NJW
Neue Juristische
Wochenschrift

Sonderdruck aus NJW Heft 18/2012

Rechtsanwalt Dr. Ulrich Schulte am Hülse und Peter Welchering

Der Anscheinsbeweis bei missbräuchlicher Bargeldabhebung an Geldautomaten mit Karte und Geheimzahl

Verlag C.H. Beck München und Frankfurt a.M.

Neue Juristische Wochenschrift (NJW)

Schriftleitung:
Rechtsanwalt *Tobias Freudenberg* (verantwortlich für den Textteil).
Beethovenstraße 7 b, 60325 Frankfurt a. M., *Postanschrift:* Postfach 11 02 41, 60037 Frankfurt a. M., Telefon: (0 69) 75 60 91-0, Telefax: (0 69) 75 60 91-49.
E-Mail: redaktion@njw.de
Internet: www.njw.de

Mitglieder der Redaktion:
Rechtsanwältin *Nathalie Dennier*, Rechtsanwalt *Jürgen Dietermann*, Rechtsanwältin *Mirjam Erb*, LL.M., Rechtsanwalt *Stefan Fahrmeier*, Rechtsanwältin *Anett Hoffmann*, Rechtsanwältin *Elisabeth Jackisch*, Rechtsanwalt *Dr. Andreas Kappus*, Rechtsanwältin *Esther Noske*, LL.M., Rechtsanwältin *Marianne Schwara-Moore*, Rechtsanwalt Professor *Dr. Martin Weber* (alle Schwerpunkt Zivilrecht); Rechtsanwalt *Dr. Stephan Tausch* (Schwerpunkt Strafrecht); Rechtsanwältin *Stephanie Kuchenbauer* (Schwerpunkt Öffentliches Recht); Rechtsanwältin *Dr. Monika Spiekermann* (NJW-aktuell); Assessorin *Anne Holtermann* (Schlussredaktion); *Bianca Bügler* (Buchbesprechungen).

Manuskripte: Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag das ausschließliche Verlagsrecht für die Zeit bis zum Ablauf des Urheberrechts. Eingeschlossen sind insbesondere auch das Recht zur Herstellung elektronischer Versionen und zur Einspeicherung in Datenbanken sowie das Recht zu deren Vervielfältigung und Verbreitung online oder offline ohne zusätzliche Vergütung. Nach Ablauf eines Jahres kann der Autor anderen Verlagen eine einfache Abdruckgenehmigung erteilen; das Recht an der elektronischen Version verbleibt beim Verlag.

Urheber- und Verlagsrechte: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Das gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, denn diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlags in irgendeiner Form – durch Fotokopie, Mikrofilm oder andere Verfahren – reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsanlagen verwendbare Sprache, übertragen werden.

Anzeigenabteilung: Verlag C. H. Beck, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: Susanne Raff (0 89) 3 81 89-601, Julie von Steuben (0 89) 3 81 89-608, Bertram Götz (0 89) 3 81 89-610, Telefax: (0 89) 3 81 89-589.
Disposition: Herstellung Anzeigen, technische Daten, Telefon: (0 89) 3 81 89-606, Telefax: (0 89) 3 81 89-599, njwanzeigen@beck.de
Anzeigenpreise: Zurzeit gilt Anzeigenpreisliste Nr. 55.
Anzeigenschluss: Ca. 9 Tage vor Erscheinen.
Verantwortlich für den Anzeigenteil: *Fritz Lebherz*.

Verlag: Verlag C. H. Beck oHG, Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: (0 89) 3 81 89-0, Telefax: (0 89) 3 81 89-3 98, Postbank München: Nr. 6 229-8 02, BLZ 700 100 80.

Erscheinungsweise:
Wöchentlich an jedem Donnerstag.

Beilagen (mehrmals jährlich):
NJW-Spezial und Zeitschrift für Rechtspolitik (ZRP).

Bezugspreise 2012: Halbjährlich (incl. NJWDirekt für 3 Nutzer) € 119,– (darin € 7,79 MwSt.); **Vorzugspreis** (gegen Nachweis) für Mitglieder des Deutschen Anwaltvereins und Forum für junge RA (incl. NJWDirekt für 3 Nutzer) € 107,– (darin € 7,– MwSt.), für Studenten, Referendare (fachbezogener Studiengang) und Anwälte, deren Zulassung jünger ist als drei Jahre (incl. NJWDirekt für 1 Nutzer) € 65,– (darin € 4,25 MwSt.), für Studenten und Referendare (fachbezogener Studiengang), die gleichzeitige Bezieher der JuS sind € 50,– (darin € 3,27 MwSt.). Der Anspruch auf den Vorzugspreis für Studenten und Referendare erlischt mit dem Ablegen des Assessorexamens. **Einzelheft:** € 5,80 (darin € –,38 MwSt.). **Versandkosten** jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden.
Jahrestitelei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

Bestellungen über jede Buchhandlung und beim Verlag.

KundenServiceCenter:
Telefon: (0 89) 3 81 89-750,
Telefax: (0 89) 3 81 89-358.
E-Mail: bestellung@beck.de

Abbestellungen: 6 Wochen vor Halbjahresschluss.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an.
Hinweis gemäß § 7 Abs. 5 der Postdienste-Datenschutzverordnung: Bei Anschriftenänderung des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen dieses Heftes beim Verlag widersprechen.

Druck: Druckerei C. H. Beck (Adresse wie Verlag). Lieferanschrift: Versand und Warenannahme, Berger Str. 3–5, 86720 Nördlingen.

Zur Rechtsprechung

Rechtsanwalt Dr. Ulrich Schulte am Hülse und Peter Welchering*

Der Anscheinsbeweis bei missbräuchlicher Bargeldabhebung an Geldautomaten mit Karte und Geheimzahl

I. Einleitung

Die Fälle, in denen Zahlungskarten durch Dritte missbräuchlich eingesetzt werden, haben zugenommen. Wenn dabei Verfügungen an Geldautomaten unter Einsatz der richtigen Persönlichen Identifikationsnummer (PIN) vorgenommen werden, haftet nach der Rechtsprechung meist der Karteninhaber. Die Begründung der Gerichte: Eine Bargeldabhebung am Geldautomaten könne nicht ohne die Kenntnis der dazugehörigen PIN erfolgen. Daher streite – obwohl die genauen Tatumstände häufig unklar bleiben – zu Gunsten der kartenausgebenden Stelle ein Anscheinsbeweis für die Tatsache, dass der Karteninhaber die PIN auf seiner Zahlungskarte oder gemeinsam mit dieser aufbewahrt habe. Da dies als grob fahrlässig anzusehen sei, hafte der Karteninhaber für den entstandenen Schaden. Allerdings hält der *XI. Zivilsenat* des *BGH* die Anwendbarkeit des Prima-facie-Beweises nach seinem Urteil vom 29. 11. 2011[1] nur noch dann für anwendbar, wenn von den Tätern die Originalkarte eingesetzt worden ist. Dafür ist die kartenausgebende Stelle darlegungs- und beweisbelastet. Zugleich wurden Einschränkungen in Bezug auf die Anwendbarkeit des Prima-facie-Beweises für die Fälle vorgenommen, in denen es zum Einsatz der Originalkarte am Geldautomaten kommt. Vor diesem Hintergrund geht der Beitrag unter Analyse der technischen Möglichkeiten der Täter beim Zugriff auf die zu einer Zahlungskarte gehörende PIN sowie der Kriminalitätsentwicklung der vergangenen Jahre der Frage nach, inwiefern die Annahme des Prima-facie-Beweises auch in den Fällen gerechtfertigt ist, in denen die Originalkarte bei einem nicht autorisierten Zahlungsvorfall zum Einsatz kommt.

II. Rechtslage bei nicht autorisierten Zahlungsvorfällen

1. Erstattungsanspruch des Karteninhabers

Hat die kontoführende Stelle einen Geldbetrag auf Grund einer Anfrage am Geldautomaten gegenüber der so genannten Clearingstelle freigegeben und wird dieser Geldbetrag durch die kontoführende Stelle als Saldo in das Konto des Karteninhabers gebucht, ohne dass dem eine wirksame Anweisung des Karteninhabers zu Grunde lag, hat die kontoführende Stelle mangels eines Auftrags keinen Entgelt- und keinen Aufwendungsersatzanspruch nach §§ 675 f IV 1, 675 c I i. V. mit § 670 BGB gegen den Karteninhaber. Der Zweck des Vertrags zwischen dem Karteninhaber und der kontoführenden Stelle ist nur darauf gerichtet, die kontoführende Stelle, die hier als angewiesene Bank tätig war, autorisierte Transaktionen vornehmen zu lassen. Unterrichtet der Karteninhaber die kontoführende Stelle unverzüglich über die nicht autorisierte Zahlung, haftet für den Schaden die ohne wirksame Anweisung ausführende Stelle[2]. Dass es auf dem Konto des Karteninhabers, der in diesem Fall nicht getäuscht wurde[3], tatsächlich zu einer Belastungsbuchung kommt, ist für den tatsächlichen Forderungsbestand gegen die kontoführende Stelle ohne Belang[4]. Insofern steht dem Karteninhaber ein Anspruch auf Erstattung des durch die nicht autorisierte Zahlungsanweisung abverfügten Geldbetrags zu (inklusive der darauf entfallenden Kreditzinsen und Kosten). Wird die Vertragsbeziehung mit der kontoführenden Stelle fortgesetzt, war bislang umstritten, ob der Anspruch im Wege der Leistungsklage oder, auf Grund des fortbestehenden Kontokorrentverhältnisses, nur als reiner Kon-

---

* Der Autor *Schulte am Hülse* ist Fachanwalt für Bank- und Kapitalmarktrecht und Mitbegründer der Potsdamer Sozietät ilex Rechtsanwälte & Steuerberater. Der Autor *Welchering* ist geschäftsführender Gesellschafter der Voxmundi Medienanstalt-GmbH und hat sich in Fachbeiträgen u. a. für die FAZ, die ARD und den Deutschlandfunk mit der Funktionsweise von Geldautomaten befasst. – Besprechung von *BGH*, Urt. v. 29. 11. 2011 – XI ZR 370/10, NJW 2012, 1277 (unter Nr. 3 in diesem Heft).

1 *BGH*, NJW 2012, 1277.

2 Pars pro toto: *BGHZ* 176, 234 (238) = NJW 2008, 2331; *BGH*, NJW 2001, 2629 = WM 2001, 1460 (1461); NJW-RR 1990, 1200 (1201); *LG Mannheim*, MMR 2008, 765; *Schulte am Hülse/Klabunde*, MMR 2010, 84 (86); *Schimansky*, in: *Schimansky/Bunte/Lwowski*, BankR-Hdb., Bd. 1, 3. Aufl. (2007), § 49 Rdnr. 93.

3 Die Täter spielen dem Server der geldfreigebenden oder -anweisenden Stelle eine autorisierte Zahlungsanweisung vor, die in Wirklichkeit nicht autorisiert ist. Getäuscht im juristischen Sinne wird insofern nicht der Karteninhaber, gegenüber dem Server der geldfreigebenden oder -anweisenden Stelle liegt ein Fall des § 263 a StGB vor.

4 *KG*, NJOZ 2010, 2164. Diese Rechtsfolge findet sich gegenwärtig u. a. in Art. 54 I 1, Art. 56 I b i. V. mit Art. 60 I der Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. 11. 2007 und wurde seit dem 31. 10. 2009 in § 675 u BGB auch gesetzlich normiert.

toberichtigungsanspruch durchgesetzt werden kann. Das *KG* hatte bereits vor der Umsetzung der SEPA-Richtlinie vertreten, dass der Durchsetzung im Wege der Leistungsklage trotz eines Fortbestehens der Vertragsbeziehung zur kontoführenden Stelle keine Bedenken entgegenstehen[5]. Seit der Umsetzung der SEPA-Richtlinie in nationales Recht dürfte sich dieser Streit erledigt haben, denn § 675 u S. 2 BGB ist zu entnehmen:

„Er ist verpflichtet, dem Zahler den Zahlungsbetrag unverzüglich zu erstatten und, sofern der Betrag einem Zahlungskonto belastet worden ist, dieses Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte."

Mit „Erstatten" ist dabei der Leistungsanspruch angesprochen und mit „wieder auf den Stand bringen" der Kontoberichtigungsanspruch. Mit „und" ist ein Wahlrecht des Anspruchsinhabers bezeichnet. Gleichwohl wird der forensisch tätige Praktiker gegebenenfalls einen Hilfsantrag stellen müssen.

2. (Gegen-)Anspruch der kontoführenden Stelle

Allerdings kann die kontoführende Stelle dem Karteninhaber einen eigenen Schadensersatzanspruch entgegenhalten, wenn sich der Karteninhaber gem. § 675 v II BGB grob fahrlässig verhalten hat. Hinsichtlich der Beweislastverteilung hat grundsätzlich die kontoführende Bank den Vorwurf der groben Fahrlässigkeit darzulegen und zu beweisen[6].

An dieser Stelle setzt die Beweiserleichterung durch den Prima-facie-Beweis ein, auf die der *BGH* seit einer Grundsatzentscheidung im Jahre 2004 zu Gunsten der kontoführenden Stelle zurückgreift[7]. Gestützt auf Erfahrungssätze soll es erlaubt sein, Schlüsse von bewiesenen auf zu beweisende Tatsachen zu ziehen. Der Anscheinsbeweis soll dabei die Annahme rechtfertigen, dass wenn es Tätern gelingt, mit der gestohlenen Zahlungskarte des Karteninhabers eine nicht autorisierte Verfügung am Geldautomaten vorzunehmen, die Ursachensphäre allein beim Bankkunden liegen müsse, der in diesem Fall die zwingend benötigte PIN nicht sicher aufbewahrt habe.

Allerdings sprach der *BGH* schon damals von der jederzeit gegebenen Möglichkeit der Entkräftung des Anscheinsbeweises durch Darlegung eines andersartigen Ursachenverlaufs. Dazu müsse der in Anspruch Genommene lediglich Tatsachen darlegen und gegebenenfalls beweisen, die die ernsthafte, ebenfalls in Betracht kommende Möglichkeit einer anderen Ursache nahelegt[8].

Mit einer weiteren Entscheidung zum Anscheinsbeweis hob der *BGH* ein Urteil des *OLG Frankfurt a. M.* auf und verwies es zur erneuten Verhandlung und Entscheidung an das Berufungsgericht zurück[9]. Das Berufungsgericht habe den Anspruch auf rechtliches Gehör verletzt, indem es den angebotenen Beweis zur Erschütterung des Anscheinsbeweises ignoriert habe, so der *BGH*. Der *Senat* legte dar, dass der Anscheinsbeweis unter anderem dadurch erschüttert werden könne, indem der Karteninhaber darlegt und beweist, dass er die PIN nicht auf der Zahlungskarte notiert habe oder die Geheimnummer etwa ohne Verschulden des Karteninhabers kurze Zeit vor der Entwendung der Karte ausgespäht worden sein könnte. In diesem Fall könne Anlass bestehen, das Sicherheitssystem der Bank einer erneuten sachverständigen Prüfung dahingehend zu unterwerfen, ob es ein ausreichendes Sicherheitsniveau biete. Sollte dies nicht der Fall sein, sei bereits der Anwendungsbereich des Prima-facie-Beweises ausgeschlossen.

Eine weitere Entscheidung zur fehlerhaften Anwendung der Grundsätze des Anscheinsbeweises bei den Zahlungskarten ergibt sich aus einem stattgebenden Kammerbeschluss des *BVerfG*[10]. Zwar erachtet es auch das *BVerfG* als zulässig, dass sich die beweisbelastete Bank zum Nachweis eines grob fahrlässigen Verhaltens des Karteninhabers in bestimmten Situationen auf die Grundsätze des Anscheinsbeweises berufen könne. Nachdrücklich wies das *BVerfG* jedoch auf die Möglichkeit der Entkräftung dieses Anscheinsbeweises hin. Bei einer Automatenabhebung unter Verwendung der EC-Karte und der dazugehörigen PIN reiche es aus, wenn der Karteninhaber der Vermutung durch die Darlegung eines atypischen Verlaufs die Grundlage entziehe; etwa dadurch, dass die EC-Karte in einem näheren zeitlichen Zusammenhang mit einem – dann naheliegend durch einen Dritten ausgespähten – eigenen Gebrauch der PIN entwendet worden sein könnte.

In seinem Urteil vom 29. 11. 2011 entschied der *BGH* nunmehr, dass die Grundsätze des Anscheinsbeweises nur noch dann in Betracht zu ziehen sind, wenn die Originalkarte am Geldautomaten eingesetzt wurde. Für den Einsatz der Originalkarte ist die ausgebende Stelle darlegungs- und beweisbelastet. Bei Abhebungen am Geldautomaten mit Hilfe einer Kartendublette fehle dagegen die für die Anwendbarkeit des Prima-facie-Beweises erforderliche Typizität[11]. Zugleich gab der *BGH* den Tatsacheninstanzen die Beachtung einiger Grundsätze auf, falls feststehen sollte, dass die Originalkarte eingesetzt worden sei. Dann, so der *BGH*, ist zu klären, ob das von der kartenausgebenden Stelle und den die Geldautomaten betreibenden Instituten konkret genutzte Sicherheitssystem überhaupt ein ausreichendes Sicherheitsniveau für die Anwendung des Prima-facie-Beweises bietet. Besonders wies der *BGH* darauf hin, dass dem Karteninhaber, sofern ihm sonstige Beweismittel nicht zur Verfügung stehen, gegebenenfalls die Möglichkeit eröffnet werden müsse, den Anscheinsbeweis, er habe Karte und PIN zusammen verwahrt, im Wege einer Vernehmung als Partei zu erschüttern[12].

III. Technische Möglichkeiten zur Kenntniserlangung der PIN

Ob eine Beweiserleichterung im Sinne des Prima-facie-Beweises zu Gunsten der kontoverwaltenden Stelle greift oder nicht, ist inzwischen auch eine technische Frage. Die Möglichkeiten und Methoden zum Ausspähen der zur Zahlungskarte gehörenden PIN sind jedenfalls so vielfältig, dass die Annahme, dass bei Automatenverfügungen unter Verwendung der richtigen PIN die Ursachensphäre allein beim Karteninhaber liegt, der mit einer erdrückenden Wahrscheinlich-

5 *KG*, MMR 2011, 338.
6 *LG Berlin*, Urt. v. 11. 4. 2007 – 10 O 238/06, BeckRS 2007, 19497; *LG Kaiserslautern*, Urt. v. 26. 11. 2004 – 2 O 394/04, BeckRS 2004, 11889; *AG Frankfurt a. M.*, Urt. v. 26. 5. 2009 – 30 C 2223/08, BeckRS 2009, 14259.
7 *BGHZ* 160, 308 (312 ff.) = NJW 2004, 3623.
8 *BGHZ* 160, 308 (314 ff.) = NJW 2004, 3623. Diese Entscheidung beendete vorerst einen zuvor heftig ausgetragenen Meinungsstreit. Für die Anwendung des Prima-facie-Beweises: *OLG Frankfurt a. M.* (*8. Zivilsenat)*, WM 2002, 2101 = BeckRS 2002, 30470028; *OLG Stuttgart*, NJW-RR 2002, 1274; a. A. *OLG Hamm*, NJW 1997, 1711; *OLG Frankfurt a. M.* (*7. Zivilsenat)*, NJW-RR 2001, 1341; *OLG Frankfurt a. M.* (*24. Zivilsenat)*, NJW-RR 2002, 692. Zuletzt gegen die Anwendung des Prima-facie-Beweises: *AG Berlin-Mitte*, NJW-RR 2010, 407; a. A. *LG Berlin*, NJW-RR 2011, 352.
9 *BGH*, WM 2011, 924 = BeckRS 2010, 18045.
10 *BVerfG*, NJW 2010, 1129.
11 *BGH*, NJW 2012, 1277.
12 *BGH*, NJW 2012, 1277.

keit die PIN auf der Karte oder in deren räumlichen Nähe notiert haben müsste, in Frage gestellt ist.

1. „Skimming"

Mit den neueren Methoden beim so genannten „Skimming" muss die Kreditwirtschaft einen modus operandi beim Ausspähen der zu Zahlungskarten gehörenden PIN zur Kenntnis nehmen. Bei der schon länger bekannten Methode bauen die Straftäter ein Kartenlesegerät vor den Kartenschlitz, an dem der Bankkunde seine Zahlungskarte einschiebt. Mit einer Minikamera wird die PIN mitgelesen. Da die Täter auf diese Weise sowohl die PIN abgreifen als auch – im Falle des Einsatzes von Magnetstreifentechnik – die übrigen Daten auf der Zahlungskarte auslesen können und sodann mit Hilfe von Kartendubletten nicht autorisierte Verfügungen tätigen können, hat der *BGH* die frühere Rechtsprechung zur Anwendung des Prima-facie-Beweises zu Recht abgelehnt[13].

Inzwischen funktionieren solche Tathandlungen nicht mehr nur durch die entsprechende Manipulation der Geldautomaten, sondern unmittelbar durch das Abfangen der in Point-of-Sales-Terminals vom Karteninhaber einzugebenden Daten, also den bei Händlern vorhandenen Bezahlterminals. An den Terminals in Tankstellen, in Supermärkten oder an anderen Orten können auf diese Weise kleine Chips auf den Kunden lauern, die während des Bezahlvorgangs die Daten auf dem Magnetstreifen inklusive der PIN abgreifen und an die Täter übermitteln. Das Auslesen der auf der Karte gespeicherten Daten funktioniert auch, wenn die Karte ausschließlich über einen EMV-Chip verfügt und nur dort Kartendaten gespeichert sind. Die PIN kann ohnehin trotzdem abgegriffen werden, da sie händisch vom Karteninhaber eingegeben werden muss. Die PIN kann ferner über Schadsoftware wie einen Keylogger oder sogar über eine direkte Seitenkanalattacke auf den Chip selbst erbeutet werden[14].

Verläuft der konkrete Einzelfall so, dass es zu einer Entwendung der Originalkarte kommt und diese anschließend bei der nicht autorisierten Geldautomaten-Verfügung von den Tätern eingesetzt wird, hält der *BGH* es für denkbar, dass auch das für die nicht autorisierte Geldautomaten-Verfügung notwendige Abgreifen der PIN ohne jeden Fahrlässigkeitsvorwurf an den Karteninhaber erfolgen konnte, wenn eine autorisierte Verfügung in einem unmittelbaren zeitlichen Zusammenhang zur anschließenden nicht autorisierten Verfügung steht[15]. Der *BGH* geht also davon aus, dass die Täter dem Karteninhaber auflauern, die PIN im Rahmen einer autorisierten Verfügung mittels eines Manipulationsvorgangs abgreifen, die Originalkarte im direkten Anschluss entwenden und die zuvor abgegriffene PIN daraufhin für eine nicht autorisierte Abhebung am Geldautomaten mit der Originalkarte einsetzen.

Irrtümlich ist es jedoch, die Kreativität der Täter zu verkennen. Dass die Täter organisiert vorgehen, ist schon lange kein Geheimnis mehr. Kaum etwas spricht für die Annahme, dass die Täter, die zunächst heimlich die PIN abgreifen, zwingend die gleichen Täter sein müssen, die anschließend oder Jahre später die Originalkarte stehlen und diese dann am Geldautomaten einsetzen. Berichte, wonach man komplette Kartendaten inklusive PIN auf illegalen Internetseiten kaufen kann, sind seit Jahren bekannt[16]. Offenkundig hat sich eine Arbeitsteilung der organisierten Täter herauskristallisiert, wobei die „PIN-Beschaffung" und das Entwenden der Originalkarte eben arbeitsteilig und insofern zeitlich versetzt und durch unterschiedliche Tätergruppen erfolgt. Von verschiedenen Sicherheitsforschern wurden in den Jahren 2008 bis 2010 so genannte „Dropzones" nachgewiesen. Das sind Server, an die Karteninformationen samt PIN von Schadsoftware geschickt werden. Diesen Dropzones nachgeschaltet sind dann oftmals Auktionsplattformen, über die derartige Karteninformationen inklusive PIN verkauft bzw. versteigert werden[17].

Ein Fall, in dem die Täter heimlich die PIN auslesen, ohne dass den Karteninhaber ein Fahrlässigkeitsvorwurf trifft, kann deshalb auch dann vorliegen, wenn die Originalkarte entwendet wurde, der Täter die richtige PIN bei der nicht autorisierten Verfügung einsetzt und kein autorisierter Zahlungsvorgang zeitlich unmittelbar davor stattgefunden hat.

2. Magnetstreifentechnik

Solange die Umrüstung auf die rein chipkartenbasierten Karten noch nicht vollständig abgeschlossen ist bzw. weiterhin der EMV-Chip neben dem Magnetstreifen auf der Karte existiert, verbleibt es vorerst zumindest bei der teilweisen Nutzung des bisherigen Magnetstreifen-Systems. Ein solcher Magnetstreifen enthält regelmäßig drei Datenspuren. Eine davon ist beschreibbar. Auf ihr wird zum Beispiel die Eingabe einer falsch eingegebenen PIN dokumentiert sowie die mit dieser EC-Karte an Geldautomaten vorgenommenen Transaktionen. Auf den ersten beiden Magnetspuren sind die Kontoinformationen (z. B. die Girokontonummer) und Bankidentifikationsdaten (z. B. die Bankleitzahl) gespeichert. Außerdem ist auf der dritten Spur verschiedentlich eine Prüfsumme abgelegt, mit der die PIN nicht nur bestätigt, sondern mit einigem Rechenaufwand auch ermittelt werden kann[18].

In der Regel werden alle drei Magnetspuren vom Kartenleser ausgelesen. Zunächst überprüft eine Sicherungsroutine, ob eine falsche PIN-Eingabe protokolliert wurde. Weist die Protokolldatenspur eine mindestens dreimalige falsche PIN-Eingabe auf, wird die Karte eingezogen oder abgewiesen. Da Magnetstreifen mitunter etwas störanfällig sind, können nicht immer alle drei Spuren ausgelesen werden. Unter Umständen lässt sich bei einer falschen PIN-Eingabe die dritte Spur auch gerade nicht beschreiben, so dass der Protokolleintrag unterbleibt. Zumindest Kontonummer und eine Angabe zur kontoführenden Bank müssen jedoch aus den ersten beiden Datenspuren ausgelesen werden können, damit der Steuerungs-PC des Automaten eine Verbindung zum Bankserver aufbaut. Diese Datenverbindung erfolgt über ein eigenes, verschlüsseltes Kommunikationsprotokoll[19].

Bestätigt der Bankserver, dass die von den Magnetspuren ausgelesenen Daten in Ordnung sind und die Karte nicht gesperrt ist, schickt eine weitere Softwareroutine eine Meldung an den Flüssigkristallbildschirm des Geldautomaten. Der Kunde wird aufgefordert, seine Geheimzahl über die Eingabetastatur einzugeben, die jede eingetippte Nummer sofort verschlüsselt. Bei einigen Softwareversionen wird über die so eingegebene PIN eine Prüfsumme gebildet, die mit der

13 *BGH*, NJW 2012, 1277.
14 *Welchering*, FAZ v. 10. 1. 2012, S. T2, und *ders.*, Funkchips geknackt, DLF v. 29. 12. 2011, dokumentiert unter http://www.dradio.de/dlf/sendungen/forschak/1640327; *Streck/Elmer/Fu* u. a., Stern Nr. 12 v. 15. 3. 2012, S. 73 (76).
15 *BGH*, WM 2011, 924 = BeckRS 2010, 18045.
16 Vgl. *Welchering*, Wie Datendiebe Kasse machen, WDR 5 v. 17. 11. 2009, dokumentiert unter http://www.wdr5.de/sendungen/leonardo/s/d/17. 11.2009-16.05/b/kreditkartendatenklau-in-spanien.html; Betrug via Kreditkarten-Klau, Deutschlandfunk v. 17. 11. 2009, dokumentiert unter: http://www.dradio.de/dlf/sendungen/umwelt/1071461/
17 Eine Mannheimer Forschergruppe unter Leitung von *Dr. Thorsten Holz* hat 70 dieser Dropzones untersucht und dort Karteninformationen teilweise mit zugeordneter PIN von 170 000 Opfern gefunden.
18 *Welchering*, FAZ v. 3. 5. 2011, S. T1.
19 *Welchering*, FAZ v. 3. 5. 2011, S. T1.

auf der dritten Magnetspur der Karte hinterlegten Prüfsumme abgeglichen wird. Stimmen die Prüfsummen überein, wird die vom Kunden eingetippte und gleich verschlüsselte PIN an den Bankserver geschickt, dort entschlüsselt und mit der auf dem Bankserver hinterlegten PIN abgeglichen[20].

Weil es beim Auslesen der PIN-Prüfsumme aus dem dritten Magnetstreifen häufig zu Leseproblemen gekommen ist, entfällt in den meisten Softwareversionen inzwischen der lokale Abgleich der PIN-Prüfsummen. Die verschlüsselte PIN wird dann direkt an den Bankserver versandt.

In einigen Fällen wurde die PIN direkt bei der Eingabe am Tastenfeld, noch bevor sie verschlüsselt wurde, von einem Keylogger abgegriffen, der alle Tastatureingaben mitschneidet. Die Kontoinformationen wurden von der Schadsoftware vom Überprüfungsalgorithmus der Geldautomatensoftware übernommen.

Der Sicherheitsexperte *Vanja Svajcer* fand heraus, dass von diesem Computervirus nur Geldautomaten betroffen waren, deren Steuerungs-PC mit dem Betriebssystem Windows-XP betrieben wurden. Und der Schweizer Sicherheitsexperte *Candid Wüest* hat Indizien zusammengetragen, die darauf schließen ließen, dass die Infektion der Automatensoftware mit diesem Computervirus über die Wartungsschnittstelle der Geldautomaten sowohl via USB-Stick als auch über den Anschluss eines Laptop an die Service-Schnittstelle erfolgt sein müsse.

Die Geldautomatenhersteller reagierten darauf, verlegten die Wartungsschnittstelle und tarnten sie zudem besser. Doch noch immer weisen zahlreiche Geldautomaten öffentlich leicht zugängliche Service-Schnittstellen auf, die unzureichend geschützt sind und einen Spionageangriff auf Kunden- und Kartendaten zulassen. Einer Skimming-Attacke direkt vom Steuerungs-PC des Geldautomaten ist der Karteninhaber jedenfalls hilflos ausgeliefert.

Schwierigkeiten bereitet den Kreditinstituten das Skimming mit modernen Aufsatzgeräten, Wärmesensoren oder Kameras. Ein falscher Kartenleser wird dabei vor den eigentlichen Automatenleser gehängt. Wenn der nichts ahnende Karteninhaber seine Zahlungskarte einschiebt, werden die drei Magnetspuren vom Lesegerät des Kriminellen ausgelesen und die Kontendaten samt Hashwert für die PIN an ein Handy oder ein in der Nähe befindliches Notebook der Datenspione übermittelt.

Die PIN-Eingabe wird entweder mit einer über das Tastenfeld eingehängten Minikamera aufgezeichnet oder von einer Aufsatztastatur, die direkt über das eigentliche Tastenfeld geklebt oder gesteckt wird, protokolliert und ebenfalls an ein Handy oder ein Notebook gesendet. Auch Minikameras zur Aufzeichnung der PIN-Eingabe werden von der organisierten Kriminalität eingesetzt, ebenso Wärmebildsysteme, mit denen auf Grund der unterschiedlichen Wärmerestabstrahlung die Reihenfolge der gedrückten Tasten bei der PIN-Eingabe nachvollzogen werden können.

3. Atypische Fälle

Daneben existieren die atypischen Fälle. Zu denen gehört eine in Betracht zu ziehende Innentäterattacke, bei der Täter mit Insiderwissen der kartenausgebenden Stelle Tathandlungen vornehmen, oder die Fälle, bei denen die Postwurfsendung mit der darin enthaltenen PIN abgefangen wird. Solche Fälle sind allerdings selten. Noch wesentlich unwahrscheinlicher und damit außer Betracht bleibt der Fall des zufälligen Erratens der PIN, für den es nur eine äußerst geringe Wahrscheinlichkeit gibt, zumal regelmäßig auch nur drei Versuche zur Verfügung stehen.

4. Grobe Fahrlässigkeit des Karteninhabers

Vollständig ist die Auflistung der denkbaren Möglichkeiten und Tatvarianten beim Abgreifen von Bankzugangsdaten am Beispiel der Kartenzahlungs-Fälle erst, wenn man auch das offenkundig für manchen Karteninhaber unentbehrliche Notieren der PIN auf oder in der räumlichen Nähe der Zahlungskarte als weitere Möglichkeit dafür in Betracht zieht, wie die Täter beim Diebstahl der Zahlungskarte zugleich an die für nicht autorisierte Verfügungen nötige PIN kommen können. Handelte der Karteninhaber gar mit den Tätern gemeinsam, liegt bereits keine nicht autorisierte Zahlung vor, sondern eine Vorsatztat des Karteninhabers.

IV. Konsequenzen für die Anwendbarkeit des Anscheinsbeweises

Wenn der *BGH* in seinem Urteil vom 29. 11. 2011 darlegt, dass die in älterer Rechtsprechung gewonnenen Erkenntnisse zum Anwendungsbereich des Prima-facie-Beweises nichts beitragen, sofern den heutigen „Kartenverfügungen neue oder wesentlich geänderte technische Verfahren zu Grunde liegen“[21], wird man in diesem Zusammenhang auch einen Blick auf die bekannt gewordenen Fallzahlen werfen müssen. Eine Zunahme der Fallzahlen könnte dafür sprechen, dass sich die oben beschriebenen Arten des Abgreifens von Bankzugangsdaten inzwischen als lukratives Strafszenario entwickelt haben. Auch dies spricht eher gegen die Annahme des Prima-facie-Beweises, der pauschal stets dem Karteninhaber ein grob fahrlässiges Verhalten unterstellt.

Die vom Bundeskriminalamt herausgegebenen Polizeilichen Kriminalstatistiken weisen seit Jahren steigende Fallzahlen auf. Die Fälle des Betrugs mittels rechtswidrig erlangter Daten von Zahlungskarten stiegen von 10 124 in der Kriminalstatistik erfassten Fälle für das Jahr 2008 auf 17 072 Fälle im Jahr 2009 an. Das ist eine Steigerung von 68,6%! Die Aufklärungsquote sank dagegen von 41,2% im Jahr 2008 auf nur noch 30,1% im Jahr 2009[22]. Die Fälle des Betrugs mittels rechtswidrig erlangter Kreditkarten sind in dieser Summe noch gar nicht enthalten, ebenso wenig die Dunkelziffer. Im Jahr 2010 stiegen die Fälle des Betrugs mittels rechtswidrig erlangter Daten von Zahlungskarten dann auf 19 100 Fälle an, was einer erneuten Zunahme von 11,9% im Vergleich zu 2009 entspricht. Die Aufklärungsquote sank nunmehr auf 27,3% ab[23]. Das Bundeskriminalamt führt die Zunahme der Fallzahlen unter anderem auf die Zunahme der so genannten „Skimming-Fälle“ zurück[24].

Solange vor diesem Hintergrund die Möglichkeit nicht ausgeschlossen werden kann, dass bei nicht autorisierten Zahlungsverfügungen am Geldautomaten die Ursache für das Abgreifen der PIN gerade nicht darin liegen muss, dass der jeweilige Karteninhaber seine PIN auf der Karte oder in der unmittelbaren räumlichen Nähe zur Karte notiert hat, rechtfertigt dies gerade nicht die Annahme eines Anscheinsbeweises. Es ist nämlich gut möglich, dass gerade der vom Gericht zu entscheidende Fall die Ausnahme darstellt. Deshalb hatte der *BGH* die mit dem Anscheinsbeweis verbundene Beweiserleichterung früher vergleichsweise selten zugelassen. In einer Entscheidung aus dem Jahre 1957 hat der *II. Zivilsenat-*

20 *Welchering*, FAZ v. 3. 5. 2011, S. T1.
21 *BGH*, NJW 2012, 1277.
22 BKA, Polizeiliche Kriminalstatistik 2009, 4.
23 BKA, Polizeiliche Kriminalstatistik 2010, 4.
24 BKA, Polizeiliche Kriminalstatistik 2009, 7.

den Anscheinsbeweis zu Gunsten eines Briefsenders für den Zugang von Einschreiben abgelehnt, weil in 266,6 von einer Million Fällen Einschreiben verloren gingen[25].

V. Zusammenfassung

Die aktuelle Entwicklung der Kriminalität und die technischen Möglichkeiten der Täter werfen bei den Fällen nicht autorisierter Zahlungsverfügungen am Geldautomaten die Frage auf, ob die Grundsätze der Beweiserleichterung durch den Anscheinsbeweis noch anwendbar sind, wenn Täter mit der Originalkarte Abhebungen vorgenommen haben. Bei den Geldautomaten-Fällen kommen inzwischen zu viele andere Möglichkeiten in Betracht, wie die Täter an die korrekte PIN kommen konnten. Das Spektrum reicht von Innentäterattacken über eine Manipulation des Kartensystems über Skimming (Ausspähung der PIN) oder der Manipulation von Kartenterminals in Geschäften, in denen bargeldlos bezahlt werden kann. Alleine die Tatsache, dass die Zahlungskarte mit der korrekten PIN verwendet wurde, vermag gegenwärtig nicht (mehr) den Beweis des ersten Anscheins dafür zu begründen, dass der Karteninhaber mit seiner Karte nicht sorgfältig umgegangen ist[26]. Die Weiterentwicklung der Kartensysteme hin zu dem EMV-Chip löst das Problem nicht wirklich. Für die Frage, wie die Täter an die PIN gekommen sind, ist es entscheidend, dass die statische PIN händisch durch den autorisierten Karteninhaber einzugeben ist und durch Dritte abgefangen werden kann.

Dem Urteil des *BGH* vom 29. 11. 2011 ist zu entnehmen, dass sich der *XI. Zivilsenat* den technischen Möglichkeiten der Täter keineswegs verschließt. Der Lösungsansatz des *BGH* liegt darin, dass er zwar einerseits den Prima-facie-Beweis unter bestimmten Voraussetzungen bei nicht autorisierten Zahlungsverfügungen mit der Original-Karte weiterhin für anwendbar erachtet. Andererseits legt er hierzu den kartenausgebenden Stellen Pflichten auf. Sie werden an die Vorlage von technischen Aufzeichnungen denken müssen bzw. nunmehr Angaben über die Qualität des Sicherheitssystems unter Einbeziehung des Geldautomaten, von dem die Verfügung getätigt wurde, vortragen müssen. Das ist kein einfaches Unterfangen, wenn die kartenausgebende Stelle und der Betreiber des Geldautomaten verschiedene Personen sind. Die Eingangsgerichte wurden aufgerufen, ihrer Pflicht zur sachgerechten Beweisaufnahme und gegebenenfalls zur Parteivernehmung des Karteninhabers zu genügen. ■

25 *BGHZ* 24, 308 (312) = NJW 1957, 1230.

26 In diese Richtung ebenfalls *AG Dortmund*, Urt. v. 26. 3. 2002 – 127 C 8948/02; *LG Berlin*, NJW-RR 1999, 1213; *LG Osnabrück*, NJW-RR 2003, 1283; *AG Berlin-Mitte*, Urt. v. 7. 10. 2002 – 20 C 59/02; NJW-RR 2010, 407.