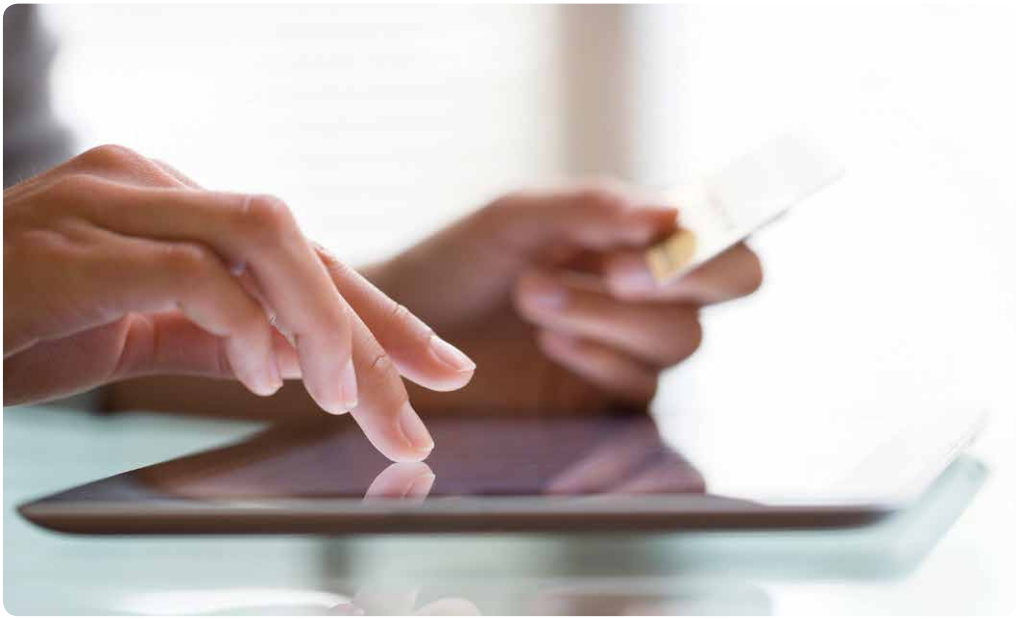
Visa. Und das Leben läuft leichter

VISA

Leitfaden für den Handel

Management von Betrugsrisiken im Fernabsatzgeschäft

Februar 2014



Inhaltsverzeichnis

Einleitung 3

Visa Europe Betrugsmanagement – Monitoring Maßnahmen 4

Betrugskennziffern – im Kontext zu Ihren eigenen Zahlen 5

Visa Europe Compliance-Programme 8

Feststellen des Betrugsausmaßes 9

Betrugserkennungssysteme 10

Aufbau und Struktur eines Betrugserkennungssystems 12

Managementinformationen und Reporting 13

Systeme und Services – zur Verbesserung Ihres Betrugsprofils 15

Unterstützung durch Visa Europe 18

Schlussbemerkung 19

Dieser Leitfaden richtet sich an europäische Händler, die im Rahmen ihres Fernabsatzgeschäfts Visa Karten als Zahlungsmittel akzeptieren. Das Dokument adressiert mögliche Betrugsszenarien und beschreibt Lösungswege, wie Händler Risiken im Fernabsatzgeschäft begegnen können.

Einleitung

Dieses Dokument gibt europäischen Händlern, die im Fernabsatzgeschäft Visa Karten als Zahlungsmittel akzeptieren, Einblick in typische Betrugsszenarien und zeigt Mechanismen auf, die für ein effizientes Risikomanagement zur Verfügung stehen.

Der Leitfaden soll Ihnen einen Überblick über Betrugscharakteristika im Fernabsatzgeschäft geben – einem Umfeld, in dem die Karte beim Bezahlvorgang nicht vorliegt und sich auch der Karteninhaber nicht am Ort der Zahlung befindet. Zudem möchten wir Ihnen Anregungen liefern, wie Sie als Fernabsatzhändler den Anteil Ihrer Kartenzahlungen ausbauen können – bei gleichzeitiger Senkung Ihrer Betriebskosten und Ihres Betrugsrisikos.

Ich hoffe, dass der Leitfaden interessante und aufschlussreiche Informationen für Sie bereithält. Sollten Sie Kommentare oder Anregungen für künftige Aktualisierungen haben, freuen wir uns über eine Mitteilung von Ihnen.

Peter Bayley
Executive Director, Risk Management
Visa Europe

E-Mail: fraudproducts@visa.com

Visa Europe Betrugsmanagement – Monitoring-Maßnahmen

Mit Visa können Karteninhaber überall auf der Welt schnell, sicher und bequem im Handel bezahlen - und jederzeit spontane Einkäufe tätigen.

Meldet jedoch ein Karteninhaber, dass eine Transaktion ohne seine Zustimmung erfolgt ist, ist jede kartenausgebende Bank – gemäß den Richtlinien von Visa verpflichtet – diesen Fall zu untersuchen.

Die Bank muss die Reklamation des Kunden einer angemessenen Prüfung unterziehen. Geht die Bank nach Überprüfung des Sachverhalts davon aus, dass es sich um einen Betrugsfall handelt, muss sie eine Betrugsmeldung an Visa senden – die sogenannte TC40-Meldung. Die TC40-Meldung enthält Details zum betrügerischen Umsatz.

Visa prüft die eingegangenen TC40-Meldungen und weist Meldungen zurück, die die Mindeststandards nicht erfüllen.

Wozu werden Visa Betrugsmeldungen verwendet?

Sie dienen u.a. als Grundlage:

- um den Visa Europe Verwaltungsrat über Betrugsentwicklungen zu informieren
- zur Unterstützung/Befürwortung von Änderungen bei Geschäftsmodellen
- zur Förderung von Investitionen in neue Systeme und Infrastrukturen
- zur Etablierung und Aufrechterhaltung von Compliance-Programmen

TC40-Meldungen sind kein perfektes Abbild von Betrug – doch für die Funktionsweise eines Zahlungssystems sind sie ein integraler Bestandteil. Zudem sind sie wichtig, um sicherzustellen, dass die folgenden Ziele auch künftig einen Schwerpunkt der Visa Europe Agenda bilden:

- Minimierung von Betrug – für alle Akteure des Zahlungssystems
- Sicherstellen, dass möglichst viele Autorisierungsanfragen autorisiert werden – zum Nutzen von Karteninhabern und Händlern
- Senkung der Risikomanagement-Kosten auf ein möglichst niedriges Niveau – für alle Beteiligten

Lassen Sie uns vor diesem Hintergrund einen Blick auf die Betrugszahlen werfen – und was diese über die Situation in Europa aussagen.

Betrugskennziffern – im Kontext zu Ihren eigenen Zahlen

Betrug ist für Visa Europe eine wichtige Größe. Im September 2013 lag die Betrugsquote bei 4,5 Basispunkten – d. h. die durch Betrug entstandenen Verluste entsprachen 0,045% des Gesamtumsatzes (100 € Umsatz = 0,045 €).

Diese Entwicklung spiegelt die Fokussierung wider sowie die Investitionen, die in den vergangenen rund 50 Jahren – seit der Gründung von Visa – von allen Marktteilnehmern getätigt wurden.

Das Betrugsausmaß variiert und ist abhängig von der Umgebung (Vertriebskanal), in der die Transaktion stattfindet. Visa Europe unterscheidet im Wesentlichen zwischen zwei Umfeldern:

- Transaktionen im stationären Handel – d. h. einem Umfeld, in dem sowohl Karteninhaber als auch Händler am Ort des Verkaufs präsent sind und die Karte zur Zahlungsabwicklung vorliegt.
- Transaktionen im Rahmen des Fernabsatzgeschäfts – d. h. einem Umfeld, in dem eine Zahlungsabwicklung stattfindet, ohne dass sich der Karteninhaber und die Karte am Ort des Verkaufs befinden – beispielsweise bei Online-Zahlungen im Internet.

Wie sich unschwer vorstellen lässt, sind die beiden Umgebungen durch unterschiedliche Betrugsquoten gekennzeichnet. Befinden sich beide Vertragsparteien (Händler und Karteninhaber) am Ort des Verkaufs und wird eine physische Karte zum Bezahlen des Einkaufs verwendet, ist das Betrugsausmaß erheblich geringer als in einem Umfeld, in dem die Karte nicht vorliegt. Zudem bietet die leistungsfähige Verschlüsselungsmethodik des EMV-Chips ein extrem hohes Maß an Sicherheit.

Die Betrugsquote im stationären Handel liegt derzeit bei knapp unter 4 Basispunkten – die Quote im Fernabsatzgeschäft hingegen bei rund 15 Basispunkten.

Was ist für Sie als Händler ein vertretbares Maß an Betrug? Und wie stellt sich Ihre Betrugsquote im Vergleich zu den oben genannten Werten dar?

Ein weiterer Ansatz, um Betrug rechtzeitig zu erkennen, ist das Überprüfen des Aufenthaltsortes Ihrer Kunden – sowie das Land, in dem die Visa Karte des jeweiligen Kunden ausgegeben wurde. Wie sich dies darstellen lässt, hängt von Ihren Systemen ab. Es ist nicht immer einfach und ist als alleiniges Beurteilungskriterium nicht ausreichend. Zudem wird es stark von Ihren geografischen Vertriebsaktivitäten beeinflusst - doch es lohnt sich.

Entfallen beispielsweise 80 Prozent Ihrer Umsätze auf Karteninhaber aus Großbritannien, verwundert es nicht, wenn die Mehrzahl Ihrer Betrugsfälle ihren Ursprung ebenfalls in Großbritannien hat.

Es gilt allerdings zu beachten, dass sich Betrug – je nach Kartenausgabeland – unterschiedlich darstellt und Betrugsszenarien sich im Laufe der Zeit auch verändern können.

Länder, deren Kartenemittenten – im Zusammenhang mit europäischen Händlern – am stärksten von Betrug betroffen sind

Land	**Anteil am VE* Fernabsatzbetrug**	**Betrugsquote** (Verhältnis Umsatz-Betrug)
Großbritannien	35,60 %	0,098 %
USA	18,04 %	2,030 %
Frankreich	5,95 %	0,626 %
Deutschland	4,35 %	0,269 %
Kanada	4,29 %	1,506 %
Italien	3,45 %	0,219 %

(Basis: Visa Europe Geschäftsjahr – Okt. 2012 bis Sept. 2013)

* VE = Visa Europe

Die Zahlen verdeutlichen, dass für europäische Händler der größte Teil des Fernabsatzbetrugs seinen Ursprung in Großbritannien hat (35,6%). Doch in Verbindung mit einer sehr niedrigen Betrugsquote – eine Quote, die zweifelsohne von äußerst wirksamen Kontrollmechanismen geprägt ist.

An zweiter Stelle folgen Visa Karten, die in den USA ausgegeben wurden – womit sich allerdings weitaus höhere Betrugsquoten verbinden. Dies macht deutlich, dass mit einer zunehmenden Entfernung zwischen kartenausgebendem Institut und Händler auch die Betrugsquote ansteigt. US-Händler, die europäische Karten akzeptieren, sehen einen ähnlichen Anstieg.

Diese Betrugsquoten spiegeln nicht primär die Performance der kartenausgebenden Bank wider. Sie zeigen vielmehr, dass mit Karten, die nicht innerhalb ihres natürlichen Marktumfeldes eingesetzt werden ein größeres Risiko verbunden ist.

Ein weiterer wichtiger Faktor ist die Sicherheitsinfrastruktur, die in den verschiedenen Ländern zum Einsatz kommt. Im Vergleich zu Karteninhabern in den meisten europäischen Ländern nutzen beispielsweise weitaus weniger US-Karteninhaber den Verified by Visa-Service. Dies hat Einfluss auf das Risikopotenzial und sollte daher bei Ihren Strategien in Sachen Betrugserkennung und Betrugsbekämpfung Berücksichtigung finden.

Betrachtet man Betrugsszenarien im Fernabsatzgeschäft etwas genauer, lässt sich Betrug auf drei weitere Kategorien herunterbrechen. Wir können so die unterschiedlichen Risiken, die abhängig sind von der Art und Weise, wie Händler ihre Transaktionen verarbeiten, besser verstehen.

Bei den drei Kategorien handelt es sich um:

- MOTO (die Abkürzung steht für schriftliche, telefonische oder wiederkehrende Transaktionen) – in der Regel Aufträge, die ein Karteninhaber dem Händler telefonisch erteilt hat.
- Sicherer eCommerce-Handel – üblicherweise Transaktionen, die online abgewickelt wurden – unter Verwendung des Verified by Visa-Services (3D-Secure-Protokoll).
- Unsicherer eCommerce-Handel – eine Online-Transaktion, der kein Verified by Visa-Service zu Grunde lag.

Betrugs-Performance – heruntergebrochen auf die drei Vertriebskanäle über die Fernabsatzgeschäft akquiriert wurde

Fernabsatz-Vertriebskanal	**Anteil am VE Fernabsatzbetrug**	**Betrugsquote** (Verhältnis Umsatz-Betrug)
MOTO	26 %	0,13 %
Sicherer eCommerce (Verified by Visa)	11 %	0,08 %
Unsicherer eCommerce	54 %	0,32 %

Wie sich unschwer erkennen lässt, resultieren die meisten Betrugsfälle aus dem unsicheren eCommerce-Umfeld. Es ist ein weitaus höherer Anteil als bei jenen Transaktionen, die durch den Verified by Visa-Service abgesichert sind.

Ein weiterer Vorteil für Händler, die Verified by Visa unterstützen, besteht darin, dass sie im Betrugsfall in der Regel von einer vollständigen Zahlungsgarantie profitieren. Die Haftung für nichterbrachte Leistungen, Produktschäden etc. bleibt jedoch bestehen – zudem findet das Verified by Visa-Haftungsumkehrprinzip nicht auf alle in den USA ausgegebenen Karten Anwendung.

Sicherlich können Sie jetzt besser verstehen, warum Visa Europe ein engagierter Befürworter von Verified by Visa ist. Niedrigere Betrugsquoten und eine Zahlungsgarantie im Betrugsfall bieten Händlern enorme Chancen. Aber auch die anderen an einer Zahlung beteiligten Akteure profitieren von Verified by Visa – durch Kosteneinsparungen und eine bequemere Zahlungsabwicklung.

Lassen Sie uns nun die Händlersegmente betrachten, die innerhalb des Zahlungssystems am stärksten von Betrug betroffen sind – und die unterschiedlichen Betrugsrisiken ausgesetzt sind.

Die Tabelle zeigt, wie sich Betrug in einigen Kernsegmenten des Handels darstellt. Zudem wird deutlich, wie Betrugsausmaß und Betrugsquote variieren können – je nachdem, welche Produkte/Services vertrieben werden (sowie in Abhängigkeit von der Art der Transaktionsverarbeitung).

Gehört Ihr Geschäftsfeld einer der genannten Kategorien an, werden Sie vielleicht Ihre Betrugsquote mit dem in der Liste genannten Wert vergleichen. Liegen Sie über dem jeweiligen Durchschnittswert, kann dies Ihre Profitabilität, Ihre Leistungsfähigkeit und Ihre Reputation unnötig belasten.

Es könnte auch zur Folge haben, dass Ihre Händlerbank – mit der Sie den Vertrag zur Akzeptanz von Visa geschlossen haben – Ihrem Unternehmen und den Bedingungen, die dem Akzeptanzvertrag zu Grunde liegen, stärkere Beachtung schenkt. Außerdem könnte eine deutliche Abweichung vom Durchschnittswert ein Anzeichen dafür sein, dass sich Ihr Unternehmen den Grenzwerten nähert, die gegebenenfalls ein Visa Compliance-Programm einleiten können.

Händlerkategorie	**Anteil am VE Fernabsatzbetrug**	**Betrugsquote** (Verhältnis Umsatz-Betrug)
Dienstleistungen	30,46 %	0,159 %
Sonstige Einzelhändler	11,36 %	0,287 %
Fluggesellschaften	9,88 %	0,228 %
Unterhaltung	8,53 %	0,164 %
Reise	7,78 %	0,193 %
Katalog-/Versandhandel	7,72 %	0,322 %
Heimwerkermärkte	6,39 %	0,242 %
Bekleidung	6,35 %	0,339 %

Visa Europe Compliance-Programme

Wie bereits erwähnt, sind die Risiken, die sich mit einem bestimmten Kartenportfolio oder einer bestimmten Händlerbranche verbinden, unterschiedlich. Und wir gehen davon aus, dass folglich auch die Betrugsquoten für die beteiligten Parteien unterschiedlich ausfallen.

Wir sind der Meinung, dass eine Reduzierung von Betrug – auf Seiten aller am Zahlungsverkehr Beteiligten – im Interesse aller Akteure und auch im Interesse der Gesellschaft insgesamt ist. Aus diesem Grund haben wir im Bereich Betrugsmanagement eine Reihe von Compliance-Programmen etabliert. Ziel ist es, mit Hilfe dieser Programme, Marktteilnehmer zu erkennen, bei denen ein hohes Maß an Betrug auftritt und Anreize für sie zu schaffen, Betrug zu reduzieren.

Die **Schwerpunkte der Programme** liegen auf den Unternehmen, die im Rahmen des Visa Zahlungssystems ein überdurchschnittlich hohes Maß an Betrug aufweisen:

- Kartenemittenten
- Händlerbanken
- Händler

Eine Bewertung im Rahmen eines Compliance-Programms erfolgt mindestens auf monatlicher Ebene – und kann für die betroffenen Unternehmen Strafzahlungen und/oder Änderungen bei der Haftungsfrage zur Folge haben.

Bitte beachten Sie, dass Visa Europe eine Reihe weiterer Compliance-Programme etabliert hat, die sich jedoch nicht zwangsläufig auf Betrugsfälle beziehen.

Sie sollten mit Ihrer Händlerbank zusammenarbeiten, um sicherzustellen, dass Sie einen niedrigen Betrugsgrenzwert einhalten. Ihre Bank wird Sie auch beraten, wenn Sie im Rahmen eines Visa Compliance-Programms auffällig geworden sind. In einem solchen Fall ist es ratsam, gemeinsam vorzugehen, um weiteren Betrug zu verhindern oder entsprechend darauf zu reagieren. Je enger Sie sich dabei mit Ihrer Händlerbank abstimmen, desto besser. Ferner ist ein Aktionsplan sinnvoll, mit dem Sie belegen können, dass angemessene Maßnahmen in Planung sind oder bereits umgesetzt wurden – die dazu beitragen sollen, ein übermäßiges Maß an Betrug und/oder Rückbelastungen zu verhindern.

Und – Sie sollten immer daran denken, dass Ihrem Unternehmen mit jedem Betrugsfall Kosten entstehen. Diese Kosten auf einem akzeptablen Niveau zu halten, zählt zu den Aufgabenschwerpunkten einer Führungskraft im Bereich Betrugsmanagement – dem sogenannten „Fraud Manager".

Feststellen des Betrugsausmaßes

Eine wichtige Aufgabe des „Fraud Managers" besteht darin, das Ausmaß des Betrugs festzustellen, der infolge Ihrer Vertriebsaktivitäten entstanden ist.

„Fraud Manager" im Bereich des Handels konzentrieren sich bei der Adressierung des Problems häufig auf Rückbelastungen, da sie einen direkten Einfluss auf die Gewinn- und Verlustrechnung haben. Während dies durchaus eine wichtige Maßnahme ist, gibt es ein weiteres gleichermaßen nützliches Instrument.

Ihre Händlerbank hat Zugriff auf Betrugsinformationen, die kartenausgebende Banken täglich im Rahmen von Betrugsmeldungen (TC40-Meldungen) an Visa übermitteln (s. „Visa Europe Betrugsmanagement - Monitoring-Maßnahmen", Seite 4). Bitte beachten Sie, dass Ihnen Ihre Händlerbank – sollte sie Ihnen diese Daten zur Verfügung stellen – möglicherweise für das Extrahieren und die Bereitstellung eine Gebühr in Rechnung stellt.

Für ein effizientes Risikomanagement ist es wichtig, dass Ihr Unternehmen, den Informationen, die den Visa Betrugsmeldungen zu Grunde liegen, Beachtung schenkt – da sich damit ein signifikanter Nutzen verbindet:

1. TC40-Meldungen umfassen alle Betrugstransaktionen, die von Kartenemittenten an Visa gemeldet wurden – nicht nur jene, die von kartenausgebenden Instituten zurückbelastet wurden.

Sie können erkennen, welche Kunden Transaktionen, die bei Ihnen stattgefunden haben, als betrügerisch gemeldet haben. Wenn Sie diese dann nicht als Betrug kennzeichnen, könnten sie sich gegebenenfalls wiederholen und einen größeren Schaden verursachen. Zudem kann es sein, dass die kartenausgebende Bank eine Rückbelastung veranlasst.

2. TC40-Meldungen enthalten alle Details zu den Karten, den kartenausgebenden Instituten und den Ländern, in denen betrügerische Umsätze erfolgt sind. Um Betrug erkennen zu können, ist es für Sie wichtig zu wissen, mit welchen Kartenemittenten und in welchen Ländern sich für Sie die meisten Betrugsumsätze verbinden. Liegen Ihnen diese Informationen vor, können Sie Ihre Verluste minimieren. Zugleich könnten Sie aber auch mit Kartenemittenten und Ländern, die kein hohes Risiko darstellen, nachsichtiger umgehen, d. h. weniger strenge Kriterien bei der Zahlungsverarbeitung anlegen.

3. TC40-Datensätze werden schneller bereitgestellt als Rückbelastungen – sie werden täglich an Ihre Händlerbank übermittelt.

Sie erlangen mit Hilfe der TC40-Meldungen früher Kenntnis über Betrugsfälle – somit lassen sich veränderte Trends früher erkennen, Folgegeschäft früher blockieren und unter Umständen können Sie den Versand von Waren – für Transaktionen, die durch das Sicherheitsnetz gefallen sind – rechtzeitig stoppen.

4. Mit den Informationen der TC40-Meldungen verfügen Sie über ein Instrument, mit dem Sie Ihre Betrugs-Performance nachverfolgen können – auf dieselbe Art und Weise, wie Visa und Ihre Händlerbank dies tun.

Sie sehen, wie sich Ihre Performance verändert, d.h. verbessert oder verschlechtert. Und Sie erfahren genauso schnell wie Visa, wenn Veränderungen auftreten. Sie können so Strategien testen und kennen zudem Ihre Betrugsquote – wissen also, wie hoch der Anteil des betrügerischen Umsatzes gemessen an Ihrem Gesamtumsatz ist.

Wenn Sie noch keinen Zugang zu den Visa Betrugsmeldungen (TC40) haben, wenden Sie sich an Ihre Händlerbank. Sollte Ihnen diese nicht weiterhelfen können, senden Sie eine E-Mail an Visa Europe fraudproducts@visa.com. Wir helfen Ihnen – gegen eine geringe Gebühr – gerne beim Aufsetzen eines geeigneten Reporting-Prozesses.

Betrugserkennungssysteme

Systeme, die der Aufdeckung von Betrug dienen, sind für alle Zahlungsverkehrsparteien, inklusive Händler, von großer Bedeutung.

Es ist häufig der Fall, dass Händler, die überdurchschnittliche Betrugs- und Rückbelastungsraten aufweisen, keine Monitoring- und Betrugserkennungsmechanismen etabliert haben.

Betrugserkennung im Bereich des Handels bedeutet in erster Linie das Einteilen von Vertriebsaktivitäten in Geschäfte, mit denen sich ein hohes Risiko verbindet und Geschäfte mit einem geringen Risiko. Dies hat den Vorteil, dass Sie einerseits Aufträge, die als risikoarm eingestuft wurden, schneller abwickeln können. Andererseits können Sie Aufträge – mit einem eindeutig betrügerischen Hintergrund – ablehnen. Des Weiteren haben Sie die Option, Transaktionen, die ein höheres Risiko aufweisen, aber nicht offensichtlich betrügerisch sind, auszusteuern und sie einer manuellen Prüfung zu unterziehen.

Leider können wir an dieser Stelle nicht im Detail auf Betrugserkennungssysteme eingehen. Ein effizientes Betrugserkennungssystem ist jedoch durch folgende Komponenten gekennzeichnet:

1. Datenauswahlbereich – im Rahmen dieser Funktion wird festgelegt, welche Daten Sie Ihrem System zur Verfügung stellen können, damit dieses eine Risikobewertung vornehmen kann.

2. Negativ-Datenbank – Datenbank, in der bekannte Betrugsmuster und die damit verbundenen Betrugsmerkmale hinterlegt sind. Eine solche Datenbank kann intern entwickelt werden oder die Informationen können über externe Quellen bezogen werden.

3. Positiv-Datenbank – Datenbank mit Kunden, die bekannt sind und eine positive Kundenhistorie aufweisen.

4. Statistisches Modell – dabei kann es sich um eine Scorecard, ein neuronales Netz oder ähnliches handeln. Die Art des Modells ist nicht wirklich von Bedeutung. Wichtig ist, dass dem Modell eine statistische Methodik zu Grunde liegt und Sie die damit verbundene Systematik verstehen. Mit Hilfe dieses Instruments können Sie, auf der Basis von Kundenprofilen, eine Risikobewertung („Risk Scoring") von Transaktionen vornehmen. Berücksichtigt werden im Rahmen dieser Bewertung beispielsweise die Bestellhistorie, Kaufhäufigkeit, Geräte über die Transaktionen erfolgt sind (geografische Ortung, Geräte-Kennung) sowie frühere Erfahrungswerte im Zusammenhang mit Betrug.

5. Regelbasiertes System – mit Hilfe eines auf Regeln basierenden Systems können Sie unter Verwendung der zuvor genannten Parameter entsprechende Strategien entwickeln. Diese Strategien sind allerdings nicht als Ersatz für ein statistisch basiertes Modell zu sehen, sondern sie verstehen sich vielmehr als Ergänzung.

6. Aussteuerungsmechanismus – im Rahmen dieser Mechanik lässt sich festlegen, wie auffällige Transaktionen, mit denen sich ein höheres Risiko verbindet, abgewickelt werden. Möglich wäre eine Weiterleitung, mit dem Ziel einer manuellen Bearbeitung oder ein anderer Ansatz der Transaktionsverarbeitung, wie beispielsweise die Abwicklung im Rahmen des Verified by Visa-Services.

Nachdem Sie die notwendigen Parameter festgelegt haben, müssen Sie kontrollieren, wie effizient Ihr Betrugserkennungssystem arbeitet.

Mit Hilfe der Visa Betrugsmeldungen (und der Rückbelastungsinformationen – die eine leicht abweichende, aber dennoch relevante Entwicklung aufzeigen), lassen sich dann die wichtigsten Kennzahlen berechnen.

1. Betrugsumsatz-Erkennungsrate
Hier wird der betrügerische Umsatz, der über alle Ihre Vertriebskanäle erfolgt ist, zu Grunde gelegt und es wird errechnet, wie hoch der Anteil ist, der von Ihrem System erkannt wurde. Dies hilft Ihnen die Effizienz der von Ihnen ergriffenen Maßnahmen zu bewerten.

2. Falsche Positivraten
Was glauben Sie, wie viele Transaktionen – für die Ihr System eine Warnung oder Aussteuerungsmeldung generiert hat – waren tatsächlich betrügerisch? Für Transaktionen, die weiterverarbeitet wurden und aus denen eine Visa Betrugsmeldung oder Rückbelastung resultiert ist, wissen Sie es genau. Für alle anderen Fälle müssen Sie gute Kriterien festlegen, um dies beurteilen zu können.

3. Auswirkung auf Kunden
Auf wie viele Ihrer Kundentransaktionen wirkt sich Ihr Betrugserkennungssystem negativ aus – sei es durch eine Lieferverzögerung, Nachfragen oder Überprüfungen vor einer Weiterbearbeitung des Auftrags oder sonstige manuelle Prüfungen.

Die genannten Kennzahlen liefern Ihnen eine solide Grundlage für eine Bewertung Ihrer Performance in puncto Betrugserkennung und den Auswirkungen, die sich damit für Ihr Unternehmen verbinden.

Erkennen Sie beispielsweise 50 Prozent des Betrugs, der über Ihr Vertriebsportal stattfindet - mit folgenden Werten:

i. einer falschen Positivrate von beispielsweise 1:7 (d.h. jeder betrügerischen Transaktion, die Sie verhindern, stehen sieben „echte" Transaktionen gegenüber)

ii. und einer Kundenauswirkungsrate von beispielsweise 5 Prozent (d.h. 95 Prozent Ihrer Transaktionen werden problemlos verarbeitet und nur 5 Prozent erfordern eine spezielle oder manuelle Bearbeitung)

Dann liefern Ihnen diese Ergebnisse eine solide Grundlage, um zu bewerten, wie gut Ihre Prozesse sind und ob Sie Kontrollmechanismen verschärfen müssen oder diese eher lockern können.

Zudem können Sie die Leistungsfähigkeit Ihres Systems über eine bestimmte Zeit verfolgen – und so erkennen, ob Ihr System besser oder schlechter wird.

Aufbau und Struktur eines Betrugserkennungssystems

Bei der Konfiguration eines Betrugserkennungssystems gibt es verschiedene Möglichkeiten. Sinnvoll ist der Aufbau einer logischen Struktur, mit der die Vorgehensweise für die Bearbeitung einer Transaktion festgelegt wird.

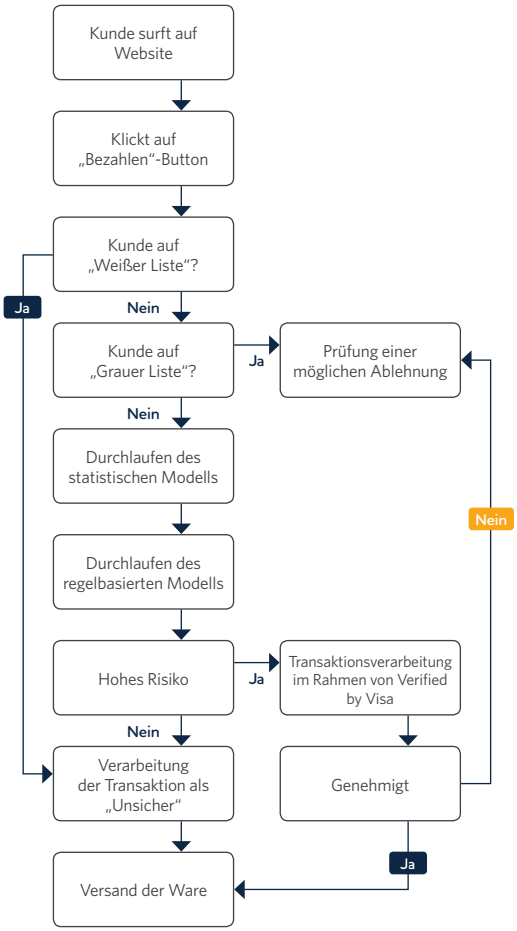
Die skizzierte Struktur zeigt einen Händler, der am Verified by Visa-Service teilnimmt und sowohl ein statistisches Modell als auch ein regelbasiertes System – das sich auf eine sogenannte „Graue Liste" und eine „Weiße Liste" stützt – verwendet.

Die „Graue Liste" umfasst beispielsweise Adressen von Kunden mit einer negativen Historie, Namen oder Geräte – kurzum Sachverhalte, bei denen davon auszugehen ist, dass Sie diese Transaktionen einer genaueren Prüfung unterziehen möchten und die Wahrscheinlichkeit einer Transaktionsablehnung groß ist. Die „Weiße Liste" enthält im Gegensatz dazu die andere Kundengruppe – Kunden, die Sie schätzen und deren Aufträge Sie ausführen möchten, unabhängig davon, was und wie diese Kunden kaufen (wenngleich auch für diese Kunden ein Umsatzlimit sinnvoll wäre).

Das statistisch basierte Modell bietet Ihnen eine einfache Möglichkeit, Ihre Regeln zu optimieren, um so eine bessere Performance zu erreichen und gleichzeitig das Einkaufserlebnis des Kunden nicht negativ zu beeinflussen – ein schwieriger Balanceakt, den es umzusetzen gilt.

Ihre Mitarbeiter aus dem Bereich Betrugsmanagement können die Regeln durch eigene Erfahrungswerte und Fachkenntnisse ergänzen.

Im gezeigten Beispiel wird der Verified by Visa-Service (3D Secure) im Rahmen eines Aussteuerungsprozesses „nur" für auffällige, risikoreichere Transaktionen genutzt. Doch die Zahl der Händler, die Verified by Visa bereits für ihre gesamten Geschäftsaktivitäten anwendet, nimmt kontinuierlich zu. Grund dafür sind die geringeren Betrugsverluste und die Tatsache, dass weniger Kunden ein negatives Einkaufserlebnis haben (s. Abschnitt „Verified by Visa", Seite 16). Aber auch dann, wenn der Verified by Visa-Service keine Option für Sie darstellt, sollten Sie über andere manuelle Methoden oder Prozesse zur Prüfung von Transaktionen nachdenken.



Managementinformationen und Reporting

Solide Managementinformationen (MI) sind eine wichtige Grundlage für alles, was Sie tun. Es sollte sich dabei um eine Kombination aus Informationen handeln, die die gegenwärtige Performance widerspiegeln und Informationen, die aktuelle Trends abbilden.

Ohne solide Daten – die regelmäßig generiert werden sollten (idealerweise täglich und wöchentlich) – und die die wichtigsten Trends in puncto Betrugs-Performance aufzeigen, sind Sie wie ein Jäger, dem die Augen verbunden sind. Was bedeutet – Sie hören die Enten um sich herum, aber eine von ihnen zu treffen wäre purer Zufall. Und Zufall ist ein Umstand, auf den ein „Fraud Manager" niemals bauen sollte.

Wenngleich es bei einigen Daten – die stets aktuelle Trends berücksichtigen müssen – etwas dauern kann, bis Sie daraus wertvolle Erkenntnisse ziehen können, liefern Ihnen Managementinformationen auf täglicher Ebene einen Überblick über:

1. Finanzen und Betrug

- Wie viele Betrugsfälle sehen Sie?
- Was können Sie anhand von Rückbelastungen erkennen? (Auswirkung auf Gewinn- und Verlustrechnung)
- Wie hoch ist der Betrugsanteil gemessen am Umsatz (Betrugs-Umsatz-Verhältnis) – netto und brutto?
- Welche Kartenemittenten, Märkte, Vertriebskanäle und Waren sind für Betrug verantwortlich?

2. Erkennung

- Wie hoch ist die Quote des erkannten Betrugs, die falsche Positivrate und die Auswirkungsrate bei Kunden?
- Wie hoch ist der aus den Erkennungsaktivitäten resultierende entgangene Umsatz?
- Welcher Anteil des entgangenen Umsatzes ist vermutlich betrügerisch und warum?
- Welche Ablehnungen generieren Sie aus Gründen, die nicht mit Betrug im Zusammenhang stehen?

3. Operative Prozessabläufe

- Wie sehen die operativen, unterstützenden Prozesse aus und wie gut funktionieren sie?
- Wie viele Arbeitsstunden entfallen auf die Betrugserkennung und welche Kosten sind damit verbunden – nach Kernfunktion?
- Werden Servicevereinbarungen („Service Level Agreements") im Zusammenhang mit operativen Prozessabläufen eingehalten – von Ihnen selbst und auch von beauftragten, externen Dienstleistern?
- Welche operativen Kosten entstehen dem Unternehmen im Zusammenhang mit der Betrugskontrolle?

4. Beschwerden

- Wie viele Beschwerden erhalten Sie und aus welchen Gründen?
- Welche anderen negativen Auswirkungen verursachen Sie?
- Was tun Sie dagegen?

5. Weiterreichende Auswirkungen für das Unternehmen

- Welche weiterreichenden Auswirkungen verbinden sich mit Ihren Betrugsmanagementsystemen – sowohl positive als auch negative?

6. Strafverfolgung

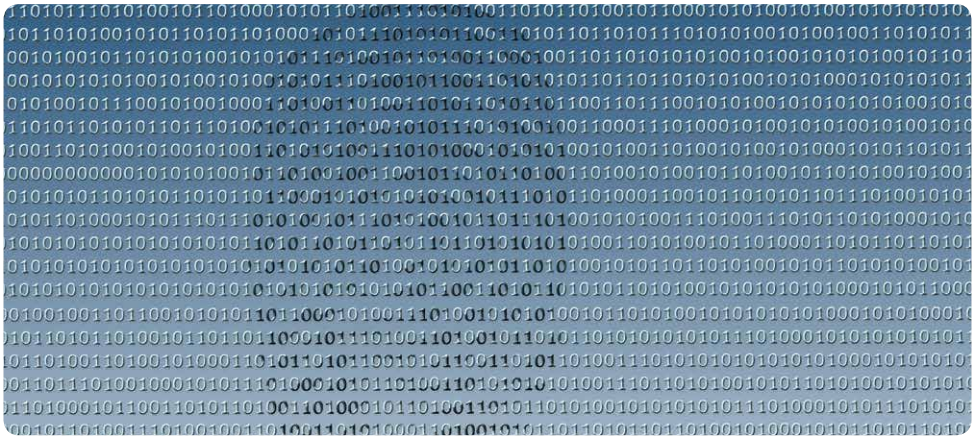
- Welche Erfolge können Sie verbuchen in Bezug auf Festnahmen, positive Prozessausgänge und Strafverfolgungen?
- Von welchen Branchenvorteilen/ Möglichkeiten haben Sie profitiert?

7. Untersuchung und daraus resultierende Änderungen

- Welche größeren Verluste und Serviceausfälle sind in den letzten Wochen aufgetreten?
- Was waren die Gründe dafür – inkl. durch Mitarbeiter verursachter Betrug / Fehler
- Welche Änderungen resultieren daraus – und wie ist der Status, zeitlicher Rahmen?

Ihre Managementinformationen sollten die meisten der oben genannten Kennzahlen berücksichtigen. Ob Sie sämtliche der genannten Punkte adressieren, liegt in Ihrem Ermessen – wenngleich wir der Meinung sind, dass es sinnvoll wäre. Doch Sie sollten zumindest alle messbaren Kennzahlen verfolgen. Darüber hinaus kann es weitere geben, die für Ihr Unternehmen relevant sind.

Systeme und Services – zur Verbesserung Ihres Betrugsprofils



Das Produkt Visa existiert bereits seit mehr als 50 Jahren. Und in all dieser Zeit war es von einem kontinuierlichen Wandel, Veränderungen und Verbesserungen gekennzeichnet.

Ursprünglich war Visa ein papiergebundenes Bezahlsystem, mit dem man schnell und bequem im stationären Handel zahlen konnte. Damals galt das Internet noch als eine Art Zukunftsvision – doch heute hat sich Visa im Online-Umfeld längst als feste Zahlungsgröße etabliert.

Im Laufe dieser Entwicklungsgeschichte wurden Produkte und Lösungen konzipiert, die dazu beitragen sollten, Risiken im Online-Handel besser und effizienter zu managen. Instrumente, die auch heute einer kontinuierlichen Weiterentwicklung unterliegen.

Wissenswertes für Fernabsatzhändler über aktuelle Visa Systeme und Services

1. Online-Autorisierung

Visa bietet Händlern ein Autorisierungssystem, das es ihnen ermöglicht, rund um die Uhr, 7 Tage in der Woche und 365 Tage im Jahr Geschäfte zu tätigen. Das System verarbeitet Transaktionen in sekundenschnelle und überprüft dabei, ob:

- die Karte als verloren oder gestohlen gemeldet ist oder diese bereits missbräuchlich eingesetzt wurde
- die Kartendetails – einschließlich der Sicherheitsmerkmale – korrekt sind
- die Adresse des Karteninhabers korrekt ist (in Ländern, in denen der Service zur Verifizierung von Adressdaten unterstützt wird)
- der Verfügungsrahmen der Karte ausreichend ist

Darüber hinaus wird im Rahmen des Autorisierungsprozesses auch bestätigt, ob die kartenausgebende Bank der weiteren Abwicklung der Transaktion zustimmt – basierend auf den Ergebnissen der bankeigenen Betrugserkennungssysteme.

Als Online-Händler müssen Sie – bevor Sie eine Visa Zahlung veranlassen – für sämtliche Transaktionen eine Autorisierung einholen. Sie sollten sich niemals dazu verleiten lassen, diesen Schritt auszulassen, da nicht-autorisierte Umsätze Ihrem Unternehmen in erheblichem Maße schaden können.

2. Verified by Visa (VbV)

Verified by Visa ist ein wichtiger Bestandteil der Visa Sicherheitsinfrastruktur. Der Verified by Visa-Service macht es möglich, die Identität eines Kunden während des Online-Einkaufs zu überprüfen.

Verified by Visa ist im eigentlichen Sinne kein Authentifizierungssystem, sondern vielmehr ein Mechanismus, der einen Dialog zwischen dem Karteninhaber und dessen kartenausgebender Bank ermöglicht. Im Rahmen dieses Dialogs kann die Bank die Checks durchführen, die sie für notwendig erachtet, um die Identität des Kunden zu prüfen. Je nach Präferenz der Bank kann es sich dabei um die Angabe eines Passwortes, eines Teil-Passwortes, eine ausgehende SMS oder sonstige verschlüsselte Mechanismen, sogenannte „Token", handeln.

Eine zunehmende Zahl von Kartenemittenten nutzt neben dem Verified by Visa-Service eigene Erkennungssysteme mit dem Ziel, auffällige und folglich risikoreichere Transaktionen zu erkennen und zu verifizieren. Dies bedeutet, dass Kunden, deren Transaktionen unauffällig sind, nicht zwangsläufig im Rahmen des Verified by Visa-Services aufgefordert werden, sich zu authentifizieren. Diese Vorgehensweise ermöglicht einen schnelleren und bequemeren Zahlungsprozess für Kunden mit unauffälligem Transaktionsverhalten, ohne dabei jedoch die Sicherheit zu verringern.

Die Betrugsquoten von Transaktionen, die durch den Verified by Visa-Service geschützt sind, betragen ein Viertel des Niveaus, das im traditionellen, unsicheren eCommerce-Handel auftritt. Aufgrund dieser deutlich vorteilhafteren Betrugs-Performance profitieren Händler, die den Verified by Visa-Service anbieten in der Regel im **Betrugsfall** von einer **Zahlungsgarantie**.

Somit sollte jeder Händler, der im Rahmen seines Online-Geschäfts Visa als Zahlungsmittel akzeptiert, den Verified by Visa-Service unterstützen. Und – falls nicht für den gesamten Zahlungsverkehr, dann doch zumindest für einen Teil davon.

Selbstverständlich entbindet die Nutzung des Verified by Visa-Dienstes den Händler nicht von seiner Verantwortung eines effizienten Managements von Betrugsrisiken sowie der Etablierung von Betrugserkennungssystemen (d.h., er ist dadurch auch nicht von Visa Compliance-Programmen ausgeschlossen). Es kann allerdings einen enormen Einfluss haben sowohl auf die Anzahl der Betrugsfälle als auch auf das dem Kunden gebotene Einkaufserlebnis (folglich ist es wichtig, nicht gegen Compliance-Programme zu verstoßen).

3. Kartenprüfnummer (CVV2)

Auf der Rückseite jeder Visa Karte befindet sich eine dreistellige Zahl – in der Regel im Unterschriftsfeld der Karte. Diese Nummer ist ein verschlüsselter Wert, der sich aus der Kartennummer auf der Kartenvorderseite sowie dem Ablaufdatum der Karte ergibt. Mit Hilfe der Kartenprüfnummer lässt sich auf einfache Art und Weise prüfen, ob die angegebenen Daten korrekt sind.

Die Kartenprüfnummer wird oftmals als Sicherheitsmerkmal nicht wirklich ernst genommen – da sie sich auf der Rückseite der Karte befindet und daher leicht ausgespäht bzw. abgegriffen werden kann. Sie spielt dennoch eine wichtige Rolle, wenn es darum geht, die Korrektheit der Kartendaten und des Ablaufdatums zu bestätigen.

Gemäß den Visa Richtlinien ist das Speichern der Kartenprüfnummer unzulässig – eine Bestimmung, die Bestandteil der PCI DSS-Anforderungen ist. Sollten Sie also Autorisierungen nicht sofort verarbeiten – wie dies bei einigen Hotels der Fall ist – können Sie die Kartenprüfnummer nicht nutzen. Wenn Sie jedoch Autorisierungen umgehend verarbeiten,

bietet Ihnen die Kartenprüfnummer ein nützliches Prüfinstrument und eine Maßnahme mit der die meisten Karteninhaber sehr gut vertraut sind.

Innerhalb Europas müssen Händler die Kartenprüfnummer (soweit dies mit den PCI DSS-Anforderungen vereinbar ist) verwenden. Für Kartenemittenten gilt die Verpflichtung, diese zu prüfen und Autorisierungsanfragen im Falle einer inkorrekten Kartenprüfnummer abzulehnen.

Visa Europe arbeitet daran, die Verwendung der Kartenprüfnummer im Rahmen anderer Vertriebskanäle zu minimieren. So wird sie beispielsweise im stationären Handel nicht erfasst. Sie ist auch nicht über kontaktlose Schnittstellen verfügbar – weder über die Karte noch über das Mobiltelefon.

Würde es bei dieser Art von Transaktionen zu einem Abgreifen der Kartendaten kommen, ist ein Fernabsatzhändler, der die Kartenprüfnummer verwendet, davon kaum betroffen.

Unser Rat lautet daher: Verwenden Sie die Kartenprüfnummer, wann immer es für Sie möglich ist. Die Richtlinien von Visa Europe sehen die Verwendung der Kartenprüfnummer im eCommerce-Handel vor, sofern die Nutzung nicht gegen geltende Datenschutzbestimmungen verstößt. Zudem ist es eine einfache Methode zu prüfen, ob alle anderen Kartendetails „unverfälscht" sind.

4. Service zur Verifizierung von Adressdaten

Der Service zur Überprüfung von Adressdaten steht nicht in allen Ländern zur Verfügung. Für den größten europäischen Markt im Fernabsatzgeschäft – Großbritannien – ist er jedoch verfügbar, ebenso wie in einigen Ländern außerhalb Europas, z. B. Kanada und USA.

Der Nutzen dieses Dienstes hängt von Ihrem Geschäftsmodell ab und davon, ob Sie Waren versenden müssen. Doch es kann auf jeden Fall ein hilfreicher, zusätzlicher Sicherheitsmechanismus sein, die vom

Karteninhaber angegebene Lieferadresse mit der Adresse abzugleichen, an die das kartenausgebende Institut dem Kunden die Kartenabrechnung zustellt.

Diese Überprüfung findet im Rahmen der Autorisierungsabwicklung statt.

Im Bereich der eCommerce-Zahlungen gibt es fortwährend Entwicklungen, die dazu beitragen sollen, Online-Bezahlverfahren noch sicherer und besser zu machen. Zu den bedeutendsten Initiativen zählt **V.me by Visa** – die neue digitale Geldbörse von Visa, die derzeit in Zusammenarbeit mit Banken schrittweise in den europäischen Ländern eingeführt wird.

Es gibt eine Reihe von Instrumenten, die eCommerce-Händlern helfen können, die Risiken im Fernabsatzgeschäft zu managen. Sie müssen nicht alle Instrumente nutzen, doch Sie sollten wissen, welche Werkzeuge zur Verfügung stehen. Und – für den Fall, dass Sie diese nicht in Anspruch nehmen, sollte dies eine bewusste Entscheidung sein und kein Versäumnis als Folge von Unkenntnis darüber, dass eine solche Option besteht.

Unterstützung durch Visa Europe

Sollte dieser Leitfaden Themen und Fragen aufwerfen, wenden Sie sich bitte diesbezüglich zunächst an Ihre Händlerbank, mit der Sie einen Vertrag zur Akzeptanz von Visa Karten geschlossen haben.

Es ist Aufgabe der Händlerbank, ihren Kunden die Akzeptanz und Abwicklung von Kartenzahlungen in einem sicheren Umfeld zu ermöglichen – und für Fragen rund um das Thema Betrug als Ansprechpartner zur Verfügung zu stehen.

Ihre Händlerbank kann Sie im Wesentlichen bei folgenden Punkten unterstützen:

- **Visa Betrugsmeldungen (TC40)**
  Ihre Händlerbank erhält täglich Berichte von Visa Europe über Betrugsfälle, die im Zusammenhang mit Ihrem Unternehmen aufgetreten sind (TC40-Dateien) und sollte in der Lage sein, Ihnen diese Informationen bereitzustellen.
- **Instrumente zum Managen von Betrugsrisiken**
  Viele Händlerbanken haben Instrumente und Lösungen etabliert, die Händler bei einem effizienten Management ihrer Betrugsrisiken helfen können. Fragen Sie Ihre Händlerbank, welche Produkte und Lösungen sie Ihnen anbieten kann und welche Kosten damit verbunden sind. Sie werden möglicherweise erstaunt sein, welche Optionen verfügbar sind.
- **Beratung und Unterstützung**
  Alle Händlerbanken verfügen über eigene Experten, die sich mit den Themen Risikomanagement und Rückbelastungen beschäftigen. Wenden Sie sich an diese Spezialisten, die Ihnen gerne helfen werden, die Betrugsrisiken, denen Sie ausgesetzt sind, zu minimieren. Für den Fall, dass Ihnen Ihre Händlerbank nicht weiterhelfen kann, können Sie sich auch direkt an Visa Europe wenden.

Visa Europe unterstützt Sie mit:

- **Berichten und Benchmarking-Daten**
  Unsere Informationen können Ihnen helfen, Ihre Performance effektiver nachzuverfolgen und Veränderungen bei der Entwicklung von Betrugsszenarien schneller zu erkennen. Diese Daten stehen sowohl als Rohdaten als auch in aufbereiteter Form zur Verfügung.
- **Risikomanagement-Lösungen**
  Visa Europe selbst bietet Händlern keine Produktlösungen zur Betrugserkennung an. Wir haben allerdings Vereinbarungen mit großen Anbietern – und können Händler, die besondere Anforderungen haben, gegebenenfalls unterstützen, eine kostengünstige Lösung zu finden.
- **Schulung und Beratung**
  Visa Europe arbeitet immer häufiger auch direkt mit dem Handel zusammen und bietet Händlern Schulungsmaßnahmen und Beratungsdienstleistungen an. Wir stützen uns dabei auf die umfassende Erfahrung, die wir mit vergleichbaren Dienstleistungen bei kartenausgebenden Instituten und Händlerbanken gewonnen haben.

Mit diesen Dienstleistungen sind jedoch Kosten verbunden – deren Höhe vom Umfang, der Häufigkeit der Inanspruchnahme und den Anforderungen abhängt.

Sollte Sie eine der Maßnahmen interessieren, senden Sie bitte eine E-Mail an: fraudproducts@visa.com.

Wir unterstützen Sie gerne.

Schlussbemerkung

Wir hoffen, dass wir Ihnen mit diesem Leitfaden interessante und aufschlussreiche Informationen bereitstellen konnten, die Ihnen helfen werden, Ihre Transaktionsrisiken im Fernabsatzgeschäft zu minimieren und effizienter zu managen.

Leider konnten wir im Rahmen dieser Publikation nicht alle Aspekte beleuchten. Wir hoffen jedoch, dass Sie durch die Lektüre interessante Erkenntnisse gewinnen konnten.

Sollten Sie Fragen haben oder wurden Sachverhalte, die Sie im Zusammenhang mit diesem Thema für wichtig erachten, nicht adressiert, senden Sie bitte eine E-Mail an: fraudproducts@visa.com.

Wir werden Ihre Anregungen gegebenenfalls bei künftigen Aktualisierungen berücksichtigen.

0514-BDG-DP-0135