierung verwenden. Die meisten europäischen Händler haben bereits die Originalversion von 3D Secure (3DS 1) integriert, welche momentan von allen Banken unterstützt wird. Jedoch sind keine Ausnahmeregelungen erlaubt, es wird keine breite Auswahl von Authentifikationsmethoden angeboten und auf vielen Märkten ist 3DS 1 mit einer hohen Kunden-Friktion verbunden. Über 80% der europäischen Einzelhändler, die sich an unserer Umfrage beteiligt haben, gaben an, dass sie die Absicht hätten 3DS 2 bis zum Ende des Jahres 2020 zu verwenden. Diese Version von 3DS ist für Handys optimiert, erlaubt Ausnahmeregelungen und bietet eine große Auswahl an Authentifizierungsmethoden. Die neuste Version von 3DS ist 2.2, welche die Ausnahmeregelungen im Rahmen von starker Kundenauthentifizierung in vollem Umfang ermöglichen. Während 3DS 2.2 auch Inhärenz bietet ist es unklar, wann Banken anfangen werden biometrische- und verhaltensbezogene Daten als Teil der Authentifizierung anzuwenden.

3DS Versions

3DS 1

Unterstützt teilweise die Anwendung von starker Kundenauthentifizierung unter PSD2

Lässt keine Ausnahmeregelungen zu (Ausnahmeregelungen können beantragt werden, aber nur aufgrund einer Autorisierungsanfrage)

Bietet nicht alle Verifikationsarten an

Häufig mit einem hohen Level an Drop-off verbunden

3DS 2

Erlaubt Ausnahmeregelungen

Unterstützt eine Reihe von Modellen zur starken Kundenauthentifizierung

Bessere risikobasierte Authentifizierung

Teilen von Daten zwischen Banken und Händlern

In Checkouts eingebettet

Optimiert für Handys, App-basierte Authentifikation, E-Wallets

3DS 2.2

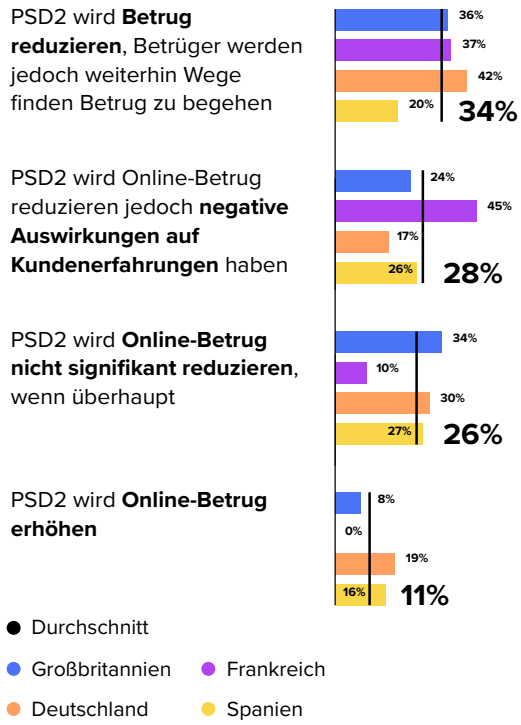
Erweiterte Version von 3DS 2, welche Ausnahmeregelungen bis zur vollen Kapazität und die Übertragung von Daten, die mit dem korrelieren, was Sie anbieten, erleichtert

Zur Zeit noch nicht bei allen Banken akzeptiert und bietet keine Biometrie an

Betrugsmanagement unter PSD2

Europäische Einzelhändlerumfrage

MIT WELCHEM DER FOLGENDEN AUSSAGEN STIMMEN SIE ÜBEREIN?



CNP-Betrug, der vor dem Hintergrund von intra-europäischen Transaktionen auftritt wird voraussichtlich nach der Anwendung von PSD2 in Europa in gewissem Umfang verhindert werden. Starke Kundenauthentifizierung ist jedoch nicht betrugssicher und Betrüger sind bereits jetzt damit beschäftigt Wege zu finden, um starke Kundenauthentifizierung zu umgehen. Unsere Umfrage ergab, dass nahezu 40% aller europäischen Händler die Möglichkeiten von PSD2 Betrug einzudämmen kritisch gegenüber stehen. Ein Viertel dieser Einzelhändler erwarten, dass Betrug ansteigen wird. Die verbleibenden 60% aller Einzelhändler gehen davon aus, dass die neuen Maßnahmen Betrug verhindern werden sind sich jedoch auch über die Negativseite im Klaren.

Aufträge, die den Rahmen sprengen

Wenn ein Unternehmen seinen Hauptsitz in der EU hat und ein Händler seine Waren nur an Kunden vertreibt, die über eine Kreditkarte aus einem EU-Land verfügen ist er auf der sicheren Seite. Wenn ein Händler jedoch beabsichtigt seine Produkte auch in Ländern außerhalb der EU zu vertreiben wird ein Teil seiner E-Commerce-Transaktionen nicht von PSD2 abgedeckt. Bei telefonischen Bestellungen, Bestellungen die vom Händler initiiert werden und allen anderen EInkäufen, die nicht in den Geltungsbereich von PSD2 fallen haften Händler weiterhin für Betrug. Betrüger, die versuchen starke Authentifizierung zu umgehen sind höchstwahrscheinlich motiviert Kreditkartendetails von Kartenbesitzern zu erlangen, die über eine Kreditkarte verfügen, welche nicht in der EU ausgestellt wurde. Wir erwarten, dass Betrüger Zahlungsmethoden verwenden werden, die in Europa nicht populär sind, um Accountübernahme-Angriffe zu verüben. Obwohl sich die meisten Händler auf grundlegende Übereinstimmungen fokussieren sowie auf technische Aspekte, welche mit der Einführung von PSD2 einhergehen ist es wichtig im Hinterkopf zu behalten, dass diese auch ein Verfahren benötigen, mit Hilfe dessen sie Aufträge abwickeln, die den üblichen Bestellrahmen sprengen.

Die Zunahme von Accountübernahme-Angriffen

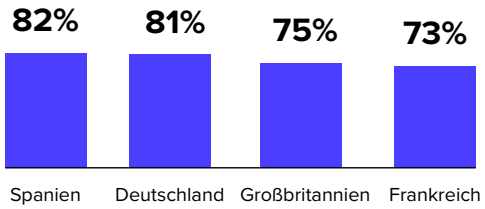
Betrüger haben bereits bewiesen, dass sie sich schnell an Veränderungen anpassen können. Obwohl PSD2 höchstwahrscheinlich ihre Machenschaften erschweren wird, werden sie dennoch versuchen etwaige Schwachstellen auszunutzen. Einer dieser Schwachpunkte ist die Login-Phase des Online-Einkaufs. Wenn Benutzerkonten-Details von einem Betrüger gestohlen werden, können sich diese in das Benutzerkonto eines legitimen Kundens einloggen. Ihre Chance eine betrügerische Transaktion zu tätigen steigt rasant an, da der Händler der Überzeugung ist, dass es sich um einen legitimen Kunden handelt, der auf seine Website zurückgekehrt ist. Dies ist jedoch ein Account-Übernahme-Angriff.

Warum nehmen wir an, dass Accountübernahme-Angriffe unter PSD2 zunehmen werden?

Betrüger können Schaden anrichten, bevor starke Kundenauthentifizierung überhaupt beim Checkout angewendet wird. Zum Beispiel kann ein Betrüger die persönlichen Daten eines legitimen Kunden stehlen und sich Zugriff zu dessen Kundenkonto verschaffen bevor der Betrüger überhaupt einen Einkauf tätigt. Die Möglichkeit der Händler Kunden in Whitelists aufzunehmen verschafft Betrügern einen weiteren Vorteil. Kreditkartendetails werden im Darknet mit den entsprechenden Angaben verkauft: Eingetragen auf einer Whitelist bei Händler XY. Wenn sich eine Kreditkarte auf einer Whitelist befindet und in einem Benutzerkonto gespeichert ist fällt es Betrügern leichter Einkäufe über dieses Benutzerkonto zu tätigen. Obwohl der Betrüger die Lieferadresse oder E-Mail-Adresse ändern kann ist die Bestellung von einer Authentifikation ausgenommen. Dies ist nur ein Grund, warum Ausnahmeregelungen im Zuge von Whitelisting bei Kreditkartenausstellern nicht beliebt sind.

Zudem ist es wichtig daran zu erinnern, dass es ein erklärtes Ziel von PSD2 ist zur Regulierung der Innovation bei Zahlungen beizutragen. Dazu zählt unter anderem ein offenes Bankwesen, welches nicht traditionelle Zahlungsmethoden miteinbezieht, die immer beliebter werden und meist anfällig für Accountübernahme-Angriffe sind. Mehr Anbieter haben die Möglichkeit Zahlungsmethoden anzubieten - Händler eingeschlossen. Jedoch auch Unternehmen, die Erfahrung mit Zahlungsmethoden haben, welche auf Benutzerkonten basieren und über eine solide Sicherheitsinfrastruktur verfügen können Opfer von Accountübernahme-Angriffen werden. Ein Händler, der beschließt als Zahlungsanbieter aktiv zu werden oder sein eigenes E-Wallet anzubieten sollte sich dieser Herausforderungen bewusst sein.

Europäische Verbraucher, die angaben, dass sie entweder sehr oder ziemlich offen für die Verwendung anderer Zahlungsmittel als einer Kredit-/Debitkarte (z. B. Google Pay, Apple Pay usw.) im Zusammenhang von Online-Einkäufen sind.



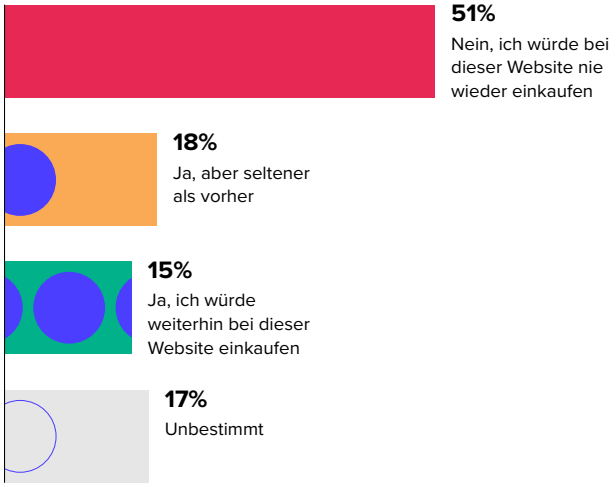
Die Auswirkungen von Betrug

Es ist allgemein bekannt, dass Kunden-Friktion zu Warenkorbabbrüchen führt und das Verkäufe von Betrug dramatisch beeinflusst werden können. Tatsächlich gaben über ein Viertel der Konsumenten an, dass der Sicherheitsfaktor einer der entscheidendsten Faktoren bei der Entscheidung für oder gegen einen Kauf bei einem bestimmten Online-Shop ist.

Online-Händler sollten sich im Zusammenhang mit der Überschreitung von Schwellenwerten und bei Verlusten durch Chargebacks Gedanken über Betrug machen, da dieser den guten Namen ihrer Marke beeinflussen kann. **Mehr als die Hälfte aller Kunden gaben an, dass sie nicht zu einem Online-Shop zurückkehren würden, wenn ihr Benutzerkonto kompromittiert werden würde**. In diesem Zusammenhang erwiesen sich die spanischen Kunden mit 62% am hartnäckigsten. Nur 15% der Befragten gaben an, dass eine Sicherheitsverletzung ihr Einkaufsverhalten nicht beeinflussen würde.

Europäische Verbraucherumfrage

WÜRDEN SIE WEITERHIN BEI EINER WEBSITE EINKAUFEN, BEI DER IHR BENUTZERKONTO KOMPROMITTIERT WURDE?



Unserer Umfrage zufolge würde ein Drittel aller Käufer sich an eine andere Website wenden, wenn beim Abschluss ihres Einkaufs Probleme auftreten würden

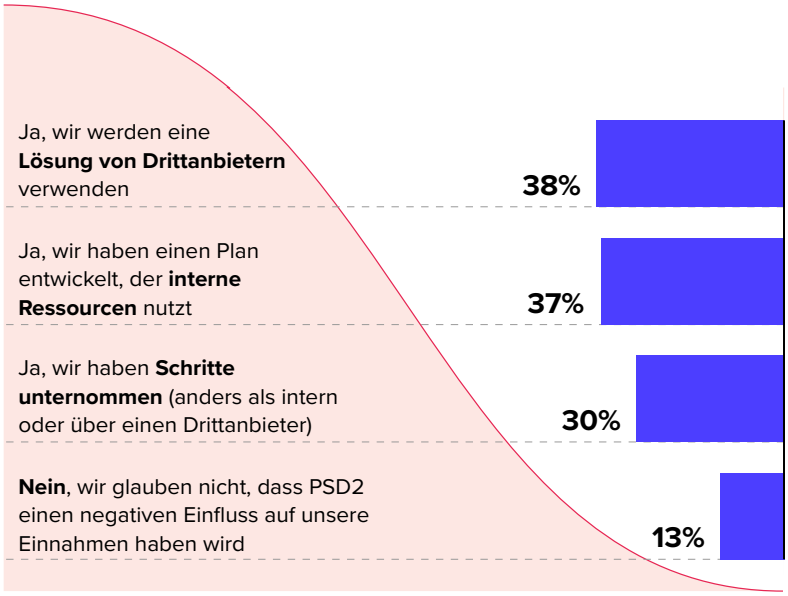
Was kann also getan werden, um ein Unternehmen PSD2-konform zu machen und zugleich effizient den Umsatz und den guten Ruf der Marke zu gewährleisten?

Der Erwerb einer PSD2-Lösung

Die Mehrheit der europäischen Händler hat bereits Schritte unternommen, um negative Auswirkungen von PSD2 auf ihre Einnahmen zu minimieren. Es ist jedoch wichtig sicherzustellen, dass ihre jetzige Lösung auf längere Sicht effektiv ist.

Europäische Einzelhändlerumfrage

HAT IHR UNTERNEHMEN SCHRITTE UNTERNOMMEN, UM DIE NEGATIVEN AUSWIRKUNGEN, DIE PSD2 AUF DIE EINNAHMEN HABEN KÖNNTE, ZU MINIMIEREN?



Der folgende Abschnitt beschreibt einige der vorhandenen Möglichkeiten, wie Händler ihre E-Commerce-Umsätze im Zuge von PSD2 schützen können. Zudem gehen wir auf wichtige Erwägungen ein, die es bei einer Entscheidung der Vorgehensweise zu berücksichtigen gilt, sowie Fragen, die Händler unbedingt stellen sollten, um sicherzustellen, dass sie die richtige entscheidung für ihr Unternehmen treffen.

Ein gemeinsamer Ansatz von Händlern zu PSD2

1. Grundlegende Übereinstimmungen

Zumindest für grundlegende Übereinstimmungen zu PSD2 ist es wichtig, dass Händler innerhalb des Geltungsbereichs 3DS für CNP-Betrug aktivieren. Sich jedoch gänzlich auf diese Protokolle zu verlassen birgt Risiken:

- Potential für mehr Kunden-Friktion
- Begrenzte Einsicht in die Erfahrung von Kunden
- Lücken im Betrugsüberprüfungsprozess
- Keine Optimierung der Ausnahmeregelungen

2. Die Entwicklung einer In-House-Lösung

Einige Händler entwickeln Mechanismen, um identifizieren zu können, welche Bestellungen sich innerhalb des PSD2-Bereichs befinden, welche davon eine starke Kundenauthentifizierung verlangen und auf welche Transaktionen eine Ausnahmeregelung angewendet werden sollte.

Händler, welche in Erwägung ziehen eine In-House-Lösung zu entwickeln um ihre Bestellungen vor dem Hintergrund von PSD2 zu verwalten, sollten sicherstellen, dass sie über genügend Ressourcen verfügen. Eine akkurate Überprüfung von CNP-Bestellungen verlangt Erfahrung sowie das nötige Know-How. Die Entwicklung eines Systems, dass in Echtzeit angewendet werden kann, Aufträge entsprechend weiterleitet und Bestellungen vorab auf Betrug überprüft ist nicht einfach. Neben vielen weiteren Komponenten verlangt eine gut funktionierende Betrugspräventionslösung nach Folgendem:

- In-House-Betrugserfahrungen
- Ein Team von Datenwissenschaftlern und -ingenieuren
- Entwicklung komplexer Modelle
- Zugriff auf umfangreiche historische Daten zum Trainieren des Modells
- Ständige Investition in Dienstleistungen zur Datenanreicherung

Die Entwicklung einer In-House-Lösung kann demnach mehr Einsichten in Kundenerfahrungen und Kontrolle über Verfahren zur Betrugsüberprüfung bieten. Die Einbeziehung einer dritten Partei erleichtert dem Händler jedoch die Arbeit.

3. Die Inanspruchnahme einer Drittlösung

Gateways

Viele Zahlungs-Gateways, die in Europa verwendet werden bieten eine Befreiung von Routing-Diensten, welche oft in Verbindung mit Produkten zur Betrugsüberprüfung stehen.

Vorteile

- Händler pflegen eine Beziehung mit einem Gateway, was recht risikofreie zu sein scheint. Zugleich sind sich Händler jedoch immer noch unsicher über die Tragweite der Verordnung.
- Einige Gateways pflegen enge Beziehungen mit Herausgeberbanken, was wichtig für den Zeitpunkt der Durchführung und bestimmter Schwellenwerte ist.

Nachteile

- Betrugserkennung lag lange nicht im Fokus von Zahlungs-Gateways, wonach unklar ist wie diese bestimmen welche Bestellungen von den Ausnahmeregelungen befreit sind.
- Gateways gehen bei Bestellungen, die nicht von Ausnahmeregelungen befreit sind typischerweise nicht von Betrug aus.
- Gateways werden risikoarme Ausnahmeregelungen entweder blockieren oder erlauben, dies hängt ganz von der Betrugsrate ab. Unweigerlich wird dies zu Zeiträumen führen, in denen Ausnahmeregelungen zu 100% gelten und wiederum zu Zeiträumen, in denen Ausnahmeregelungen zu 0% gelten, etc.

Lösungen zur Erst-Authentifizierung

Eine Reihe von Anbietern bieten friktionslose starke Kundenauthentifizierung an, welche auf biometrischen Merkmalen und Verhaltensmustern basiert und eine Alternative zu 3DS darstellt.

Vorteile

- Inhärenzbasierte Authentifizierung zielt darauf ab Kunden-Friktion zu vermeiden (verglichen mit anderen Formen von starker Kundenauthentifizierung). Einige Anbieter sind von dieser Vorgehensweise so überzeugt, dass sie behaupten, dass Ausnahmeregelungen überflüssig werden könnten.
- Es gibt keinen Grund abzustreiten, dass die Verifizierung durch Inhärenz langfristig ein Schritt in die richtige Richtung ist (zum Beispiel in drei Jahren).

Nachteile

- Starke Kundenauthentifizierung ohne Friktion stützt sich auf inhärente Daten, die mit Hilfe von 3DS 2.2 an Banken transferiert werden. Diese Vorgehensweise wird momentan jedoch noch nicht von vielen Banken in Anspruch genommen.
- Da es bis jetzt noch unklar ist, welche Lösungen, die auf Inhärenz basieren mit starker Kundenauthentifizierung kompatibel sind, werden einige Bestellungen wohl noch aufgrund von fehlgeschlagenen Authentifizierungsversuchen mit älteren Versionen von 3DS oder Erfahrungen zur Kunden-Friktion überprüft werden,
- Diese Art der Authentifizierung muss FIDO-Zertifiziert sein (was sehr schwierig zu erreichen ist).

Lösungen zur Erst-Freistellung

Einige Anbieter, darunter namhafte E-Commerce-Unternehmen, bieten Lösungen deren Ziel es ist auf so viele Bestellungen, wie möglich friktionslose Transaction Risk Analysis (TRA), anstatt starke Kundenauthentifizierung anzuwenden.

Vorteile

- Unternehmen, die sich der Betrugsprävention verschrieben haben sind meist Experten in ihrem Bereich - und einige haben Jahre verbracht, um TRA zu perfektionieren.
- Einige dieser Anbieter bieten eine ganzheitliche Lösung, die Betrug außerhalb des PSD2-Bereichs abdeckt. Im Allgemeinen sind diese Anbieter am besten auf Accountübernahme-Angriffe, Omnichannel-Aufträge, grenzüberschreitende Bestellungen und ein hohes Bestellvolumen spezialisiert.
- Anbieter, die über eine große Datenbasis an Transaktionen verfügen werden in der Lage sein Daten von Herausgebern zu sammeln und über den Zeitpunkt der Durchsetzung zu beraten.

Nachteile

- Die Voraussetzung dieser Anbieter, dass sich PSD2-Produkte auf Ausnahmeregelungen stützen und sich in diese Lösungen integrieren bevor starke Kundenauthentifizierung angewandt wird, mag voreilig erscheinen.

Fragen potentieller Anbieter

F: **Habe ich Einsicht in meine Bestellungen?**

Eine der Herausforderungen von PSD2 ist die Verschiebung von Betrugsbekämpfung zu den herausgebenden Banken und die Verminderung von Kontrolle über die Kundenerfahrung unter einen Hut zu bringen. Viele Händler befürchten, dass sie im Zuge von PSD2 die Kontrolle über ihre E-Commerce-Bestellungen verlieren. Wenn ein Händler seine Optionen abwägt sollte er in Erfahrung bringen, ob der Anbieter ihm Einsicht in folgende Punkte gewährleistet: Welche Transaktionen wurden aufgrund von Betrugsverdacht abgelehnt, Antrag auf Ausnahmestellungen (welche Bestellungen wurden zur Ausnahmeregelung freigestellt und welche Ausnahmeregelungen wurden bewilligt); Wie werden Bestellungen behandelt, die sich außerhalb des Umfangs befinden; und was passiert mit Bestellungen, die starke Kundenauthentifizierung durchlaufen sind (inklusive derer, die fehlgeschlagen sind).

F: **Über welche Erfahrungen verfügen Sie in den Märkten auf denen ich präsent bin?**

Sie sollten sicherstellen, dass Anbieter über eine Erfolgsbilanz in der Zusammenarbeit mit Händlern auf dem europäischen E-Commerce-Markt verfügen. Händler sollten sich idealerweise Daten über die Möglichkeiten des Anbieters verschaffen den Umsatz in der jeweiligen Branche, in der ein Händler tätig ist zu erhöhen. Zudem ist es wichtig herauszufinden inwieweit Anbieter auf globalen Märkten erfahren sind, um sicherzustellen, dass diese eine hohe Leistungsfähigkeit basierend auf Plänen einer internationalen Unternehmensausweitung garantieren können. Bei diesen Erfahrungen sollte auch in Betracht gezogen werden, dass Bestellungen außerhalb des Geltungsbereichs von PSD2-Transaktionen beinhalten können, bei denen sich entweder das PSP des Käufers oder Empfängers außerhalb der EU befinden.

F: **Wie ist es vor dem Hintergrund eines sich weiterentwickelnden Betrugs möglich mich gegen MOs zu schützen?**

Starke Authentifizierung ist eingeschränkt, wenn es um die Prävention von CNP-Betrug geht. Händler profitieren von einer Zusammenarbeit mit einem Anbieter, der ihnen eine ganzheitliche Lösung anbieten kann. Wenn es um Risikomanagement geht sind Banken stets sehr konservativ, demnach macht es Sinn eine Lösung auszuwählen, welche die Auswirkung auf Betrug abschwächt, Betrugsüberprüfungen vorab und Präventionen von Accountübernahme-Angriffen mit eingeschlossen.

F: **Wie können Sie meine Ausnahmeregelungen zu starker Kundenauthentifizierung maximieren?**

Anbieter, die allgemeine Regeln festlegen, um festzustellen, wann sie zu Ausnahmeregelungen drängen müssen oder die Prozesse nicht optimiert haben, werden den Umsatz von Händlern negativ beeinflussen. Händler sollten sicherstellen, dass Anbieter Betrug vor der Autorisierung herausfiltern, um ihre Stellung bei Banken zu verbessern, Zahlungsrückgänge zu reduzieren und Ausnahmen bei starker Kundenauthentifizierung zu maximieren.

Über Riskified

Riskified ist ein führender Anbieter zu E-Commerce-Lösungen mit einer nachgewiesenen Erfolgsbilanz. Wir erhöhen E-Commerce-Einnahmen und verbessern die Kundenzufriedenheit führender Einzelhändler weltweit. Seit 2012 haben wir über eine Milliarden Bestellungen für tausende E-Commerce-Händler überprüft, darunter Fortune 500 Unternehmen.

Die Reihe unserer Angebote bietet Händlern eine große Auswahlmöglichkeit. Ausgehend von generellem Betrug bis hin zu anspruchsvollen Accountübernahme-Angriffen. Riskifieds AI-Plattform erkennt Betrug bei jedem Schritt des Online-Einkaufs, über Kanäle, Standorte und Branchen hinweg. Dies ermöglicht Händlern mehr Bestellungen zu genehmigen und ihren Kunden zusätzlich ein friktionsloses Einkaufserlebnis zu bieten.

Eine PSD2-Optimierung ist eins unserer neusten Angebote, das Händlern hilft legitime Kunden zum Checkout zu bewegen. Wollen Sie mehr darüber erfahren, wie wir Ihnen mit PSD2 behilflich sein können und dennoch einen proaktiven Ansatz zum Schutz Ihrer Online-Einkünfte und der Reputation Ihrer Marke verfolgen, dann kontaktieren Sie uns bitte unter: sales@riskified.com.

riskified

© Riskified Inc. 2020. All rights reserved.