Missbrauchsbekämpfungsmaßnahmen – Anlage zum Vertrag über die Kartenakzeptanz, Stand 01/2019

Allgemeine Informationen

Bargeldlose Zahlungen erfreuen sich einer immer größer werdenden Beliebtheit. Der Schutz von Karteninformationen und Transaktionsdaten ist jedoch Voraussetzung für das Vertrauen der Verbraucher in diese Zahlungsform. Diese Anlage beschreibt die wesentlichen obligatorischen Sicherheitsanforderungen für die Kartenakzeptanz und stellt eine wesentliche Vertragsanlage dar.

Die beschriebenen Missbrauchsbekämpfungsmaßnahmen umfassen aktuell die Themen:

1. Generelle Sicherheitsanforderungen Kartenakzeptanz Präsenz- und Fernabsatzgeschäft
   1.1 Verbindliche Maßnahmen durch die Akzeptanzstelle
   1.2 Der Weg zu Ihrer persönlichen PCI DSS-Konformität
2. Sicherheitsanforderungen Kartenakzeptanz im Präsenzgeschäft
3. Sicherheitsanforderungen Kartenakzeptanz im Fernabsatzgeschäft
   3.1 Verbot der Kartenakzeptanz
   3.2 Auffällige Bestellungen
   3.3 Einsatz von 3D Secure Verfahren von Mastercard, Visa, JCB und Diners
4. Verhalten bei Verdacht von Datenmissbrauch

1. Generelle Sicherheitsanforderungen Kartenakzeptanz Präsenz- und Fernabsatzgeschäft

Ein von führenden Kreditkartenorganisationen eingeführter Sicherheitsstandard ist der PCI DSS (Payment Card Industry Data Security Standard). Der PCI DSS stellt sicher, dass die im Bezahlvorgang verarbeiteten, sensiblen Kreditkartendaten nicht entwendet und zu kriminellen Zwecken missbraucht werden. Jede Akzeptanzstelle, die Kartenzahlungen akzeptiert oder Kreditkartendaten speichert, verarbeitet oder übermittelt, ist **verpflichtet**, die Sicherheitsvorgaben des PCI DSS einzuhalten. **Diese Verpflichtung besteht unabhängig von Unternehmensgröße und Anzahl der jährlich abgewickelten Kreditkartentransaktionen**. Die vollständige Einhaltung der Sicherheitsvorgaben wird auch als Konformität oder Compliance bezeichnet. Einmal jährlich muss die PCI DSS Compliance durch einen Nachweisprozess belegt werden.
Das gilt auch für Akzeptanzstellen, welche die Abwicklung von Kartenzahlungen an externe Unternehmen ausgelagert haben und deshalb erst gar nicht mit Kartendaten in Berührung kommen.

Nachfolgende Tabelle stellt die Anforderungen der Kartenorganisationen nach Anzahl und Art der Transaktionen (kurz: Trx) der angeschlossenen Akzeptanzstellen dar.

Level	Visa	Mastercard	JCB	American Express	Discover Financial Services	Prüfmethode	Security Scan
Level 1	> 6 Mio. Trx p. a.	> 6 Mio. Trx p. a.	> 1 Mio. Trx p. a.	> 2,5 Mio. Trx p. a.	> 6 Mio. Trx p. a.	**Onsite Audit** (jährlich)	**vierteljährlich**
Level 2	1 Mio. – 6 Mio. Trx p. a.	--------	--------	50.000 – 2,5 Mio. Trx p. a.	1 Mio – 6 Mio. Trx p. a.	**Selbstauskunft** (jährlich)	**vierteljährlich**
Level 2 Mastercard	--------	1 Mio. – 6 Mio. Trx p. a.	--------	--------	--------	**Onsite Audit oder Selbst-auskunft** (jährlich)	**vierteljährlich**
Level 3	20.000 – 1 Mio. E-Commerce Trx p. a.	20.000 – 1 Mio. E-Commerce Trx p. a.	--------	< 50.000 Trx p. a.	20.000 – 1 Mio. E-Commerce Trx p. a.	**Selbstauskunft** (jährlich)	**vierteljährlich***
Level 4	< 20.000 E-Commerce bzw. < 1 Mio. nicht E-Commerce Trx p. a.	Alle anderen Händler	< 1 Mio. Trx p. a.	--------	Alle anderen Händler	**Selbstauskunft** (jährlich)	**vierteljährlich***

* Für Händler der Level 3 und 4 sind keine PCI Schwachstellen Scans erforderlich, sofern sie keine Kreditkatendaten speichern, verarbeiten oder übertragen und zusätzlich mit einem PCI DSS zertifizierten Payment Service Provider arbeiten..

1.1 Verbindliche Maßnahmen durch die Akzeptanzstelle

a) Alle Akzeptanzstellen, die keine sensiblen Kartendaten in ihren Systemen speichern, aber über eine Million Transaktionen jährlich verarbeiten, müssen einmal jährlich zur PCI DSS-Zertifizierung ein Onsite Audit (Vor-Ort-Prüfung) durchführen lassen.

b) Speichert die Akzeptanzstelle Kreditkartendaten in eigenen Systemen, muss sie zusätzlich viermal im Jahr einen sogenannten Security Scan durchführen lassen.
Das nachfolgende von den Kartenorganisationen akkreditierte deutschsprachige Prüfungsunternehmen kann für ein qualifiziertes Assessment (Audit, Security Scan) herangezogen werden:
usd AG
Frankfurter Straße 233, Haus C1
63263 Neu-Isenburg
Internet: www.usd.de

c) Alle weiteren zertifizierungspflichtigen Akzeptanzstellen, die Kreditkarten als Zahlungsmittel akzeptieren, müssen den PCI DSS-Sicherheitsstandard erfüllen und durch eine jährlich neu durchzuführende Zertifizierung nachweisen. Aufschluss darüber, ob der PCI DSS-Sicherheitsstandard erfüllt ist und die Kartendaten der Kunden gesichert sind, erhalten Akzeptanzstellen grundsätzlich nach dem Ausfüllen einer Selbstauskunft (SAQ). Die zu beantwortenden Fragen sind hierbei durch das von den Kartenorganisationen gegründete PCI Security Standards Council vorgegeben und beziehen sich überwiegend auf technische und organisatorische Gegebenheiten der Systeme.
Um den geforderten Nachweis möglichst einfach und komfortabel erbringen zu können, hat die VR Payment zusammen mit ihrem Zertifizierungspartner, der usd AG, eine PCI DSS Sicherheitsplattform entwickelt, welche die PCI DSS Zertifizierung Akzeptanzstellen deutlich erleichtert. Diese steht unter folgendem Link zur Verfügung:
https://kartensicherheit.vr-payment.de
Transaktionseinreichungen sind erst nach einer PCI DSS-Zertifizierung zulässig! Die Akzeptanzstelle wird der VR Payment auf Nachfrage eine Kopie des Zertifikats zukommen lassen.

1.2 Der Weg zu Ihrer persönlichen PCI DSS-Konformität

I. Anmeldung auf https://kartensicherheit.vr-payment.de mit Ihren persönlichen Zugangsdaten, die Sie vorab per E-Mail erhalten haben
II. Bestätigen Sie Ihre Unternehmens- und Kontaktdaten
III. Per Kurzfragebogen erfolgt die Einstufung in den passenden Selbstauskunftsfragebogen
IV. Beantworten Sie die Fragen und erbringen so den geforderten Nachweis über Ihre PCI DSS-Konformität
V. Im Falle einer Nichtübereinstimmung mit dem Sicherheitsstandard unternehmen Sie bitte die auf der Plattform angegebenen Schritte

2. Sicherheitsanforderungen Kartenakzeptanz im Präsenzgeschäft

Bei Akzeptanz einer Karte im Präsenzgeschäft sind mindestens folgende Sicherheitsanforderungen durch die Akzeptanzstelle einzuhalten:

a) Die Akzeptanzstelle verfügt über ein EMV-fähiges Terminal gemäß den Anforderungen des Vertrages über die Kartenakzeptanz und wird dieses entsprechend den dort beschriebenen Angaben bedienen.

b) Soweit die Akzeptanzstelle über das POS-Terminal aufgefordert wird, die Karte einzubehalten („pick-up"), hat sie die Karte einzuziehen, sofern dies für das Kassenpersonal ohne Gefährdung möglich ist.

c) Entsteht bei der Akzeptanzstelle der Verdacht, dass eine vorgelegte Karte gefälscht oder verfälscht ist (siehe Aufzählung unten), hat sie die Vorlage eines gültigen Lichtbildausweises zu verlangen und bei Übereinstimmung des Namens auf der Karte die Nummer des Lichtbildausweises auf dem Leistungsbeleg zu notieren. Bei Nichtübereinstimmung des Namens oder bei Zutreffen einer der u.a. Aufzählungspunkte, hat die Akzeptanzstelle die VR Payment in diesem Fall unverzüglich und möglichst noch vor Rückgabe der Karte telefonisch zu informieren und auf Verlangen der VR Payment die Karte einzuziehen sowie auf Aufforderung der VR Payment durch einmaliges Zerschneiden zu entwerten und an die VR Payment zu senden.
In folgenden Fällen hat die Akzeptanzstelle unwiderleglich von einer Fälschung oder Verfälschung der Karte auszugehen:
- wenn bei der Autorisierungsanfrage auf dem Display des POS-Terminals der Akzeptanzstelle „Karte einziehen" („pick-up") oder ein sinngleicher Vermerk erscheint;
- wenn die Kartennummer oder das Ablaufdatum der Karte in dem elektronisch erstellten Leistungsbeleg mit den Kartendaten (Kartennummer und Ablaufdatum) auf der Vorderseite der Karte nicht übereinstimmt;
- wenn der Karteninhaber nicht mit einem eventuellen Foto auf der Karte übereinstimmt.

d) Im Fall mehrfacher Vorlage gefälschter oder gestohlener Karten ist die Akzeptanzstelle nach schriftlicher Aufforderung der VR Payment dazu verpflichtet, durch Verwendung einer UV-Lampe zu prüfen, ob auf der Vorderseite der Karte unter Schwarzlicht (UV-Licht) folgende Dinge sichtbar sind: bei
   - Visa-Karten das Hologramm einer „Taube"
   - Mastercard-Karten die Buchstaben „M" und „C"
   - JCB-Karten der Schriftzug „JCB",
   - Karten von Union Pay International der aus zwei chinesischen Schriftzeichen bestehende Union-Pay-Schriftzug (analog dem im Logo abgebildeten)
   - Diners Discover auf der Rückseite ein holografischer Magnetstreifen, der ein sich wiederholendes Logo und Name von Diners Club International sowie die Weltkarte aufzeigt.

3. Sicherheitsanforderungen Kartenakzeptanz im Fernabsatzgeschäft

3.1 Verbot der Kartenakzeptanz

Abgesehen von den in den Vertragsbedingungen für die Kartenakzeptanz in Ziffer 3.1 aufgeführten Fällen ist die Akzeptanzstelle im Fernabsatzgeschäft nicht berechtigt, Kreditkarten zu akzeptieren und Kartenumsätze bei der VR Payment zur Abrechnung einzureichen, insbesondere wenn

a) sie nicht auf eigene Rechnung oder im Auftrag Dritter erbracht werden;
b) sie Folgendes zum Gegenstand haben (oder verbunden sind mit nach deutschem Recht dem Jugendschutz unterliegenden Inhalten): Obszönität, Pornographie, Gewaltdarstellung, Rassismus, Anleitungen zur Herstellung von Waffen oder Explosivkörpern sowie Tabakwaren, illegales Glücksspiel und Sportwetten. Ausnahmen hiervon bedürfen der vorherigen schriftlichen Zustimmung der VR Payment. Ein Anspruch auf rechtliche Prüfung durch die VR Payment oder darauf, das Ergebnis der Prüfung zu erfahren, besteht nicht.
   Ferner ist die Einreichung von Kartenumsätzen im Rahmen des Vertrages über die Kartenakzeptanz (im Präsenz- und Fernabsatzgeschäft) untersagt, wenn sie im Zusammenhang steht mit:
   - Adoptionsvermittlung
   - Cash-Back-Transaktionen
   - Call-by-Call/Mehrwertdienstnummern, z. B. (0900)-Provider
   - Direktverkauf von Waren und Dienstleistungen
   - Elektronische Geldbörsen (Wallets)
   - Free-Trial-Geschäfte mit anschließendem Abonnement
   - Haustürgeschäfte (außer Strukturvertrieb)
   - Inkassounternehmen/Schuldnerberatung/Factoring
   - Internet-Auktionen (vorwärts & rückwärts)
   - One-Click-Hoster (Internetplattformen mit Möglichkeiten für illegale Downloads)*
   - Radikale Organisationen
   - Schneeballsysteme/Kettensysteme
   - Sekten
   - Sub-Acquiring
   - Time-Sharing
   - Usenet-Provider**
   - Verkauf von Repliken oder Plagiaten
   - Verlosungen oder Glücksspiele mit Verkaufs-Charakter
   - Währungsgeschäfte, Handel mit Aktien

* Internetdienstanbieter für unmittelbaren Download von Dateien mit oder ohne vorherige Anmeldeprozedur
** Internetdienstanbieter, die den Zugang zu Binary Newsgroups, in denen Dateien zum Download öffentlich in Diskussionsgruppen gepostet werden, bereitstellen

3.2 Auffällige Bestellungen

Die Akzeptanzstelle wird darüber hinaus die Zahlung durch Kreditkarte nicht akzeptieren, wenn nach den von ihr zu beurteilenden konkreten Umständen der Transaktion Anlass zu der Vermutung besteht, dass ein Missbrauchsfall vorliegen könnte („auffällige Bestellungen"):

a) Der Kunde möchte mit mehreren Namen und/oder mehreren Adressen Kartenumsätze tätigen (z. B. Kundenname weicht von Karteninhabername oder Lieferadressat ab).
b) Der Kunde möchte den Gesamtbetrag vorab auf mehrere Karten aufteilen bzw. in der Bestellung wurden mehrere Kartennummern zum Zahlungsausgleich angegeben.
c) Der Kunde kündigt bereits bei der Übermittlung der Kartendaten mögliche Akzeptanzprobleme der Karte an;
d) Derselbe Kunde hat während zwei aufeinander folgenden Kalendertagen einzeln oder in mehreren Bestellungen zusammen mit der betreffenden Bestellung

- identische Artikel oder Dienstleistungen in untypischen Mengen bestellt oder
- zur Lieferung an Adressen außerhalb der Europäischen Union Bestellungen über mehr als € 1.500,– getätigt oder
- Bestellungen über mehr als € 3.500,– getätigt oder
- mehr als eine Kreditkartennummer verwendet oder
- einen Gesamtbetrag angegeben, der auf mehrere Kreditkartennummern aufgeteilt werden soll.

e) Während zwei Kalendertagen sind unter Angabe derselben E-Mail-Adresse Bestellungen unterschiedlicher Kunden vorgenommen worden.

f) Bei Angabe einer E-Mail-Adresse eines Kunden mit einer nationalen Domain (.de, .at, .ch usw.) weicht das Land der Lieferadresse von dem Land der betreffenden Domain ab.

g) Nach einer Autorisierungsablehnung wird ein anderes Verfalldatum oder eine andere Kartennummer von dem Kunden zur Bezahlung angegeben.

h) Der Kunde bittet vorab um den Tracking Code bzw. die Liefernummer des Lieferunternehmens.

i) Die Wohn-, Versand- oder Rechnungsanschrift des Kunden liegt in einer der unten aufgeführten oder in einem/einer in Bezug auf die Bestellung ungewöhnlichen Land/Region und/oder die Bestellung ist für den Kundenkreis der Akzeptanzstelle unüblich.
Ferner ist eine Bestellung insbesondere dann auffällig, wenn sich Wohn-, Versand- oder Rechnungsanschrift des Kunden in einem der folgenden Länder befindet:
Afrika: Elfenbeinküste, Nigeria, Ghana, Ägypten
Asien: Indonesien, Indien, Philippinen, Malaysia, Singapur
Osteuropa: Bulgarien, Kasachstan, Ukraine, Balkanstaaten
Mitteleuropa: Rumänien, Ungarn, Litauen
Westeuropa: Großbritannien (hier speziell Großraum London), Niederlande (hier speziell Rotterdam, Amsterdam, Hakfort)
Nordamerika: USA

j) Die Gesamtumstände der Bestellung sind ungewöhnlich.

Die VR Payment gibt im Zusammenhang mit den oben aufgeführten Geschäften kein abstraktes Schuldversprechen nach Ziffer 3.1 des Vertrags über die Kartenakzeptanz ab.

3.3 Einsatz von 3D Secure Verfahren von Mastercard, Visa, JCB und Diners

3D Secure ist ein von den Kartenorganisationen entwickeltes Authentifizierungsverfahren, das unter jeweils eigenen Namen vermarktet wird (u. a. Mastercard Identity Check, Verified by Visa, J/Secure und Protect Buy), das den Karteninhaber durch die Abfrage eines persönlichen Codes während des Kaufvorgangs eindeutig identifizieren kann. So können Akzeptanzstellen sicher sein, dass es sich bei der Bezahlung um den rechtmäßigen Karteninhaber handelt. Mit dem Einsatz von 3D Secure verringern Akzeptanzstellen ihr Rückbelastungsrisiko für alle Zahlungen, bei denen der Karteninhaber die Zahlung bestreitet. Die VR Payment schreibt den Einsatz von 3D Secure für jede eCommerce-Akzeptanzstelle verbindlich vor.
Die Akzeptanzstelle gestattet der VR Payment und ihren Dienstleistern zum Zwecke der Anbindung bzw. Anerkennung eines Payment Service Providers ausdrücklich die Kontaktaufnahme mit diesem sowie die Weitergabe der hierfür nötigen Daten der Akzeptanzstelle. Für den erfolgreichen Einsatz des 3D Secure Verfahrens bestehen Beistellungspflichten des Payment Service Providers, deren Sicherstellung der Akzeptanzstelle obliegen. (Sofern der Payment Service Provider unterschiedliche Produkte oder technische Anbindungsvarianten anbietet, liegt es in der Verantwortung der Akzeptanzstelle, diejenige Variante zu nutzen, die die Nutzung von 3D Secure ermöglicht).

4. Datenschutz

Die Parteien beachten bei ihrer Zusammenarbeit die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) sowie der EU-DSGVO und sonstiger einschlägiger datenschutzrechtlicher Bestimmungen und verpflichten sich darauf, die erhobenen Daten ausschließlich zur Vertragserfüllung zu verwenden.

Die Parteien informieren sich gegenseitig unverzüglich bei Verdacht auf Verletzung von Datenschutzbestimmungen.

Die detaillierten Datenschutzinformationen der VR Payment GmbH
können unter www.vr-payment.de/datenschutz-haftung/ abgerufen werden, und werden, soweit einschlägig zum Bestandteil der vorliegenden Geschäftsbedingungen.

5. Verhalten bei Verdacht von Datenmissbrauch

Sobald von Seiten der Akzeptanzstelle der Verdacht besteht, dass eine missbräuchliche Benutzung eines kartenrelevanten EDV-Systems oder ein möglicher Abgriff von Kartendaten stattgefunden hat, wird die Akzeptanzstelle die VR Payment unverzüglich hierüber unterrichten. Im Fall der Anzeige des Verdachts eines Datenabgriffs ist die Akzeptanzstelle verpflichtet, die VR Payment unverzüglich hierüber zu benachrichtigen und ein von den Kartenorganisationen zugelassenes Prüfunternehmen auf eigene Kosten mit der Erstellung eines PCI Prüfberichts zu beauftragen. Bei dieser Prüfung wird festgestellt, ob der PCI DSS Standard durch die Akzeptanzstelle eingehalten und die Kartendaten in den Systemen der Akzeptanzstelle oder eines von ihm beauftragten Unternehmens von Dritten ausgespäht wurden. Nach finaler Erstellung und Vorlage des Prüfberichts bei der VR Payment hat die Akzeptanzstelle alle festgestellten Mängel innerhalb einer von der VR Payment festzusetzenden angemessenen Frist zu beheben.