Der Gesetzgeber reagierte darauf rasch im AbgÄG 2011 und verschob das Inkrafttreten der neuen Bestimmungen auf 1. 4. 2012. Zudem gilt für die Steuerpflicht von Veräußerungsgewinnen eine besondere Befristung: diese gilt nur für jeweils zu folgenden unterschiedlichen Zeitpunkten neu angeschaffte Wirtschaftsgüter:

- Anteile an Investment- und Immobilienfonds nach dem 31. 12. 2010,
- Anteile an Körperschaften nach dem 31. 8. 2011,
- Wertpapiere nach dem 31. 3. 2012,
- Derivate und andere Wirtschaftsgüter nach dem 30. 9. 2011.

SCHLUSSSTRICH

Die neue Vermögenszuwachsbesteuerung wird auch weitgehende Auswirkungen auf die Besteuerung von KöR haben. Neben der bisherigen Steuerpflicht für KESt-pflichtige Einkünfte wurden nunmehr auch veranlagungspflichtige Tatbestände eingeführt (Substanzgewinne aus Anteilen an Körperschaften, nicht öffentlich begebenen Wertpapieren und stille Beteiligungen). Der Umfang der bisherigen Steuerbefreiungen auf Einkünfte aus nicht verbrieften Forderungen ohne Bankgeschäft (Privatdarlehen, obligationenartige Genussrechte) sowie auf Wohnbauanleihen bleibt jedoch im Wesentlichen bestehen.

Kreditkartenmissbrauch im Fernabsatz – Neuregelung nach dem ZaDiG

Mit der Einführung des ZaDiG erfolgte eine Neuregelung des Zahlungsverkehrs mit Zahlungsinstrumenten, welche ua die bisherige Regelung des § 31 a KSchG zum Missbrauch von Zahlungskarten im Fernabsatz beseitigte. Der folgende Artikel stellt die Neuregelung dieses Problemkreises kurz dar, zeigt die damit verbundenen Probleme anhand eines Vergleichs der Zahlungsinstrumente Kreditkarte und Bankomatkarte auf und präsentiert einen möglichen Lösungsansatz.

Sinn und Sinnwidrigkeit der Kreditkartenprüfnummer

STEFAN ZIEGLER

A. Besonderheiten des Zahlungsinstruments Kreditkarte

Unter den Begriff Zahlungsinstrumente fallen Geräte („physical devices") und Anwendungen („set of procedures") mit personalisierten Sicherheitsmerkmalen.[1]) Die Bankomatkarte kann als typisches Beispiel eines Zahlungsinstruments iSd ZaDiG angesehen werden. Die personalisierten Sicherheitsmerkmale sind hier einerseits auf der Karte selbst (Name, Kontonummer, Bankleitzahl, Unterschriftsprobe) enthalten, andererseits bedarf der Einsatz des Zahlungsinstruments einer PIN, die dem Nachweis dienen soll, dass der rechtmäßige Karteninhaber die Karte nutzt. Eine Kreditkarte weist ebenfalls personalisierte Sicherheitsmerkmale auf; im Einzelnen sind dies die Kreditkartennummer, die Angabe der Gültigkeitsdauer, die Unterschriftsprobe und die Kreditkartenprüfnummer. Im Geschäftsgebrauch unter Anwesenden läuft die Autorisierung einer Zahlung wie bei der Bankomatkarte in zwei Stufen ab, nämlich durch Vorweisen der Karte und Leisten einer Unterschrift auf der Rechnung. Im Fernabsatz besteht allerdings nach wie vor die Besonderheit, dass sämtliche zum Auslösen eines Zahlungsvorgangs notwendigen personalisierten Sicherheitsmerkmale auf dem Zahlungsinstrument selbst aufgedruckt sind. Damit kann aber nicht mit an Sicherheit grenzender Wahrscheinlichkeit nachvollzogen werden, ob die Anweisung durch den berechtigten Zahlungskarteninhaber vorgenommen wurde.

§ 36 Abs 1 ZaDiG sieht vor, dass der Zahlungsdienstnutzer alle zumutbaren Vorkehrungen zu treffen hat, „um die personalisierten Sicherheitsmerkmale und das Zahlungsinstrument vor unbefugtem Zugriff zu schützen". Ob man dieser Pflicht überhaupt nachkommen kann, soll im Folgenden geklärt werden.

B. Grundsätzliche Regelungen des ZaDiG

Das Zahlungsdienstegesetz (ZaDiG) findet auf alle relevanten Zahlungsdienste Anwendung. Zahlungsdienste sind etwa Überweisungen, Lastschriften, Zahlungen oder Behebungen mit Bankomatkarten, Kreditkartenzahlungen oder Daueraufträge (§ 1 Abs 2

Mag. *Stefan Ziegler* ist Rechtsanwaltsanwärter bei Kerres | Partners in Wien und betreut Causen mit wirtschaftlichem Hintergrund sowie insolvenz- und exekutionsrechtliche Fragestellungen für ein führendes österreichisches Kreditkarteninstitut.

1) *Kind/Steinmaurer,* RdW 2011/9 mwN, insb unter Berufung auf die Interpretation der Europäischen Kommission; dies ergibt sich bereits aus der Begriffsbestimmung des § 3 Z 23 ZaDiG: „Jedes personalisierte Instrument oder jeder personalisierte Verfahrensablauf (...)".

ZaDiG). In diesem Zusammenhang interessieren va die Bestimmungen hinsichtlich der Sorgfaltspflichten sowie die Regelung der Haftung für nicht autorisierte Zahlungen:

1. Sorgfaltspflichten des Zahlungsdienstleisters – § 35 ZaDiG

Für den Zahlungsdienstleister besteht nach § 35 Abs 4 und 5 ZaDiG jedenfalls eine Überprüfungspflicht, dh er muss, soweit dies technisch und ohne manuelles Eingreifen möglich ist, die Übereinstimmung mit einem angegebenen Empfänger überprüfen (§ 35 Abs 4 Z 3 und 4 ZaDiG). Außerdem muss der Zahlungsdienstleister seinem Zahlungsdienstnutzer jederzeit die wirksame Sperre des Zahlungsinstruments ermöglichen und sicherstellen, dass die personalisierten Sicherheitsmerkmale des Zahlungsinstruments niemandem außer seinem Kunden zugänglich sind. § 35 Abs 2 ZaDiG ordnet explizit die Haftung des Zahlungsdienstleisters für den Fall an, dass Zahlungsinstrumente bzw personalisierte Sicherheitsmerkmale des Zahlungsinstruments versendet werden und dabei in falsche Hände geraten.

2. Sorgfaltspflichten des Zahlungsdienstnutzers – § 36 ZaDiG

Der Zahlungsdienstnutzer hat va die Pflicht, die personalisierten Sicherheitsmerkmale von Zahlungsinstrumenten vor unbefugtem Zugriff zu schützen. Außerdem muss er Verlust, Diebstahl sowie eine missbräuchliche oder nicht autorisierte Nutzung unverzüglich ab Kenntnis dem Zahlungsdienstleister anzeigen. Daneben muss der Zahlungsdienstnutzer die Ausgabe- und Nutzungsbedingungen des Zahlungsdienstleisters einhalten. § 36 Abs 3 ZaDiG normiert eine Rügeobliegenheit – nicht autorisierte oder fehlerhaft ausgeführte Zahlungsvorgänge muss der Verbraucher unverzüglich rügen, um eine Berichtigung erwirken zu können. Die absolute Frist zur Erstattung einer entsprechenden Anzeige beträgt 13 Monate ab dem Tag der Belastung oder Gutschrift und kann zu Lasten von Verbrauchern nicht verkürzt werden (Abs 4). Den Verbraucher trifft jedoch *keine Prüfpflicht* hinsichtlich der Belastungen oder Gutschriften auf der Abrechnung – in der Praxis wird es daher grundsätzlich genügen, wenn der Verbraucher innerhalb von 13 Monaten ab Belastung bzw Gutschrift anzeigt, dass die Zahlung nicht ordnungsgemäß erfolgt ist.[2]) Der Zahlungsdienstleister muss den Nachweis der früheren Kenntnis führen. Er darf sich auch nicht auf die Rügepflicht berufen, wenn ihm kein Schaden entstanden ist.[3])

3. Haftung für nicht autorisierte Zahlungen – § 44 ZaDiG

Eine Zahlung ist nur dann autorisiert, wenn die Zustimmung des Zahlers in der Form und in dem Verfahren abgegeben worden ist, welche zwischen dem Zahler und seinem Zahlungsdienstleister vereinbart worden ist (§ 34 ZaDiG). Diese Regelung muss zwingend im Rahmenvertrag zwischen Zahlungsdienstleister und Zahler enthalten sein.[4]) Bestreitet der Zahlungsdienstnutzer die Autorisierung der Zahlung, ist der Zahlungsdienstleister verpflichtet, die ordnungsgemäße und autorisierte Durchführung der Zahlung nachzuweisen. Liegt eine nicht autorisierte Zahlung vor, muss der Zahlungsdienstleister den Betrag unverzüglich erstatten, darüber hinaus können dem Zahler weitere gesetzliche oder vertragliche Ansprüche zustehen.

Bei Verstoß gegen seine Sorgfaltspflichten gem § 35 ZaDiG bzw bei Verstoß gegen die vereinbarten Ausgabe- und Nutzungsbedingungen kann dagegen der Zahlungsdienstnutzer seinem Zahlungsdienstleister schadenersatzpflichtig werden: Bei der unberechtigten Verwendung eines gestohlenen, verlorenen oder missbräuchlich verwendeten Zahlungsinstruments haftet der Nutzer *höchstens mit € 150,–, außer es liegt grobe Fahrlässigkeit oder Vorsatz vor.* Die Beweislast, dass der Nutzer grob fahrlässig gehandelt hat, trifft den Zahlungsdienstleister.[5]) Der Zahlungsdienstnutzer haftet nicht für Zahlungen, die nach erfolgter Anzeige des Verlusts, Diebstahls, der missbräuchlichen oder nicht autorisierten Verwendung vorgenommen werden.

Kreditkartengesellschaften legen die Nutzungsbedingungen der von ihnen ausgegebenen Zahlungsinstrumente in den zwischen ihnen und den Zahlungsdienstnutzern vereinbarten AGB fest. Darin wird regelmäßig vorgesehen, dass der Zahlungsdienstnutzer sich bei der Weitergabe seiner Kreditkartendaten eines sicheren Weges bedienen muss.[6]) Bei Missachtung solcher AGB wird der Zahlungdienstnutzer idR dennoch nicht schadenersatzpflichtig werden: So wie nach allgemeinem Zivilrecht beim Missbrauch einer Zahlungskarte der Zahlung keine gültige Anweisung zugrunde liegt, mangelt es im Kontext des § 44 ZaDiG an einer Zustimmung des Zahlers. Der Zahler kann daher die Rückbuchung der Zahlung gem § 44 ZaDiG fordern. Ist diese erfolgreich, hat der Zahlungsdienstleister des Zahlers keinen Schaden, den er von diesem verlangen könnte. Einen allfälligen Differenzschaden kann der Zahlungsdienstleister gem § 44 Abs 2 ZaDiG von seinem Zahlungsdienstnutzer nur dann zurückfordern, wenn die Rückforderung etwa wegen Insolvenz nicht erfolgreich ist.

C. Hintanhalten des Missbrauchs von Kreditkarten im Fernabsatz durch die Kreditkartenprüfnummer (KPN)

1. Zweck und Grenzen der KPN

Erst kürzlich hat ein gezielter Angriff auf interne Datenbanken des von Sony betriebenen PSN- und SOE-

2) *Haghofer,* Kundenschutz im neuen Zahlungsdienstegesetz, ecolex 2010, 128 (131) – Vertragsklauseln, die dem Kunden eine Prüfpflicht auferlegen, sind unwirksam.

3) Voraussetzung für die Anwendung des § 44 Abs 2 ZaDiG ist das Vorliegen eines Schadens beim Zahlungsdienstleister.

4) § 28 Abs 1 Z 2 lit c ZaDiG.

5) Vgl *Schrank/Marx-Rajal,* ecolex 2009/811 mwN.

6) Aktueller Standard ist die Verschlüsselung mittels SSL, erkennbar in der Statuszeile des Browsers: SSL-verschlüsselte Homepages beginnen mit https://

Netzwerkes stattgefunden, bei dem insgesamt über 100 Millionen Datensätze gestohlen wurden. Sony hat die betroffenen Kunden damit beruhigt, dass die Kreditkartenprüfnummern nicht gespeichert worden sind, tatsächlich sind in Österreich bis jetzt keine Missbrauchsfälle bekannt geworden. Im Folgenden soll die Schutzwirkung der Kreditkartenprüfnummer einer kritischen Betrachtung zugeführt werden.

Wenn Einkäufe im Wege des Fernabsatzes, insb im Rahmen von Zahlungen in Online-Shops oder via Telefon-Hotlines getätigt werden (sog Telefon- und Mailorderverfahren, auch MOTO-Verfahren genannt), genügte bis vor einigen Jahren noch die Angabe der Kreditkartennummer und des Ablaufdatums der Kreditkarte, um wirksam einen Zahlungsvorgang auslösen zu können. Aufgrund der damit verbundenen hohen Missbrauchsanfälligkeit haben die Kreditkartengesellschaften die Kreditkartenprüfnummer (KPN)[7]) eingeführt. Die KPN besteht aus drei bis vier zusätzlichen Ziffern, die idR auf der Rückseite der Karte aufgedruckt sind und nicht im Reliefdruck der Karte enthalten bzw im Magnetstreifen gespeichert sind. Bei Telefon- und Mailorderverfahren ist diese Kartenechtheitsprüfung inzwischen zwingend vorgesehen.[8]) Die KPN muss bei jeder Bestellung erneut eingegeben werden, da sie nicht gespeichert, sondern nur „durchgereicht" wird. Mit dem Prüfnummern-Verfahren wird so in der Praxis wirksam sichergestellt, dass die Ausforschung von Kreditkartennummern, die in Datenbanken gespeichert werden, nicht per se zu einem Zahlungskartenmissbrauch im Internet führen kann. Jedoch geht der Schutz über diese Funktion grundsätzlich nicht hinaus, da die KPN für jeden sichtbar auf der Rückseite des Zahlungsinstruments notiert ist. So kann bspw der Kellner, der die Kreditkarte auf dem Tablett zum Lesegerät transportiert, die Kreditkartennummer samt KPN notieren, bzw ein Gast in einem unbemerkten Moment die Daten einsehen. Wenn die Karte nicht physisch gestohlen wird, wird der Kreditkarteninhaber davon in der Regel auch nichts bemerken, und wenn man bejaht, dass das Aushändigen der Kreditkarte im Restaurant normalen Geschäftsgebrauch darstellt, wird man auch keine Sorgfaltswidrigkeit des Zahlungsdienstnutzers konstruieren können. Dennoch kann derjenige, der sich die Kreditkartendaten notiert, das Zahlungsinstrument im Fernabsatz einsetzen, ohne dieses physisch inne zu haben. Als praktischen Anwendungsfall kann man sich etwa das Ordern von Zug- oder Konzerttickets im Online-Verkehr vorstellen. Die Tickets werden anonym ausgestellt und eine Zustellung an die Bestelleradresse scheidet aus, wenn der Nutzer sich das Ticket selbst ausdrucken kann.

2. Vergleich KPN – PIN

Das ZaDiG unterscheidet nicht zwischen einer Bankomatkarte und einer Kreditkarte. Im Gegensatz zur PIN einer Bankomatkarte ist die KPN einer Kreditkarte jedoch auf der Rückseite der Karte vermerkt. Würde der Zahlungsdienstnutzer bei einer Bankomatkarte die PIN auf der Karte selbst notieren, wäre dies nach dem ZaDiG als grob fahrlässige Sorgfaltspflichtverletzung gem § 36 Abs 1 ZaDiG zu qualifizieren und der Zahlungsdienstnutzer wurde bei Missbrauch seines Zahlungsinstruments seinem Zahlungsdienstleister gegenüber unbeschränkt haften. Nur ein (grob) sorgfaltswidriges Verhalten des Zahlungsdienstnutzers kann seine (un)beschränkte Haftung begründen. Da es im Geschäftsverkehr durchaus als üblich angesehen werden kann, dass man etwa im Restaurant die Kreditkarte dem Kellner im Billet übergibt, also aus der Hand gibt, wird ein derartiges Verhalten wohl nicht als sorgfaltswidrig iSd § 36 ZaDiG eingestuft werden können. Durch den Vermerk der KPN auf dem Zahlungsinstrument schaffen die Kreditkartengesellschaften also Situationen herbei, die den haftungsrechtlichen Regress gegen ihre Zahlungsdienstnutzer verhindern können. Dabei könnte mit einfachen Mitteln Abhilfe geschafft werden, *indem die KPN nicht auf die Karte gedruckt wird, sondern wie bei der Bankomatkarte dem Kunden in einem getrennten Schreiben bekannt gegeben wird.* Dies würde mE ausschließlich Vorteile mit sich bringen:

- Nur dann könnte der Zahlungsdienstnutzer auch wirksam entsprechend § 36 Abs 1 ZaDiG dazu verpflichtet werden, die personifizierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen;
- für das Kreditkarteninstitut würden sich die Anforderungen an den Nachweis einer Sorgfaltspflichtverletzung gem § 36 ZaDiG verringern;
- die Judikatur zum Missbrauch von Bankomatkarten könnte unverändert auf den Missbrauch von Kreditkarten im Fernabsatz umgelegt werden.

Der OGH hat sich bereits ausgiebig mit dem Problemkreis der missbräuchlichen Verwendung von Bankomatkarten beschäftigt und dabei die folgende Lösung vertreten: Bei Verwendung einer Karte mit PIN bleibt es grundsätzlich bei der normalen Beweislastverteilung. Wenn der Kartenherausgeber Aufwandersatz verlangt, muss er beweisen, dass der Karteninhaber die Karte selbst verwendet hat. Die Verwendung der richtigen PIN ist aber ein gewichtiges Indiz dafür, dass der Karteninhaber die Karte selbst verwendet hat oder jedenfalls den Missbrauch schuldhaft ermöglicht hat. Damit spricht der Beweis des ersten Anscheins für eine Nutzung der Karte durch den Karteninhaber selbst oder für eine Verletzung der Geheimhaltungspflicht. Dieser Anscheinsbeweis kann durch den Karteninhaber dadurch entkräftet werden, dass er die ernsthafte Möglichkeit eines atypischen Geschehensablaufs beweist.[9]) Auch wenn das ZaDiG die Zahlungsinstrumente Kreditkarte und Bankomatkarte gleich regelt, unterscheiden diese sich doch erheblich faktisch, sodass mE diese Rsp keinesfalls auf den Missbrauch von Kreditkarten im Fernabsatz um-

7) Dieser Standard nennt sich bei VISA CVV2 (Card Verification Value 2) und bei Euro/Mastercard CVC2 (Card Verification Code 2). CVV2 wurde 2001, CVC2 1997 eingeführt. Auch American Express hat eine (vierstellige) KPN eingeführt, welche 4DBC genannt wird (4 Digit Batch Code).

8) Vgl etwa *Krügel*, Die Zukunft der Kreditkarte als Zahlungssystem im Internet – Die Rechtslage im Anschluss an das Urteil des BGH vom 16. 4. 2002, ZR 375/00, 55 f mwN.

9) RIS-RS0104837; 2 Ob 133/99 v RdW 2000, 559 = RZ 2000, 253 = ÖBA 2001, 250 *(Koziol)* = SZ 73/107 = ÖBA 2008, 329.

gelegt werden kann. Es kann kein Anscheinsbeweis im oben dargestellten Sinn angenommen werden, wenn im Telefon- oder Mailorderverfahren eine Zahlung unter Angabe der KPN erfolgt, da dieser Code auch ohne Setzen eines sorgfaltswidrigen Verhaltens durch den Zahlungsdienstnutzer einem Dritten bekannt werden kann. Damit bleibt es aber bei der klassischen Beweislastverteilung – der Zahlungsdienstleister, der Aufwandersatz von seinem Zahlungsdienstnutzer fordert, muss im Fall der Verwendung einer Kreditkarte im Fernabsatz jedenfalls beweisen, dass die Karte vom Karteninhaber verwendet worden ist.

D. AGB zwischen Kreditkartengesellschaft und Vertragsunternehmen

Im Verhältnis zwischen Kreditkartengesellschaft und Vertragsunternehmen trifft das ZaDiG keine besonderen Regelungen. Die Haftung wird hier regelmäßig von den wirtschaftlich stärkeren Kreditkartengesellschaften in ihren AGB auf die Vertragsunternehmen überantwortet. Der OGH hat in seiner E 10 Ob 54/04w ausgesprochen, dass aufgrund der typischen Ungleichgewichtslage zwischen Vertragsunternehmen und Kreditkartengesellschaft auch für zwischen diesen vereinbarte AGB-Klauseln die Bestimmung des § 879 Abs 3 ABGB zur Unwirksamkeit von Klauseln wegen gröblicher Benachteiligung heranzuziehen ist. Dennoch wurde in der bisherigen Rsp die in der Praxis geübte Überwälzung des Risikos auf die Vertragsunternehmen grundsätzlich akzeptiert, hauptsächlich mit zwei Begründungen: Einerseits sei ein Zahlungsausfall eher dem Vertragsunternehmen als der Kreditkartengesellschaft zuzurechnen.[10]) Andererseits bieten Kreditkartenunternehmen in der Regel neben der gewöhnlichen Zahlungsmethode auch ein sicheres Verfahren an, bei dem die Kreditkartengesellschaft das Ausfallsrisiko bei Rückabwicklungen nicht autorisierter Zahlungen übernimmt – naturgemäß ist dieses Verfahren für die Vertragsunternehmen mit erheblichen Mehrkosten verbunden.[11]) Die Hauptargumentation in der bisherigen Rsp war der Ansatzpunkt des Unternehmerrisikos, weshalb sich daran auch durch die Neuregelung des ZaDiG wohl nichts ändern wird.

E. Fazit: Handlungsbedarf des Gesetzgebers

Das ZaDiG ist mit dem Spezialfall der Kreditkarte als Zahlungsinstrument überfordert, wenn es normiert, dass der Zahlungsdienstnutzer die personifizierten Sicherheitsmerkmale vor unbefugtem Zugriff schützen muss und damit hinsichtlich der Kreditkarte etwas im Geschäftsgebrauch faktisch Unmögliches verlangt. Das ZaDiG scheitert beim Versuch, dieselben Regelungen für Kreditkarten zu normieren, die auch für Bankomatkarten gelten. Es wäre wünschenswert, dass die Kreditkartengesellschaften der legistischen Gleichregelung der Zahlungsinstrumente folgen und die KPN in Zukunft nicht mehr auf der Kreditkarte selbst notieren, wodurch sie unmittelbar eine Vergleichbarkeit der beiden Zahlungsinstrumente Bankomatkarte und Kreditkarte herbeiführen würden. Solange sich die Rsp des OGH nicht ändert, mit der die pauschale Überwälzung der Haftung auf die Vertragsunternehmen zugelassen wird, tragen die Kreditkartengesellschaften aber faktisch keinen Schaden davon. Umso mehr ist der Gesetzgeber gefordert, der faktischen Ungleichheit der Zahlungsinstrumente zu folgen und abweichende Sorgfaltsbestimmungen für Zahlungsdienstnutzer zu normieren, die das Zahlungsinstrument Kreditkarte im Fernabsatz einsetzen.

10) Vgl 1 Ob 1/07i.

11) Vgl 10 Ob 54/04w (zum damaligen SET-Verfahren: Annahme des wirtschaftlichen Risikos des Vertragsunternehmens insb dort, wo diesem die Wahl zwischen dem normalen Mailorder-Verfahren und einem sicheren Verfahren ohne Ausfallsrisiko gegeben wird).

SCHLUSSSTRICH

Das ZaDiG kann gegenwärtig keine befriedigende Regelung in den Fällen des Missbrauchs von Kreditkarten im Internet herbeiführen, da es tatsächliche Unterschiede bei den einzelnen Zahlungsinstrumenten unberücksichtigt lässt. Hinsichtlich der Regelung der Sorgfaltspflichten des Zahlungsdienstnutzers besteht legistischer Handlungsbedarf, wenn die Haftung nicht pauschal zu Lasten der Vertragsunternehmen gehen soll.