Christian Prantner, Michaela Kollmann, Martin Korntheuer,
Benedikta Rupprecht und Jakob Kalina

SICHER BEZAHLEN

Antworten auf häufig gestellte Fragen (FAQ) zu Zahlungsmitteln aus Konsumentensicht

November 2020

AK 100 JAHRE GERECHTIGKEIT

Inhalt

In dieser Publikation sind die **Antworten auf wichtige Fragen** (FAQ) zu finden, die ein sicheres Bezahlen ermöglichen – sei es bei Online-Käufen, in Geschäften an POS-Kassen oder im Zuge von Internet Banking. Sie finden in diesen FAQ eine **Beschreibung der wichtigsten Bezahlformen**, deren Vor- und Nachteile sowie die **Spesen**, die dafür anfallen. Wie ist die Haftung der Zahlerin bzw. des Zahlers ausgestaltet, wenn bei einer Überweisung etwas schiefgeht oder ein Missbrauch der Bankomat- oder Kreditkarte passiert? Sie finden im Rahmen dieser Abhandlung auch die wichtigsten Bestimmungen zu Fragen der **Haftung** im Missbrauchsfall oder bei fehl geschlagenen Überweisungen.

1. WELCHE BEZAHLFORMEN GIBT ES?

Es gibt ein paar wichtige Gruppen rund um Bezahlen:

- Bezahlung mit Bargeld (Barzahlung)
- Bezahlen mit Zahlungsanweisung in der Bankfiliale (am Schalter, am Foyer-Automat)
- Bezahlung mit Bankomat- oder Kreditkarte (unbar im Geschäft oder via Internet Banking)
- Zahlformen im Online-Shopping (Bankomat-, Kreditkarte, Überweisung, Lastschrift vom Konto mit oder ohne Unterstützung eines Zahlungsdienstleisters, der zwischen Bank und Händler geschaltet ist).

1.1. Wie ist die Haftung des Konsumenten bei Missbrauch eines Zahlungsinstrumentes ausgestaltet?

Das Zahlungsdienstegesetz sieht bei der **missbräuchlichen Verwendung** eines Zahlungsinstruments **eine Haftung des Zahlungsdienstleisters** vor, sodass der die Bank, die Kreditkartenfirma etc. das Risiko eines nicht ordnungsgemäß autorisierten Zahlungsvorgangs zu tragen hat. Das bedeutet, dass der Schaden aus einer missbräuchlichen Verwendung (zB nach einem Diebstahl) einer Bankomat- oder Kreditkarte oder eines sonstigen Zahlungsinstruments von dem Zahlungsdienstleister zu tragen ist.

Achtung, es wird für Sie als Zahlender heikel, wenn Sie ein (Mit-)Verschulden am Missbrauch trifft – wenn **Sie vor allem Sorgfaltspflichten bei der Benutzung des Zahlungsinstrumentes verletzt** haben. Banken wenden nämlich häufig ein, dass Kunden, die einen Schaden aus einem Missbrauch erlitten haben, mit personalisierten Sicherheitsmerkmalen (zB Transaktionsnummer – TAN) bei einem Zahlungsinstrument (zB Online-Überweisung) sorglos umgegangen (also fahrlässig oder grob fahrlässig) wären – wie zum Beispiel die aktive Bekanntgabe an einen Dritten (in dem Fall: an die Betrüger, die zum Beispiel vorgeben, im Auftrag der Bank neue Sicherheitsstandards zu etablieren). Das gipfelt häufig darin, dass eine Bank den entstandenen Schaden gar nicht oder nur teilweise übernehmen will.

Das Zahlungsdienstegesetz 2018 hat in diesem Zusammenhang eine Neuerung eingeführt, die im Sinne der betrogenen Konsumenten wirken soll. Wenn Sie ein Verschulden an dem Missbrauch trifft (zum Beispiel wegen grober Sorgfaltspflichtverletzung bei Nutzung eines Zahlungsinstrumentes), dann haften Sie nur dann, wenn Sie bei missbräuchlicher Verwendung eines Zahlungsinstruments vor der Zahlung in der Lage waren, den Verlust, den Diebstahl oder die sonstige missbräuchliche Verwendung des Zahlungsinstruments zu bemerken. Neu ist auch, dass die **Haftung des Zahlers auf höchstens 50 Euro beschränkt** ist – diese Haftungsgrenze gilt nur dann nicht, wenn Sie Ihre Sorgfaltspflichten grob fahrlässig verletzt haben.

Die Beweispflicht für Betrug, Vorsatz oder grobe Fahrlässigkeit trägt nach dem Gesetz der Zahlungsdienstleister. KonsumentInnen haben in der Praxis und bei einem allfälligen Gerichtsverfahren aber erst recht wieder Beweisprobleme, weil durch den so genannten Anscheinsbeweis, also wenn die richtigen PIN-Codes oder TANs etc. für eine missbräuchliche Zahlung verwendet wurden, die Beweislast wiederum oft beim Zahler liegt. Der Zahler muss dann beweisen oder glaubhaft darlegen, dass ihn kein grobes Verschulden trifft. Das ist schwierig, vor allem, weil es noch wenig Rechtsprechung gibt und immer gefinkeltere Betrugsmaschen auftauchen. In vielen aktuellen Betrugsfällen in Zusammenhang mit dem Onlinebanking zeigt sich, dass der **Betrug so professionell und geschickt** abläuft, dass KonsumentInnen gar nicht bemerken, dass sie selbst mitwirken, indem etwa TANs bekannt gegeben oder auf einer gut gemachten Fake-Seite eingegeben werden. Banken argumentieren im Regelfall, dass der Kunde grob fahrlässig gehandelt hat.

1.2. Wie wichtig ist Barzahlung?

Die Barzahlung ist und bleibt die dominante Zahlform. Studien der Österreichischen Nationalbank zeigen in regelmäßigen Abständen, dass Bargeld in Österreich für die meisten Rechtsgeschäfte verwendet wird. Bargeld ist – aus der Sicht der KonsumentInnen – also sehr wichtig.

Die AK tritt für die Beibehaltung des Bargeldes ein und beobachtet laufend alle Entwicklungen kritisch, die eine Forcierung des bargeldlosen Verkehrs durch die Kreditwirtschaft zum Ziel haben (wie zB automatisierte Bankdienstleistungen über Selbstbedienung, Internet Banking oder Zahlungen mit Kredit- oder Bankomatkarte mittels NFC – Near Field Communication). Es sollte – im Sinne einer echten Wahlfreiheit – zwischen der Möglichkeit der Barzahlung und elektronischer Zahlung gewählt werden können.

Darf ein Unternehmen eine Barzahlung verweigern?

Es gibt **eine in Österreich gesetzlich festgelegte Annahmeverpflichtung von Euromünzen und Banknoten**, die in Österreich die Funktion eines gesetzlichen Zahlungsmittels erfüllen. Bestimmungen dazu finden sich im Scheidemünzengesetz sowie im Nationalbankgesetz.

Unternehmen können allerdings den Abschluss eines Geschäftes von bestimmten Bedingungen abhängig machen. Dazu zählt auch, dass die Bezahlung nur mit Scheinen bis zu bestimmten Wertgrenzen erfolgen kann. Eine einschränkende Annahmebestimmung ist jedoch rechtzeitig mitzuteilen, damit sich ein Kunde/eine Kundin gegebenenfalls dazu entscheiden kann, die Leistung (zum Beispiel an einer Tankstelle oder beim Bäcker) anderswo zu beziehen. Wann dürfen Unternehmen die Annahme von Münzen beschränken? Das Scheidemünzengesetz sieht eine Annahmepflicht von Euro- und Cent-Münzen im Ausmaß von bis zu fünfzig Stück vor. Eine generelle „Nichtannahme-Bereitschaft“ eines Unternehmens ist zwar rechtswidrig. Allerdings ist diese gesetzliche Bestimmung nicht mit Sanktionen unterlegt und kann daher auch nicht erzwungen werden.

Können Sie zur Verwendung einer bestimmten Zahlungsart gezwungen werden?

Nein. Es gibt ein oberstgerichtliches Urteil, das besagt, dass der Zwang zu einer einzigen Zahlungsart wie die Lastschrift rechtswidrig ist – es gilt als gröbliche Benachteiligung, wenn die Wahlmöglichkeit zwischen Zahlungsmitteln beschnitten wird. Ebenso sind Extrakosten

für die Verwendung eines bestimmten Zahlungsinstruments nicht erlaubt - zB Kreditkarte oder Überweisung statt der bei Firmen beliebten Lastschrift. Unternehmen können aber vertraglich vorsehen, dass es bei der Verwendung einer bestimmten Zahlungsart eine Preisermäßigung gibt.

1.3. Was ist eine SEPA-Banküberweisung?

Bei einer Überweisung beauftragen Sie die Bank, einen bestimmten Geldbetrag (entweder in Euro oder Fremdwährung, wie US Dollar etc.) an einen Zahlungsempfänger (Privatperson, Unternehmen oder Organisation) zu übermitteln. Es gibt seit einigen Jahren einen einheitlichen Zahlungsverkehrsraum in Europa, die sogenannte Single European Payment Area, kurz: SEPA. Dieses Zahlungsverkehrsformat hat für Konsumenten Vorteile gebracht, vor allem eine **verkürzte, gesetzliche Überweisungsdauer innerhalb des Euro-Raumes**. Vor SEPA konnte es passieren, dass eine Überweisung etliche Tage „unterwegs" war – durch SEPA landet das Geld schneller auf einem Empfängerkonto. Achtung, eine von Ihnen freigegebene und von der Bank durchgeführte Überweisung **kann nicht rückgängig** gemacht werden – was liegt, das pickt.

Welche Formen der Überweisung gibt es?

Es gibt in der Zwischenzeit etliche Formen einer Überweisung. In der einfachsten Form kann eine elektronische Überweisung – durchgeführt mittels Online-Banking – von einer papiergebundenen Überweisung am Bankschalter unterschieden werden. In der Praxis gibt es jedoch etliche Zwischenformen, die in einem Bankfoyer an Selbstbedienungsautomaten (kurz: SB-Automaten) durchgeführt werden. Eine Auflistung:

- Überweisung mit Zahlschein am Bankschalter (Ausnahme: Direktbanken)
- Überweisungen im Internet (über das Onlinebanking)
- Überweisungen am Überweisungsautomaten: Einlesen von Belegen oder Eingabe über die Tastatur
- Überweisungen über telefonischen oder schriftlichen Auftrag per Post (die Überweisungsboxen gibt es nicht mehr)
- Instant Payments – Sofort-Überweisungen in Sekundenschnelle, ebenfalls nur im Onlinebanking möglich

Wie teuer sind Überweisungen?

Es gibt **unterschiedliche Spesensätze je Überweisungsart**. Es gilt: die beleghaften, manuellen Überweisungen kosten deutlich mehr als die elektronischen Überweisungen. Ein Beispiel aus dem Gebührenblatt einer Bank zeigt, dass eine elektronische Überweisung und vom Kunden am Selbstbedienungsautomat durchgeführte Überweisungen kostenfrei erfolgen; hingegen können die am Schalter beauftragte Überweisungen richtig ins Geld gehen. Die Überweisung mit einer **Bareinzahlung mittels Zahlschein** („Zahlungsanweisung") **am Bankschalter** ist – vor allem die Bareinzahlung zugunsten eines institutsfremden Kontos - sehr spesenintensiv. Die Bareinzahlung am Schalter auf ein bankeigenes oder bankfremdes Konto kann bis zu 10 Euro ausmachen. Auf manchen Zahlscheinen ist ein QR-Code angebracht, der über das Smartphone eingescannt und dadurch die Zahlungsdaten direkt in die jeweilige Banking App übernommen werden können. Fragen Sie daher nach, wieviel die Überweisung mittels QR-Code kostet.

Generell gilt, dass die **Entgelte für Zahlungstransaktionen** nicht nur unterschiedlich hoch sind, sondern auch **vom gewählten Kontomodell** abhängen. Es kann also sein, dass bestimmte – zumeist elektronische – Überweisungen in der laufend zu zahlenden Kontoführungsgebühr inkludiert oder überhaupt spesenfrei sind. Faustformel: Je teurer das gewählte Kontopaket, desto mehr Transaktionen sind im Kontopreis inkludiert. Leider gibt es davon etliche Ausnahmen – als preisbewusste Bankkundin sind Sie also angehalten, die Preisblätter der Banken zu studieren. Achten Sie auf Spesen, die insbesondere dann anfallen können, wenn Sie Transaktionen mittels Beleg oder direkt am Bankschalter durchführen. Einen Überblick über einzeln verrechnete Spesen ist im Konditionenvergleich des **AK-Bankenrechners** (www.bankenrechner.at/girokonto) zu finden.

Die Banken sind nach dem Verbraucherzahlungskontogesetz dazu verpflichtet, die wichtigsten Kontopreise in der sogenannten **Entgeltinformation** zu veröffentlichen, die Sie auch auf den Webseiten der Banken finden können (zumeist im Anhang zu den Produktbeschreibungen eines Kontos).

Was sollten Sie über Zahlungsanweisungen am Selbstbedienungsautomaten (SB-Automat) wissen?

Die klassische Überweisung am Schalter verliert immer mehr an Bedeutung, denn fast alle Banken mit Schalterbetrieb bieten ihren Kunden **S**elbst**b**edienungsautomaten (kurz: SB-Automaten) im Foyer an. Es gibt Überweisungsautomaten, die die Zahlungsanweisungen einlesen bzw. scannen und die Überweisung somit „halbelektronisch“ durchführen. Die sogenannten **SB-Überweisungen** sind jedenfalls kostengünstiger als die Überweisungen, die am Schalter durchgeführt werden. Achtung, diese Buchungen gelten auch als beleghafte Überweisungen – weil auf der Basis des Zahlungsanweisungsbeleges durchgeführt – und können daher trotzdem empfindlich teuer werden. Wie bei allen anderen Buchungen fällt dafür entweder eine Zeilen- bzw. Postengebühr an oder sie sind in der Kontopauschale inkludiert. Zusammenfassend lässt sich sagen, dass diese Spesen nicht so hoch wie Bartransaktionen am Schalter sind, aber auch beleghafte Buchungen sind teuer – bis zu 3 Euro.

Wie geht die Bank vor, wenn es fehlerhafte (unvollständig, nicht leserliche) Überweisungsbelege gibt?

Im Idealfall werden Sie direkt beim **Einscannen** am **Überweisungsautomaten** durch einen **Fehlerhinweis** darauf aufmerksam gemacht, dass die von Ihnen befüllten Belegdaten nicht lesbar oder unvollständig sind. Eine Korrektur bzw. Nacherfassung von fehlerhaften Daten am Bildschirm des Automaten ist bei den meisten Banken vor Bestätigung des Auftrags noch möglich. Jedoch kam es in der Vergangenheit auch zu Fällen, bei denen der Automat die Daten falsch interpretiert, und der Kunde in weiterer Folge keinen unmittelbaren Hinweis am Gerät erhalten hat. Erst später wurde durch die Bank über die Nichtdurchführbarkeit des Auftrags zB postalisch informiert, und es wurden für diese Mitteilung noch saftige Spesen verrechnet.

Wie sich aufgrund von AK-Interventionen bei der betroffenen Bank herausstellte, handelte sich um Gerätefehler, die für die fehlerhafte Verarbeitung verantwortlich waren – trotz gut leserlich ausgefüllter Belege. Dennoch wurden betroffenen Kunden für eine **„manuelle Nachbearbeitung“** zusätzliche Spesen um drei Euro in Rechnung gestellt. Ein durch die Arbeiterkammer angestrengter **Gerichtsprozess** stellte schlussendlich klar, dass für jene Fälle, in denen der Fehler nicht in die Sphäre des Kunden fällt, eine **Spesenverrechnung unzulässig** ist.

1.3.1. Sind elektronische Überweisungen (Online Banking) wirklich spesengünstig?

Ja, die elektronischen Überweisungen, die Sie mittels Online Banking durchführen, sind am spesengünstigsten. Die Online-Banking-Zugänge (also der Login auf der Webseite) der Banken sind **im Regelfall kostenlos** bzw. im Angebot eines Girokontos inkludiert. Online-Überweisungen sind aber auch nicht kostenlos – es sei denn, dass im gewählten Kontopaket die elektronischen Buchungen inkludiert bzw. durch die Kontoführung abgedeckt sind. Wenn diese Buchungen separat verrechnet werden, dann fallen Spesen bis zu 30 Cent an.

Wie können Sie Zahlscheinspesen verhindern?

Sie könnten diese Gebühren insbesondere mit einer Überweisung von Ihrem Girokonto vermeiden. Voraussetzung ist, dass der **Eigenerlag** auf das Konto kostenlos bzw. spesengünstig ist. Eventuell verfügt Ihre Bank über einen spesengünstigen Einzahlungsautomaten im Foyer – statt der spesenintensiven Bareinzahlung am Bankschalter. Wenn Sie den gesamten Betrag über das Konto laufen lassen, dann erfolgt eine **unbare Überweisung**, die – je nach Kontomodell – eine Buchungszeile am Konto kostet. Je mehr Zahlscheine (Zahlungsanweisungen) vorhanden sind, desto höher ist das Einsparungspotenzial im Vergleich zur Bareinzahlung der Zahlscheine am Schalter.

Kann eine beauftragte Überweisung rückgängig gemacht oder gestoppt werden?

Achtung, eine einmal von Ihnen beauftragte und freigegebene Überweisung kann im Regelfall nicht rückgängig gemacht werden. In wenigen Ausnahmefällen kann eine Bank eine Überweisung stoppen. Erfolgen irrtümliche Überweisungen, dann müssen Sie sich mit dem Inhaber des Empfängerkontos über eine Rückbuchung einigen.

Wie komme ich zu meinem Geld, wenn die Überweisung irrtümlich auf einem falschen Empfängerkonto gelangt ist?

Grundsätzlich hängt es davon ab, ob Sie die Daten falsch erfasst haben oder die Bank den Auftrag fehlerhaft weitergeleitet hat. Liegt der **Fehler bei Ihrer Bank**, ist diese gesetzlich verpflichtet, den Betrag unverzüglich Ihrem Girokonto **gutzuschreiben**. Haben Sie einen **falschen IBAN** verwendet, so trifft Ihre **Bank** allerdings **keine Haftung**. In der Praxis müssen Sie Ihre Bank mit einer **Nachforschung** beauftragen. Ihre (Auftraggeber)Bank wendet sich in einem ersten Schritt an die Bank des Empfängers. Diese wiederum nimmt mit dem Kontoinhaber Kontakt auf, der den Betrag fälschlicherweise erhalten hat. Der wesentliche Punkt ist, dass der Zahlungsempfänger um sein Einverständnis für eine Rückbuchung ersucht werden muss. Denn ohne diese **Zustimmung des Empfängers** gibt es keine Retournierung. Stimmt dieser zu, erhalten Sie den irrtümlich überwiesenen Betrag - im Idealfall - nach einigen wenigen Tagen zurück.

Erfolgt **keine Zustimmung vom Zahlungsempfänger**, dann sind Ihrer Hausbank und der Bank des Zahlungsempfängers die Hände gebunden. In diesem Fall liegt es leider bei Ihnen, **zivilrechtlich** gegen den falschen Zahlungsempfänger vorzugehen. Dieses Prozedere kann mühsam werden, denn aus Gründen des Bankgeheimnisses darf die Empfängerbank den Namen und die Adresse nicht einfach bekanntgeben. Es bleibt womöglich nichts Anderes übrig, bei der Polizei eine **Anzeige zu erstatten** und in der Folge zu hoffen, dass die Staatsanwaltschaft den Fall

weiterverfolgt. Bei Konten, die im Ausland liegen, kann es sein, dass Ihre Bemühungen gänzlich im Sand verlaufen. Achtung, Ihre Hausbank wird Ihnen wegen des Aufwandes eventuell Bearbeitungsspesen (zum Beispiel 30 Euro) verrechnen. Es ist also empfehlenswert, dass Sie vor jedem Schritt erwägen, welche Kosten Ihnen anfallen könnten.

Achtung: der IBAN allein reicht mittlerweile als sogenannter **Kundenidentifikator** aus – das heißt, selbst wenn der Name des Empfängers nicht mit jenem des Kontoinhabers übereinstimmt, besteht dennoch kein Rückforderungsanspruch für Sie, wenn ein Betrag an einen falschen Empfänger weitergeleitet wurde.

Warum ist eine nicht durchgeführte Überweisung mangels Kontodeckung besonders ärgerlich?

Sie erhalten von Ihrer Hausbank eine Benachrichtigung, wenn eine Überweisung mangels Kontodeckung nicht durchgeführt wurde – Achtung, diese Information über die **Nichtdurchführung einer Überweisung** kann empfindlich teuer werden. Spesen zwischen 5 und 12 Euro können dafür anfallen – und leider werden **diese Spesen im Regelfall doppelt verrechnet**: einmal direkt seitens Ihrer Hausbank, bei der Sie das Girokonto haben; und einmal seitens der Bank des Kontoempfängers, die diese Spesen Ihrer Hausbank anlastet – und die Ihnen wiederum die Spesen weiter verrechnet. Auf diese Weise können Ihnen Spesen zwischen 10 und 20 Euro erwachsen. Eine weitere Folge dieser nicht durchgeführten Überweisung kann sein, dass Sie eine fällige Rechnung nicht fristgerecht bezahlen und daher in Verzug geraten – auch für nicht fristgemäß einbezahlten Mieten, Versicherungsprämien, Gas- und Stromrechnungen etc. können Zusatzkosten (Spesen, Verzugszinsen) anfallen.

Wie sicher sind Überweisungen und wer haftet bei Fehlern?

Laut österreichischem Zahlungsdienstegesetz (ZaDiG) ist als „Kundenidentifikator“ alleine die „IBAN“ (**I**nternational **B**ank **A**ccount **N**umber) entscheidend, wobei die Bank nur prüfen muss, ob die angegebene IBAN tatsächlich existiert. Falls die IBAN existent ist, dann erfolgt die unwiderrufliche Überweisung. Die Bank haftet jedenfalls nicht, wenn die angeführte IBAN mit dem Empfängernamen nicht übereinstimmt. Die Bank kann eine Fehlüberweisung (auf eine existente IBAN) auch dann nicht rückgängig machen, wenn sie sofort versucht, die Überweisung zu stornieren. Mehr über Urteile zum Thema „Geld und Versicherung“ finden Sie auf www.verbraucherrecht.at

Wenn Sie sich bei der IBAN verschreiben oder vertippen, dann ist zu hoffen, dass die angegebene IBAN schlicht nicht existiert. In diesem Fall ist eine Überweisung nicht möglich. Bei elektronischen Buchungen – also bei Buchungen mittels Online-Banking – wird der Auftraggeber der Überweisung während des Beauftragungsversuches auf eine nicht existente IBAN aufmerksam gemacht. Generell gilt: **Bei nicht autorisierten Zahlungen** (gleichgültig ob mittels Bankomat, Kreditkarte oder Überweisung) **trägt** grundsätzlich die **Bank das Missbrauchsrisiko**. Die Bank muss gemäß Zahlungsdienstegesetz das Konto rückwirkend wieder auf den Stand vor dem nicht autorisierten Zahlungsvorgang bringen. Trifft Sie als Bankkunde allerdings ein Verschulden am Missbrauch, dann werden Sie der Bank gegenüber schadenersatzpflichtig. Die Haftung ist **bei leichter Fahrlässigkeit** auf 50 Euro beschränkt. Wenn Sie ein **grob fahrlässiges Verschulden** trifft, dann kann es sein, dass Sie den gesamten entstandenen Schaden tragen müssen.

Wie lange dauert eine Überweisung bis zur Gutschrift am Empfängerkonto?

Ein weiteres Unterscheidungsmerkmal innerhalb der Gruppe der Überweisungen sind unterschiedlich geregelte Überweisungsdauern: Bei einer Bareinzahlung am Schalter muss der Betrag sofort auf dem Konto gutgeschrieben werden (taggleiche Gutschrift bzw. Valutierung). Eine **elektronische Überweisung**, die in Euro lautet, muss am nächsten Werktag dem Konto gutgeschrieben werden. Wird die **Überweisung in Papierform** beauftragt, verlängert sich die Ausführungsfrist um einen Tag und muss daher spätestens am zweiten Werktag am Konto einlangen. Achtung, es kann sein, dass eine Bank einen erhaltenen Zahlungsauftrag von Ihnen nicht am Tag des Einlangens, sondern erst am darauffolgenden Geschäftstag bearbeitet: es gibt von der Bank festgelegte Zeitpunkte (Cut-off-Fristen), die nahe am Ende eines Geschäftstages liegen und festlegen, ob eine Überweisung taggleich oder am Folgetag bearbeitet werden. Erkundigen Sie sich also, wann die Cut-Off-Fristen Ihrer Bank festgelegt sind – Aufträge vor der Cut-off-Frist werden taggleich, Aufträge nach der Cut-Off-Frist werden erst am Folgetag bearbeitet. Beispiel: Die Cut-off-Frist der Bank ist 16 Uhr, sie beauftragen am 1. Juni eine Überweisung mittels Online-Banking um 16.30 Uhr. Die Bank bearbeitet den Auftrag erst am 2. Juni, die Gutschrift am Empfängerkonto ist der 3. Juni.

Für Transaktionen in **anderen europäischen Währungen** als den Euro gelten **andere Abwicklungskonditionen** (z. B. bezüglich Ausführungsfristen und Gebühren) - für Auslandsüberweisungen innerhalb des Europäischen Wirtschaftsraumes (EWR), die nicht in Euro erfolgen (= keine SEPA-Überweisung), beträgt die Frist vier Tage.

Darf ein zahlungsempfangendes Unternehmen Zahlscheingebühren verrechnen?

Eine Verrechnung von Zusatzkosten durch den Zahlungsempfänger (etwa eines Unternehmens) bei Verwendung eines bestimmten Zahlungsinstrumentes wie eines Zahlscheins ist unzulässig. Das Unternehmen kann allerdings für die Nutzung eines bestimmten Zahlungsinstrumentes, wie zum Beispiel einer Einziehung, einen Preisnachlass anbieten. Achtung, **Spesen von Banken, die für Barüberweisungen auf ein fremdes Konto** verrechnet werden, fallen nicht darunter und können weiter verlangt werden, da es sich um eine Gebühr für eine Bankdienstleistung handelt.

1.3.2. Was ist eine eps-Überweisung?

Die eps-Überweisung (**E**lectronic **P**ayment **S**tandard) ist ein **speziell entwickeltes Online-Bezahlverfahren für Einkäufe im Internet** sowie für die Bezahlung von Gebühren und Abgaben an Behörden und öffentliche Institutionen in Österreich. Das Ziel ist die sichere Zahlungsabwicklung zwischen einem Käufer (Konsument, Zahler) und dem Verkäufer (Webshop/Händler, Zahlungsempfänger).

Beim Kauf einer Ware oder Dienstleistung in einem Webshop kann der Käufer/die Käuferin das Bezahlsystem eps-Überweisung auswählen. Es erfolgt die Weiterleitung an eine Bankenauswahlliste, aus der die Hausbank ausgewählt werden kann. Im nächsten Schritt wird der Kunde mit dem Online-Banking verbunden, von wo die Online-Überweisung – vom Zahlungskonto auf das Empfangskonto des Händlers – mittels TAN oder elektronischer Signatur durchgeführt werden kann.

Einige von der AK befragte Banken gaben an, dass die Eps-Überweisung keine Preisvorteile gegenüber anderen Überweisungen aufweist. Sie sind den Spesen einer elektronischen Überweisung gleichgestellt.

1.3.3. Instant Payments: Was ist unter Echtzeitüberweisungen zu verstehen?

Bei Echtzeitüberweisungen (Instant Payments) können die Banken **Überweisungen in Sekundenschnelle** abwickeln. Die Funktionsweise: der Auftrag des Zahlers erfolgt per Online-Banking oder mit einer Smartphone-App unter Eingabe von IBAN und BIC. Im Unterschied zu einer „klassischen" Überweisung, die in der Regel am folgenden Bankarbeitstag beim Empfänger gutgeschrieben wird, soll bei der Echtzeitüberweisung der Überweisungsbetrag (in Euro) innerhalb von **maximal zehn Sekunden** gutgeschrieben sein. Echtzeitüberweisungen können von Ihnen rund um die Uhr und über das gesamte Kalenderjahr – auch an Sonn- und Feiertagen – genutzt werden. Es wird keine Cut-off-Fristen wie bei der klassischen Überweisung geben – ungeachtet des Zahlungszeitpunktes erfolgt die Gutschrift in Sekundenschnelle. Ein Nachteil für den Auftraggeber der Echtzeitüberweisung ist, dass eine **Rückholungsmöglichkeit ausgeschlossen** ist. Wenn Sie eine Echtzeitüberweisung beauftragen, dann ist eine Stornomöglichkeit des Zahlungsauftrages gänzlich ausgeschlossen. Sie sollten sich also gut überlegen, ob Sie diese Form der Überweisung wirklich tätigen wollen – prüfen Sie also den Empfänger und die Höhe des Überweisungsbetrages besonders sorgfältig.

1.4. Wie funktioniert eine SEPA-Lastschrift?

Bei einem SEPA-**Lastschriftauftrag** – vormals die Einzugsermächtigung („Einzieher") und der Abbuchungsauftrag - ermächtigen Sie ein Unternehmen, dass Ihnen ein einmaliger Betrag oder ein **variierender Rechnungsbetrag** (zB Telefonrechnung, Gast/Strom etc.) in einem festgelegten Rhythmus (monatlich, quartalsweise, halbjährlich oder jährlich) von Ihrem Konto abgebucht wird. Die SEPA-Lastschrift darf nur **aufgrund eines gültigen Lastschriftmandates eingezogen** wird – das passiert in der Regel dann, wenn Sie bei einem Kaufvorgang Ihre Kontonummer bekanntgeben. Sie ermächtigen also mit Ihrer Zustimmung ein Unternehmen, dass entweder einmalig ein Betrag oder in wiederkehrenden Abständen Beträge von Ihrem Konto abgebucht werden. Wichtig: Sie können dieses Lastschriftmandat bei Ihrer kontoführenden Hausbank jederzeit oder sperren lassen. Sie sollten jedoch einen Widerruf immer auch an das Unternehmen richten, dem Sie zuvor eine Ermächtigung erteilt haben – andernfalls wird die Bank des Händlers wieder eine Einziehung versuchen, was zu Spesen führen kann.

Welche üblichen Spesen fallen an, wenn SEPA-Lastschriften durchgeführt werden?

Je nach Kontomodell der Bank sind die Durchführungen von Lastschriften entweder in der Kontoführung inkludiert oder sie werden als Zeilen-, Transaktionsgebühr verrechnet.

Wie hoch sind die Spesen einer unterbliebenen, nicht durchgeführten Lastschrift?

Leider können Spesen in erheblicher Höhe anfallen, wenn eine Lastschrift „schief" läuft. Misslingt die Einziehung aufgrund eines technischen Gebrechens oder eines Fehlers im Bereich der Bank, haftet Ihnen die Bank für allfällige Schäden, die Ihnen dadurch entstehen (wie etwa daraus entstehende Mahngebühren). Wird die Abbuchung der Lastschrift allerdings mangels Deckung auf Ihrem Konto von Ihrer Bank zu Recht abgelehnt, sind die dadurch entstehenden Kosten von Ihnen zu tragen. Die Bank darf für die **Benachrichtigung der nicht-durchgeführten** Lastschrift Spesen von Ihnen verlangen, die üblicherweise beträchtlich sind – bis zu 12 Euro.

Welche Einspruchsfristen bei einer Lastschrift gibt es?

Generell: Geben Sie nicht unbegründet Ihre Bankverbindung im Internet, wie zum Beispiel auf Ihrer Website oder gegenüber Privatpersonen, bekannt. Das kann dazu führen, dass Kriminelle mit Ihren Bankdaten zum Beispiel in der Form einer Lastschrift einkaufen können. Das fällt Ihnen als Opfer in der Regel erst verspätet auf, weil die missbräuchlich abgebuchten Geldbeträge meist niedrig sind und in der alltäglichen Geschäftsabwicklung untergehen. Darüber hinaus gibt es Fälle, in denen unseriöse Anbieter für ihre Dienstleistungen niedrige Testpreise verlangen und im Kleingedruckten den Hinweis verstecken, dass es nach dem Testzeitraum zu wesentlich höheren Geldabbuchungen kommt.

Bei Lastschriften gibt es jedoch – im Gegensatz zur „klassischen“ Überweisung - eine gesetzlich festgelegte „Rückholmöglichkeit“. Als Bankkundin haben Sie eine **Einspruchsfrist**, die **unterschiedlich lange** ist. Die Länge der Einspruchsfrist hängt davon ab, ob eine Lastschrift autorisiert (genehmigt/erteilt) oder nicht autorisiert wurde. Wurde keine Einzugsermächtigung erteilt, liegt eine nicht autorisierte Zahlung vor.

- Eine **autorisierte Einziehung** (wenn Sie also ein Lastschriftmandat erteilt haben) können Sie als KontoinhaberIn auch ohne Angabe von Gründen **innerhalb von 56 Tagen** (acht Wochen) rückbuchen lassen. Häufiger Anwendungsfall: wenn die Betragshöhe nicht korrekt ist und nicht vereinbart war. Sie wenden sich an Ihre Hausbank, die Ihnen den abgebuchten Betrag auf Ihrem Konto wieder gutzuschreiben hat. Parallel müssen Sie aber Ihren Vertragspartner auch über Ihre Beanstandung informieren, damit es nicht zu Mahnungen oder Inkassospesen kommt.

- Bei einem **nicht autorisierten Zahlungsauftrag** (wenn Sie also kein Lastschriftmandat erteilt haben) haben Sie ebenfalls Anspruch darauf, dass das Konto wieder auf seinen ursprünglichen Stand gebracht wird. Das Gesetz sieht hier eine Rügeobliegenheit vor. Das bedeutet, Sie müssen die Bank, sobald Ihnen die falsche Buchung auffällt, darüber informieren. Die Frist für die Anzeige endet spätestens **13 Monate** nach der Information über die Belastung.

Was ist eine ems-Lastschrift?

Die ems-Lastschrift („e-Mandat-Service“) ist ein Service für Zahlungsempfänger (sogenannte „Creditoren“), um von ihren Zahlungspflichtigen („Debitoren“) die Autorisierung eines SEPA-Lastschriftmandats zu erhalten. Es handelt sich um einen Online-Prozess, der elektronisch zwischen den Teilnehmern abläuft. Die ems-Lastschrift ist somit ein besonderes, technisches Zahlungsformat.

1.5. Welchen Unterschied gibt es zwischen Lastschrift und Dauerauftrag?

Sie geben bei einem **Dauerauftrag** einmalig schriftlich einen Auftrag an Ihre Bank, dass wiederkehrende **fixe Beträge an einem bestimmten Termin** an einen Begünstigten überwiesen werden (zum Beispiel ein monatlich durchgeführter Dauerauftrag auf ein Sparkonto). Wurde der Betrag bereits vom Konto abgebucht, ist eine Rückbuchung durch die Bank nicht mehr möglich. Sie müssen sich – um die Zahlung zu beanstanden bzw. zurückzuholen – direkt mit dem Zahlungsempfänger in Verbindung setzen.

Welche Spesen fallen bei einem Dauerauftrag an?

Es kann sein, dass die Bank – je nach Kontomodell – für die **Neuanlage, Änderung oder Schließung** eines Dauerauftrages Spesen verrechnet. Es wird meist unterschieden, ob diese in der Filiale (zB am Schalter) oder elektronisch bzw. über Internet Banking erfolgen. Nicht-elektronische Beauftragungen können bis zu 4 Euro betragen, die neu angelegten Daueraufträge mittels Internet Banking sind zumeist kostenlos oder deutlich günstiger als Daueraufträge, die Sie in einer Bankfiliale anlegen.

Je nach Kontomodelle der Bank sind die Durchführungen von Daueraufträgen (also die Buchungsposten) entweder in der Kontoführung inkludiert oder sie werden als **einzelne Zeilen-, Transaktionsgebühr** verrechnet.

Wenn Ihr Konto nicht gedeckt ist und die Bank benachrichtigt Sie über die Nichtdurchführung des Dauerauftrages mangels Kontodeckung, dann können dafür ebenfalls empfindlich hohe Spesen – ähnlich wie bei der Nichtdurchführung einer Lastschrift– bis zu 12 Euro anfallen.

1.6. Wie teuer ist eine Bankomatbehebung?

Damit Sie Geldausgabeautomaten benutzen können, brauchen Sie zunächst eine Debitkarte (früher: Bankomatkarte). Die von Banken ausgegebenen Bankomatkarten sind zumeist Bestandteil eines Girokontopaketes, wobei die jährlich verrechneten Kartengebühren stark divergieren: die Bandbreite reicht von kostenlos bis 25 Euro.

Neben der jährlichen Kartengebühr – sie ist häufig im Kontoführungsentgelt (Kontoführungsgebühr pro Quartal oder Monat) inkludiert - gibt es eine Reihe von Zusatzspesen, die anfallen können:

Für die Barbehebung mit der Bankomatkarte ebenso wie für die unbare Zahlung an einem Terminal in einem Einzelhandelsgeschäft verrechnet die Bank **eine Posten- bzw. Zeilengebühr** bei Konten mit Einzelpreisverrechnung; bei Konten mit Pauschalpreisverrechnung sind diese Transaktionen häufig in der Kontoführungspauschale abgedeckt. Sowohl bei der Bankomatbehebung als auch bei der POS-Zahlung ist die Eingabe des PIN erforderlich – dadurch legitimiert sich der Karteninhaber. Leider gibt es jedoch immer häufiger einen zusätzlichen Spesensatz, der mit einer Bargeldbehebung an einem Automaten anfallen kann. Denn manche Betreiber von Bankomaten verrechnen für die Behebung eine Gebühr in Österreich (Firma Euronet: aktuell 1,95 Euro), die gemeinsam mit dem behobenen Betrag vom Bankkonto abgebucht wird – es handelt sich also um eine separate Bargeldbehebungsgebühr, die empfindlich teuer werden kann. Der **Oberste Gerichtshof hat die Bankomatentgelte der sogenannten Drittanbieter für zulässig befunden**, weil KonsumentInnen bei einer solchen Abhebung mit dem Drittanbieter einen eigenen kostenpflichtigen Vertrag abschließen und die Bankomatgebühr daher außerhalb des Girokontovertrages mit der Hausbank zu zahlen ist. Diese Drittanbieter von Bankomaten sind eigene Betreibergesellschaften, die unabhängig vom österreichischen Bankomaten-Netz ihre Geräte an verschiedenen Standorten aufstellen. Sie finden diese Geräte an Stellen mit hoher Passantenfrequenz, in Eingangsbereichen von Geschäftslokalen usw.

1.6.1. Wie erkennt man Bankomaten von Drittanbietern, die eigene Geldausgabeautomaten aufstellen?

Sie müssen sich den Bankomat genau ansehen: ist darauf ein gängiges Bankenlogo am Banko-

maten nicht ersichtlich, so kann es sich um einen solchen Anbieter (First Data - www.firstdata.com/de_at/home.html, Euronet - www.euronetatms.at/) handeln. Achten Sie während des Behebungsvorganges auf allfällige Spesenhinweise, die am Bildschirm angezeigt und mittels einem Button akzeptiert werden. **Die Anzeige der Spesen am Bildschirm ist verpflichtend** vorgesehen. Üblicherweise können Sie zu diesem Zeitpunkt den Behebungsvorgang abbrechen und somit die kostenpflichtige Behebung vermeiden. Besonders teuer sind Abhebungen von Drittanbietern in Deutschland. So genannte Abwicklungsgesellschaften verlangen beispielsweise 6,50 Euro pro Behebung. Diese betreiben ihre Geldautomaten meistens nicht direkt bei einer Bankfiliale, sondern beispielsweise an Autobahnraststätten.

1.6.2. Welche Bankomatspesen darf Ihre kontoführende Bank verrechnen?

Nach Ansicht der Arbeiterkammer haben Banken dafür Sorge zu tragen, dass ihre Kunden ihr Geld an Automaten ohne Zusatzkosten beheben können. Es ist eine nicht-konsumentenfreundliche Praxis, wenn die Dienstleistung Bargeldbehebung zunehmend anderen Anbietern überlassen wird, die in der Folge Behebungsspesen verrechnen. Auf diese Weise zahlen die Bankkunden dreifach für die Bankomatbehebung: erstens, sie zahlen für die Nutzung der Bankomatkarte die Jahresgebühr; zweitens, die Transaktion wird im Rahmen des Girokontovertrages verrechnet (zum Beispiel in der Form einer Transaktions- bzw. Postengebühr); drittens, bei bestimmten Bankomaten (von „Drittanbietern“) fällt eine zusätzliche Bargeldbehebungsgebühr an (zum Beispiel in der Höhe von 1,95 Euro).

Generell: Erkundigen Sie sich bei Ihrer Bank, welche Spesen bei der Bankomatbehebung **im Rahmen Ihres Girokontovertrages** verrechnet werden. Wichtig: Möchte Ihre Bank eine Bankomatgebühr für jede Behebung (auch bei eigenen Bankomaten) verrechnen, so muss eine entsprechende vertragliche Vereinbarung individuell mit Ihnen ausverhandelt werden. Diese Bestimmung basiert auf einer gesetzlichen Regelung, die der Verfassungsgerichtshof als zulässig beurteilt hat.

1.6.3. Was ist bei Bankomatbehebungen außerhalb des Euro-Raumes zu beachten?

Bei Bankomatbehebungen außerhalb des Euro-Raumes können nicht nur hohe Spesen anfallen, sondern die Schwankungen des Wechselkurses können sich nachteilig auf den letztlich abgebuchten Betrag auswirken. Sie sollten sich mit einer besonders teuren Spesenfalle vertraut machen: Die sogenannte **dynamische Währungsumrechnung** (im Englischen: **D**ynamic **C**urrency **C**onversion, kurz: DCC) kann zu unangenehmen Überraschungen führen. Bei Bankomaten außerhalb des Euro-Raumes kann der Bankomatbetreiber nämlich anbieten, dass der behobene Geldbetrag in der Landeswährung (zum Beispiel britische Pfund, kroatische Kuna etc.) ausbezahlt wird, jedoch sofort in Euro umgerechnet wird. Das kann für Sie als Bargeldbeheber nachteilig sein, denn diese sofortige Umrechnung ist sehr häufig teurer als die Abrechnung in fremder Währung. Sie sollten also **auf die Dynamische Währungsumrechnung verzichten**, indem Sie die Option Abrechnung in Fremdwährung auswählen – der dafür verrechnete Wechselkurs ist nämlich zumeist günstiger als die sofortige Umrechnung des behobenen Betrages in Euro.

1.6.4. Wie ist die Haftung des Inhabers einer Bankomatkarte geregelt?

In den letzten Jahren gab es mehrere Urteile, die die Haftung der Bank bzw. des Karteninhabers

bei Missbrauch der Karte – vor allem nach Aussähen des Codes und darauffolgendem Diebstahl – zum Gegenstand hatten. So stellte der Oberste Gerichtshof (OGH) fest, dass die Bank im Normalfall für den Schaden durch den Missbrauch einer Bankomatkarte nach Ausspähung des Codes und Diebstahl der Karte aus dem Rucksack des Karteninhabers haftet („Rucksack-Urteil“). Aus Entscheidungen des Obersten Gerichtshofs (OGH) ging hervor, dass Besitzer von Bankomatkarten den ihnen von den Banken zur Verfügung gestellten PIN-Code für die Bankomatkarte sehr wohl auch aufschreiben dürfen. Der Code muss aber an einem für Dritte nicht zugänglichen Ort sorgfältig verwahrt werden. Auch ist es grundsätzlich nicht verboten, die Bankomatkarte in einem abgestellten Fahrzeug aufzubewahren. Sie finden Urteile unteranderem zu Bankomatkarten-Missbrauch auf www.verbraucherrecht.at und www.arbeiterkammer.at.

1.7. Welche Arten von Kreditkarten gibt es?

Es gibt eine sehr große Palette an Kreditkarten. Die AK untersucht alljährlich die Konditionen der Kreditkarten, die von den vier Kreditkartenorganisationen angeboten werden. In Österreich stehen KonsumentInnen vier Kreditkartenunternehmen zur Verfügung:

- American Express Europe S.A.-Austrian Branch
- card complete Service Bank AG (VISA, MasterCard, JCB Balance)
- Diners Club DC Bank AG und
- PayLife (VISA und MasterCard) – easybank AG

PayLife und card complete bieten als Komplettanbieter sowohl Karten von MasterCard als auch von VISA an. Daneben existieren immer mehr in Lizenz vergebene Kreditkarten für Banken (zB easybank Kreditkarte etc.) oder andere Dienstleistungsunternehmen (wie zB ÖAMTC-Kreditkarte etc.), die über diese Unternehmen erworben werden können. In sehr vielen “Girokonto-Paketen” von Banken sind ein oder sogar zwei Kreditkarten in der Kontoführung inkludiert. Eine Übersicht dieser Kontopakete – mit oder ohne Kreditkarte - ist unter www.bankenrechner.at/girokonto abrufbar.

1.7.1. Welche Kosten fallen bei Kreditkarten an?

Bei Kreditkarten gibt es zumeist Jahresgebühren, die – ausgenommen kostenlose Kreditkarten etwa im Rahmen von Girokonto-Packages – die zwischen 20 Euro (Kreditkarten ohne Versicherungsschutz) und rund 60 Euro (Karten mit Zusatzleistungen, wie zB Versicherungsschutz) ausmachen. Dementsprechend unterschiedlich sind die Leistungsumfänge. Bei Spesen, die für einzelne Transaktionen verrechnet werden, ist zu unterscheiden:

- Wenn **die Kreditkarte** im Inland oder Euro-Raum **zum Einkaufen** verwendet wird, fallen keine Kosten an. Die Manipulationsgebühr für Umsätze im Nicht-Euro-Raum beträgt je nach Kreditkarte zwischen 1,5 % und 2 %. Achtung, es gibt Ausnahmen von der Manipulationsgebühr bzw. dem Bearbeitungsentgelt. Zudem gibt es unterschiedliche Spesen je Kreditkartengesellschaft.

- Die **Bargeldbehebung an Geldautomaten** (auch in Österreich) ist jedenfalls kostspielig: Die Provision beträgt – je nach Kreditkartengesellschaft – zwischen **3 und 3,3 % bzw. mindestens 2,50 Euro (bis mindestens 4 Euro)**. Bei Behebungen im Ausland kommt noch die Manipulationsgebühr dazu (1,5 bis 2 %, siehe oben). Die Kreditkartenfirmen können einen Höchstbetrag vorsehen, der behoben werden kann (zB im Kartenantrag).

1.7.2. Wie ist der Datenschutz bei der Kreditkartenzahlung ausgestaltet?

Bezahlen Sie Ihre Einkäufe mit Ihrer Kreditkarte, übermitteln Sie der Kreditkartengesellschaft Informationen, wie zum Beispiel das Einkaufdatum, den Händler, den Standort oder die Kaufpreishöhe. In ihren Datenschutzerklärungen halten die Kreditkartenanbieter Visa und Mastercard fest, dass sie die Einkaufsdaten von KundInnen für die Erstellung anonymer Marketingberichte nutzen und diese anderen Unternehmen zur Verfügung stellen. **Wollen Sie das nicht, können Sie bei Visa der Datenverarbeitung widersprechen.** Der Widerspruch gilt für fünf Jahre und muss danach erneuert werden. Bei Mastercard können Sie eine „Datenanalyse-Abmeldung“ unter www.mastercard.at/de-at/datenschutz/data-analytics-opt-out.html vornehmen.

1.7.3. Wo lauern Betrugsgefahren bei Kreditkarten?

Kriminelle versenden gefälschte SMS, Messenger-Nachrichten oder E-Mails und geben mit diesen vor, Ihr Kreditkartendienstleister oder ein Händler zu sein. In diesen Schreiben nennen sie einen erfundenen Grund, wie zum Beispiel

- die Rückerstattung eines nicht getätigten Einkaufs,
- die Notwendigkeit einer Datenaktualisierung oder
- die Versäumnis, eine Sicherheits-App installiert zu haben,

der es angeblich notwendig macht, dass Sie eine Website aufrufen und auf dieser

- persönliche Angaben machen,
- Ihre Kreditkartendaten nennen oder
- eine vermeintliche Sicherheits-App installieren.

Wenn Sie der Aufforderung nachkommen, dann übermitteln Sie Kriminellen diese persönlichen, höchst heiklen Daten, die die Voraussetzung dafür sind, Ihre Kreditkarte missbräuchlich zu verwenden. Es kommt immer wieder vor, dass Sie in betrügerischen E-Mails aufgefordert werden, einen Link anzuklicken – das birgt die Gefahr in sich, dass auf Ihrem Handy oder PC eine Schadsoftware installiert wird. Auch das kann die Datendiebe („Phishing“, also der Datenklau steht für Password Fishing) in die Lage versetzen, dass auf Ihre Kosten eingekauft wird.

Achtung: In einigen Fällen geben **betrügerische Online-Shops**, die trotz Bezahlung keine Ware liefern, vor, dass sie eine Bezahlung mit Kreditkarte akzeptieren. Wählen Sie diese Zahlungsmethode aus, werden Sie auf eine vermeintlich echte Zahlungsdienstleister-Website weitergeleitet. In Wahrheit ist sie gefälscht. Das erkennen Sie an der Adressleiste Ihres Browsers, die Ihnen eine unbekannte Adresse anzeigt. Kriminelle verfolgen mit der gefälschten Website das Ziel, Ihre Kreditkartendaten zu stehlen. Damit können die Datendiebe auf Ihre Kosten einkaufen. Aus diesem Grund seien Sie vorsichtig, wenn Sie bei unbekannten Anbietern einkaufen und kontrollieren Sie zu jedem Zeitpunkt, auf welcher Website Sie sich gerade befinden.

Wie ist es um die Sicherheit bei Kreditkarten bestellt?

Wenn Sie mit der Kreditkarte eine Zahlung durchführen, dann müssen Sie dieser Zahlungsvorgang von Ihnen genehmigt (autorisiert) werden. Das erfolgt durch Unterschrift, die Eingabe einer Personal Identification Number (PIN) oder durch sonstige Daten, die – wie bei Online-Zahlungen gefordert – auf der Kreditkarte ersichtlich sind (wie insbesondere Name, Gültigkeitsdauer oder

des Zahlencodes, der auf der Rückseite der Kreditkarte aufgedruckt ist. Die Sicherheit bei Online-Zahlungen wurde erhöht, in dem die Kreditkartenunternehmen das sogenannte **„3D-Secure-Verfahren“** (Mastercard SecureCode, Verified by Visa) entwickelt haben – eine **zusätzliche Online-Registrierung** des Karteninhabers. Und: im Zuge der sogenannten starken Kundenauthentifizierung – das beinhaltet das Anfragen von zumindest 2 unterschiedlichen Kennungsmerkmalen – haben die Karteninhaber zusätzlich zu den oben angegebenen Daten auch eine für den Zahlungsvorgang erzeugte Transaktionsnummer (TAN) einzugeben, die dem Kunden auf sein Mobiltelefon übermittelt wird.

Was kann ich tun, wenn meine Kreditkarte missbräuchlich verwendet wurde?

Wenn Sie eine Kreditkartenzahlung nicht genehmigt (also nicht autorisiert) haben, dann hat Ihnen **die Kreditkartenfirma den Betrag unverzüglich gutzuschreiben** – das betrifft also vor allem jene Fälle, in denen die Karte von Betrügern missbräuchlich verwendet wurde. Die Kreditkartenfirma sperrt die Karte. Für die Ausstellung einer neuen Karte dürfen Kosten verrechnet werden, die direkt mit dem Ersatz verbunden sind.

Was kann ich tun, wenn ein nicht korrekter Betrag abgebucht wurde?

Keine Autorisierung liegt vor, wenn Sie keine Zustimmung zu Abbuchungen erteilt haben – das betrifft auch wiederkehrende Zahlungen im Rahmen von angeblich abgeschlossenen Abonnements. Achtung, die Kreditkartenfirmen verweigern bisweilen die Rückerstattung von Beträgen, wenn Sie Ihnen vorwerfen, dass sie **grob fahrlässig** gehandelt haben. Ein häufiger Vorwurf an den Karteninhaber lautet, dass Sie eine Transaktionsnummer (TAN) an unbefugte Dritte weitergegeben haben.

Das Gesetz sieht bei **leichter Fahrlässigkeit** des Karteninhabers eine Haftungsgrenze vor: Sie haften bei einem allfälligen Schaden nur bis maximal 50 Euro.

Wenn die Kreditkartenfirma beim Zahlungsvorgang keine starke Kundenauthentifizierung (mehr dazu unter 2.5 auf Seite 24) verlangt hat, dann haftet die Kreditkartenfirma für den gesamten Schaden – auch wenn Sie grob fahrlässig gehandelt haben sollten. Regelmäßig wiederkehrende Zahlungen müssen auch mittels starker Kundenauthentifizierung genehmigt werden.

1.7.4. Was sind Prepaid-Kreditkarten?

Die Kartenanbieter card complete Service Bank AG und PayLife bieten so genannte Prepaid-Karten an. Diese Karten werden **mit einem Guthaben aufgeladen** werden (zB durch Bareinzahlung oder Überweisung) und können innerhalb der Laufzeit wieder aufgeladen werden. Ein eigenes Bankkonto ist für die Ausstellung einer Prepaid-Karte nicht unbedingt erforderlich. Die Karten können weltweit verwendet werden. Die Akzeptanzstellen für die österreichischen Prepaid-Karten sind entweder mit dem Maestro-Logo (für Maestro-Traveller Karte von PayLife) oder mit dem VISA Electron Logo (für Prepaid Karte von card complete) gekennzeichnet.

Prepaid-Karten können auch für Zahlungen im Internet verwendet werden. Die dazu benötigen Codes sind beim Kartenanbieter zu beantragen. Jugendliche ab 14 Jahren können mit Zustimmung des gesetzlichen Vertreters eine Prepaidkarte beantragen. Vorteile: Das Urlaubsbudget kann aufgrund der Aufladung im Vorhinein festgelegt werden. Wenn die Karte gestohlen wird –

insofern ist die Prepaid-Karte sicherer als Bargeld – kann sie gesperrt werden. Zudem ist keine Bankverbindung notwendig. Nachteile: Die **Prepaid-Karte ist spesenintensiv**: es fallen Kosten sowohl beim Aufladen als auch beim Verbrauch an. Ein Guthaben auf der Karte bleibt unverzinst. Zudem gibt es – wie bei allen Kreditkarten – ein Kursrisiko bei Auslandsumsätzen. Achten Sie daher bei Prepaid-Kreditkarten auf die teilweise beträchtlichen Spesen.

1.7.5 Worauf ist zu achten, wenn ich mit der Kreditkarte außerhalb des Euro-Raumes bezahle?

In Ländern außerhalb des Euro-Raumes getätigte Einkäufe/Barbehebungen werden bei der nächsten Monatsrechnung zum Wechselkurs („Referenzkurs“) der Kreditkartengesellschaft abgerechnet. Es gibt seit 1999 keine einheitlichen Wechselkurse mehr, **jede Bank und Kreditkartengesellschaft verrechnet eigene Wechselkurse**. Achtung, bei Kreditkartenzahlungen im Nicht-Euro-Raum kann aufgrund von Wechselkursschwankungen die tatsächliche Belastung von der ursprünglich angenommenen abweichen. Die Umrechnung erfolgt nämlich zum Kurs des Tages, an dem der Umsatz bei der Kreditkartengesellschaft zur Verrechnung eintrifft (Buchungsdatum).

Welche Wechselkurse zur Anwendung kommen, ist in den Allgemeinen Geschäftsbedingungen (AGB) festgehalten. Die Kreditkartenfirmen veröffentlichen die konkret zur Anwendung kommenden Kurse auf ihren Homepages. Allerdings ist ein Vergleich, welche Kreditkarte bei Auslandsumsätzen am günstigsten ist, für den Kunden schwer möglich. Das Vertragsunternehmen (zB Hotel, Restaurant, Einzelhandelsunternehmen etc.) oder der Geldautomatenbetreiber kann dem Karteninhaber anbieten, dass der Umsatz sofort in Euro umgerechnet wird. Bei Zustimmung des Karteninhabers kommt der Wechselkurs des Vertragsunternehmens zur Anwendung. Der Wechselkurs muss dabei offengelegt werden. Der Karteninhaber kann aber auch die Abrechnung seines Umsatzes in Fremdwährung verlangen - dann es kommt der Kurs der Kreditkartenfirma zur Anwendung. Welcher Wechselkurs günstiger ist, kann nicht pauschal beantwortet werden. Wichtig ist, dass Sie sich vorher über den Wechselkurs und dessen Schwankungsbreite im Ausland informieren (zB auf den Internetseiten der Kreditkartenunternehmen).

1.8. Bankomat- und Kreditkarte: Was bedeutet kontaktloses Bezahlen (NFC)?

Kontaktloses Bezahlen, auch Near Field Communication (NFC) genannt, ist eine **Zahlungstechnologie auf der Bankomat- oder Kreditkarte**. Sie ermöglicht es, an ausgewählten und entsprechend gekennzeichneten Akzeptanzstellen im In- und Ausland kontaktlos zu bezahlen - einfach durch Halten der Bankomatkarte an einen speziellen Kartenleser. Es ist also weder die Eingabe des PIN (Personal Identification Number) noch eine Unterschriftsleistung notwendig. Diese Zahlungsmethode soll den Bezahlvorgang verkürzen und vereinfachen.

Wie funktioniert kontaktloses Bezahlen?

Ein Geschäft (zB Einzelhändler) stellt an der Kassa einen Terminal zur Verfügung, dort wird der Bezahlvorgang gestartet. Am Display des Terminals erscheint der zu bezahlende Betrag mit der Aufforderung, die Karte an das Lesegerät zu halten. Der Höchstbetrag für kontaktloses Bezahlen ohne PIN-Code Eingabe für NFC-fähige Karten wurde im April 2020 – also in der COVID-19-Pandemie – von 25 Euro auf 50 Euro pro Bezahlvorgang angehoben. Der Grund dafür lag daran,

dass mehr Kleinzahlungen ohne physischen Kontakt stattfinden sollen, damit die Wahrscheinlichkeit einer COVID-19 Übertragung weiter verringert wird.

Die Sicherheit der Zahlungen besteht darin, dass der Karteninhaber nach einigen NFC-Zahlungen aufgefordert wird, eine PIN einzugeben – damit sichergestellt wird, dass die Transaktionen wirklich der legitimierte Karteninhaber durchführt (und nicht etwa ein Dieb oder eine sonstige unbefugte Person). Die Zahlung mit NFC-Funktion ist eine POS-Zahlung (Point of Sale = Bankomatkassa). Bei der Bezahlung mit der **Bankomatkarte** fallen die Kosten einer Buchungszeile an; bei Pauschalverrechnungskonten sind diese Spesen in der Kontoführungsgebühr (zumeist) inkludiert. Bei der **Kreditkarte** fallen keine gesonderten Spesen an.

Wie ist die Haftung bei NFC-Zahlungen ausgestaltet?

Höherer Komfort und die Zeitersparnis durch schnelleres Bezahlen bei Kassen in Handelsunternehmen stehen dem Risiko gegenüber, dass bei Verlust oder Diebstahl bis zur Sperre der Bankomatkarte jeder, der die Karte unrechtmäßig besitzt, mit der Karte einkaufen kann. In jedem Fall sollten KarteninhaberInnen im Verlust- oder Diebstahlsfall die Karte umgehend sperren lassen. **Grundsätzlich ist der Schaden, der durch den Missbrauch der NFC-Funktion entsteht, von der kartenausgebenden Bank zu tragen** – ausgenommen der Kunde geht betrügerisch vor. Das Zahlungsdienstegesetz sieht eine (Mit-) Haftung der KundInnen im Missbrauchsfall nämlich nur bei Zahlungsmethoden vor, die mit persönlichen Sicherheitsmerkmalen (z.B. PIN-Code bei „normaler“ Bankomatbezahlung) durchgeführt werden. Die Sorgfaltspflichten, die für alle Bankkarten gelten, sollten aber jedenfalls auch bei NFC-Karten eingehalten werden, denn ein Missbrauch kann die Bankomatfunktion betreffen und bei Fahrlässigkeit zur Haftung führen. Achtung, leider kann das Limit für Bezahlvorgänge nicht verändert werden – die 50 Euro pro Bezahlvorgang sind fix vorgegeben.

Welches Zahlungsmittel ist günstiger – die Bankomat-oder Kreditkarte?

Der AK-Zahlungskarten-Rechner berechnet, welche Spesen mit der Bankomat- und Kreditkarte beim Einkaufen oder Geld abheben in Euro-Ländern oder außerhalb von Euro-Ländern anfallen. Denn es gibt bei Bankomat- und Kreditkarten **höchst unterschiedliche Spesenmodelle** von Mindestgebühren in Kombination mit prozentabhängiger Spesenberechnung. Zusätzlich wird bei den Spesen zwischen Umsätzen im Euro-Raum und außerhalb des Euro-Raumes unterschieden – das ist Kartenbesitzern nicht immer bewusst. Der Link zum Rechner: www.bankenrechner.at/zahlkartenrechner

2. WELCHE INNOVATIONEN GIBT ES IM ZAHLUNGSVERKEHR?

2.1. Was sind Mobile Payments?

Die Banken werden sich Bankgeschäfte weiter digitalisieren, zudem dränge neue Dienstleistungsunternehmen – sogenannte FinTechs oder auch „Drittanbieter“ genannt - in den dynamischen Markt des Zahlungsverkehrs. Es wird viele technische Neuerungen geben, zum Beispiel neue Bezahlmöglichkeiten durch sogenannte „wearables“ (also tragbare Geräte) auf einer Uhr oder einem Fitnessarmband. Denkbar sind auch fix eingebaute „smart devices“ (also kluge Endgeräte) in Autos. **Mobile Payment** (auch **M-Payment**) sind elektronische Zahlungsformen, die an die Verwendung von mobilen Endgeräten geknüpft sind. Darunter fallen vor allem Mobiltelefone, Tablet-Computer oder Smartwatches.

2.2. Was ist von Kryptowährungen zu halten?

Nach der Finanzkrise 2008 gab es einen Boom an Kryptowährungen – Bitcoin war die erste etablierte Kryptowährung – es folgten viele tausende andere. Kryptowährungen werden auch als neue Zahlungsmittel angeboten, also als Möglichkeit, Ware gegen Kryptogeld zu tauschen.

Es gibt für das Krypto-Geld einige Bezeichnungen: digitales Geld, digitale Assets oder digital currencies (Englisch: digitale Währungen). Der Begriff „Kryptowährung“ gehört jedenfalls zum allgemeinen Sprachgebrauch. Gleichzeitig ist klar, dass Kryptowährungen – trotz der Bezeichnung „Währung“ – nicht als gesetzliches Zahlungsmittel einzuordnen sind. Handelsplattformen für Kryptowährungen unterliegen derzeit keiner behördlichen Aufsicht. Auch die **Rechtsnatur** von Kryptowährungen ist gesetzlich nicht ausdrücklich geregelt. Wenn man den Kauf einer Kryptowährung auf einer Online-Plattform als „digitalen Inhalt“ im Sinn des Fern- und Auswärtsgeschäfte-Gesetz (FAGG) einstuft, dann kann das Rücktrittsrecht unter den gesetzlich definierten Voraussetzungen des § 18 Absatz 1 Ziffer 11 FAGG ausgeschlossen werden. Fest steht, dass Kryptowährungen **keine gesetzlichen Zahlungsmittel** darstellen – wenn also beispielsweise ein Händler oder ein Restaurant Bitcoins als Bezahlung gegen Ware anbietet, dann ist das ein freiwilliges Tauschgeschäft zwischen zwei Vertragsparteien (also zwischen einem Konsumenten, der Bitcoin zur Zahlung anbietet und einem Händler/Restaurant, der Bitcoin als Zahlungs- und Tauschmittel akzeptiert).

2.3. Welche neuen Anbieter gibt es im Zahlungsverkehr?

Es gibt also im Zahlungsverkehr immer mehr Anbieter, die Zahlungsdienstleistungen anbieten, die zwischen Händler, Bank und Konsument „geschaltet“ sind. Am Markt etablieren sich sogenannte Zahlungsauslöse- und Kontoinformationsdienste. Die Unterschiede: Zahlungsauslösedienste lösen auf Antrag des **Zahlungsdienstnutzers** (zB Konsument, Zahler) einen Zahlungsauftrag auf, der dem Girokonto des Konsumenten (Zahler) angelastet wird. Ein Beispiel: ein Auslösedienst kann im Auftrag des Kunden zum Beispiel eine Überweisung zu Lasten seines Zahlungskontos beim kontoführenden Kreditinstitut ausführen.

Wie erfolgt der Zugriff eines **Zahlungsauslösedienstes** auf das Girokonto? Der Zugriff ist nur durch Ihre Beauftragung mittels Anmeldenamen, PIN (**P**ersonal **I**dentification **N**umber) und TAN (Transaktionsnummer) möglich. Die neuen Zahlungsdiensteanbieter sind verpflichtet, die abgerufenen Daten **nur für den vorgegebenen Zweck zu verwenden** (zum Beispiel für eine Überweisung, um eine im Internet bestellte Ware zu bezahlen).

Kontoinformationsdienste sind Online-Dienste, die Informationen über ein Zahlungs- bzw. Girokonto zur Verfügung stellen, das Sie bei Ihrer Hausbank führen. Für diese Kontoinformationsdienste ist charakteristisch, dass **sie mit den Geldbeträgen nicht in Berührung** kommen. Das bedeutet: Sie können künftig wählen, ob Sie direkt auf Ihr Zahlungskonto zugreifen – zum Beispiel, das Online-Banking Ihrer Bank direkt aufrufen oder eine Banking-App nutzen – oder ob der Zugriff über einen anderen Zahlungsdiensteanbieter erfolgt. Dies kann entweder ein Kontoinformationsdienst oder ein Zahlungsauslösedienst sein. Achtung: Diese neuen Dienste können aber nur mit Ihrer ausdrücklichen Zustimmung Kontodaten abrufen beziehungsweise Zahlungen auslösen.

Hinweis: Sie können auf der Webseite der Finanzmarktaufsicht nach Banken, Zahlungsinstituten etc. suchen und überprüfen, welche Konzession ein Unternehmen hat: www.fma.gv.at/unternehmensdatenbank-suche/

Was sind die rechtlichen Grundlagen für die neuen Anbieter, die Zahlungen auslösen oder Informationsdienste (wie zB den Kontostand) anbieten können?

Die EU-Zahlungsdienste-Richtlinie hat die rechtliche Basis dafür geschaffen, dass Zahlungsauslösedienste (ZAD) oder Kontoinformationsdienste (KID) tätig werden dürfen. Erstens, diese Zahlungsinstitute unterliegen der Aufsicht der Finanzmarktaufsicht (FMA). Zweitens, diese Dienstleister dürfen nur dann tätig werden, wenn Sie einen Vorgang (zB die Anweisung einer Überweisung) ausdrücklich beauftragt haben. Die derzeitige Rechtslage sieht vor, dass Drittanbieter nur mit Ihrem Girokonto „arbeiten" dürfen – es geht also nicht um Kreditkarten, Sparverträge oder Kredite. Die EU-Zahlungsdienste-Richtlinie wurde in Österreich durch das Zahlungsdienstegesetz (ZaDiG) umgesetzt.

Nicht zu übersehen sind in den letzten Jahren die Aktivitäten der großen amerikanischen IT-Konzerne mit globaler Wirtschaftsmacht. PayPal gibt es bereits seit einigen Jahren, ebenso den Dienst paysafecard. Google bietet „Google Pay" an, ebenso gibt es „Apple Pay" oder „Amazon Pay". Facebook hat mit „Libra" eine eigene Kryptowährung kreiiert.

Wie funktioniert Apple Pay?

Apple Pay wird als einfach und sicher präsentiert – so hieß es beim Abruf im August 2020 auf der Homepage: „*Apple Pay ist ganz einfach und funktioniert mit den Apple Geräten, die du jeden Tag nützt. Du kannst damit in Geschäften, Apps und im Internet sicher einkaufen. Es ist so, als würdest du mit einer physischen Karte bezahlen – und dazu noch sicherer.*" heißt es auf der Startseite. Und: „*Apple Pay mit deinem iPhone oder deiner Apple Watch zu nützen geht schneller als mit Karte zu zahlen. Denn Bezahlen soll schließlich möglichst wenig Zeit kosten.*" Die Besitzer von Apple-Produkten müssen **wahlweise ihre Debit-, Kredit- oder Prepaidkarte** ihrem iPhone, ihrem iPad, einer Apple Watch oder einem Mac hinzufügen. Wichtig: Apple speichert diese Daten nicht und hat darauf auch keinen Zugriff. Kommt es zu einer Bezahlung mit Apple Pay, erfährt der Händler die Zahlungsdaten ebenso wenig. Dieser erhält lediglich einen einmalig generierten Code. Der Kunde autorisiert die Transaktion mit einem Code, mit der Face- oder mit der Touch-ID. Die Bezahlung im Internet ist mit Apple Pay ebenso möglich.

In Österreich gibt es Apple Pay seit April 2019. Die Online-Bank N26 und die Erste Bank bzw. alle Sparkassen in Österreich waren bei der Einführung dabei. Mittlerweile unterstützen unter anderem auch die Bank Austria oder die Raiffeisenbank Apple Pay.

Wer Apple Pay nutzen möchte, der benötigt ein Konto bei einer teilnehmenden Bank, danach sind die Debit- bzw. Kreditkarte bei Apple Pay zu hinterlegen.

Wie funktioniert Google Pay?

Google Pay funktioniert über eine kostenlose mobile App, die im Google Play Store oder im Apple App Store heruntergeladen werden kann. Wenn Sie in einem Geschäft mit Google Pay bezahlen, dann wird die von Ihnen zuvor **hinterlegte Kredit- oder Debitkartennummer nicht an den Händler weitergegeben**. Google Pay sendet beim Bezahlen keine Kartennummer, sondern eine virtuell erzeugte Nummer (einen „Token"), der die Debit- oder Kreditkarte repräsentiert. Für Sie als Service-Nutzer entstehen keine zusätzlichen Transaktionskosten.

Bei Google Pay ersetzt ein Telefon die Kreditkarte, zum Zahlen hält man das Gerät im Laden an das Terminal. Bei Online-Zahlungen wird die mit dem Google-Konto verbundene Zahlungskarte belastet - hier ist damit egal, von welcher Bank sie ist.

Google kann Daten, die im Rahmen einer Bezahlung mit Google Pay generiert werden, wie zum Beispiel das Datum, die Uhrzeit und die Höhe des Einkaufs oder den Standort des Händlers, bei dem eingekauft wird, an mit dem Konzern verbundene Unternehmen übermitteln. Diese können die auf diese Weise gewonnen Informationen für ihre Zwecke nutzen („Our affiliates, which can be financial and non-financial entities, will use such information for their everyday business purposes"). Mehr dazu finden Sie unter https://payments.google.com

Sie können der Datenverarbeitung

- zum Informationsaustausch über ihre Kreditwürdigkeit,
- zu Zwecken der Direktwerbung oder
- zur Übermittlung der Information an Händler, ob Sie Google Pay nutzen,

in den Privatsphäreneinstellungen Ihres Google Pay-Kontos widersprechen.

Was kann die Paysafecard?

Auf der Homepage von paysafecard.com heißt es (Stand August 2020) „Paysafecard ist einer der globalen Marktführer im Bereich der Online-Prepaid-Zahlungsmittel und Teil der Paysafe Holdings UK Limited. Prepaid bedeutet, Sie kaufen paysafecard vorab in einer von 650.000 Verkaufsstellen und bezahlen dann online bei tausenden Partnern aus verschiedensten Branchen."

Die Paysafecard ist ein **Prepaid-Zahlungsmitte**l und ist unter anderem in Trafiken erhältlich. Nach der kostenlosen Neuanmeldung können gekaufte Paysafecard-PINs (also Personal Identification Numbers) in dem Paysafecard-Konto hochladen werden. **Das gekaufte Guthaben** ist somit an einem zentralen Ort verfügbar, beim Online-Bezahlen sind der Benutzernamen und ein Passwort zu nutzen.

Der Vorteil der Paysafecard besteht darin, dass Internetkäufe anoym erledigt werden können. Sie erhalten eine sechszehnstellige Personal Identification Number (PIN), die bei allen Händlern, die Paysafecard als Zahlungsform akzeptieren, beim Kauf eingegeben wird. Damit wird die Streuung von heiklen personenbezogenen Daten vermieden. Nachteil: Falls der Code aus irgendeinem Grund nicht funktioniert, müssen Sie Ihre Konto- und Adressdaten an Paysafecard schicken, damit das Guthaben auf Ihr Konto überwiesen werden kann. Außerdem sollten die

Guthaben-Bons innerhalb eines Jahres verbraucht werden; ab dem 13. Monat fallen pro Monat 3 Euro Gebühr an. Die Spesen sind auf der Homepage von Paysafecard unter der Rubrik „Gebühren und Limits“ abrufbar.

Wie funktioniert PayPal?

Paypal ist ein international agierendes Unternehmen, das in Österreich unter PayPal (Europe) S.à r.l. et Cie, S.C.A. firmiert und als Bank geführt wird. Die zuständige **Aufsichtsbehörde ist die luxemburgische Bankenaufsicht** CSSF (Commission de Surveillance du Secteur Financier). Paypal ist als Bezahlsystem weit verbreitet. Sie können mit Paypal Bezahlen (Einkaufen), Geld senden und entgegennehmen (Überweisungen), Warenverkäufe durchführen (also Geld erhalten) oder auch „digitale Gutscheine“ erwerben (siehe dazu Details auf der Homepage www.paypal.com). Als Kunde registrieren Sie sich auf der Webseite und geben PayPal ihre Kreditkartendaten oder eine Bankverbindung bekannt. Sobald Sie bestellen und als Zahlungsform PayPal wählen, überweist PayPal den entsprechenden Betrag von der angeführten Zahlungsquelle zum Händler. **Sobald der Händler den Eingang verbucht, schickt er die Ware ab.**

Das Basiselement bei Paypal ist ein Gratis-Konto, das kostenlos ist (mehr dazu ist auf der Webseite von Paypal unter der Rubrik „Gebühren“ (Englisch: fees) zu erfahren. Aber der Service ist offenbar nicht immer kostenlos (Stand August 2020): „*Erst bei einem Verkauf bzw. Geldempfang erheben wir eine Gebühr von 3,4% + 0,35 Euro. Außerhalb der EU gelten unsere Gebühren für weltweite Zahlungen.*“ Bei Eröffnung des Kontos werden eine E-Mail-Adresse und ein Passwort als Zugangskennung eingerichtet – das sind recht niedrige Zugangshürden, Missbrauch ist also denkbar. **Sie brauchen daher sichere Mailadressen und Passwörter.**

Paypal bietet zum Beispiel die Möglichkeit, zum Beispiel US-Dollar zu kaufen oder Einkünfte in einer Fremdwährung zu erhalten; Fremdwährungen werden zu Tageskursen abgerechnet, es fallen „Festgebühren“ an, die unterschiedlich sind, Das zeigt ein Blick auf die Spesenstruktur, die auf der Webseite in der Rubrik „Gebühren“ (fees) aufgelistet ist. Zu den Spesen heißt es: Bezahlen in Euro ist gebührenfrei. Erst beim Verkauf erheben wir eine Gebühr. Sie zahlen in den meisten Fällen nur 3,4% + 0,35 Euro pro Transaktion und noch weniger, wenn Sie mehr verkaufen.“

Auf der Webseite von Paypal wird groß mit „Käuferschutz“ geworben (Stand August 2020): „Fehlkauf?“ Rückerstattung kein Problem!“. Kaufen Sie mit PayPal ein, schützt **Sie in einigen Fällen der sogenannte PayPal-Käuferschutz**. Er deckt Streitfälle ab, bei denen Händler keine oder falsche Leistungen erbringen oder bei denen Unbekannte Zugriff auf Ihr PayPal-Konto erlangen und nicht erlaubte Zahlungen durchführen. Für die **Aktivierung des PayPal-Käuferschutzes** müssen Sie sich zunächst über Ihr PayPal-Konto bei den Verkäufern melden und versuchen, mit ihnen das Problem zu lösen. Dafür haben sie 180 Tage Zeit.

Kommt es zu keiner Einigung können Sie innerhalb von 20 Tagen den Streitfall an PayPal übergeben. Daraufhin nimmt PayPal Kontakt mit dem Unternehmen auf. Erfolgt von diesem keine oder eine unzureichende Rückmeldung zum Problemfall, gibt Ihnen der Zahlungsdienstleister Recht. In diesem Fall erhalten Sie den Kaufpreis zurück und müssen allenfalls erhaltene Ware an den Online-Shop retournieren. Ist es zu einem nicht autorisierten Zugriff auf Ihr PayPal-Konto gekommen, können Sie das dem Zahlungsdienstleister melden und ebenso eine Rückerstattung der gestohlenen Geldbeträge fordern. Das klingt grundsätzlich gut, aber diese werbliche Ankündigung von Problemlosigkeit trifft in der Praxis nicht immer zu: in der AK Wien-Konsumentenberatung häufen sich Beschwerden, wonach der Käuferschutz nach strittigen oder dubiosen Umsätzen nicht greift – PayPal lehnt die Retournierung des Kaufpreises immer wieder ab.

Achtung, kein Käuferschutz: Betrügerische Verkäufer bieten Ihnen eine Bezahlung mit PayPal an. Die von ihnen angebotene Ware sollen Sie mit der Funktion „Geld an Familie und Freunde senden“ bezahlen. Das führt – so die Argumentation der Kriminellen - zu einer schnelleren Warenlieferung. In Wahrheit umgehen BetrügerInnen damit den PayPal-Käuferschutz, denn er gilt bei dieser Art der Bezahlung nicht. Aus diesem Grund ist es wichtig, dass Sie kein Geld „an Familie und Freunde“ senden, wenn Sie bei Unbekannten einkaufen.

Wie ist es bei PayPal um den Datenschutz bestellt?

PayPal verarbeitet laut Datenschutzerklärung auf der Homepage Ihre Daten, um unter anderem Ihre Identität zu bestätigen, für Bonitätsprüfungen, für andere Überprüfungen der Kreditwürdigkeit oder um den Zahlungsverkehr durchzuführen. PayPal nutzt Ihre personenbezogenen Daten aber auch – so steht es auf der Website - „um die Marketinginhalte und bestimmte Dienste oder Seiteninhalte so abzustimmen, dass Sie Ihren Interessen auf PayPal und anderen Websites von Drittanbietern besser entsprechen“. Im Rahmen der „interessenbasierte(n) Werbung“ verwertet das Unternehmen Informationen über Sie, um „Ihnen so personalisierte Anzeigen, Funktionen, Dienste oder Angebote bereitzustellen und/oder um mit anderen Drittanbietern wie Händlern, Werbe- oder Analytikunternehmen zusammenzuarbeiten und Ihnen so diese personalisierten Dienste zur Verfügung zu stellen“.

Fazit: Damit nutzt PayPal Ihre Daten nicht ausschließlich zur Durchführung von Geldüberweisungen, sondern ebenso zu Werbezwecken. **Der Datenverarbeitung können Sie in Ihren PayPal-Einstellungen widersprechen.**

Wie funktionieren Amazon-Payments?

Sie können in Ihrem Amazon-Kundenkonto eine Zahlungsart hinterlegen – also zum Beispiel einen Bankeinzug, eine Bankomat- und/oder Kreditkarte. Amazon Payments wird aktiviert, wenn Sie erstmals auf der Webseite eines Händlers, der Amazon Payments akzeptiert, Waren oder Dienstleistungen bestellen. Für Sie als Zahler entstehen keine Kosten, die Händler, die eine Zahlung empfangen, haben an Amazon eine Gebühr zu entrichten.

2.4. Was verbirgt sich hinter dem Namen Klarna?

Klarna ist eine schwedische Bank mit Hauptsitz in Stockholm, die als Zahlungsdienstleister immer bedeutender wird. Bei Internet-Zahlungen taucht der Name Klarna häufig auf. Leider gibt es keine österreichische Kontaktadresse, was bei Reklamationen ein Nachteil ist – wenn es etwa darum geht, strittige Zahlungen zu reklamieren oder zu beanstanden.

Auf der Klarna-Homepage (www.klarna.com) wird das Bezahlen über Klarna als einfach, sicher und problemlos beschrieben. Konsumenten wird beschieden, dass sie mit Klarna als Bezahlpartner in ihren Lieblingsshops sofort, später oder in Raten bezahlen können. Eine Sofortzahlung erfolgt mit einer Zahlungskarte oder über das Bankkonto, zum Beispiel mittels Sofortüberweisung oder Lastschrift. So heißt es zum sofortigen Bezahlen im Geschäft (Stand August 2020): „Bezahle zum Beispiel direkt an der Kasse. Sekunden später bekommst du eine Push-Benachrichtigung in der Klarna App. In genau dieser App kannst du übrigens auch all deine Zahlungen und Einkäufe managen.“

Die späteren Zahlungen können binnen 14 Tagen oder „ein bisschen später“ erfolgen; die Zahlung in Raten kann in festen oder flexiblen Raten in bis zu 24 Monaten erfolgen. In den FAQ zum Ratenkauf finden sich keine Informationen über Zinsen und Spesen. Lediglich der Zahlungsverzug wird angeführt, aber sonstige Zahlenangaben waren nicht zu finden.

Klarna bewirbt – ähnlich wie PayPal - auch einen Käuferschutz, insbesondere für den Fall nicht gelieferter oder fehlerhafter Ware. Anfragen in der AK-Konsumentenberatung zeigen jedoch, dass es offenbar **Unklarheiten zum Deckungsbereich des Klarna-Käuferschutzes** gibt. Für Feedback und Beschwerden steht ein Kundenservice zur Verfügung, der vorsieht, einen Chat führen zu können oder anzurufen. Anfragen und Beschwerden in der AK-Konsumentenberatung zeigen: In der Praxis fällt es Konsumenten sehr oft schwer, Probleme mit dem Zahlungsdienstleister lösen zu können. Anfragende Konsumenten haben zum Beispiel das Gefühl, ständig im Kreis herum geschickt zu werden. In der Sache selbst drehen sich viele Beschwerden darum, dass Kunden eine Ware nicht geliefert bekommen oder ordnungsgemäß retourniert haben – aber trotzdem sollen sie den Kaufpreis bezahlen. Konsumenten, die sich über Klarna beschweren, berichten weiters von nicht nachvollziehbaren Mahnschreiben, Betreibungsschritten durch das von Klarna beauftragte Inkassobüro (hohe Spesen!) oder einen Rechtsanwalt, den Klarna zur Forderungseintreibung bestellt hat. Die AK kann Sie mit Interventionsschreiben an den Betreiber (z.B. Klarna, Inkassobüro, Rechtsanwalt) unterstützen.

2.5. Sicherheitsmerkmale: Wie sicher ist Internet Banking?

Seit dem 14. September 2019 gibt es etwa für Überweisungen neben Verfügernummer, PIN und TAN-Code einige technische Neuerungen beim Online Banking – es gibt die sogenannte „starke Kundenauthentifizierung“, bei der mehrere Sicherheitsmerkmale abgefragt werden.

Die BankkundInnen benötigen für Zahlungsvorgänge im Internet **ein Passwort, eine Verfügernummer und – zur endgültigen Bestätigung – einen TAN-Code**. Dieser wird künftig mehr und mehr durch körperliche Merkmale wie Fingerabdruck oder Gesichtserkennung ergänzt werden. Einen einheitlichen Vorgang zur starken Kundenidentifizierung gibt es nicht, jede Bank setzt auf ihr eigenes System. Um den neuen Sicherheitsbestimmungen gerecht zu werden, bieten die Banken eigene Sicherheit-Apps für Smartphones an. Sehr kompliziert wird es für BankkundInnen ohne Smartphone. Diese brauchen einen TAN-Generator, also ein Gerät, das TAN-Codes erzeugt.

Was ist ein CardTAN-Generator?

Das ist ein zusätzliches kleines **technisches Gerät**, das einem Taschenrechner ähnelt. Die BankkundInnen können das Gerät bei Ihrer Bank erwerben (meist kostenlos). Sie brauchen aber auch eine CardTAN-fähige Debitkarte (Bankomatkarte). BankkundInnen, die einen CardTAN-Generator verwenden, geben im Online-Banking wie gewohnt ihre Überweisung ein – aber statt eines SMS-TAN wird der TAN mittels CardTAN-Generator erstellt. Am besten ist es, wenn Sie sich die Videos ansehen, die die Banken dazu auf den jeweiligen Homepages zur Verfügung stellen. Gibt es Ausnahmen bei der „starken“ Kundenauthentifizierung? Es gibt Ausnahmen, z.B. bei Kleinbeträgen (zB 30 Euro) oder bei wiederkehrenden Zahlungen an Empfänger, die nicht als „sensibel“ eingestuft werden. Allerdings legt nach derzeitigem Wissenstand jede Bank ihre Ausnahmen individuell fest.

Was können Multibanking-Apps?

Das sind neue, noch nicht sehr weit verbreitete Apps, die am Smartphone einen Echtzeit-Überblick über Ihre Finanzen anbieten. Sie können in diesen Apps ein Girokonto oder mehrere Konten (zB bei verschiedenen Banken), Kreditkarte(n) oder Sparkonten verwalten, Umsätze übersichtlich auflisten oder verschiedene Analysetools nutzen, um Ihre Finanzgebarung (besser) zu planen. Bei einigen dieser Apps können auch Überweisungen durchgeführt werden.

2.6. Wie ist die Haftung der Kunden ausgestaltet?

Das Zahlungsdienstegesetz sieht vor, dass die Haftung für sogenannte **nicht autorisierte Zahlungen (Missbrauch) auf 50 Euro begrenzt** ist, und zwar für den Fall, dass nur leichte Fahrlässigkeit des Kunden vorliegt. Bei **grober Fahrlässigkeit** ist eine volle Haftung für den entstandenen Schaden möglich. Wenn der Verlust, der Diebstahl oder die missbräuchliche Verwendung eines Zahlungsinstruments für den Zahler vor einer Zahlung nicht bemerkbar war, dann gibt es nach dem Gesetz jedenfalls keine Haftung für den Kunden. Zu beachten sind immer **Sorgfaltspflichten im Umgang mit den Zahlungsinstrumenten (zB Zahlungskarten, PC, Handy)** und den geheimen Passwörtern. Weiters gibt es die Verpflichtung einen Missbrauch, Verlust oder Diebstahl sofort der Bank oder Kreditkartenfirma zu melden, sobald man ihn bemerkt hat. Ab der Sperre trifft den Kunden keine Haftung mehr. **Wichtig: wenn eine Bank eine missbräuchliche Zahlung ohne starke Kundenauthentifizierung (also mit mindestens zwei Sicherheitsmerkmalen) durchführt, dann trägt der Bankkunde keine Haftung, außer er hat selbst betrügerisch gehandelt.**

2.7. Wie ist der Datenschutz beim Internet Banking ausgestaltet?

Nicht alle Banken informieren KonsumentInnen vor dem Installieren der App darüber, welche Folgen das auf die Verarbeitung ihrer personenbezogenen Daten hat. Das erschwert es NutzerInnen, ein klares Bild darüber zu erhalten, weshalb die Anwendung den Zugriff auf bestimmte Funktionen ihres Endgeräts benötigt und welche Folgen das für ihre Privatsphäre hat. Die Beratung der AK Wien zeigt, dass KundInnen bei persönlicher Rückfragen dazu von ihren Banken oft keine Informationen erhalten. Die Anwendungen setzen auf verschlüsselte Kommunikation und erhöhen damit die Sicherheit ihrer KundInnen.

2.8. Was ist unter Phishing zu verstehen?

Grundsätzlich: **Banken verschicken keine E-Mails oder SMS**, die Sie auffordern, dass Sie persönliche Pass- oder Kennwörter oder Transaktionssummern (TANs) bekanntgeben sollen. Leider benutzen Betrüger genau diese Masche: sie kontaktieren Bankkundinen per E-Mail oder telefonisch, geben sich als Bankmitarbeiter aus und vor, dass bestimmte Tätigkeiten durchzuführen sind, um zum Beispiel Bankgeschäfte sicherer zu machen. Das Ziel von Betrügern besteht darin, dass sie an persönliche Bankdaten von KonsumentInnen (wie Passwort, Kontonummer.) gelangen wollen, um Zugang zu einem Konto zu erhalten, das „leergeräumt“ werden soll.

Die häufigste Methode besteht darin, dass Bankkundinnen auf gefälschte E-Mails, SMS oder Messenger-Nachrichten hereinfallen, die einen Wunsch oder Zweck (zum Beispiel die Aktualisierung von Sicherheitsbestimmungen, Updates von Bank-Anwendungen oder die Notwendigkeit, eine Sicherheits-App installieren zu müssen etc.) vortäuschen. In diesen betrügerischen Nach-

richten sind Links auf die vermeintliche Bank-Website enthalten – klickt der Bankkunde diesen Link jedoch an, landet er auf der Webseite der Betrüger, die in der Folge die Zugangsdaten zu einem Konto abfragen. Dass der Kunde auf einer betrügerischen Website ist, ist in der Adressleiste des Browsers erkennbar. Sehr häufig wird der **Betrug durch Telefonanrufe der Betrüger vollendet**, die zum Schluss nach einer Transaktionsnummer (TAN) fragen, die – vom angerufenen Bankkunden bekanntgeben– die letztlich eine betrügerische Abbuchung vom Konto ermöglicht. Wurde aus unbekannten Quellen die vermeintliche Sicherheits-App installiert, kann diese das Endgerät des Opfers ausspähen und damit die TANs an Kriminelle übermitteln.

Da Phishing-Angriffe immer geschickter eingefädelt werden, ist es für den Laien immer schwerer, eine E-Mail, Messenger-Nachricht oder SMS mit Betrugsabsicht zu erkennen. Auf den Betrug kommen viele erst drauf, wenn das Konto leergeräumt ist.

Wer haftet für den Schaden?

Die Opfer von Phishing-Attacken müssen dann nicht für den Schaden haften, **wenn keine Fahrlässigkeit vorliegt**. Dann haftet nämlich die Bank. Wenn jedoch ein Konsument eindeutig erkennen konnte, dass ein Phishing-Angriff vorliegt, dann handelt er/sie grob fahrlässig. In diesem Falle müsste eine Bank nicht haften. Bei leichter Fahrlässigkeit hat der Kunde, der einer Phising-Attacke zum Opfer gefallen ist, einen Selbstbehalt von 50 Euro zu zahlen. Achtung, die Banken reklamieren in der Regel, **dass der Kunde grob fahrlässig gehandelt hat** – zumeist mit dem Argument, dass der Zugang zum Internet Banking gewährt und Transaktionsnummern an die Betrüger mitgeteilt worden sind.

2.9. Worauf müssen Sie beim Bezahlen im Internet achten?

Beim Online-Shopping stehen Ihnen unterschiedliche Zahlungsmöglichkeiten zur Verfügung. Sie sehen beispielsweise vor, dass Sie eine Vorauszahlung leisten, die bestellte Ware bei Entgegennahme bezahlen oder die Rechnung im Nachhinein begleichen. Bevor Sie jedoch bei einem Online-Shop einkaufen, müssen Sie Grundsätzliches beachten, damit Sie kein Opfer von VerbrecherInnen und Datendieben werden:

- Vor einem Einkauf ist es notwendig, dass Sie sich darüber informieren, **welche Erfahrungen und Meinungen es zu einem Unternehmen gibt**: Bewerten es KundInnen schlecht oder liegen noch keine Rückmeldungen zu einem Anbieter vor, ist es am sichersten, wenn Sie bei anderen Händlern einkaufen. Andernfalls setzen Sie sich dem Risiko aus, dass Sie sensible Daten, wie zum Beispiel Ihre Wohnadresse oder Ihre Kreditkartennummer, und Ihr Geld an Kriminelle verlieren. Das kann dazu führen, dass TäterInnen Verbrechen unter Ihren Namen begehen oder Ihre Kreditkarte für missbräuchliche Einkäufe verwenden.

- Bevor Sie bei einem Unternehmen ein Produkt einkaufen oder eine Dienstleistung bestellen, ist es empfehlenswert, dass Sie sich auf Preisvergleichsportalen, wie zum Beispiel geizhals.at, idealo.at, preisvergleich.at, dem **AK - Handytarif-Simulator oder dem AK - Bankenrechner**, über dafür normalerweise verlangte Preise informieren. Gibt es auffällige und nicht erklärbare Preisunterschiede, ist das zumeist ein Hinweis darauf, dass ein Anbieter unseriös ist und mit den günstigen Preisen versucht, Opfer für seine betrügerischen Machenschaften zu finden.

- **Seriöse Händler bieten Ihnen unterschiedliche Zahlungsmöglichkeiten** beim Einkaufen an. Aus diesem Grund ist Vorsicht geboten, wenn Sie ausschließlich eine Bezahlung im Voraus tätigen oder mit Geschenkgutscheinen, Kryptowährungen – das sind digital Zahlungsmittel – sowie Western Union und MoneyGram bezahlen können. Das sind für den Einkauf untypische Zahlungsmittel. Sie sind ein Hinweis darauf, dass Sie an einen kriminellen Online-Shop geraten sind.

- Im Fall einer Bezahlung im Internet muss die **Verbindung zum Online-Shop sicher** sein. Das schließt einen Einkauf über eine offene WLAN-Verbindung aus. Sie ermöglicht es Dritten, Eingaben von Ihnen im Klartext mitzulesen. Das geht mit dem Risiko eines Datendiebstahls einher. Sie erkennen eine offene WLAN-Verbindung daran, dass Sie Ihr Endgerät ohne Passworteingabe mit einem Netzwerk verbinden können.

- Genauso wichtig wie eine Passwort-geschütze Netzwerkverbindung ist eine vom Online- Shop **genutzte https-Verbindung**. Sie lässt für Außenstehende ausschließlich Rückschlüsse darüber zu, welche Website Sie besuchen. Die Inhalte, die Sie sich darauf ansehen und die Eingaben, die Sie darauf machen, sind für Dritte nicht einsehbar. Eine sichere https-Verbindung erkennen Sie an einem versperrten Sicherheitsschloss in der Adressleiste Ihres Browsers.

- Sie müssen darauf achten, dass **Ihr Betriebssystem und Ihre Programme auf dem neuesten Stand** sind. Nur das verhindert, dass Kriminelle bereits mit Aktualisierungen geschlossene Sicherheitslücken für ihre Verbrechen ausnützen und ohne Aufwand Ihre Daten abfangen können. Die Aktualisierung des Betriebssystems oder die Aktualisierung von Programmen ist zumeist über die „Einstellung“ der Software möglich.

3. TIPPS, WIE SIE PROBLEME IM ZAHLUNGSVERKEHR LÖSEN KÖNNEN

- Bitte beachten Sie, dass Sie bei der Verwendung Ihres Zahlungsmittels Sorgfaltspflichten einzuhalten haben. Die Kreditkartenunternehmen und Banken sehen in ihren Geschäftsbedingungen umfangreiche **Obliegenheiten** des Karteninhabers und Sorgfaltspflichten vor. Folgende Punkte sind bei der Verwendung von Zahlungskarten besonders wichtig:

  - Die Karte sofort nach Erhalt unterschreiben
  - Karte, PIN Code nicht an Dritte weitergeben und PIN-Code nicht notieren
  - Die Karte sorgfältig verwahren
  - Bei Nutzung der Karte im Internet auf Verschlüsselung der Homepage des Online-Shops achten

- Kontrollieren Sie Ihre **Kontoauszüge** regelmäßig. Entsorgen Sie jedoch die Auszüge nicht achtlos – zB im Papierkorb gleich neben dem Kontoauszugsdrucker der Bank – so können Daten an unberechtigte Dritte gelangen.

- Der **Verlust, Diebstahl oder missbräuchliche Verwendung** (= nicht autorisierter Zahlungsvorgang) der Debit- oder Kreditkarte sind unverzüglich (sobald man davon Kenntnis hat) der Kreditkartenfirma/Bank zu melden). Erfolgt ein Missbrauch nach der Anzeige (Sperre) haften Sie als Kunde nicht mehr.

- Der Karteninhaber haftet vor der Sperre mit maximal 50 Euro bei leichter Fahrlässigkeit, bei grober Fahrlässigkeit ist **eine Haftung** für den gesamten Schaden möglich. Wenn Ihnen keinerlei Fahrlässigkeit vorwerfbar ist, trifft Sie keine Haftung, aber unter Umständen die Beweislast (Zahlungsdienstegesetz).

- Das Kreditkartenunternehmen ist gesetzlich verpflichtet, den Betrag des nicht autorisierten Zahlungsvorganges **unverzüglich zu erstatten** und das belastete Konto wieder auf den Stand zu bringen, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte.

- Grundsätzlich ist der Schaden, der durch den Missbrauch der **NFC-Funktion** im Rahmen der Debit- und Bankomatkarte entsteht, von der kartenausgebenden Bank zu tragen – ausgenommen der Kunde geht betrügerisch vor. Das Zahlungsdienstegesetz sieht eine Haftung des Kunden im Missbrauchsfall nämlich nur bei Zahlungsmethoden vor, die mit persönlichen Sicherheitsmerkmalen (zB Pin-Code) genehmigt werden. Die Sorgfaltspflichten, die für alle Bankkarten gelten, sollten aber jedenfalls auch bei NFC-Karten eingehalten werden, denn ein Missbrauch kann die Bankomatfunktion betreffen und bei Fahrlässigkeit zur Haftung führen.

- Alle Banken und Kreditkartenunternehmen haben **Ombuds- bzw. Beschwerdestellen**, die Sie bei Problemen rund um die Zahlungskarte unterstützen können. Neben diesen unternehmensinternen Ombudsstellen gibt es auch Einrichtungen, die in den Banksektoren angesiedelt sind (also zum Beispiel im Bankenverband, im Sparkassenverband usw.)

- Bei **Missbrauch** veranlassen Sie eine Anzeige bei der nächsten Polizeidienststelle.

- Die österreichische Kreditwirtschaft unterhält eine eigene **Schlichtungsstelle**, die auch für Zahlungsverkehrsfragen zuständig ist: www.bankenschlichtung.at

- Bei Problemen, die internationalen Bezug haben, kann das **Europäische Verbraucherzentrum (EPVZ)** Unterstützung anbieten (www.europakonsument.at).

- Es gibt die unabhängige **Verbraucherschlichtungsstelle**, die auch für Finanzdienstleistungen zuständig ist: www.verbraucherschlichtung.at.

- Auch die Internet Ombudsstelle (www.ombudsstelle.at) kann Streitschlichtung und Beratung bei diesen Themen anbieten.

- Der Verein für Konsumenteninformation (VKI – www.vki.at) bietet Beratung für ratsuchende Konsumenten. **Die Arbeiterkammern bieten ihren Mitgliedern in allen Bundesländern umfangreiche, kostenlose Beratungsleistungen an** (www.arbeiterkammer.at).

Impressum

Medieninhaber: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65 0
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum

Zulassungsnummer: AK Wien 02Z34648 M

AuftraggeberInnen: AK Wien, Konsumentenschutz
Autoren: Christian Prantner, Michaela Kollmann, Martin Korntheuer, Benedikta Rupprecht, Jakob Kalina (Datenschutz)
Grafik Umschlag und Druck: AK Wien
Verlags- und Herstellungsort: Wien

Stand November 2020
Im Auftrag der Kammer für Arbeiter und Angestellte für Wien

#FÜRIMMER

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Download:
wien.arbeiterkammer.at/service/studien

youtube.com/AKoesterreich
twitter.com/arbeiterkammer
facebook.com/arbeiterkammer
@ich.bin.die.gerechtigkeit

ARBEITERKAMMER.AT/100

AK 100 JAHRE GERECHTIGKEIT