Anmerkung zu:	BGH 11. Zivilsenat, Urteil vom 29.11.2011 - XI ZR 370/10	**Quelle:**	juris
Autoren:	Dr. Anna-Maria Beesch, RA'in und FA'in für Bank -und Kapitalmarktrecht, Dr. Claudia Willershausen, RA'in und Justiziarin	**Normen:**	§ 1 ZAG, § 675u BGB, § 675j BGB, § 675v BGB, § 675c BGB, § 676c BGB, § 675m BGB, § 284 ZPO, § 281 ZPO, § 411a ZPO, § 675w BGB, § 675l BGB
Erscheinungsdatum:	20.09.2012	**Fundstelle:**	jurisPR-BKR 9/2012 Anm. 1
		Herausgeber:	Prof. Dr. Stephan Meder, Universität Hannover Dr. Anna-Maria Beesch, RA'in und FA'in für Bank- und Kapitalmarktrecht
		Zitiervorschlag:	Beesch/Willershausen, jurisPR-BKR 9/2012 Anm. 1

Bedeutung der zu unterscheidenden Schadens-Fallgruppen Lost/Stolen vs. Skimming und deren Klärbarkeit bei Anwendung des neuen Zahlungsdiensterechts und der Anscheinsbeweis-Grundsätze im Zahlungskartenrecht

A. Einleitung

In vielen Rechtsstreitigkeiten, die Zahlungskartenemittenten (im neuen Zahlungsdiensterecht der §§ 675c bis 676c BGB „Zahlungsdienstleister“ genannt) und Karteninhaber („Zahler“ bzw. „Zahlungsdienstnutzer“) in Schadensfällen aufgrund von Missbrauchseinsätzen von Zahlungskarten nebst PIN an Geldautomaten und POS-Terminals austragen, wird von Rechtsanwendern wie Kommentatoren verkannt, dass zwingend zwischen den sog. Lost/Stolen-Fällen und den sog. Skimming-Fällen zu differenzieren ist, da sie jeweils unterschiedlichen Rechtsfolgen unterliegen. Schäden infolge von Skimming werden von der Kreditwirtschaft anstandslos reguliert. Hingegen greift in der Lost/Stolen-Fallgruppe, für die im Grundsatz die herrschende Anscheinsbeweis-Rechtsprechung im Zahlungskartenrecht entwickelt wurde, die volle Schadenshaftung der Karteninhaber ein, wenn sie ihnen obliegende Sorgfaltspflichten im Umgang mit Zahlungskarte und/oder PIN grob fahrlässig verletzt haben (jetzt: §§ 675l, 675v Abs. 2, 675w BGB).

Die erforderliche Unterscheidung der Fallgruppen (Lost/Stolen vs. Skimming) fehlt auch im Aufsatz von Schulte am Hülse/Welchering (NJW 2012, 1262), einhergehend mit einer darauf beruhenden irreführenden und unzulässigen Vermengung der Fallgruppen und deren Fallzahlen. Dem Aufsatz ist aus mehreren Gründen, insbesondere wegen unrichtiger Darstellungen und technischer Fehlinformationen, zu widersprechen. Zugleich erfolgen Anmerkungen zum neuen Urteil des XI. Zivilsenats des BGH vom 29.11.2011 (XI ZR 370/10 - NJW 2012, 1277), in dem er seine bisherige Anscheinsbeweis-Rechtsprechung nicht geändert, sondern nur konkretisiert hat. Der Gang der Darstellung folgt im Wesentlichen derjenigen des Aufsatzes von Schulte am Hülse/Welchering (NJW 2012, 1262).

I. Begriffliche Klarstellungen

Vorangestellt seien einige begriffliche Klarstellungen:

Zahlungskarten – Karten, die vom Kunden vertragsgemäß eingesetzt werden können, um einen Zahlungsauftrag zu erteilen (Maihold in: Schimansky/Bunte/Lwowski, Bankrechtshandbuch, Bd. 1, 4. Aufl. 2011, § 54 Rn. 12), namentlich Debitkarten (ec-Karten bzw. heute girocards) und Kreditkarten; Zahlungskarten mit zugehöriger persönlicher Geheimzahl (PIN) als personalisiertes Sicherheitsmerkmal sind gemäß § 1 Abs. 5 ZAG Zahlungsauthentifizierungsinstrument. Die Darstellung beschränkt sich auf Missbrauchseinsätze mit Zahlungskarte und PIN.

Lost/Stolen-Fälle bzw. Verlust-Fälle – Gestohlene oder anderweitig abhanden gekommene bzw. zeitweise entwendete Zahlungskarten werden von unberechtigten Dritten unter Verwendung der zugehörigen PIN für missbräuchliche Verfügungen am Geldautomaten oder POS-Terminal (Point-of-Sale-Terminal im Handel) eingesetzt. Bei diesen Fällen kommt ausschließlich die Originalkarte zum Einsatz. Die Darstellung beschränkt sich auf Missbrauchsfälle mit Zahlungskarte und PIN.

Skimming-Fälle bzw. Kartendubletten-Fälle – Von Skimming (hergeleitet von „to skim" = „abschöpfen") spricht man, wenn die auf dem Magnetstreifen einer Karte befindlichen Daten an manipulierten Geldautomaten, POS-Terminals oder Türöffnern mit Hilfe von sogenannten Skimmingmodulen gelesen, die PIN ausspioniert und danach die Karte dupliziert wird, d.h. mit den gewonnenen Kartendaten Kartendubletten gefertigt werden. Diese werden nebst ausspionierter PIN für missbräuchliche Verfügungen durch die Täter an Geldautomaten oder POS-Terminals eingesetzt, während die Original-Zahlungskarte im Besitz des Karteninhabers verbleibt.

II. Richtigstellung der relevanten Fallzahl-Entwicklungen

Ebenso jedoch wie die Sachverhalte der zu unterscheidenden Fallgruppen nicht in einen Topf geworfen werden können, verbietet es sich, die in den einzelnen Fallgruppen unterschiedlichen Entwicklungen von Fallzahlen und Schäden zu vermengen und daraus eine „aktuelle Kriminalitätsentwicklung" mit „seit Jahren steigenden Fallzahlen" zu konstruieren, die es so (vgl. NJW 2012, 1262, 1265) nicht gibt.

Um zu einem adäquaten Ergebnis bei der Betrachtung der Anzahl der Fälle von Kartenmissbräuchen und deren Entwicklung zu kommen, muss bereits unterschieden werden zwischen den verschiedenen Tathandlungen. So differenziert z.B. das Bundeskriminalamt (BKA) in seiner jährlichen Kriminalstatistik zwischen „Betrug mittels rechtswidrig erlangter Debitkarten ohne PIN (Lastschriftverfahren)", „Betrug mittels rechtswidrig erlangter Kreditkarten" und „Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten".

Irreführend und unzulässig ist jedenfalls eine zusammenfassende Datenmaterial-Auswertung, wie sie durch Schulte am Hülse/Welchering (NJW 2012, 1262) vorgenommen wird. Dies gilt vor allem deshalb, weil die von ihnen in Frage gestellte Anscheinsbeweis-Rechtsprechung zwar in Fällen abhanden gekommener Zahlungskarten (Lost/Stolen-Fälle) zur Anwendung kommt, nicht hingegen in Skimming-Fällen. Damit ist im Zusammenhang mit der Frage der (weiteren) Anwendbarkeit des Anscheinsbeweises allein die Fallzahlen-Entwicklung in der Fallgruppe Lost/Stolen relevant, nicht hingegen die Entwicklung der Anzahl der Fälle, in denen Kartendaten rechtswidrig eingesetzt werden.

Analysiert man die Fallzahlentwicklungen in den zu unterscheidenden Fallgruppen Lost/Stolen und Skimming, so lässt sich die These von Schulte am Hülse/Welchering, aufgrund der aktuellen Kriminalitätsentwicklung sei der Anscheinsbeweis nicht (mehr) begründet, nicht halten.

Dass die einzelnen Fallgruppen eine unterschiedliche Fallzahlen- und Schadens-Entwicklung aufweisen, zeigt sich anhand der folgenden differenzierten Auswertungen für Debitkarten (Quelle: EURO Kartensysteme GmbH, www.kartensicherheit.de):

Lost/Stolen Debitkarten	2006	2007	2008	2009	2010	2011
Fälle (d.h. betroffene Karten am Geldautomat (POS-Terminal) mit PIN-Einsatz)	12.963 (1.955)	11.481 (1.731)	10.045 (1.589)	14.357 (2.276)	11.846 (1.912)	11.924 (1.755)
Schaden (Schäden an Geldautomaten und POS-Terminals mit PIN im Inland und Ausland)	16,8 Mio. Euro	17,2 Mio. Euro	13,3 Mio. Euro	19,9 Mio. Euro	16,6 Mio. Euro	15,8 Mio. Euro

Diese Zahlen zeigen deutlich, dass von einer Zunahme der missbräuchlichen Einsätze von abhanden gekommenen Debitkarten (Lost/Stolen Debitkarten) nicht gesprochen werden kann. Vielmehr stagniert

die Anzahl derartiger Missbrauchsfälle in den letzten sechs Jahren, wie auch zuvor, auf etwa gleichem Niveau.

Eine ähnliche Entwicklung mit nahezu konstanten Fallzahlen zeigt sich für abhanden gekommene Kreditkarten (Lost/Stolen Kreditkarten) in den Veröffentlichungen des BKA. Die polizeiliche Kriminalstatistik, jeweils für die Jahre 2006 bis 2010, weist folgende Zahlen aus: für das Jahr 2006: 8.932 Fälle, für das Jahr 2007: 9.271 Fälle, für das Jahr 2008: 7.940 Fälle, für das Jahr 2009: 8.971 Fälle und für das Jahr 2010: 8.974 Fälle (vgl. BKA Polizeiliche Kriminalstatistik 2007, S. 3, BKA Polizeiliche Kriminalstatistik 2009, S. 4, und BKA Polizeiliche Kriminalstatistik 2010, S. 4).

Nur in der BKA-Kategorie „Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten“, der auch die Skimming-Schäden unterfallen, finden sich in den letzten Jahren bis 2010 die Fallzahlzunahmen in den Veröffentlichungen des BKA (Polizeiliche Kriminalstatistiken), die von Schulte am Hülse/Welchering (NJW 2012, 1262, 1265 Fn. 22 bis 24) angeführt werden (2008: 10.124 Fälle, 2009: 17.072 Fälle, 2010: 19.100 Fälle). Hervorzuheben ist allerdings, dass in den Fallzahlen dieser Kategorie sowohl Skimming-Schäden als auch Internet-Schäden zu allen Zahlungskarten (Debit und Kredit) zusammengefasst sind; auf Internet-Schäden, die eine nochmals gesondert zu betrachtende Fallgruppe sind, wird hier nicht eingegangen. So erläutert das BKA, dass die Fallzahl-Zunahme in dieser Kategorie „unter anderem“ auf „Serientaten mit Gebrauch sogenannter Dublettenkarten“ zurückzuführen sei, jedoch „vor allem“ in der generell gestiegenen Nutzung des Mediums Internet, über welches Kartendaten bei den verschiedenen Transaktionen erlangt werden können, begründet sei (BKA, Polizeiliche Kriminalstatistik 2009, S. 7). Die BKA-Statistik sagt jedoch nichts darüber aus, welchen Anteil die Internet-Schäden und die Skimming-Schäden am Gesamtanstieg der Fallzahlen in dieser Kategorie hatten.

III. Markanter Fallzahlen-Rückgang bei Skimming-Fällen seit Einsatz der EMV-Chip-Technologie ab Anfang 2011

Selbst bei den Skimming-Schäden sind tatsächlich nicht nur Fallzahlzunahmen festzustellen. Vielmehr ist zu betonen, dass die Missbrauchsschäden mit geskimmten deutschen Debitkarten im Jahr 2011 markant um ca. 43% abgenommen haben. Insbesondere war im Jahr 2011 ein starker Rückgang der Geldautomatenmanipulationen im Inland zu verzeichnen. Von den rund 60.000 Geräten wurden nur 775 Geräte, d.h. nur ca. 1% der Geräte, manipuliert; gegenüber dem Jahr 2010 bedeutet dies einen Rückgang um 55% (vgl. Debit-Statistik Gesamtjahr 2011, abrufbar unter: https://www.kartensicherheit.de/de/pub/oeffentlich/newsletter/newslettermeldungen/archiv_2012/debit_statistik_2011.php).

Hauptgrund für den Rückgang der durch Skimming verursachten Schäden war vor allem die europaweite Einführung des EMV-Sicherheitsstandards seit Anfang des Jahres 2011). Hiervon profitiert nicht nur die deutsche Kreditwirtschaft. Auch europaweite Statistiken zu Schadensfällen im Zahlungskartensegment weisen eine starke Abnahme der Schadensfälle auf; auch dort wird dies mit der Einführung der EMV-Chip-Technologie für alle Zahlungskarten begründet (vgl. EAST-Statistik 2011, abrufbar unter: www.european-atm-security.eu; vgl. auch Europäische Zentralbank (EZB), Report on Card Fraud, July 2012.).

B. Rechtslage bei nicht autorisierten Transaktionen

I. Erstattungsanspruch des Karteninhabers (§§ 675u, 675w BGB)

Zunächst gehen Schulte am Hülse/Welchering (NJW 2012, 1262) zutreffend davon aus, dass unter dem neuen Zahlungsdiensterecht nunmehr § 675u Satz 2 BGB die gesetzliche Anspruchsgrundlage für den Erstattungsanspruch bildet, der einem Zahlungsdienstnutzer (= Karteninhaber, Zahler, Kunde) gegen seinen Zahlungsdienstleister (= Kartenemittent) bei Fehlen der (An-)Weisung des Zahlungsdienstnutzers bzw. bei Wirksamkeitshindernissen zusteht.

1. Anspruchsvoraussetzung: „Vorliegen“ eines nicht autorisierten Zahlungsvorgangs

Jedoch ist, was vielfach übersehen wird, Anspruchsvoraussetzung des § 675u Satz 2 BGB, dass unbestrittenermaßen ein „nicht autorisierter Zahlungsvorgang“ gemäß § 675u Satz 1 BGB vorliegt. Für das Vorliegen aller Voraussetzungen eines Erstattungsanspruchs gemäß § 675u Satz 2 BGB ist grundsätzlich der Zahlungsdienstnutzer darlegungs- und beweispflichtig, wozu gehört, dass er den Zahlungsvorgang nicht autorisiert hat.

2. Eingreifen des § 675w BGB bei streitigen Autorisierungen

Besteht allerdings gerade Streit darüber, ob ein „autorisierter“ oder „nicht autorisierter“ Zahlungsvorgang vorliegt, greift § 675w BGB ein. Die einfache Behauptung des Zahlungsdienstnutzers, nicht auto-

risiert zu haben, genügt nicht; hierzu ist qualifizierter Vortrag und Nachweis des Zahlungsdienstnutzers erforderlich.

3. Neue gesetzliche – durch Dokumentation verstärkte – Beweisvermutungen des § 675w BGB

Für die Darlegungs- und Beweislast bei streitigen Autorisierungen mittels eines Zahlungsauthentifizierungsinstruments bzw. -verfahrens ausgelöster Zahlungsvorgänge (z.B. Debit- oder Kreditkarte mit PIN) greifen auch hier (wie bei § 675v BGB) die neuen gesetzlichen – durch Dokumentation verstärkten – Beweisvermutungen des § 675w BGB (Beweisvermutung der Autorisierung des Zahlungsvorgangs gemäß § 675w Satz 2 und Satz 3 Nr. 1 BGB und Beweisvermutung grob fahrlässiger Pflichtverletzung gemäß § 675w Satz 2 und Satz 3 Nr. 3 BGB), jedenfalls die im Zahlungskartenrecht entwickelten (Anscheins-)Beweisgrundsätze ein (weiterführend vgl. Beesch in: NK-BGB, 2.Aufl. 2012, § 675u Rn 1 ff, §§ 675v-w Rn. 23 ff, Rn. 27, Rn. 29 ff, Rn. 36 ff, m.w.N.).

Der Dokumentation der Zahlungsvorgänge kommt somit eine größere praktische Bedeutung als nach bisherigem Recht zu, da durch die neuen gesetzlichen Beweisvermutungen des § 675w BGB zugunsten des Zahlungsdienstleisters zunächst alles dafür spricht, dass die dem Zahlungsdienstnutzer zuzuordnende Autorisierung der streitigen Zahlungsvorgänge vorliegt, und zwar entweder durch ihn selbst oder durch eine von ihm autorisierte Person (§ 675w Satz 2 und Satz 3 Nr. 1 BGB) oder durch einen unbefugten Dritten aufgrund grob fahrlässiger Verletzung der Pflichten des § 675l BGB bzw. vertraglicher Sorgfaltspflichten (§ 675w Satz 2 und Satz 3 Nr. 3 BGB) (Beesch in: NK-BGB, §§ 675v-w Rn. 27 f.). Dies ist auch sachlich auf der Basis des Grundsatzes gerechtfertigt, dass sich die Beweislastverteilung an den Verantwortungsbereichen von Schuldner und Gläubiger zu orientieren hat (Grüneberg in: Palandt, BGB, 71. Aufl. 2012, § 280 Rn. 37; Sprau in: Palandt, BGB, 71. Aufl. 2012, § 675v Rn. 7 und § 675w Rn. 4; Beesch in: NK-BGB, §§ 675v-w Rn. 27 f., Rn. 40; Willershausen, jurisPR-BKR 11/2010 Anm. 6).

Inhalt der geforderten Dokumentation sind u.a. die Informationen, die auch der positiven Genehmigung der jeweiligen Transaktion seitens des Zahlungsdienstleisters zu Grunde lagen, d.h. solche Informationen, aus denen der Zahlungsdienstleister entnehmen konnte, dass das Zahlungsauthentifizierungsinstrument mit den hierfür vorgesehenen Autorisierungs- und Authentifizierungskomponenten genutzt wurde. Der Zahlungsdienstleister liefert mit der Dokumentation der Zahlungsvorgänge alles, was er aus seinem Gefahrenkreis heraus zu beschaffen in der Lage ist, wozu ihn § 675w BGB verpflichtet, und was gemäß § 675w BGB zunächst zum Nachweis der Nutzung des Zahlungsauthentifizierungsinstruments bzw. -verfahrens (Autorisierung, § 675j BGB) einschließlich der Authentifizierung genügt (BT-Drs. 16/11643, S.114 zu § 675w BGB; Sprau in: Palandt, BGB, § 675w Rn. 2; Omlor in: Staudinger, BGB, §§ 675c-676c Zahlungsdiensterecht, 2012, § 675w Rn. 4; Nobbe, WM 2011, 961, 968; Meckel, jurisPR-BKR 2/2010 Anm. 1; Beesch in: NK-BGB, §§ 675v-w Rn. 23 ff., Rn. 27 f.).

4. Widerleglichkeit der neuen gesetzlichen Beweisvermutung(en)

Will der Karteninhaber die Beweisvermutung(en) des § 675w BGB anzweifeln, ist zur Widerlegung (wie auch zur Entkräftung des Anscheinsbeweises) vom Karteninhaber konkreter und substantiierter Vortrag und Nachweis dazu erforderlich, dass es sich um einen nicht autorisierten Zahlungsvorgang handelt. Der – nunmehr auch durch die Neufassung des § 675w BGB – anerkannte Rechtsgrundsatz, dass sich die Beweislastverteilung auch an den Verantwortungsbereichen von Schuldner und Gläubiger zu orientieren hat, liefe ansonsten leer (Grüneberg in: Palandt, BGB, § 280 Rn. 37; Sprau in: Palandt, BGB, § 675v Rn. 7; Beesch in: NK-BGB, §§ 675v, 675w Rn. 36; Lohmann/Koch, WM 2008, 57, 63; Grundmann, WM 2009, 1157, 1163; Meckel, jurisPR-BKR 2/2010 Anm. 1; Willershausen, jurisPR-BKR 4/2010 Anm. 6; Willershausen, jurisPR-BKR 11/2010 Anm. 6; vgl. bereits BGH, Urt. v. 22.10.2008 - XII ZR 148/06 - NJW 2009, 142; OLG Stuttgart, Urt. v. 13.03.2002 - 9 U 63/01 - NJW-RR 2002, 1274; vgl. auch LG Frankfurt am Main, Urt. v. 14.07.2004 - 2/1 S 248/03 und Urt. v. 14.05.2003 - 2/1 S 1/03; BGH, Urt. v. 05.10.2004 - XI ZR 210/03 - BGHZ 160, 308 = NJW 2004, 3623; OLG Frankfurt am Main, Urt. v. 30.03.2006 - 16 U 70/05 - NJW-RR 2007, 198 (abrufbar unter www.dr-beesch.de/urteile), und OLG Frankfurt am Main, Urt. v. 07.05.2002 - 8 U 268/01 - WM 2002, 2101 = WuB I D 5 a Kreditkarte 1.03 m. Anm. Meder).

II. (Gegen)-Schadensersatz-Anspruch des Kartenemittenten (§ 675v Abs. 2 BGB)

1. Grundlagen

Schulte am Hülse/Welchering gehen zwar noch zutreffend davon aus, dass im Missbrauchsfall dem Kartenemittenten ein Schadensersatzanspruch gemäß § 675v Abs. 2 BGB zusteht, wenn der Karteninhaber grob fahrlässig seine Pflicht(en) aus dem Zahlungsdienste(rahmen)vertrag verletzt hat (NJW 2012, 1266, 1263). Jedoch wird in der Folge zur Frage der Beweislastverteilung auf abzulehnende – und auf altem Recht beruhende – Mindermeinungen abgestellt, die herrschende Meinung in Literatur und Recht-

sprechung nur unzureichend dargestellt und das neue Zahlungsdiensterecht der §§ 675c bis 676c BGB verkannt.

Die grob fahrlässige Verletzung der Pflicht des Karteninhabers zur Geheimhaltung der PIN ist nach neuem Zahlungsdiensterecht gemäß § 675l i.V.m. § 675w Satz 2 und Satz 3 Nr. 3 BGB bei hinreichender vorgelegter Transaktionsdokumentation – widerleglich – gesetzlich zu vermuten (vgl. weiterführend Beesch in: NK-BGB, §§ 675v-w Rn. 27, Rn. 29 ff., m.w.N.).

Jedenfalls besteht nach h.M. in Literatur und Rechtsprechung auch nach neuem Zahlungsdiensterecht neben dem Anscheinsbeweis der Zahlerautorisierung der Anscheinsbeweis grob fahrlässiger Pflichtverletzung(en) des Karteninhabers im Umgang mit Zahlungskarte und PIN. Die bereits nach altem Recht entwickelten Anscheinsbeweis-Grundsätze gelten damit auch nach neuer Gesetzeslage fort. Somit kann davon ausgegangen werden, dass ein unbefugter Dritter zeitnah nach einer Entwendung oder dem sonstigen Abhandenkommen der Karte an Geldautomaten Bargeld unter Verwendung dieser Karte und Eingabe der richtigen PIN nur deswegen abheben kann, weil der Karteninhaber die PIN auf der Zahlungskarte notiert oder gemeinsam mit dieser aufbewahrt hat, wenn andere Ursachen für den Missbrauch nach der allgemeinen Lebenserfahrung ausscheiden (vgl. BVerfG, Beschl. v. 08.12.2009 - 1 BvR 2733/06 - NJW 2010, 1129, 1130 = WM 2010, 208, 209 m. Anm. Martinek/Omlor, WuB I D 5 b Debit-Karte 1.10; BGH, Urt. v. 29.11.2011 - XI ZR 370/10 - WM 2012, 164; Grundsatzurteil des BGH v. 05.10.2004 - XI ZR 210/03 - BGHZ 160, 308 = NJW 2004, 3623; BGH, Beschl. v. 06.07.2010 - XI ZR 224/09 Rn.10 - WM 2011, 924 m. Anm. Meder, WuB I D 5 a Kreditkarte 1.11; OLG Karlsruhe, Urt. v. 21.10.2008 - 17 U 222/07 - WM 2009, 1549, 512 m. Anm. Willershausen, jurisPR-BKR 8/2009 Anm. 5; OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 - WM 2008, 534 m. Anm. Meder/Flick, WuB I D 5 b Debit-Karte 1.08; OLG Brandenburg, Urt. v. 07.03.2007 - 13 U 69/06 - WM 2007, 2193; vgl. LG Berlin, Urt. v. 22.06.2010 - 10 S 10/09 - WM 2010, 2353 – unter Aufhebung von AG Berlin-Mitte, Urt. v. 25.11.2009 - 21 C 442/08 - NJW-RR 2010, 407 m. Anm. Willershausen, jurisPR-BKR 11/2010 Anm. 6; AG Frankfurt am Main, Urt. v. 10.11.2010 - 29 C 1461/10 - 85 - WM 2011, 496 m. Anm. Richrath, WuB I D 5 b Debitkarte 2.11; AG Hamburg, Urt. v. 28.09.2010 - 4 C 178/10 - WM 2011, 498 m. Anm. Richrath, WuB I D 5 b Debitkarte 2.11; AG München, Urt. v. 28.09.2011 - 233 C 3757/11 Rn. 16; vgl. Sprau in: Palandt, BGB, § 675w Rn. 4, m.w.N.; Werner in: Soergel, BGB, 13. Aufl. 2012, § 675v Rn. 13, 675w Rn. 8 ff., m.w.N.; Omlor in: Staudinger, BGB, §§ 675c-676c Zahlungsdiensterecht, 2012, § 675w Rn. 7; Beesch in: NK-BGB, §§ 675v-w Rn. 29 ff., Rn. 37 ff., m.w.N.; Maihold in: Schimanski/Bunte/Lwowski, Bankrechts-Handbuch, § 54 Rn. 49, 108, 111; Nobbe in: Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, 2010, § 675w Rn. 25 ff., Rn. 30, Rn. 33, Rn. 46, jew. m.w.N.; Werner in: Hellner/Steuer, Bankrecht und Bankpraxis, Bd. 3 unter 6/1463 ff., m.w.N.; Bunte, AGB-Banken und Sonderbedingungen, 3. Aufl. 2011, SB girocard Rn. 79 fn; Langenbucher/Gößmann/Werner, Zahlungsverkehr, 2010, § 3 Rn. 56; Casper in: MünchKomm BGB, 5. Aufl. 2009, § 676h Rn. 34; Kollrus, MDR 2012, 377, 378; Haertlein, WuB I D 5 a. Kreditkarte 1.12; Nobbe, WM 2011, 961, 968; Zwade/Mühl, WM 2006, 1225, 1228, m.w.N.; Oechsler, WM 2010, 1381; Casper/Pfeifle, WM 2009, 2343, 2347; Grundmann, WM 2009, 1157, 1163).

Dies gilt gleichermaßen für ec-Karten (girocards) wie auch für Kreditkarten, für die eine entsprechende h.M. und feststehende PIN-Anscheinsbeweis-Rechtsprechung etabliert ist (vgl. BGH, Urt. v. 29.11.2011 - XI ZR 370/10 - WM 2012, 164; BGH, Beschl. v. 06.07.2010 - XI ZR 224/09 - WM 2011, 924 m. Anm. Meder, WuB I D 5 a. Kreditkarte 1.11; OLG Brandenburg, Urt. v. 07.03.2007 - 13 U 69/06 - WM 2007, 2193; OLG Frankfurt am Main, Urt. v. 30.03.2006 - 16 U 70/05 - NJW-RR 2007, 198; OLG Frankfurt am Main, Beschl. v. 15.07.2003 - 19 U 71/03 - NJW-RR 2004, 206; OLG Frankfurt am Main, Urt. v. 07.05.2002 - 8 U 268/01 - WM 2002, 2101 m. Anm. Meder, WuB I D 5 a. Kreditkarte 1.03; Haertlein, WuB I D 5 a. Kreditkarte 1.12; LG Magdeburg, Beschl. v. 29.10.2009 - 2 S 312/09; AG Offenbach am Main, Urt. v. 31.05.2011 - 30 C 111/07 (abrufbar unter www.dr-beesch.de/urteile)).

Die wenigen die Ablehnung des Anscheinsbeweises vertretenden Gerichtsentscheidungen, die Schulte am Hülse/Welchering anführen (NJW 2012, 1262, 1263 und Fn. 8), sind Mindermeinungen – überdies noch zu alter überholter Technik vor 1998, 56-Bit-Schlüsselbreite – geblieben. Das neuere Urteil des LG Berlin vom 22.06.2010 (10 S 10/09 - NJW-RR 2011, 352 = WM 2010, 2353) wird in Fn. 8 unkorrekt mit „a.A.“ gegenüber dem AG Berlin-Mitte (Urt. v. 25.11.2009 - 21 C 442/08 - NJW-RR 2010, 407) zitiert, denn das AG Berlin-Mitte, das die Anwendbarkeit des Prima-facie-Beweises nach neuem Zahlungsdiensterecht ablehnte (vgl. hierzu Willershausen, jurisPR-BKR 11/2010 Anm. 6, sowie jurisPR-BKR 4/2010 Anm. 4), wurde vom LG Berlin, das die Fortgeltung des Anscheinsbeweises nach neuem Recht bejahte (vgl. hierzu Willershausen, jurisPR-BKR 11/2010 Anm. 6), aufgehoben.

Im Übrigen wird, was ebenfalls im Aufsatz von Schulte am Hülse/Welchering (NJW 2012, 1262, 1263 Fn. 8) nicht zum Ausdruck kommt, in den zum neuen Zahlungsdiensterecht ergangenen Entscheidungen der Instanzgerichte ausnahmslos die Fortgeltung des Anscheinsbeweises bejaht (AG München, Urt. v. 28.09.2011 - 233 C 3757/11 Rn. 16; AG Frankfurt am Main, Urt. v. 10.11.2010 - 29 C 1461/10 - 85 - WM

2011, 496 m. Anm. Richrath, WuB I D 5 b Debitkarte 2.11; AG Hamburg, Urt. v. 28.09.2010 - 4 C 178/10 - WM 2011, 498 m. Anm. Richrath, WuB I D 5 b Debitkarte 2.11). Das AG Dieburg (Urt. v. 27.07.2012 - 20 C 387/12 (26), nicht rechtskräftig), greift darüber hinausgehend die neue, durch Dokumentation verstärkte Beweisvermutung des § 675w Satz 2 und Satz 3 Nr. 1 BGB (Zahlerautorisierung) auf und sieht sie als durch das dortige Prozessvorbringen des Karteninhabers als nicht widerlegt an.

2. Typischer Geschehensablauf/Anknüpfungstatsachen

Nach h.M. in Literatur und höchstrichterlicher Rechtsprechung sind die Grundsätze des Beweises des ersten Anscheins bei typischen Geschehensabläufen anwendbar, d.h. in Fällen, in denen ein bestimmter Sachverhalt feststeht, der nach der allgemeinen Lebenserfahrung auf eine bestimmte Ursache oder einen bestimmten Ablauf als maßgeblich für den Eintritt eines bestimmten Erfolges hinweist. Im Zahlungskartenrecht besteht der typische Lebenssachverhalt darin, dass mit Zahlungskarten nebst PIN nur dann erfolgreich Geld am Geldautomaten abgehoben werden kann, wenn dies vom Karteninhaber selbst erfolgt, wenn der Karteninhaber Dritte dazu bevollmächtigt hat oder wenn unbefugte Dritte durch unsorgfältigen Umgang des Karteninhabers mit Kreditkarte und PIN an diese gelangt sind, insbesondere der Karteninhaber die PIN entweder auf der Karte notiert oder sie gemeinsam mit dieser aufbewahrt hat. Dabei bedeutet Typizität nicht, dass die Ursächlichkeit einer bestimmten Tatsache für einen bestimmten Erfolg bei allen Sachverhalten dieser Fallgruppe notwendig immer vorhanden ist; sie muss aber so häufig gegeben sein, dass die Wahrscheinlichkeit, einen solchen Fall vor sich zu haben, sehr groß ist (Grundsatzurteil des BGH v. 05.10.2004 - XI ZR 210/03 Rn. 22, 23 - NJW 2004, 3623).

Nach diesen Maßstäben greift der Beweis des ersten Anscheins zu Lasten eines Karteninhabers ein, dass er – wenn Geld am Automaten erfolgreich abgehoben werden konnte – seine persönliche Geheimzahl (PIN), die nur ihm bekannt ist und bekannt sein darf, entweder auf seiner Zahlungskarte notiert oder sie gemeinsam mit dieser aufbewahrt hatte (BGH v. 05.10.2004 - XI ZR 210/03 Rn. 24), wenn alle erforderlichen und die Typizität des Sachverhalts prägenden Anknüpfungstatsachen für die Anscheinsbeweisregel vorliegen:

- ursprünglicher Besitz (= Erhalt) der Original-Karte durch den Karteninhaber,
- Kenntnis des Karteninhabers von der ihm zugewiesenen PIN (Erhalt der PIN),
- nachfolgender Diebstahl bzw. Verlust bzw. sonstiges, evtl. auch nur zeitweises Abhandenkommen der Karte,
- zeitnah nach dem Abhandenkommen der Karte erfolgte erfolgreiche Bargeldauszahlung mittels Karte und PIN am Geldautomaten.

3. Ausnahme: Atypischer Geschehensablauf

Ausnahmen vom typischen Geschehensablauf können nach zutreffender h.M. in Literatur und Rechtsprechung nur dann in Betracht kommen, wenn der Karteninhaber „Tatsachen“ schlüssig und substantiiert darlegt und gegebenenfalls beweist, die die ernsthafte, ebenfalls in Betracht kommende Möglichkeit einer anderen Ursache nahe legen (Möglichkeit der Entkräftung des Anscheinsbeweises; Grundsatzurteil des BGH v. 05.10.2004 - XI ZR 210/03 Rn. 22, 23 - NJW 2004, 3623; Otto in: Staudinger, BGB, 2009, § 280 Rn. F 6; Schiemann in: Staudinger, BGB, 2005, Vorbem. §§ 249 ff., Rn. 99 f.).

Anders als Schulte am Hülse/Welchering annehmen (NJW 2012, 1262, 1263), sind die Anforderungen hierfür jedoch hoch. Mit „Tatsachen“ sind nicht etwa lediglich einfache Behauptungen oder angebliche theoretische oder praktische Möglichkeiten gemeint.

a) Ausspähen

So hat der BGH der Ansicht, die theoretische, nicht auszuschließende Möglichkeit des „Ausspähens“ der PIN sei ausreichend, um der Anwendung des Anscheinsbeweises zugunsten des Zahlungsinstituts die Grundlage zu entziehen, eine klare Absage erteilt (BGH, Urt. v. 05.10.2004 - XI ZR 210/03 Rn. 31; Werner in: Soergel, BGB, § 675w Rn. 17). Die Möglichkeit, des Ausspähens der PIN bei einem vorherigen Eigeneinsatz von Karte und PIN wurde, anders als Schulte am Hülse/Welchering im Rahmen ihrer Ausführungen zum Beschluss des BVerfG vom 08.12.2009 (1 BvR 2733/06) darstellen, nicht erst vom BVerfG, sondern bereits vom BGH in seiner Grundsatzentscheidung vom 05.10.2004 (vgl. XI ZR 210/03 - BGHZ 160, 308, 317) erwogen und für all die Fälle abgelehnt, in denen sich das Ausspähen und der anschließende Kartendiebstahl in zeitlicher und/oder örtlicher Hinsicht als unwahrscheinlich darstellen. Anhaltspunkte sind bei dieser Erwägung, dass der Täter den Karteninhaber regelmäßig nicht kennt, dass der Kartendiebstahl alsbald nach dem Ausspähen der PIN bewerkstelligt wurde, dass der für den Eigeneinsatz genutzte Geldautomat in örtlich für den Täter erreichbarer Nähe des missbräuchlich genutzten

Geldautomaten liegt, und/oder dass der Karteninhaber die Karte unverzüglich nach Verlust sperrt, er andernfalls wegen grob fahrlässiger verspäteter Kartensperre haftet (vgl. näher Werner in: Soergel, BGB, § 675w Rn. 17). Überdies sind Angaben des Karteninhabers zu vorangegangenen Eigeneinsätzen von Karte und PIN und sonstige Sachverhaltsumstände anhand der Dokumentation der Zahlungsvorgänge (Transaktionsprotokolle, Geldautomatenprotokolle, etc.) sowie anhand polizeilicher oder staatsanwaltschaftlicher Akten klärbar.

b) Sicherheitstechnik/Triple-DES-Systeme

Der Anscheinsbeweis erfordert keine 100%ige Sicherheit, sondern nur, dass der fragliche Vorgang auf den ersten Blick nach einem durch Regelmäßigkeit, Üblichkeit und Häufigkeit geprägten Muster abzulaufen pflegt (Zwade/Mühl, WM 2006, 1225, 1228).

Alle bisher von Karteninhabern ins Feld geführten angeblichen Möglichkeiten von Systemschwächen der Zahlungskartensysteme, von PIN-Entschlüsselungen und von PIN-Abgriffen (u.a. Themen wie Ungleichverteilung der PIN, mehrere PINs, Erraten der PIN, Angriffe auf Master- bzw. Institutsschlüssel (key-management), Sicherheitskriterien bei PIN-Generierung bzw. PIN-Verifizierung, Smart-attacks, Angreifbarkeit von Knotenpunkten bzw. Switch-Stellen (HSMs), Ausnutzen verschiedener Funktionen wie z.B. der „change account number-Funktion“ oder der „PVV-Funktion“, Zufallszahlengenerator, RFID-Transponder, Bekanntwerden vertraulicher Dokumente, Innentäterattacken, Öffnung verschlossener PIN-Umschläge, Funktionsstörungen von Geldautomaten, etc., unter Verweis auf Veröffentlichungen von Berkman/Ostrovsky, Mike Bond, a Campo, etc.) liegen bis heute als Ursache der PIN-Erlangung durch unbefugte Dritte im Missbrauchsfall bei wertender Betrachtung außerhalb der Lebenserfahrung und sind höchst unwahrscheinlich geblieben (vgl. nur OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 - WM 2008, 534; zu den grundlegenden Anforderungen vgl. BGH, Urt. v. 05.10.2004 - XI ZR 210/03). Behauptungen allgemeiner Natur zur angeblichen Möglichkeit einer PIN-Ermittlung sind in Zivilprozessen nicht berücksichtigungsfähig und eher spekulativ und laufen ohne konkrete Anknüpfungstatsachen auf eine unzulässige Ausforschung hinaus (OLG Frankfurt am Main, Urt. v. 30.03.2006 - 16 U 70/05 - NJW-RR 2007, 198).

Nach Expertenwissen sind bis dato keine Angriffe gegen DES-basierte Realwelt-PIN-Systeme bekannt. In allen bisher geführten prozessualen Auseinandersetzungen konnte karteninhaberseits kein einziger erfolgreicher Angriff auf die PIN-Systeme nachgewiesen werden. Im Gegenteil gilt (jedenfalls) für die ab 1998 von der Kreditwirtschaft für die PIN-Generierung wie auch für die PIN-Verifizierung angewandten sog. Triple-DES-Verfahren (mit 128-Bit-Verschlüsselungen bzw. 112-Bit beim sog. 2-Key-Triple-DES-Verfahren), die bis heute State-of-the-Art-Technologie sind, das Brechen der Schlüssel und die Lesbarmachung einer PIN weltweit nach wie vor als praktisch unmöglich (Lochter/Schindler, MMR 2006, 292, 293; AG Offenbach am Main, Urt. v. 31.05.2011 - 30 C 117/07 Rn. 16, das auf einem neuen Gutachten des Sachverständigen Prof. Schindler vom 05.07.2010 basiert; vgl. auch OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 - WM 2008, 534).

Selbst der Sachverständige Prof. Pausch, der Ende der 1990er Jahre u.a. im Verfahren des OLG Hamm (Urt. v. 17.03.1997 - 31 U 72/96 - NJW 1997, 1711; s.a. AG Darmstadt, Urt. v. 24.02.1989 - 36 C 4386/87 - WM 1990, 543 m. Anm. Reiser, WuB I D 5 Kartensysteme 3.90; NJW-CoR 1997, 283 und NJW-RR 1989, 1138) zum alten (seit 1998 jedoch abgelösten) ec-System mit 56-Bit-Schlüsselraum noch angebliche Systemschwächen begutachtete, hat in einem neueren Gutachten vom 28.04.2008 zu einem Master-Card-PIN-Lost/Stolen-Fall (LG Magdeburg, Beschl. v. 29.10.2009 - 2 S 312/09) die Auffassung vertreten, dass etwaige Lücken in einem Triple-DES-Sicherheitssystem des Kartenemittenten als Ursache der Kenntniserlangung der PIN durch Unbefugte ausscheiden und eine „eher theoretische Möglichkeit“ bleiben.

Nach wie vor gelten die Triple-DES-Sicherheitssysteme als sicher und mathematisch-technisch unüberwindbar (Werner in: Soergel, BGB, § 675w Rn. 24; Maihold in: Bankrechts-Handbuch, § 54 Rn. 114; Hönn in: jurisPK-BGB, § 670 Rn. 19, m.w.N.; BGH, Urt. v. 05.10.2004 - XI ZR 210/03 Rn. 30, an dem durch das Urteil des BGH v. 29.11.2011 (XI ZR 370/10 Rn. 37) festgehalten wird).

4. Anforderungen an die Widerlegung der Beweisvermutungen des § 675w Satz 2 und Satz 3 BGB/Entkräftung des Anscheinsbeweises

Erforderlich für die Widerlegung der Beweisvermutungen des § 675w Satz 2 und Satz 3 BGB oder die Entkräftung des Anscheinsbeweises ist die konkrete Darlegung und der Nachweis der Möglichkeit eines atypischen Verlaufs durch den Zahlungsdienstnutzer. Der Karteninhaber genügt seiner Substantiierungspflicht nicht, wenn er nicht auch vorträgt, auf welche Weise es zum Kartenmissbrauch gekommen sein kann (Werner in: Soergel, BGB, § 675w Rn. 25, m.w.N.; Otto in: Staudinger, BGB, § 280 Fn. 53; Hönn in: jurisPK-BGB, § 670 Rn. 19, m.w.N.). Denn es reicht für einen atypischen Geschehensab-

lauf nicht aus, wenn der Karteninhaber (nur) darlegt und beweist, dass er die PIN nicht notiert mitführte. Notwendig darüber hinaus ist nämlich die konkrete Darlegung, wie der Dieb Zugang zur PIN bekommen haben kann; eine nicht bloß vage, sondern ernsthafte Möglichkeit einer anderen (als durch Mitführung der PIN verursachten) Kenntniserlangung der PIN muss nahe liegen (BGH, Urt. v. 05.10.2004 - XI ZR 210/03 - BGHZ 160, 308 = NJW 2004, 3623 m. Anm. Werner, WuB I D 5 b - 1.11; vgl. Werner in: Sorgel, BGB, § 675w Rn. 25, m.w.N.; BGH, Beschl. v. 06.07.2010 - XI ZR 224/09 m. Anm. Meder, WuB I D 5 a Kreditkarte 1.11; LG Berlin, Urt. v. 22.06.2010 - 10 S 10/09 m. Anm. Willershausen, jurisPR-BKR 11/2010 Anm. 6; Grüneberg/Sprau in: Palandt, BGB, § 280 Rn. 37, § 675v Rn. 7 und § 675w Rn. 2 und Rn. 4, jew. m.w.N.; Nobbe in: Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, § 675w Rn. 25 ff., Rn. 30, Rn. 33, Rn. 46, jew. m.w.N.; Baumbach/Lauterbach, ZPO, 69. Aufl. 2011, Anh. § 286 Rn. 18 f; so auch Koch/Vogel in: Albrecht/Karahan/Lenenbach u.a., Fachanwaltshandbuch Bank- und Kapitalmarktrecht, 2010, § 20 Rn. 80 f. und Rn. 166; Lohmann/Koch, WM 2008, 57, 62).

Die gesetzlichen Beweisvermutungen des § 675w Satz 2 und Satz 3 BGB blieben unangewendet und es käme einem Wegfall des Anscheinsbeweises im Zahlungskartenrecht gleich, wenn Karteninhaber einfach durch bloße Behauptung, ihre PIN nicht dabei gehabt zu haben, den Anscheinsbeweis entkräften könnten. Ihnen würde quasi ein Freibrief ausgestellt, die sicheren Geldausgabeautomatensysteme pauschal in Frage zu stellen; eine Durchsetzung von Schadensersatzansprüchen der Kartenunternehmen, die auf aus dem Gefahrenkreis der Karteninhaber hervorgehenden Schadensursachen beruhen, wäre erheblich erschwert, wenn nicht gar regelmäßig unmöglich (Nobbe in: Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, § 675w Rn. 25 ff., Rn. 33; Meder, WuB I D 5 a Kreditkarte 1.11; Hellner/Steuer, Bankrecht und Bankpraxis, Bd. 3 Rn. 6/1966; Beesch in: NK-BGB, §§ 675v-w Rn. 40, m.w.N.).

Nobbe (Nobbe in: Ellenberger/Findeisen/Nobbe, Kommentar zum Zahlungsverkehrsrecht, § 675w Rn. 25 ff., Rn. 33) formuliert zusammenfassend zutreffend, dass „der Anscheinsbeweis ... danach geradezu Voraussetzung für den Betrieb von Geldautomaten und automatisierten Kassen für bargeldlose Zahlungen (ist)“.

5. Keine Änderung, nur Konkretisierung der Anscheinsbeweis-Rechtsprechung des BGH durch Urteil vom 29.11.2011 (XI ZR 370/10)

Anders als Schulte am Hülse/Welchering (NJW 2012, 1262, 1263) darstellen, hat das BVerfG in seinem Beschluss vom 08.12.2009 (1 BvR 2733/06 - NJW 2010, 1129 = WM 2010, 208, 209) die herrschende Anscheinsbeweis-Rechtsprechung bestätigt und auch der BGH hält in seinen neueren Entscheidungen (Urt. v. 29.11.2011 - XI ZR 370/10 - NJW 2012, 1277; Beschl. v. 06.07.2010 - XI ZR 224/09 - WM 2011, 924) an seiner Anscheinsbeweis-Rechtsprechung fest; er hat lediglich Konkretisierungen vorgenommen. Es sind somit keine Änderungen in der bisherigen etablierten Anscheinsbeweis-Rechtsprechung eingetreten; die bisherigen Grundsätze bleiben in vollem Umfang anwendbar.

Das BVerfG hat in seinem Beschluss vom 08.12.2009 (1 BvR 2733/06 - WM 2010, 208, 209) (dem der unstreitig gebliebene Sachverhalt zugrunde lag, dass die Karteninhaberin zu keiner Zeit im Besitz der bei den streitigen Abhebungen genutzten ec-Karte war; sie hatte die (Nachfolge)-ec-Karte nicht erhalten) lediglich noch einmal klargestellt, dass Voraussetzung für die Anwendbarkeit des Anscheinsbeweises (auch) ist, dass der Karteninhaber ursprünglich, also vor Verlust der Karte, im Besitz derselben war – anderenfalls es an einem maßgeblichen Teil des die Typizität begründenden Sachverhalts fehle (vgl. Willershausen, jurisPR-BKR 11/2010 Anm. 6). Im Beschluss des BGH vom 06.07.2010 (XI ZR 224/09) wurden seine bisherigen Anforderungen an eine Entkräftung des Anscheinsbeweises verkürzt dargestellt, denn es reicht für einen atypischen Geschehensablauf nicht aus, wenn der Karteninhaber (nur) darlegt und beweist, dass er die PIN nicht notiert mitführte. Notwendig darüber hinaus ist nämlich die konkrete Darlegung, wie der Dieb Zugang zur PIN bekommen haben kann (vgl. insbes. Meder, WuB I D 5 a Kreditkarte 1.11).

Schließlich fokussiert auch das neue Urteil des BGH vom 29.11.2011 (XI ZR 370/10 Rn. 18 ff., Rn. 37 - WM 2012, 164 = NJW 2012, 1277) lediglich erneut die (u.a. Typizität begründende) erforderliche Anknüpfungstatsache des ursprünglichen Besitzes der Original-Karte. Das Erfordernis des Einsatzes der Originalkarte für die Anwendbarkeit des Anscheinsbeweises ist damit nichts Neues, sondern wurde bereits im Urteil des BGH vom 05.10.2004 (XI ZR 210/03 Rn. 18) vorausgesetzt. Im dortigen Fall war der Verlust und der kurzfristig danach erfolgte Einsatz der Original-Karte unstreitig. Im Übrigen liegt der Einsatz der Original-Karte ohnehin auf der Hand, wenn dem Karteninhaber kurze Zeit vor dem streitbefangenen Missbrauchsumsatz „die Karte“ gestohlen worden ist. Es ergibt für einen Dieb einer Original-Karte schlechthin auch keinen Sinn, noch eine Dublette anzufertigen und diese dann einzusetzen, wenn er die gestohlene Originalkarte in Händen hält.

Die Besonderheit des Sachverhalts im – allerdings noch nach altem Recht zu würdigenden – Fall des BGH vom 29.11.2011 (XI ZR 370/10 Rn. 4) bestand darin, dass sich der Karteninhaber „auf einen Missbrauch der Kreditkarte“ berufen hatte und dass das Berufungsgericht keine Feststellungen zur Verwendung der Originalkarte bei den missbräuchlichen Abhebungen getroffen hatte; zur Klärung wurde der Rechtsstreit an das Berufungsgericht zurückverwiesen. Dass, wie der BGH in seinem Urteil vom 29.11.2011 ausführt, im Falle von Abhebungen an Geldautomaten mithilfe einer Kartendublette die Typizität fehlt, da für diesen Missbrauch bedeutungslos ist, ob die – nicht eingesetzte – Originalkarte und die PIN gemeinsam aufbewahrt worden sind (BGH, Urt. v. 29.11.2011 - XI ZR 370/10 Rn. 16), stellt sich nur als zutreffende Schlussfolgerung aus seinen bisherigen Anscheinsbeweisgrundsätzen dar. Die Anscheinsbeweis-Rechtsprechung kommt in Fällen, in denen nachweislich eine Kartendublette verwendet wurde (sog. Skimming/Dubletten-Fälle, bei denen auf dem Magnetstreifen gespeicherte Daten ausgelesen und auf einen Kartenrohling kopiert werden sowie zusätzlich die PIN ausspioniert wird), gar nicht zur Anwendung.

6. Klärbarkeit der Fallgruppen (Lost/Stolen vs. Skimming)

Ob es sich um einen Skimming/Dubletten-Fall oder um einen Lost/Stolen-Fall handelt, ist für die rechtliche Bewertung des jeweiligen Falles entscheidend und aufklärbar. Anhaltspunkte bieten bestimmte, immer wiederkehrende Tatmuster; die diesbezüglichen Erkenntnisse ergeben sich aus der jahrelangen Präventionsarbeit der Kreditwirtschaft wie auch der Kriminalistik.

Selbstverständlich ist die Betrugsmasche des Skimming, die im Jahr 2002 erstmals vereinzelte Schäden verursachte, in der Kreditwirtschaft bekannt, und es wurden ab dem Jahr 2003, in dem erstmals eine geringe Zunahme der Schadensfälle verzeichnet wurde, Bündel von Maßnahmen zur Abwehr derartiger Angriffe entwickelt und erfolgreich umgesetzt. So haben z.B. schon seit vielen Jahren viele Kreditinstitute zur Abwehr der Angriffe auf Geldautomaten u.a. mit der Installation elektronischer Anti-Skimming-Module (sog. „Card Protection Kits“ – CPK) reagiert, die Manipulationen verhindern. Die verschiedenen Staatsanwaltschaften, die Kriminalpolizei und die Netzbetreiber arbeiten gemeinsam mit der Kreditwirtschaft, der EURO Kartensysteme GmbH, den Kreditkartenorganisationen, den Landeskriminalämtern und dem BKA wirksam an der Betrugsbekämpfung und an der Aufklärung – unter engem Informationsaustausch zwischen allen am Zahlungsverkehr Beteiligten, auch in Kooperation mit den Terminalherstellern und -betreibern.

Bei der EURO Kartensysteme GmbH mit Sitz in Frankfurt am Main ist seit 1990 die „Zentrale Debit-Schadensbekämpfung der deutschen Kreditwirtschaft“ (ZDS) angesiedelt, die insbesondere auch eng mit den internationalen Kreditkartensystemen MasterCard und VISA zusammenarbeitet. Fällt auf, dass ein Geldautomat oder ein Terminal manipuliert wurde, erhält diese sofort eine Manipulationsanzeige. Anhand der ihr dann zugeleiteten Transaktionsdokumentationen und/oder Geldautomatenprotokolle können der Datenabgriffszeitraum festgelegt und die potentiell betroffenen Zahlungskarten bestimmt werden – um deren Kartensperren und Schadensregulierungen einzuleiten. Alle Informationen über manipulierte Geldautomaten laufen – bezogen auf deutsche Zahlungskarten – sowohl bei der ZDS wie auch bei den entsprechenden MasterCard- und VISA-Institutionen über die sog. Card-Schemes zusammen, so dass etwaige deutsche Zahlungskarten betreffende Schadensfälle aus dem In- und Ausland, insbesondere Dublettenschadensfälle, zentral erfasst und ausgewertet werden können. Hierdurch und durch weitere postpräventive Maßnahmen kann die deutsche Kreditwirtschaft in ca. 90% der potentiell abgefischten Daten eine betrügerische Verwendung durch die Datendiebe verhindern. Schließlich kann hierdurch festgestellt werden, ob (generell oder zu einem konkreten Zeitpunkt) an einem bestimmten Geldautomaten eine Skimming-Attacke zu verzeichnen war oder nicht.

Wie eingangs bereits dargelegt, werden beim Skimming lediglich Daten abgegriffen. Die Installation von sog. Skimmingmodulen ist für die Täter mit erheblichem technischem Aufwand und Know-how und erheblichen Kosten verbunden und wird in der Regel arbeitsteilig durch mehrere Täter/Tätergruppen durchgeführt. Daher werden bei einer Skimming-Attacke regelmäßig nicht nur die Daten zu einer einzigen Zahlungskarte abgeschöpft, sondern eine Vielzahl von Zahlungskarten-Daten über Zeiträume von mehreren Tagen hinweg. Diese Tatsache wird sich bei der Bearbeitung der Schadensfälle insofern zunutze gemacht, als bei der Auswertung der Informationen zu den Verwertungstaten Rückschlüsse auf die manipulierten Geldautomaten gezogen werden können. Die jeweiligen Originalkarten der verwendeten Dubletten sind folglich zuvor immer an demselben Geldautomaten vom (rechtmäßigen) Karteninhaber selbst eingesetzt worden. Zudem entspricht es typischem kriminalistischen Muster, dass erfolgreich hergestellte Kartenduplikate von Tätern nicht nur für eine oder zwei Abhebungen eingesetzt werden, sondern so oft wie möglich in kurzer zeitlicher Abfolge für eine Vielzahl von Abhebungen – bis alle Limits zu den betreffenden Karten ausgeschöpft sind. Denn die Täter müssen mit schneller Entdeckung

und mit in der Regel kurzfristig erfolgenden Kartensperren rechnen (Kochheim, Skimming – Hintergründe und Strafrecht, 2. Aufl. 2011, S. 6 ff.).

Skimming/Dubletten-Fälle können insbesondere anhand von Zeitfaktoren gegenüber Lost/Stolen-Fällen abgegrenzt werden. So fanden in allen tatsächlich vorgekommenen Dubletten-Schadensfällen die sog. Verwertungstaten (Cashing) nicht am gleichen Tag statt wie das Skimming, d.h. das Auslesen der Kartendaten und Abgreifen der PIN. Denn die Täter benötigen grundsätzlich einige Zeit zum Herstellen der Dubletten. Eine kriminalistische Studie (Kochheim, Skimming – Hintergründe und Strafrecht, S. 53) kommt zu dem Ergebnis, dass „die kürzesten Abstände zwischen Skimming und Cashing inzwischen zwei Tage betragen". Da dem Karteninhaber bei Skimming/Dubletten-Fällen die Karte typischerweise nicht abhandenkommt, bemerkt der Karteninhaber eine Skimming-Attacke nicht sofort. Hingegen findet in Lost/Stolen-Fällen der Missbrauchseinsatz von Zahlungskarte nebst PIN typischerweise kurz nach dem Diebstahl/Verlust der Karte statt (binnen weniger Minuten, binnen weniger Stunden, am gleichen Tage), da der Karteninhaber den Diebstahl/Verlust sofort bemerken und die Sperrung der Karte veranlassen kann.

Nach allen kriminalistischen Erkenntnissen und Erfahrungen bei der Schadensbearbeitung von Dublettenfällen findet ferner die Verwertung der Kartendaten mittels Dublette durch die Täter (Cashing) nie an demselben Geldautomaten wie das Auslesen der Kartendaten (Skimming) statt, so dass auch über dieses Merkmal eine Identifizierung der Fallgruppe möglich sind.

Schließlich setzt das Vorliegen eines Skimming/Dubletten-Falls stets voraus, dass der Karteninhaber noch im Besitz seiner Original-Karte ist; dagegen ist in den Lost/Stolen-Fällen die Original-Karte den Karteninhabern ja gerade abhandengekommen.

Zusammenfassend ist daher festzustellen, dass bereits unter Zusammenführung der kriminalistischen Erkenntnisse und Erfahrungen der Kreditwirtschaft bei der Schadensbearbeitung sowie durch Auswertung der zu streitbefangenen Transaktionen vorliegenden Transaktionsdokumentation (Transaktionsprotokoll, Geldautomatenprotokoll, Rückbelastungsdokumentation) aufklärbar ist, ob ein Karteninhaber Opfer einer Skimming-Attacke geworden sein kann und welcher Fallgruppe ein konkreter Schaden zuzuordnen ist.

7. Klärbarkeit des Einsatzes der Original-Karte

a) EMV-Chip-Technologie/EMV-Sicherheitsstandard

Mit der EMV-Chip-Technologie wurde seit dem 01.01.2005 ein internationaler Standard definiert, der zur Reduktion des Kartenmissbrauchs führte. Seit Jahresbeginn 2011 sind im 31 Länder umfassenden einheitlichen europäischen Zahlungsverkehrsraum SEPA (Single European Payment Area, vgl. hierzu Meckel, jurisPR-BKR 11/2009 Anm. 1, m.w.N.) alle Debit- und Kreditkarten mit dem fälschungssicheren EMV-Chip ausgestattet und die Geldautomaten sowie POS-Terminals auf den EMV-Standard umgerüstet. Innerhalb Europas sind Transaktionen mit Zahlungskarten seither grundsätzlich EMV-Chip-basiert. Nur in technisch bedingten Ausnahmefällen kann ein sog. Fallback auf den Magnetstreifen erfolgen (sog. Fallback-Transaktion). Fallbacks werden allerdings im Autorisierungssystem des jeweiligen Kartenemittenten (Genehmigungsvorgang) erkannt, geprüft und protokolliert (AuthCode = Authorization Code). Wenn Geldautomaten und Zahlungskarte EMV-Chip-fähig sind, wird eine Magnetstreifentransaktion nicht autorisiert, d.h. die Transaktion wird „abgelehnt". Die EMV-Chip-Fähigkeit von Geldautomat und Zahlungskarte sowie Transaktionsart des Zahlungsvorgangs (über EMV-Chip oder Magnetstreifen) werden ebenfalls im Transaktionsprotokoll dokumentiert (vgl. die Positionen „Servicecode BMP35", „Terminalausstattung BMP22" und „Transaktionstechnologie").

Mit dem EMV-Chip kann somit anhand und in Verbindung mit der Transaktionsdokumentation nachgewiesen werden, dass die Original-Karte für die Transaktion eingesetzt wurde, und dass der EMV-Chip von dem Geldautomaten bzw. POS-Terminal zur Kartenechtheitsprüfung tatsächlich ausgelesen wurde (BGH, Urt. v. 29.11.2011 - XI ZR 370/10 Rn. 18 f. - WM 2012, 164; Maihold in: Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, § 54 Rn. 5 f., Rn. 10, Rn. 119, m.w.N.; zur größeren praktischen Bedeutung der Transaktionsdokumentation im neuen Zahlungsdiensterecht vgl. Beesch in: NK-BGB, §§ 675v-w Rn. 27 f.; Omlor in: Staudinger, BGB, §§ 675c-676c Zahlungsdiensterecht, § 675w Rn. 4; Lohmann/Koch, WM 2008, 57, 62 f.; Koch/Vogel in: Albrecht/Karahan/Lenenbach, Fachanwaltshandbuch Bank- und Kapi-talmarktrecht, S. 445).

Der technische Hintergrund lässt sich wie folgt skizzieren: Der EMV-Chip kann nicht nur Daten speichern, sondern auch komplexe Berechnungen durchführen. Der Nachweis der Authentizität und somit der Echtheit der eingesetzten deutschen Zahlungskarte geschieht auf der Grundlage anerkannter kryptographischer Verfahren. Hierzu wird in jeden EMV-Chip einer Karte ein individueller kryptographi-

scher Schlüssel eingebracht. Im Rahmen einer Transaktion wird unter Verwendung dieses Schlüssels ein Transaktionskryptogramm gebildet, in welches wichtige Bestandteile der Transaktion, wie z.B. der Betrag, eingehen. Das Autorisierungssystem des Kartenemittenten prüft dieses Kryptogramm und erteilt nur dann eine positive Genehmigung mit Genehmigungsnummer (Autorisierung des Emittenten), wenn unter anderem diese Prüfung korrekt verläuft; zusätzlich erfolgt natürlich noch eine Prüfung der PIN (Triple-DES-Technologie) und eine Prüfung der bankfachlichen Anforderungen.

Es ist eine wesentliche Eigenschaft symmetrischer kryptographischer Verfahren, dass die Ver- und Entschlüsselung nur mit demselben Schlüssel erfolgen können, und dass selbst bei minimaler Änderung des Schlüssels vollständig andere Ergebnisse erzielt werden. Somit kann bei erfolgreicher Prüfung der von der Karte erstellten verschlüsselten Daten darauf geschlossen werden, dass nur der in der Karte vorhandene Schlüssel verwendet werden konnte.

Im Rahmen von Sicherheitsgutachten, die Bestandteil des Zulassungsverfahrens der Deutschen Kreditwirtschaft (DK) sind, wird geprüft, ob die in einer Chipkarte gespeicherten sensitiven Daten ausgelesen werden können, oder ob es möglich ist, eine Karte zu „clonen“. Im Rahmen dieser Sicherheitsuntersuchung werden sowohl die Hardware als auch das Betriebssystem und die Anwendungssoftware von unabhängigen Gutachtern untersucht. Bezüglich der Bewertung der oben genannten Aspekte wird auf das Begutachtungsschema ISO 15408 (auch bekannt als Common Criteria) zurückgegriffen. Der Standard unterscheidet verschiedene Prüftiefen und Angriffsstärken. Bei einer Untersuchung für die Deutsche Kreditwirtschaft (DK) wird bezüglich der Prüftiefe und der Angriffsstärke der gleiche hohe Maßstab verwendet wie bei der Bewertung der Sicherheit von Signaturkarten nach dem Signaturgesetz (SigG) oder beim neuen Personalausweis (nPA). Dies bedeutet, dass selbst Angreifern mit großem Expertenwissen, aufwändigem technischen Equipment und hohem zeitlichen Aufwand ein Angriff auf durch EMV-Chip geschützte Informationen von Zahlungskarten nicht möglich ist. Der EMV-Chip ist nach heutigem Expertenwissen datenfälschungs- und kopiersicher. Dadurch ist es möglich, zum einen das Herstellen von Kartenduplikaten (Dubletten) oder -fälschungen zu verhindern und Kartenduplikate oder -fälschungen am Geldautomaten oder POS-Terminal zu erkennen. Über den EMV-Chip wird eine nochmals sicherere Karteninhaber-Verifikation (Authentifizierung) ermöglicht und eine Kartenechtheitsprüfung durchgeführt.

Soweit Schulte am Hülse/Welchering meinen, „die Weiterentwicklung der Kartensysteme hin zu dem EMV-Chip (lösten) das Problem nicht wirklich“ (NJW 2012, 1262, 1266), ist dem zu widersprechen. Tatsächlich sind die Fallzahlen seit Einführung der EMV-Chip-Technologie ab Anfang 2011 markant zurückgegangen.

b) MM-Merkmal

Deutsche Debit-Karten sind schon seit 30 Jahren mit dem sog. MM-Merkmal ausgestattet, dessen – flächendeckend in Deutschland – durchgeführte Prüfung bei einem Karteneinsatz mit PIN am Geldautomaten oder Terminal eine Kartenechtheitsprüfung gewährleistet; dies wurde und wird immer wieder von Trittbrettfahrern übersehen, die die Erstellung von Dubletten nach professionellem Ausspähen als Missbrauchsursache vortäuschen (Lochter/Schindler, MMR 2006, 292, 296).

Die Prüfung des MM-Merkmals verhindert anerkanntermaßen, dass Dubletten deutscher Debitkarten an deutschen Geldautomaten eingesetzt werden können (OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 - WM 2008, 534).

c) Kriminalitätsverlagerung ins Ausland

Der EMV-Chip sowie das MM-Merkmal gewährleisten, dass in den Skimming-Fällen Kartendubletten nur im Ausland zum sog. Cashing eingesetzt werden können. Da allerdings auch im europäischen Ausland seit Beginn des Jahres 2011 nur noch EMV-Chip-Transaktionen möglich sind, führt dies dazu, dass das nach einem Skimming-Angriff von den Tätern durchzuführende sog. Cashing nur noch im außereuropäischen Ausland stattfindet (Kochheim, Skimming – Hintergründe und Strafrecht, S. 9). Erkenntnissen der EURO Kartensysteme GmbH zufolge werden Kartendubletten seit dem 4. Quartal 2010 daher von Betrügern zunehmend in Regionen außerhalb des SEPA-Raumes eingesetzt.

C. Entgegnung auf angeblich technische Möglichkeiten zur Kenntniserlangung der PIN (NJW 2012, 1262, 1264 f.)

Soweit Schulte am Hülse/Welchering Behauptungen zu angeblichen „technischen Möglichkeiten der Täter“ zur PIN-Erlangung aufstellen und aufgrund dessen die Anwendbarkeit der Anscheinsbeweisgrundsätze wegen angeblich geschwundener Wahrscheinlichkeiten (NJW 2012, 1262, 1264) in Frage stellen,

sind die unrichtigen Darlegungen, insbesondere die technischen Fehlinformationen, im Folgenden richtigzustellen.

I. Zu „Skimming“ (NJW 2012, 1262, 1264)

1. Keine „frühere Rechtsprechung“ zu „Skimming“ vorhanden

Wie bereits oben dargelegt, ist die Anscheinsbeweis-Rechtsprechung im Grundsatz für die sog. Lost/Stolen-Fälle entwickelt. Für Skimming-Fälle gab es keine „frühere Rechtsprechung“, anders als Schulte am Hülse/Welchering meinen (NJW 2012, 1262, 1264); der BGH hat sie demgemäß in seinem Urteil vom 29.11.2011 (XI ZR 370/10) auch nicht etwa „abgelehnt“.

2. Sicherheitsniveau

Unrichtig ist auch die Wiedergabe des BGH-Urteils vom 29.11.2011 insoweit, dass nach Feststehen des Einsatzes der Originalkarte zu klären sei, ob das konkret genutzte Sicherheitssystem überhaupt ein ausreichendes Sicherheitsniveau bietet (NJW 2012, 1262, 1263). Der BGH stellt nur darauf ab, dass der Einsatz der Originalkarte feststehen müsse. Dies kann u.a. bei EMV-Chip-Transaktionen durch den EMV-Chip nachgewiesen werden; bei einem Fallback auf den Magnetstreifen stehen, je nach Sachverhaltskonstellation, andere Nachweismöglichkeiten zur Verfügung.

3 EMV-Chip nicht auslesbar

Unrichtig ist die Aussage von Schulte am Hülse/Welchering, das Auslesen der auf der Karte gespeicherten Daten funktioniere auch, wenn die Karte ausschließlich über einen EMW-Chip verfüge und nur dort Kartendaten gespeichert seien (NJW 2012, 1262, 1264). Richtig demgegenüber ist, dass der EMV-Chip deutscher Debit- und Kreditkarten nicht auslesbar ist; insbesondere können keine Schlüsseldaten oder PINs ausgelesen werden. Sind also Daten nur auf dem EMV-Chip, ist eine Auslesbarkeit ausgeschlossen. Der EMV-Chip ist nach heutigem Expertenwissen datenfälschungs- und kopiersicher.

4. Abgriff allein der PIN nutzlos

Abgesehen davon, dass den Karteninhaber anerkanntermaßen ohnehin die Sorgfaltspflicht trifft, einen Abgriff der PIN bei deren händischer Eingabe (z.B. durch Abdecken des Eingabefelds mit der Hand) zu verhindern, ist in Entgegnung zu den Ausführungen von Schulte am Hülse/Welchering, dass „die PIN ohnehin trotzdem abgegriffen werden kann, da sie händisch vom Karteninhaber eingegeben werden muss“ (NJW 2012, 1262, 1264), festzustellen, dass die PIN alleine dem Täter nichts nutzt. Denn der Täter braucht für eine erfolgreiche Abhebung von Bargeld am Geldautomaten auch die echte EMV-Chip-Karte, jedenfalls eine Kartendublette für den Fall, dass ausnahmsweise noch ein Fallback auf den Magnetstreifen möglich ist.

5. Kein heimlicher PIN-Abgriff und „Jahre später“ liegender Diebstahl der Original-Karte

Anders als Schulte am Hülse/Welchering darstellen, greifen Täter auch nicht heimlich die PIN ab, um anschließend oder „Jahre später“ die Original-Karte zu stehlen (NJW 2012, 1262, 1264). Dies widerspricht allen kriminalistischen Erkenntnissen und Erfahrungen in der Schadensbearbeitung. Eine Zahlungskarte wird niemals „Jahre später“ gestohlen. So hat schon der BGH in seinem Grundsatzurteil vom 05.10.2004 (XI ZR 210/03) zutreffend erkannt, dass – da der Täter den Karteninhaber regelmäßig nicht persönlich kennt – der Täter die Zahlungskarte alsbald nach dem Ausspähen der PIN entwenden muss (BGH, Urt. v. 05.10.2004 - XI ZR 210/03 - WM 2004, 2309, 2312; OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 - WM 2008, 534 m. Anm. Meder/Flick, WuB I D 5 b. - 1.08). Desgleichen erfolgt beim Skimming der Datenabgriff vom Magnetstreifen in unmittelbarem zeitlichen Zusammenhang mit dem Ausspionieren der PIN, da ansonsten den Tätern keine Zuordnung zwischen jeweiliger Karte und PIN möglich ist, weil bei einem Skimming-Angriff immer eine Vielzahl von Kartendaten ausgelesen werden.

6. Keine arbeitsteilige Beschaffung von PIN und Karte in der Lost-/Stolen-Fallgruppe, nur bei Skimming

Unrichtig ist auch, dass die PIN-Beschaffung und das Entwenden der Original-Karte arbeitsteilig erfolgen würde (NJW 2012, 1262, 1264). Tatsächlich ist die von Schulte am Hülse/Welchering angesprochene arbeitsteilige Vorgehensweise der Täter nur beim Skimming, nicht bei Diebstahl, üblich.

7. Keine Erbeutung der PIN über Keylogger oder Seitenkanalattacke

Auch entspricht die Aussage von Schulte am Hülse/Welchering, die PIN könne „ferner über Schadsoftware wie einen Keylogger oder sogar über eine direkte Seitenkanalattacke auf den Chip selbst erbeutet

werden“ (NJW 2012, 1262, 1264 m. Eigenzitat in Fn.14 und unter Berufung auf eine Pressequelle in der Zeitschrift „Stern“), nicht empirisch verifizierbaren Erkenntnissen.

Tatsächlich sind derartige PIN-Abgriffe bei Zahlungskarten technisch nicht möglich. Seitenkanalattacken beziehen sich nur auf „Funkchips“, nicht auf EMV-Chips, wie sie ausschließlich in Zahlungskarten der deutschen Kreditwirtschaft und der internationalen Kreditkartenorganisationen, wie MasterCard und VISA, eingebaut werden. Für EMV-Chips ist dies keine bekannte und auch keine technisch mögliche Vorgehensweise. EMV-Chips werden im Übrigen bei Sicherheitsuntersuchungen der Kreditwirtschaft stets auf Resistenz gegen Seitenkanalangriffe überprüft. Sicherheitstechnisch gilt, dass PINs von Zahlungskarten über Funkschnittstellen nicht ausgelesen werden können.

„Funkchips“ dienen lediglich z.B. dem Kopieren anderer (entwendeter) Karten (wie z.B. Fahrkarten, Eintrittskarten), damit mehrere Personen in den Genuss von nur einer Fahrkarte oder Eintrittskarte kommen können. Selbst bei letztgenannten Karten ist dann aber auch immer zusätzlich noch die PIN erforderlich.

II. Zu „Magnetstreifentechnik“ (NJW 2012, 1262, 1264)

1. Tatsächlicher Aufbau und Inhalt der Spuren von Magnetstreifen

Auch die Ausführungen von Schulte am Hülse/Welchering zu den Spuren der Magnetstreifen entsprechen nicht den tatsächlichen Gegebenheiten. Es ist unrichtig, dass nur eine von den drei Spuren eines Magnetstreifens von Zahlungskarten beschreibbar wäre, dass auf ihr eine falsch eingegebene PIN und Transaktion dokumentiert würde und dass auf den ersten beiden Spuren eine Prüfsumme abgelegt wäre, mit der die PIN nicht nur bestätigt, sondern mit einigem Rechenaufwand auch ermittelt werden könnte (NJW 2012, 1262, 1264).

Demgegenüber entspricht das Folgende den technischen Tatsachen der Kreditwirtschaft: Spur 1 eines Magnetstreifens einer Zahlungskarte ist nicht belegt. Spur 3 enthält u.a. die BLZ und die Kontonummer im Klartext, jedoch keinen Karteninhabernamen; Spur 3 wird nur im Inland (Bundesrepublik Deutschland) gelesen. Spur 2 enthält u.a. die PAN (Primary Account Number) und wird im Ausland gelesen. Grundsätzlich wird jedoch vorrangig – im In- und Ausland – der EMV-Chip gelesen (vgl. oben; vgl. auch Kochheim, Skimming, S. 8). Auch kann aus dem Prüfwert nicht die PIN zurückgerechnet werden, auch nicht mit „einigem“ Rechenaufwand (Lochter/Schindler, MMR 2006, 292).

Dementsprechend unrichtig ist auch die Aussage von Schulte am Hülse/Welchering, „alle drei Spuren des Magnetstreifens (würden) vom Kartenleser ausgelesen“ (NJW 2012, 1262, 1264). Richtig ist, dass immer nur eine Spur gelesen wird: Im Inland Spur 3, im Ausland Spur 2; Spur 1 ist gar nicht belegt.

2. Keine Defekte beim Auslesen von Magnetstreifen

Weiter unzutreffend ist, dass „aufgrund technischer Defekte ... nicht immer alle drei Spuren ausgelesen werden (könnten), so dass dann auch der Protokolleintrag unter(bleiben würde)“ (NJW 2012, 1262, 1264). Tatsächlich gibt es, da immer nur eine Spur des Magnetstreifens gelesen wird bzw. ohnehin in erster Linie der EMV-Chip, die von Schulte am Hülse/Welchering behaupteten „technischen Defizite“ nicht. Es erfolgt auch immer eine Protokollierung der Daten.

Es ist auch nicht so, dass nur „zumindest“ die Kontonummer und eine Angabe zur kontoführenden Bank (ausgelesen) werden könnten. Richtig ist vielmehr, dass alle Daten gelesen werden müssen, denn ansonsten wird die Transaktion (der Zahlungsvorgang) nicht ausgeführt.

Nach Expertenwissen und mehrfach dokumentiert durch Sachverständigengutachten gilt im Übrigen, dass die PIN nicht auf dem Magnetstreifen der Zahlungskarten gespeichert ist; sie wird auch nicht am Geldautomaten oder im Kassenterminal aufgezeichnet. Eine PIN ist demzufolge auch aus einem Magnetstreifen einer Zahlungskarte nicht auslesbar.

3. Kein „verschlüsseltes Kommunikationsprotokoll“

Es entspricht auch nicht den Tatsachen, dass „die Datenübermittlung ... über ein eigenes, verschlüsseltes Kommunikationsprotokoll“ erfolgen würde (NJW 2012, 1262, 1264). Technisch korrekt ist vielmehr, dass das Kommunikationsprotokoll selbst nicht verschlüsselt ist; nur die PIN wird verschlüsselt und die komplette Nachricht wird auf dem Übertragungsweg über einen sog. Message Authentification Code (MAC) integritätsgeschützt übermittelt und protokolliert; das MAC-System basiert, wie das PIN-System selbst, auf dem Triple-DES-Algorithmus (Lochter/Schindler, MMR 2006, 292, 295).

4. Keine „Hinterlegung der PIN auf dem Bankserver“/Online-PIN-Prüfung

Das Halbwissen zu den technischen Vorgängen von Schulte am Hülse/Welchering findet ferner seinen Niederschlag in deren Aussage, die PIN sei „auf dem Bankserver hinterlegt“ (NJW 2012, 1262, 1264), und wegen „Leseproblemen“ entfalle in den meisten Softwareversionen der lokale Abgleich der PIN-Prüfsumme, d.h. die verschlüsselte PIN würde direkt an den Bankserver gesandt. Tatsächlich zutreffend ist hingegen, dass die PIN auf dem Bankserver nicht hinterlegt ist. Auch wird bei Geldautomaten-Transaktionen immer mit Online-PIN-Prüfung gearbeitet; lokal am Geldautomaten findet keine PIN-Prüfung statt. Die PIN wird vom PIN-Pad verschlüsselt zum Bank-Server bzw. zur betreffenden Autorisierungsstelle des für die jeweilige Transaktion zuständigen Autorisierungssystems gesendet. Die PIN-Prüfung findet dann ausschließlich in einem Rechenzentrum in einem Hardwaresicherheitsmodul (Hardware Security Module, HSM) statt (Lochter/Schindler, MMR 2006, 292; Kochheim, Skimming – Hintergründe und Strafrecht, S. 12). Im Übrigen findet auch eine effektive Sicherung der sog. Switch-Stellen durch HSMs statt, die die PINs gar nicht entschlüsseln (vgl. nur OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 Rn. 37 - WM 2008, 534).

5. Keine PIN-Angriffsmöglichkeiten über „Wartungs- oder Service-Schnittstellen von Geldautomaten“

Ebenso wenig enthalten die Ausführungen von Schulte am Hülse/Welchering zu angeblichen An- und Abgriffen über Wartungs- oder Service-Schnittstellen von Geldautomaten den technischen Tatsachen entsprechende Angaben. Sie sprechen selbst nur davon, dass (in der Kreditwirtschaft allerdings unbekannte) Sicherheitsexperten, deren berufliche oder wissenschaftliche Position bzw. Funktion oder Ausbildung von Schulte am Hülse/Welchering nicht näher benannt werden, angebliche „Indizien zusammengetragen“ hätten. Demgegenüber ist Tatsache, dass Hackerangriffe auf Geldautomaten bisher nicht erfolgt sind; ebenso wenig sind Spionageangriffe auf Kunden- und Kartendaten erfolgt.

III. Zu „Atypische Fälle“ (NJW 2012, 1262, 1265)

1. Kein PIN-Abgriff über „Innentäterattacken“

Auch der Spekulation über angeblich mögliche Innentäterattacken, d.h. Angriffen von Bankmitarbeitern unter Ausnutzung von Insiderwissen, etwa zur Ausspähung des der Verschlüsselung dienenden Institutsschlüssels, Angriffen gegen Rechenzentren, etc. (sog. Innentäterattacken), welche immer wieder und so auch von Schulte am Hülse/Welchering ins Feld geführt werden (NJW 2012, 1262, 1265 unter 3.), ist bereits vom BGH in seinem Grundsatzurteil vom 05.10.2004 (XI ZR 210/03 Rn. 33 - WM 2004, 2309) zutreffend eine klare Absage erteilt und keine dem Anscheinsbeweis entgegenstehende Wahrscheinlichkeit zugemessen worden.

Bis heute ist in der Zahlungskartenwirtschaft keine einzige Innentäterattacke bekannt geworden; in keinem Prozess wurde jemals eine solche Attacke dokumentiert oder nachgewiesen (OLG Frankfurt am Main, Urt. v. 30.01.2008 - 23 U 38/05 Rn. 35 - WM 2008, 534).

2. Kein PIN-Abgriff durch „Abfangen von Postsendungen“

Ebenso wenig kann der Abgriff durch Abfangen von PIN-Briefen Tätern den Erfolg bescheren, den Schulte am Hülse/Welchering anführen (NJW 2012, 1262, 1265). Zur PIN wird stets auch die Karte benötigt, um mit dem Zahlungsauthentifizierungsinstrument erfolgreich zu Geld zu gelangen. Karte und PIN sind jedoch niemals in einer Postsendung enthalten. Der PIN-Brief wird immer separat von der Karte verschickt, so dass Tätern eine Zusammenführung der notwendigen Komponenten des Zahlungsauthentifizierungsinstruments nicht möglich ist. Im Übrigen ist im neuen Zahlungsdiensterecht in § 675m Abs. 2 BGB geregelt, dass der Emittent die Gefahr der Versendung von Karte und PIN an den Kunden trägt.

IV. Zu „Grobe Fahrlässigkeit des Karteninhabers“ (NJW 2012, 1262, 1265)

In der Tat stellt das – für manchen Karteninhaber unentbehrliche – Notieren der PIN (und die Zusammenaufbewahrung mit der Karte) die wahrscheinlichste Ursache dafür dar, dass Täter im Diebstahls- oder Verlustfall (Lost/Stolen-Fall) die PIN auf-finden und zusammen mit der Karte an sich bringen können: Genau dieser typische Verlauf stellt die Grundlage für die neuen gesetzlichen Beweisvermutungen des § 675w BGB und die herrschende Anscheinsbeweis-Rechtsprechung dar.

Da die Zahlungssysteme als sicher anzusehen sind und technische Schwächen, die zu einer PIN-Entschlüsselung oder einem PIN-Abgriff durch unbefugte Dritte geführt hätten, bis heute nicht nachgewiesen sind, sind es die im Verantwortungsbereich der Karteninhaber liegenden „Sicherheitslücken“, gerade in Form der Notiz und Mitführung der PIN gemeinsam mit der Karte, die vom „System“ (Zahlungskartensystem) nicht mehr erfasst werden (können), und die dann zu den Missbrauchsschäden führen.

D. Konsequenzen für die Anwendbarkeit des Anscheinsbeweises (NJW 2012, 1262, 1265, 1266)

Wie zuvor dargelegt, können weder angebliche Fallzahlentwicklungen noch angebliche (neuere) technische Angriffsmöglichkeiten für einen Wegfall der Voraussetzungen des Anscheinsbeweises herangezogen werden. Beides ist tatsächlich nicht gegeben, so dass die Anwendung der Anscheinsbeweis-Grundsätze im Zahlungskartenrecht gerechtfertigt bleibt.

I. Fortgesetzter Einsatz der Triple-DES-Technik

Zwar ist – in Einklang mit dem Urteil des BGH vom 29.11.2011 (XI ZR 370/10 Rn. 37 - WM 2012, 164) und mit Maihold (in: Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, § 54 Rn. 114, Rn. 116, Rn. 118) – auf das „für die konkrete Abhebung eingesetzte System“ abzustellen und kann für das neue (ab 31.10.2009 geltende) Zahlungsdiensterecht „angesichts der fortschreitenden technischen Entwicklung“ für neue PIN-Fälle die Frage bedeutsam werden, ob der Anscheinsbeweis (noch) auf ältere gutachtliche Stellungnahmen gestützt werden kann.

Jedoch ist auch stets zu prüfen, ob sich das „im konkreten Fall eingesetzte System“ im Hinblick auf die streitbefangene(n) Transaktion(en) tatsächlich überhaupt im Hinblick auf die Parameter verändert hat, die für die Anwendung des Anscheinsbeweises relevant sind. Hier ist festzustellen, dass in der Kreditwirtschaft seit 1998 bis heute die Triple-DES-Technologie als State-of-the-Art-Technologie für die PIN-Generierung und die PIN-Verifizierung fortgesetzt angewandt wird, die von Sachverständigen und Gerichten als sicher anerkannt ist. Es ist also davon auszugehen, dass nach wie vor die im konkreten Fall verwendete Technik ein ausreichendes Sicherheitsniveau für die Anwendung des Anscheinsbeweises bietet. Die Einführung der EMV-Chip-Technologie seit Anfang 2011 hat die Sicherheit in der Kartentechnologie nur noch weiter erhöht.

II. Keine Notwendigkeit, für jeden Einzelfall neue Sachverständigengutachten einzuholen

Es ist auch nicht in jedem Einzelfall notwendig, neue Sachverständigengutachten zum Sicherheitsniveau einzuholen, wenn ein Karteninhaber vorträgt, er habe die Karte nicht benutzt, die PIN nicht dabeigehabt, etc. (Werner in: Sorgel, BGB, § 675w Rn. 25, m.w.N.). Vorausgesetzt, dem Karteninhaber gelingt die erst einmal notwendige Beweisvermutungs-Widerlegung oder Anscheinsbeweis-Entkräftung, ist die Einholung neuer Sachverständigengutachten auch dann entbehrlich, wenn z.B. an den Sitzgerichten von Kartenemittenten und Processing-Unternehmen die Tatsachen das konkret genutzte Sicherheitssystem betreffend und dessen ausreichendes Sicherheitsniveau für die Anwendung des Anscheinsbeweises gerichtsbekannt (§ 284 ZPO) oder offenkundig (§ 281 ZPO) sind. Auch kann die Verwertung von in Parallelprozessen eingeholten Sachverständigengutachten nach § 411a ZPO oder die Verwertung von Sachverständigengutachten als Urkundenbeweis die erneute sachverständige Begutachtung entbehrlich machen (BGH, Beschl. v. 06.07.2010 - XI ZR 224/09 Rn. 12); Baumbach/Lauterbach, ZPO, § 411a Rn. 1; Eichele in: Saenger, ZPO, 4. Aufl. 2011, § 411a Rn. 2; Greger in: Zöller, ZPO, 29. Aufl. 2012, § 411a Rn. 1).

Die Aussage im BGH-Urteil vom 29.11.2011 (XI ZR 370/10 Rn. 37), „in älterer Rechtsprechung gewonnene Erkenntnisse (trügen für die Frage des ausreichenden Sicherheitsniveaus) nichts bei, wenn den (streitbefangenen) Kartenverfügungen neue oder wesentlich geänderte technische Verfahren zugrunde liegen“, ist als Bedingung gefasst und auch so zu verstehen. Liegen keine neuen oder wesentlich geänderten technischen Verfahren zugrunde, steht einer Verwertung älterer Erkenntnisse und Sachverständigengutachten nichts im Wege. Dies ist insbesondere dann der Fall, wenn und solange in dem fraglichen Sicherheitssystem nach wie vor die als sicher anerkannten Triple-DES-Verfahren für die PIN-Generierung und PIN-Verifizierung eingesetzt werden – was bis dato der Fall ist.

Geklärt ist nach dem BGH-Urteil vom 29.11.2011 (XI ZR 370/10 Rn. 37), dass nur auf das „für die konkrete Abhebung eingesetzte System“ im Zeitpunkt der Transaktion abzustellen ist (so auch Maihold in: Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, Rn. 118). Insofern erscheint es widersprüchlich, dass der BGH einerseits im Urteil vom 29.11.2011 (XI ZR 370/10) auf das konkrete System im Zeitpunkt der Abhebung abgestellt hat, andererseits es aber im Fall seines Beschlusses vom 06.07.2010 (XI ZR 224/09 Rn. 12) ablehnte, alte – das dortige konkrete System betreffende – Sachverständigengutachten aus den Jahren 2000 und 2002 für die im dortigen Fall ebenso alten streitigen Transaktionen aus den Jahren 2001 bis 2003 zu verwerten.

E. Zusammenfassung

Anders als Schulte am Hülse/Welchering (NJW 2012, 1262) meinen, sind weder aufgrund einer „aktuellen Entwicklung der Kriminalität“ noch aufgrund angeblicher „technischer Möglichkeiten der Täter“ zur PIN-Erlangung Zweifel daran angebracht, dass die nach h.M. in Literatur und Rechtsprechung – auch im

neuen Zahlungsdiensterecht – anerkannten Anscheinsbeweis-Grundsätze im Zahlungskartenrecht weiterhin anzuwenden sind.

Die Fälle der Lost/Stolen-Fallgruppe sind von denen der Skimming-Fallgruppe zwingend zu unterscheiden, da sie jeweils unterschiedlichen Rechtsfolgen unterliegen. Die aktuelle Entwicklung der Kriminalität in den sog. Lost-Stolen-Fällen, für die die Anscheinsbeweis-Rechtsprechung im Grundsatz entwickelt wurde, gibt für Änderungen keinen Anlass, da die Fallzahlen in dieser Fallgruppe nahezu konstant geblieben sind. Soweit es in den vergangenen Jahren Steigerungen der Fallzahlen in der Skimming/Dubletten-Fallgruppe gegeben hat, ist dies für die Frage der Fortgeltung des Anscheinsbeweises irrelevant, da für diese Fälle die Anscheinsbeweis-Rechtsprechung nicht zur Anwendung kommt. Unabhängig hiervon hervorzuheben ist, dass selbst in der Skimming/Dubletten-Fallgruppe Fälle und Schäden seit Anfang 2011 insbesondere aufgrund der Einführung der EMV-Chip-Technologie markant zurückgegangen sind.

Die Frage, welcher Fallgruppe – ob der Lost/Stolen-Fallgruppe oder der Skimming/Dubletten-Fallgruppe – ein Schadensfall zuzuordnen ist, und ob eine Original-Zahlungskarte bei der streitigen Transaktion zum Einsatz kam, ist klärbar. Hierzu tragen insbesondere neben der neuen, ab Anfang 2011 europaweit eingeführten EMV-Chip-Technologie auch die erfolgreichen Abwehr- und Aufklärungsmöglichkeiten der Kreditwirtschaft entscheidend bei.

Keine der angeblichen PIN-Abgriffs- und Missbrauchsmöglichkeiten, die Schulte am Hülse/Welchering (NJW 2012, 1262) anreißen, existieren nach Expertenwissen in den DES-basierten Realwelt-PIN-Systemen der nationalen und internationalen Zahlungskartenwirtschaft. Sie kommen daher auch nicht als – atypische – Möglichkeiten in Betracht, wie Täter (anders als durch grob fahrlässige Verletzung der Sorgfaltspflicht zur Geheimhaltung der PIN durch den Karteninhaber) an die korrekte PIN hätten herankommen können. Ebenso wenig vermögen die vorgebrachten alten und abzulehnenden Mindermeinungen in instanzgerichtlichen Entscheidungen aus den Jahren 1999, 2002 und 2003 oder das in Fn. 26 zitierte Urteil des AG Berlin-Mitte (Urt. v. 25.11.2009 - 21 C 442/08 - NJW-RR 2010, 407), welches vom LG Berlin aufgehoben wurde, die Fortgeltung des Anscheinsbeweises in Frage zu stellen.

Anders als Schulte am Hülse/Welchering meinen (NJW 2012, 1266), sind Zahlungskartenemittenten nicht erst seit dem BGH-Urteil vom 29.11.2011 (XI ZR 370/10) gehalten, in Streitfällen technische Aufzeichnungen über die Zahlungsvorgänge vorzulegen; dies war auch bisher erforderlich.

Im neuen Zahlungsdiensterecht kommt jedoch der Dokumentation der Zahlungsvorgänge (in Form von Transaktionsprotokollen, Geldautomatenprotokollen, Rückbelastungsdokumentationen, etc.) eine größere praktische Bedeutung als nach bisherigem Recht zu. Denn zum einen wurde durch § 675w BGB im Streitfall den Zahlungsdienstleistern die Pflicht zum Nachweis der Authentifizierung und der ordnungsgemäßen Aufzeichnung, Verbuchung und störungsfreien Durchführung des Zahlungsvorgangs auferlegt, zum anderen jedoch wurden neue – durch Dokumentation verstärkte – gesetzliche Beweisvermutungen zugunsten der Zahlungsdienstleister eingeführt (gemäß § 675w Satz 2 und Satz 3 Nr. 1 BGB für die Verwendung des Zahlungsauthentifizierungsinstruments bzw.-verfahrens durch den Zahlungsdienstnutzer selbst oder durch eine von ihm autorisierte Person, oder gemäß § 675w Satz 2 und Satz 3 Nr. 3 BGB für die Verletzung einer oder mehrerer Pflichten des Zahlungsdienstnutzers gemäß § 675l BGB bzw. vertraglichen Sorgfaltspflichten). Der Zahlungsdienstnutzer kann diese Beweisvermutungen nur mit qualifiziertem Vortrag und Nachweis unter Erfüllung bestimmter Anforderungen, allerdings nicht durch bloße Behauptungen, widerlegen – ebenso wie er auch den Anscheinsbeweis nur mit entsprechendem qualifizierten Vortrag und Nachweis entkräften kann.