Zeitschrift für
Informations-,
Telekommunikations-
und Medienrecht

MMR
MultiMedia und Recht

■ IT-Vertragsrecht und eCommerce ■ Immaterialgüterrecht ■ Wettbewerbs- und Kennzeichenrecht
■ Telekommunikations- und Medienrecht ■ Datenschutzrecht ■ Verfahrensrecht

Sonderdruck aus MMR Heft 2/2010

ULRICH SCHULTE AM HÜLSE / SEBASTIAN KLABUNDE

Abgreifen von Bankzugangsdaten im Onlinebanking

Vorgehensweise der Täter und neue zivilrechtliche Haftungsfragen des BGB

Telekommunikations- und Medienrecht

Verlag C.H.Beck München

ULRICH SCHULTE AM HÜLSE / SEBASTIAN KLABUNDE

Abgreifen von Bankzugangsdaten im Onlinebanking

Vorgehensweise der Täter und neue zivilrechtliche Haftungsfragen des BGB

Telekommunikations- und Medienrecht

Für den Kriminellen der Gegenwart bilden Zugangs- und Transaktionskennwörter die Eintrittskarte in die geschützten Bereiche von Banktransaktionen, deren Abgreifen seit einigen Jahren einen Brennpunkt im Bereich der IuK-Kriminalität bildet. Die Täter machen es sich zunutze, dass die Kommunikation zwischen Bank und Kunde durch Fernkommunikationsmittel geprägt ist und den persönlichen Kontakt verdrängt hat. Bei der (zivil-)rechtlichen Durchdringung dieser Thematik sind zwei Aspekte bedeutsam: Auf der Ebene des Sachverhalts haben sich die Methoden der Täter beim Abgreifen von Kontozugangsdaten in den letzten Jahren konsequent weiterentwickelt. Auf der rechtlichen Ebene tritt seit dem 31.10.2009 eine veränderte Rechtslage auf Grund der Umsetzung der sog. Sepa-Richtlinie in den §§ 675u ff. BGB hinzu.

I. Unterschiedliche Fallvarianten

Dem Abgreifen von Kontozugangsdaten kommt durch die seit Jahren kontinuierlich angestiegenen Fallzahlen eine erhebliche Praxisrelevanz zu.[1] Zugleich liegt ein Grundproblem in der (zivil-)rechtlichen Durchdringung darin, dass Kontozugangsdaten auf unterschiedliche Weise abgegriffen werden und Kriminelle sich dabei sehr geschickt an die jeweiligen technischen Systeme der Banken anpassen. Ein kurzer Blick auf die aktuellen Varianten dieser Kriminalitätsform erscheint deshalb angezeigt.

1. Vortäuschen eines Kommunikationspartners

Mit dem Begriff „Man in the Middle" oder „der dritte Mann" wird eine Angriffsform des Abgreifens von Kontozugangsdaten bezeichnet, bei dem sich die Täter zwischen den Rechner des Bankkunden und das Rechenzentrum der Bank schalten. Dabei übernehmen sie die Kontrolle über den Datenverkehr und manipulieren ihn.[2]

1 Die Fallzahlen im Bereich des Abfangens von Kontozugangsdaten steigen nach Aussage des *BKA* seit Jahren kontinuierlich an: Lt. einer PM v. 20.11.2007 nahmen die Fälle schon 2006 um 26,4% im Vergleich zum Vorjahr zu. 2007 stiegen sie erneut an. Im Jahre 2008 war dann lt. einer PM v. 8.10.2009 nochmals eine Steigerung von mehr als 60% im Vergleich zum Vorjahr zu verzeichnen, vgl. www.bka.de. In den USA wurde der Schaden durch „Identitätsdiebstahl" schon 2003 auf US-$ 2,4 Mrd. geschätzt (*Löhnig/Würdinger* WM 2007, 961).

2 Nicht außer Acht gelassen werden darf, dass ein erfolgreiches Abgreifen von Kontozugangsdaten prinzipiell auch daran liegen kann, dass es den Tätern gelungen ist, die Post mit der TAN-Liste abzufangen oder dass ein untreuer Bankmitarbeiter, der Zugang zu vertraulichen Zugangsdaten hat, diese Daten unberechtigt nutzt.

a) Scannen der Internet-Knotenrechner

Bei einer typischen Transaktion im Onlinebanking sendet der Bankkunde vom heimischen PC mit Hilfe seines Browsers Daten an das Rechenzentrum seiner Bank, die zunächst am nächstgelegenen Internet-Knotenrechner eintreffen. Dieser berechnet den schnellsten Weg durch das Netz zum Bankrechner. Im Rahmen der notwendigen Authentifizierung des Bankkunden wird nun eine ggf. indizierte und unverbrauchte „Transaktionsnummer" (TAN) abgefragt. Nach erfolgter Authentifizierung führt die Bank die Transaktion aus und schickt eine Bestätigung an den Kunden-PC zurück. Laut einem Bericht der FAZ gelang es Tätern aus St. Petersburg im Jahre 2008, ca. 430 Internet-Knotenrechner in Deutschland zu scannen, die Kontozugangsdaten abzufangen und durch nicht autorisierte Überweisungen insgesamt knapp € 25 Mio. zu erbeuten.[3] Da die Daten per „Secure Sockets Layer" (SSL) verschlüsselt waren, konnten die Täter sie nicht direkt auslesen. Sie erfuhren jedoch, von welchem Anschluss die Daten an einen bestimmten Bankrechner gesendet werden sollten. Die Täter leiteten die Daten um und täuschten die Bankkunden mit einer nachgeahmten und vertrauenserweckenden Internetseite, die derjenigen der eigenen Bank täuschend echt ähnlich sah. Von dort wurden dann Zugangsdaten, wie die „Persönliche Identifikations-Nummer" (PIN) und eine oder mehrere TAN, vom Bankkunden abgefordert. Mit den so erbeuteten Daten meldeten die Täter sich dann unter der Identität des Bankkunden beim Rechner der kontoführenden Bank an und überwiesen Geld auf ein Konto in Südafrika.[4]

b) Datenmanipulation mit Hilfe von „Trojanern"

Als eine Tatvariante und ein Tatmittel für die „Man in the Middle"-Angriffe verwenden Täter häufig kleine Computerprogramme („Trojaner"). Das *AG Hamm* hatte diese Tatvariante bereits 2005 in einem Strafverfahren beschrieben: Zunächst wird ein „Trojaner" auf dem PC des Geschädigten installiert, den dieser sich beim „Surfen" im Internet oder durch den Empfang einer „Spam-E-Mail" eingefangen hat. Sobald der Geschädigte eine Internetverbindung zu seiner Bank herstellt, liest das Programm unerkannt auch die für eine Transaktion notwendige PIN und eine oder mehrere TAN mit, indem der Trojaner sich unbemerkt zwischen die Datenverbindung des Kunden und seiner Bank schaltet.[5] Inzwischen ist diese Methode derart verfeinert worden, dass sie auch bei den „indizierten TAN-Verfahren" (iTAN) funktioniert[6] und sogar dann, wenn ein eigener Zugangsrechner den Austausch von in Echtzeit ermittelten Zahlenkolonnen zur Authentifizierung abverlangt[7]. Zwar können derartige Angriffe durch die regelmäßige Verwendung von Virenschutzprogrammen und die Installation einer Firewall reduziert werden. Gänzlich zu verhindern sind sie hierdurch jedoch nicht; vor allem dann nicht, wenn der „Trojaner" dem Schutzprogramm zum Tatzeitpunkt noch unbekannt war.[8]

c) Variationen

Die Art und Weise der Datenmanipulation unterscheidet sich im Einzelfall, je nachdem welches System die jeweilige Bank bereithält und wie dieses zu überwinden ist. In einer Variante wird der Kunde mit Hilfe des Schadprogramms von vornherein auf eine gefälschte Internetseite geleitet, die derjenigen der eigenen Hausbank täuschend ähnlich sieht. Technisch wird dabei die „Übersetzung" von Domainnamen zu numerischen IP-Adressen manipuliert (sog. Pharming oder DNS-Spoofing).[9] Der Namensserver wird mit Hilfe der „Malware" derart verändert, dass er selbst bei Eingabe der richtigen URL nicht mehr die echte IP-Adresse (die Internetseite der eigenen Hausbank) ermittelt, sondern der Nutzer direkt zu der IP-Adresse der gefälschten Internetseite geleitet wird. Scheinbar gibt der Kunde seine Transaktionsdaten nun im geschützten Bereich der vermeintlich angewählten Hausbank ein. Tatsächlich aber landen alle Daten bei den Tätern. Aus der Kundensicht findet die Tathandlung statt, wenn sich der Bankkunde gerade in das Onlinebanking einloggt oder einen Überweisungsauftrag abschließt. In diesem Augenblick öffnet sich ein neues Fenster, welches in den Leitfarben der eigenen Bank gehalten und mit deren Logo ausgestattet ist. Dem Kunden wird mitgeteilt, der Login sei nicht erfolgreich verlaufen oder die letzte Überweisung habe nicht abgeschlossen werden können. Deshalb wird gebeten, eine neue, unverbrauchte TAN zur Authentifizierung oder zur Freischaltung nach Fehleingabe einzugeben. Auch bei dieser Variante schöpfen Bankkunden häufig keinen Verdacht, da sie sich in diesem Moment in die ihnen vertraute Umgebung des Onlinebanking eingeloggt haben. In einer anderen Variante wird der Trojaner so programmiert, dass er die Tastatureingaben protokolliert (sog. „Keylogger"). Im Verborgenen werden die Daten dann an die Täter gesendet.

Diese kurze Übersicht bildet nur einen Auszug der gegenwärtig bekannten Alternativen zu den Sachverhalten, die jeweils kombinierbar und im Hinblick auf Verbesserungen der Sicherheitsanforderungen auch jederzeit erweiterbar und veränderbar sind.

2. Zwischengeschalteter Geldkurier

Ein Konto kann im Onlinebanking nur durch eine Überweisung auf ein anderes Konto abgeräumt werden, dessen Inhaber sich mit Hilfe der Strafverfolgungsorgane eventuell ermitteln lässt. Ein Dritter muss deshalb für die Täter die Geldkurierfunktion übernehmen, wobei es für die Täter von Bedeutung ist, dass sie über den Geldkurier nicht entdeckt werden. Aus diesem Grunde suchen sich die Täter den Geldkurier, dem meist eine geringe Provision versprochen wird, gerne anonym über das Internet oder sie sprechen eine fremde Personen in der Öffentlichkeit an.[10] Dieser erhält den Auftrag, das auf seinem Konto empfangene Geld abzuheben und z.B. mit Hilfe von Barüberweisungen (z.B. per Western Union) ins Ausland zu transferieren.

---

3 *Welchering*, FAZ Nr. 196 v. 25.8.2009, „Motor und Technik", S. T1.

4 Demgegenüber steht die klassische Variante des Leerräumens von Konten, die zwar bis in die jüngste Zeit in der Rechtsliteratur beschrieben wird (etwa *Popp*, NJW 2004, 3517 f.; *Gercke*, CR 2005, 606; *Beck/Dornis*, CR 2007, 642), der seit dem Systemwechsel der meisten Banken zum iTAN- bzw. HBCI-Verfahren jedoch die geringste Bedeutung zukommt. In der klassischen Variante wurden Bankkunden noch mittels Spam-E-Mails dazu aufgefordert, einem vermeintlichen in der E-Mail enthaltenen Link auf die Internetseite der eigenen Hausbank zu folgen und wegen einer angeblichen Sicherheitsüberprüfung eine oder mehrere unverbrauchte TAN einzugeben. Allerdings berichtete bereits *Borges*, NJW 2005, 3314, von der Methode des Ausspähens mittels Trojaner; zu den aktuellen Begehungsformen vgl. außerdem *Welchering* (o. Fußn. 3, S. T1) sowie *Goeckenjan*, wistra 2008, 128, 129, und *Graf*, NStZ 2007, 129, dort Fußn. 1).

5 *AG Hamm* CR 2006, 70 f. m. Anm. *Werner*.

6 Der Bankkunde tippt einen Überweisungsauftrag über € 10,– an X ein und sendet die Daten an seine Bank. Noch bevor das Datenpäckchen per SSL verschlüsselt und durch das Internet gesendet wird, fängt der Trojaner es ab und verändert die Daten in eine Überweisung i.H.v. € 10.000 an Y. Nur dieser manipulierte Überweisungsauftrag wird verschlüsselt an die kontoführende Bank gesendet. Die Bank verlangt vom Bankkunden als Rückfrage zur Authentifizierung: „Bitte bestätigen Sie die Überweisung in Höhe von € 10.000,– an Y mit der iTAN Nr. 37". Nachdem die Rückfrage am PC des Bankkunden angekommen ist und entschlüsselt wurde, aber noch bevor sie auf dem Bildschirm des Bankkunden angezeigt wird, fängt der Trojaner die Daten erneut ab, verändert sie und zeigt dem Bankkunden am Bildschirm als Rückfrage lediglich an: „Bitte bestätigen Sie die Überweisung in Höhe von € 10,– an X mit der iTAN Nr. 37". Sobald der Kunde seine unverbrauchte iTAN Nr. 37 eingegeben hat, gibt der Trojaner diese an die Bank für die vom Bankkunden nicht gewollte Überweisung an Y weiter. Die Bank überweist nun € 10.000,– an Y. Wenn der Trojaner professionell programmiert wurde, überprüft er vor dem Angriff den Verfügungsrahmen des Bankkunden und zeigt dem Bankkunden nach dem Angriff noch einige Tage lang in der Kontoübersicht eine tatsächlich nicht existente Überweisung i.H.v. € 10,– an X an.

7 Zur Kritik am HBCI-Verfahren, SMS-TAN-Verfahren oder e-TAN vgl. *Welchering* (o. Fußn. 3), S. T2.

8 *LG Mannheim* MMR 2008, 765.

9 *Borges* (o. Fußn. 4), S. 3314.

10 Vgl. den Tatbestand bei *AG Neukölln* MMR 2010, 137 (Ls.) – in diesem Heft = BeckRS 2009 28105, amtl. Umdr. S. 2–3.

3. Manipulation von Aktienkursen

Eine weitere gefährlichere Variante des Abfangens von Zugangsdaten richtet sich gezielt gegen die Inhaber von Online-Depots. Um die Zugangsdaten zum Depot und einige unverbrauchte TAN abzufangen, nutzen auch diese Täter meist „Trojaner". Mit Hilfe der abgefangenen Zugangsdaten werden der Depotbank „im Namen des Bankkunden" unter Ausschöpfung des Verfügungsrahmens Order zum Kauf von „geeigneten" Aktien erteilt.[11] Der Vermögenszuwachs besteht für die Täter darin, dass sie bereits im Vorfeld die gleichen riskanten Aktien gekauft hatten. Zu diesem Zeitpunkt war der Kurswert noch niedrig. Die anschließende Order dient dem Zweck, den Aktienkurs künstlich in die Höhe zu treiben. Sobald der Kurs gestiegen ist, verkaufen die Täter ihre Aktien zum hohen Kurswert und streichen den Gewinn ein. Bis der Depot-Kunde davon etwas bemerkt, ist der Kurs meist schon wieder gefallen. Auf diese Weise entsteht auch der Vermögensschaden, denn der Bankkunde kann seine unfreiwillig im Depot gehaltenen Aktien nur noch zu einem niedrigeren Wert verkaufen.

II. Zivilrechtliche Fragen

Die Rückabwicklung des eingetretenen Schadens vollzieht sich im Mehrpersonenverhältnis: der Bankkunde, dessen Konto abgeräumt wurde, unterhält eine Vertragsbeziehung zur konto- oder depotführenden Bank, die den Auftrag ausführt (anweisende Bank), ohne vom Bankkunden beauftragt worden zu sein. Begünstigte des Auftrags sind sodann die Täter; wobei beim Abräumen des Kontos – nicht jedoch beim Manipulieren von Aktienkursen – noch ein Geldkurier (Finanzagent) dazwischengeschaltet ist. In einigen Fallvarianten ist die kontoführende Bank des Bankkunden zugleich die Hausbank des Geldkuriers.[12] Ist dies nicht der Fall, wäre noch zwischen der anweisenden Bank des Bankkunden und der angewiesenen Bank des Geldkuriers zu unterscheiden. Dass der Bankkunde oder die anweisende Bank die Täter in Anspruch nehmen können, ist unproblematisch zu bejahen. Da die Täter aber gerade die durch den gewählten Transaktionsvorgang geprägte Anonymität für sich nutzen, werden sie vergleichsweise selten ermittelt.

1. Anspruch des Bankkunden gegen die anweisende Bank

Von großem praktischem Interesse ist die Frage, ob der Bankkunde von seiner Bank den Ersatz des von seinem Konto zu Unrecht abgebuchten Betrags zurückverlangen kann. Hat die ausführende Bank den Betrag vom Geschädigten abgebucht, ohne dass eine wirksame Anweisung vorlag, so kann sie mangels Auftrag keinen Entgelt- und Aufwendungsersatzanspruch nach §§ 675f Abs. 4 Satz 1, 675c Abs. 1 i.V.m. 670 BGB gegen den Kunden haben. Wie der *BGH* bereits für den Fall eines gefälschten Schecks exemplarisch ausführte, haftet zunächst die ohne wirksame Anweisung ausführende Bank, d. h. sie trägt das Risiko, dass der fälschlicherweise überwiesene Betrag nicht zurückgebucht werden kann.[13] Dass es tatsächlich auf dem Konto des Bankkunden – der in diesem Fall streng genommen kein Geschädigter ist – zu einer Belastungsbuchung kommt, ist für den tatsächlichen Forderungsbestand gegen die Bank ohne Belang.[14] Bereits aus dem Vertragsverhältnis zwischen dem Bankkunden und der angewiesenen Bank, deren Zweck gerade darin besteht, der Bank nur autorisierte Transaktionen vornehmen zu lassen, ergibt sich, dass der Kunde gegen die Bank einen Anspruch auf Berichtigung des insoweit fehlerhaft ausgewiesenen Kontostands hat. Diese Rechtsfolge hat der Gesetzgeber in § 675u BGB seit dem 31.10.2009 gesetzlich normiert.[15]

2. Aufrechenbarer Anspruch der Bank gegen den Bankkunden

Die davon zu trennende Frage, inwiefern der Bank gegenüber dem Bankkunden ein Schadensersatzanspruch zustehen kann, mit dem sie zumindest teilweise die Aufrechnung erklären könnte, regelt seit dem 31.10.2009 nun § 675v BGB.

a) Haftung nach § 675v Abs. 1 BGB

Beruht ein nicht autorisierter Zahlungsvorgang auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Zahlungsauthentifizierungsinstruments, kann die Bank gem. § 675v Abs. 1 Satz 1 BGB vom Bankkunden verschuldensunabhängig einen Eigenanteil am entstandenen Schaden verlangen, der jedoch auf max. € 150,– begrenzt ist.[16] Die Tatbestandsvoraussetzungen des § 675v Abs. 1 Satz 1 BGB passen nicht auf die vorgenannten Fallkonstellationen, da dem Bankkunden regelmäßig keine TAN-Listen gestohlen oder geraubt werden und die TAN auch nicht auf sonstige Weise abhandenkommen, wenn die Täter einzelne TAN abgreifen, die TAN-Liste aber zugleich im Besitz des Bankkunden bleibt. Die verschuldensunabhängige Gefährdungshaftung des § 675v Abs. 1 Satz 1 BGB setzt aber die Feststellung voraus, dass die personalisierten Sicherheitsmerkmale dem Inhaber durch einen tatsächlichen Besitzverlust ohne seinen Willen abhanden gekommen sind. § 675v Abs. 1 Satz 1 BGB ist jedoch nicht eröffnet, wenn die Methode der Datenausspähung ohne einen Besitzverlust der TAN-Liste abläuft und das Abgreifen der Kontozugangsdaten insgesamt dem Verantwortungsbereich der technischen Sicherheit des jeweiligen Onlinebanking-Systems zugeordnet werden kann.[17]

Zwar stellt § 675v Abs. 1 Satz 2 BGB klar, dass die im Satz 1 geregelte und auf einen maximalen Eigenanteil von € 150,– be-

11 Die Täter machen sich gezielt die Möglichkeiten des weltweiten Handels von Aktien zunutze und manipulieren Aktienkurse von vergleichsweise unbekannten Unternehmen, die an Börsen in anderen Kontinenten gehandelt werden. Auf diese Weise zwingen die Täter die Strafverfolgungsorgane dazu, ihre Ermittlungstätigkeit auf ein Rechtshilfeersuchen abzustützen. Meist werden die Verfahren nach kurzer Zeit eingestellt, da die Täter nicht ermittelt werden konnten, etwa: Einstellungsbescheid der *StA München II* v. 30.4.2008 – 63 UJs 22209/07, n.v.

12 Um nicht entdeckt zu werden, sind die Täter darauf angewiesen, dass die Geldtransaktion vom Konto des Geschädigten auf das Konto des Geldkuriers zügig verläuft. Dies funktioniert am besten, wenn eine reine Hausüberweisung vorgenommen wird, bei der die Bank des Bankkunden und diejenige des Geldkuriers identisch sind. Deshalb suchen sich Täter gezielt Geldkuriere aus, die ein Konto bei der Bank führen, bei der sie zuvor die Kontozugangsdaten der Bankkunden ausgespäht haben.

13 *BGH* NJW 2001, 2629, 2630; *BGH* NJW-RR 1990, 1200, 1201; *BGH* NJW 2008, 2331; *LG Mannheim* MMR 2008, 765; *Schimansky*, in: Schimansky/Bunte/Lwowski, Bankrechts-Hdb., Bd. 1, 3. Aufl. 2007, § 49 Rdnr. 93.

14 *KG* MMR 2010, 128 – in diesem Heft.

15 § 675u BGB ist insofern Teil der Umsetzung der Sepa (Single € Payments Areal)-Richtlinie: Die fehlende Zustimmung zu einer Zahlung führt gem. Art. 54 Abs. 1 Sepa-Richtlinie zur Annahme eines nicht autorisierten Zahlungsvorgangs. Informiert der Bankkunde die Bank umgehend nach Kenntniserlangung über den erfolgten Angriff, kommt ihm ein Erstattungsanspruch zugute.

16 Der Tatbestand des „sonst abhanden gekommenen Zahlungsauthentifizierungsinstruments" wurde i.R.d. Gesetzgebungsverfahrens auf Wunsch des *Bundesrats* in § 675v Abs. 1 BGB aufgenommen, BR-Drs. 848/08, B. v. 19.12.2008, Nr. 20 = S. 15 f.: „Offen bleibt dabei, was für andere Situationen des Abhandenkommens eines Zahlungsauthentifizierungsinstruments gilt. Als Beispiel zu nennen ist der Raub, der auch ein Abhandenkommen (d.h. einen Besitzverlust ohne Willen des Inhabers) darstellt. Auch in solchen Fällen erscheint es gerechtfertigt, dass sich der Zahler vor einer Verlustmeldung an einem Schaden beteiligt. Es sollte daher geprüft werden, ob „Verlust" und „Diebstahl" europäisch nicht so auszulegen sind, dass jegliches Abhandenkommen erfasst ist."

17 In den Erwägungsgründen der Sepa-Richtlinie wird ausgeführt, dass die verschuldensunabhängige Haftung dazu dient, dem „Zahlungsdienstnutzer einen Anreiz zu geben, seinem Dienstleister jeden Diebstahl oder Verlust eines Zahlungsinstruments unverzüglich anzuzeigen". Um „das Risiko nicht autorisierter Zahlungen zu verringern", soll „der Nutzer für einen begrenzten Betrag selbst haften". Durch die Sepa-Richtlinie soll allerdings die „Verantwortung der Zahlungsdienstleister für die technische Sicherheit" nicht berührt werden (RL 2007/64/EG des Europäischen Parlaments und des Rates v. 13.11.2007, ABl. EU Nr. L 319/1 v. 5.12.2007, Erwägungsgrund Nr. 32).

grenzte Haftung auch bei allen „sonstigen missbräuchlichen Verwendungen" eingreift, „sofern der Zahler die personalisierten Sicherheitsmerkmale nicht sicher aufbewahrt hat". Insofern eröffnet Satz 2 im Verhältnis zu Satz 1 zwar einen gesonderten verschuldensabhängigen Haftungstatbestand. § 675v Abs. 1 Satz 2 BGB setzt jedoch den wenigstens leicht fahrlässigen Nachweis der Nichtaufbewahrung der Sicherheitsmerkmale voraus.[18]

b) Haftung nach § 675v Abs. 2 BGB

Allerdings ist eine Haftung des Bankkunden auch über den auf € 150,– begrenzten Eigenanteil hinaus gem. § 675v Abs. 2 BGB denkbar, wenn der Bankkunde den Schaden herbeigeführt hat, indem er in betrügerischer Absicht gehandelt oder eine oder mehrere seiner Pflichten nach § 675l BGB wenigstens vorsätzlich oder grob fahrlässig verletzt hat.[19] § 675v BGB enthält eine abschließende Regelung, deren Wertung im Anwendungsbereich dieser Vorschrift durch andere Vorschriften (etwa § 280 Abs. 1 BGB) nicht umgangen werden kann.

Diese Haftungsfreizeichnung der Bank ist allerdings nur bei einer grob fahrlässigen Pflichtverletzung des Bankkunden möglich. Grobe Fahrlässigkeit liegt vor, wenn der Schuldner bei seinem Handeln ganz nahe liegende Überlegungen nicht anstellt oder beiseiteschiebt und dasjenige unbeachtet lässt, was sich im gegebenen Fall jedermann aufgedrängt hätte.[20] Während bei der einfachen Fahrlässigkeit ein objektiver Maßstab anzulegen ist, sind bei grober Fahrlässigkeit auch subjektive Erwägungen, die in der Person des Bankkunden liegen können, zu berücksichtigen. Soweit es sich bei dem Bankkunden um einen ungeübten Nichtfachmann handelt, ist es berücksichtigungsfähig,[21] dass bei grober Fahrlässigkeit den Handelnden auch in subjektiver Hinsicht ein schweres Verschulden treffen muss.[22]

Abschied vom Prima-facie-Beweis

Vereinzelt wurde früher vorgeschlagen, im Bereich des Onlinebanking einen Ausweg zu Gunsten der Bank über die Grundsätze des Anscheinsbeweises zu eröffnen.[23] Zumindest bei Sicherheitssystemen, die dem aktuellen Stand der Technik entsprechen, sei es gerechtfertigt, das Risiko vollmachtlosen Handelns dem Kontoinhaber aufzubürden. Schließlich benötigt der Täter die aktuelle PIN des Opfers, die Kontonummer und eine nicht verbrauchte TAN, die häufig nur für eine und manchmal auch nur für eine konkrete, von der Bank vorgegebene, Transaktion gültig sei.

Über die Grundsätze des Anscheinsbeweises ist es jedoch nicht möglich, dem Bankkunden eine grob fahrlässige Pflichtverletzung nachzuweisen. Bereits die Folgerung, dass ein Missbrauch der Zugangsdaten nur aus einer dem Kunden zuzurechnenden Verletzung der Geheimhaltungspflicht resultieren kann, entspricht einer veralteten Sichtweise. Ein Blick auf den Stand der heutigen, den Tätern zur Verfügung stehenden Technik der Datenausspähung zeigt, dass ein Abgreifen der sensiblen Daten wesentlich raffinierter durchgeführt wird als noch zu Zeiten, wo man scheinbar mit einer vom Kreditinstitut stammenden E-Mail, zumeist noch in schlechtem Deutsch, kurzerhand zur Eingabe von PIN und TAN aufgefordert wurde.[24] Inzwischen fangen Trojaner-Programme die Eingabe der jeweils verlangten TAN ab und eröffnen den abfangenden Tätern die Möglichkeit, anstelle des Kunden eine beliebige Transaktion mit dieser TAN auszuführen. Der Kunde merkt in diesen Fällen allenfalls dann etwas, wenn die sonst übliche Auftragsbestätigung nicht auf dem Bildschirm erscheint. Im Einzelfall wird sogar diese Auftragsbestätigung durch den „Trojaner" vorgespielt. Alternativ wird der Kunde nicht auf die tatsächliche Homepage seiner Bank, sondern auf eine täuschend ähnliche Internetseite durch den Trojaner geleitet (Pharming). Auch hier gibt er im Vertrauen auf die gewohnte Umgebung und die Authentizität der Website die entsprechenden Daten ein, die kurz darauf von den Tätern zur Kontoabräumung missbraucht werden.[25] Durch die Tatsache, dass die Viren- und Trojanervarianten naturgemäß den entsprechenden Schutzprogrammen immer einen Schritt voraus sind, kann auch ein noch so auf Sicherheit bedachter Nutzer von Onlinebanking nicht vor dem Ausspähen seiner Daten sicher sein. Ein zurechenbarer Anscheinsbeweis lässt sich demzufolge aus der Täterkenntnis der relevanten Zugangsdaten heute nicht mehr herleiten.[26]

Ansatzpunkte für Pflichtverletzungen des Kunden

Als grob fahrlässig könnte man es im Einzelfall ansehen, wenn der Bankkunde auf die klassische Variante des Abgreifens von Kontozugangsdaten hereinfällt, d.h. er folgt dem in einer Spam-E-Mail enthaltenen Link und gibt daraufhin bewusst eine ganze Serie unverbrauchter TAN preis – soweit im Einzelfall in der Person des Handelnden ein schweres Verschulden in subjektiver Hinsicht nicht ausgeschlossen ist. Bereits beim Abgreifen der Kontozugangsdaten mittels Trojaner, insbesondere beim Weiterleiten auf einer gefälschten Internetseite mittels Pharming, lässt sich bereits nicht mehr von einer groben Fahrlässigkeit sprechen. Dies gilt auch dann, wenn der Kunde im Vertrauen auf die gewohnte Umgebung unbewusst eine oder mehrere TAN preisgibt.[27]

Allerdings hat ein Bankkunde die Pflicht, eventuelle Auffälligkeiten bei Überweisungen oder sonstige Anhaltspunkte für Unregelmäßigkeiten unverzüglich nach Kenntniserlangung seinem Kreditinstitut anzuzeigen. Entsprechend der Rechtslage bei gestohlenen EC-Karten, bei denen der Karteninhaber ebenfalls unverzüglich den Verlust dem ausgebenden Institut anzuzeigen hat,[28] begründet eine verspätete Meldung einen Schadensersatzanspruch in Höhe der erfolgten Kontoverfügung durch die Täter. Hätte eine rechtzeitige Anzeige dagegen nichts gebracht, da die Verfügung bereits vor oder unmittelbar zeitgleich mit der Kenntniserlangung des Kunden von der Auffälligkeit vorgenommen wurde, scheidet mangels Kausalität der Pflichtverletzung ein Schadensersatzanspruch der Bank aus.

Zwar wird man von einem durchschnittlich informierten Nutzer von Onlinebanking-Systemen verlangen können, dass er ein aktuelles Virenschutzprogramm sowie eine geeignete Firewall in Betrieb hält, um das Risiko von Datenausspähungen über Trojaner nach Möglichkeit zu begrenzen. Ob der Bankkunde bei einem Unterlassen jedoch ganz nahe liegende Überlegungen

---

18 Die Formulierung geht auf Art. 61 Abs. 1 Sepa-Richtlinie zurück, die unter einem sonst abhanden gekommenen Zahlungsauthentifizierungsinstrument die „missbräuchliche Verwendung" des Zahlungsinstruments versteht, wenn „der Zahler die personalisierten Sicherheitsmerkmale nicht sicher aufbewahrt hat". Der Begriff meint vorrangig den Aufbewahrungsort von PIN und TAN-Listen. Die Interessenlage ist vergleichbar mit der vom EC-Karteninhaber geheimzuhaltenden PIN i.R.d. bargeldlosen Zahlungsverkehrs. Der Nutzer eines Onlinebanking-Systems hat deshalb darauf zu achten, dass die ihm zur Verfügung gestellten PIN und TAN-Listen an einem sicheren Ort und für Dritte unzugänglich aufbewahrt werden. Gelingt es den Tätern, PIN und TAN mit Hilfe von Trojanern abzugreifen, ist davon jedoch nicht der Aufbewahrungsort betroffen.

19 Vgl. *Dienstbach*, Tagungsbericht a-i3/BSI Symposium 2008: Sicherheit von Internetportalen und Identitätsschutz – Bürgerportale – ePA – Crimeware – Haftung – Authentisierung, Bochum, 22.–23.4.2008, JurPC Web-Dok. 104/2008, Abs. 9.

20 St. Rspr.: BGHZ 10, 14, 16; BGHZ 89, 153, 161; *BGH*, B. v. 12.6.2008 – IX ZB 61/06 = BeckRS 2008 13007; *BGH* NJW 1992, 316, 317.

21 Palandt/*Heinrichs*, BGB, 67. Aufl. 2008, § 277 Rdnr. 5.

22 *BGH* NJW 1988, 1265, 1266; *BGH* NJW 2001, 2092, 2093.

23 *Gößmann*, in: Schimansky/Bunte/et al. (o. Fußn. 13), § 55 Rdnr. 26 m.w.Nw.

24 Krit. zum Anscheinsbeweis beim Phishing: *AG Wiesloch* MMR 2008, 626 ff.

25 Zu den technischen Abläufen sehr instruktiv: *LG Köln* WM 2008, 354, 356.

26 *LG Mannheim* MMR 2008, 765.

27 Zur Einordnung der unbewussten Preisgabe von vier TAN als leichte Fahrlässigkeit vgl. *LG Berlin* MMR 2010, 137 (Ls.) – in diesem Heft = BeckRS 2009 28142, amtl. Umdr. S. 5.

28 *OLG Hamm* NJW 1997, 1711.

außer Acht lässt, dürfte fraglich sein; solange es bei dieser Pflichtverletzung auch an der Kausalität zum entstandenen Schaden fehlt, etwa dann, wenn selbst die Nutzung einer geeigneten Schutzsoftware die Tat nicht verhindert hätte.[29]

Verschulden der Bank

Beim Abgreifen von Kontozugangsdaten lässt sich ein Anspruch des Bankkunden gegen seine kontoführende Bank auch auf Grund eines Verschuldens der Bank denken. Aus dem Girokontovertrag ergeben sich wechselseitige Pflichten zur Rücksichtnahme, die jeweils einen Schadensersatzanspruch nach §§ 280 Abs. 1 Satz 1, 241 Abs. 2, 675f BGB begründen können.

Ein solcher Anspruch lässt sich etwa auf eine nur ungenügende technische Aktualisierung der Onlinebanking-Systeme stützen. So kann der Bank zumindest dann ein Vorwurf gemacht werden, wenn sie auch heute noch das veraltete TAN-Verfahren nutzt, bei der für eine Transaktion jede beliebige TAN aus einer Liste verwendet werden kann. Noch weitaus problematischer ist die sog. „Sitzungs-TAN", bei der nach Eingabe einer einzigen TAN beliebige Transaktionen bis zum Ausloggen des Nutzers getätigt werden können. Hier potenziert sich das Risiko, weil das Abfangen einer einzigen TAN ausreicht, um einen großen Schaden zu verursachen. Die Täter erhalten nicht bloß eine ungleich breitere Angriffsfläche, sondern sie fokussieren ihre Angriffe außerdem auf Banksysteme, bei denen sie sich die meisten Chancen ausrechnen können. Den Tätern genügt das Ausspähen einer beliebigen Nummer, ohne dass sie auf die Kombination mit einer speziellen Transaktion angewiesen wären. Obwohl längst nicht mehr Stand der Technik, nutzen auch heute noch einige Kreditinstitute diese unsicheren Systeme.

Weiterhin vermag die Nichtrückbuchung des fälschlicherweise angewiesenen Betrags vom Konto des Geldkuriers im Einzelfall ein Mitverschulden der Bank begründen. Die Bank hat gegen den Geldkurier einen Kondiktionsanspruch aus § 812 Abs. 1 Satz 1 Alt. 2 BGB, welchen sie im Einzelfall gem. Nr. 8 AGB-Banken direkt durch Rückbuchung des Betrags durchsetzen kann, ohne den Rechtsweg beschreiten zu müssen. Erfährt die Bank rechtzeitig, d.h. vor Abschluss der Rechnungsperiode, von der Fälschung der Überweisung, so muss sie im Rahmen ihrer Schadensminderungspflicht zunächst versuchen, ihr Stornorecht auszuüben. Allerdings dürfte es hierbei häufig zu dem Problem kommen, dass eine Rückbuchung nur theoretisch möglich ist. Da die Täter das Guthaben zügig vom Konto des Geldkuriers abheben, würde die Stornobuchung u.U. zu einem Negativsaldo auf dem Konto des Geldkuriers führen, mit der Konsequenz, dass die Bank faktisch auf dem Schaden sitzen bleibt. Insoweit würde es die Anforderungen an die Schadensminderungspflicht überspannen, das Insolvenzrisiko des Geldkuriers der Bank aufzubürden. Jedoch hat sie darzulegen, inwieweit eine Durchsetzung nach Kenntniserlangung von der Fehlbuchung nicht mehr möglich war.

Dogmatisch ergibt sich aus den neuen Regelungen in den §§ 675j ff. BGB folgende Prüfungsreihenfolge: Gem. § 675u BGB hat der Kunde einen Berichtigungsanspruch des fehlerhaft ausgewiesenen Kontostands gegen seine Bank. Auf die verschuldensunabhängige Haftung des § 675v Abs. 1 Satz 1 BGB vermag sich die Bank bei europarechtskonformer Auslegung ebenso wenig zu berufen wie im Regelfall auch nicht auf die verschuldensabhängige Haftung des § 675v Abs. 1 Satz 2 BGB. Allerdings kann die kontoführende Bank dem Anspruch des Kunden einen Schadensersatzanspruch nach § 675v Abs. 2 BGB entgegenhalten, wenn sie im Einzelfall den Nachweis einer grob fahrlässigen Pflichtverletzung des Bankkunden führt. Berücksichtigungsfähig in Höhe des Verursachungsanteils gem. § 254 Abs. 1 BGB ist ggf. ein Verschulden der Bank, das gesondert zum Schaden beigetragen hat.

3. Inanspruchnahme des Geldkuriers

a) Inanspruchnahme durch den Bankkunden

Die Frage nach einer Inanspruchnahme des Geldkuriers durch den Bankkunden stellt sich entsprechend den o.g. Ausführungen insbesondere dann, wenn ein Bankkunde im Verhältnis zur Bank auf einem Teil des Schadens sitzen bleibt. Ein ersatzfähiger Schaden i.S.d. § 249 Abs. 1 BGB liegt bereits dann vor, wenn bei wirtschaftlicher Betrachtungsweise eine konkrete Vermögensgefährdung anzunehmen war.[30] Allerdings kann der Bankkunde den Geldkurier nicht über das Bereicherungsrecht in Anspruch nehmen. Hier fehlt es an einer Leistung, sodass § 812 Abs. 1 Satz 1 1. Alt. BGB ausscheidet. Eine Eingriffs- oder Durchgriffskondiktion steht nur der angewiesenen Bank zu, da die fälschliche Belastungsbuchung zunächst zu ihren Lasten geht.[31] Scheitert das Stornorecht der Bank am fehlenden Guthaben auf dem Konto des Geldkuriers und nimmt der Bankkunde einen Ausgleich vor, kann er gegen die Bank zumindest einen Anspruch auf Abtretung des allein der Bank zustehenden Kondiktionsanspruchs geltend machen.

b) Inanspruchnahme durch die angewiesene Bank

Von praktischem Interesse ist die Frage, ob und unter welchen Voraussetzungen die angewiesene Bank bei dem oftmals identifizierbaren Geldkurier den täuschungsbedingt gutgeschriebenen Betrag zurückfordern kann:

■ Bedeutung der Nr. 8 Abs. 1 AGB-Banken

Existiert zwischen dem Geldkurier und der angewiesenen Bank ein Girovertrag, so ist dieses Rechtsverhältnis i.V.m. Nr. 8 Abs. 1 AGB-Banken maßgeblich. Der Bank steht demnach ein Stornorecht bei fehlerhaften Gutschriften bis zum nächsten Rechnungsabschluss unter der Voraussetzung zu, dass ihr auch ein materieller Rückzahlungsanspruch gegen den Geldkurier zur Verfügung steht.[32] Im Ergebnis begründet Nr. 8 Abs. 1 AGB-Banken somit keinen eigenständigen Anspruch auf Rückzahlung einer fehlerhaften Überweisung, sondern schneidet dem Geldkurier lediglich die Einrede der Entreicherung gem. § 818 Abs. 1 BGB ab. Dies führt dazu, dass die Bank nicht mehr bezüglich der insoweit strengen Voraussetzungen der verschärften Haftung nach § 819 Abs. 1 BGB darlegungs- und beweisbelastet ist. Aus diesen Gründen hält Nr. 8 Abs. 1 AGB-Banken auch einer Inhaltskontrolle nach §§ 307 ff. BGB stand.[33] Eine unangemessene Benachteiligung des Geldkuriers ist darin nicht zu sehen, zumal dieser als begünstigter Kontoinhaber im Regelfall eine irrtümlich erfolgte Gutschrift erkennen wird und die Voraussetzungen der verschärften Haftung somit ohnehin vorliegen.

■ Kondiktionsanspruch der Bank gegen den Geldkurier

Im normalen Überweisungsverkehr ist die gutschreibende Bank lediglich Leistungsmittlerin des Anweisenden. Dem Normalfall

29 Gerade bei Tathandlungen, bei denen Konten mehrerer Bankkunden etwa zeitgleich abgeräumt werden, zeigt sich häufig, dass darunter stets auch solche Bankkunden sind, die über eine entsprechende Schutzsoftware verfügten. Ein Beispiel aus der Praxis ist der Fall *AG Neukölln* (o. Fußn. 10), der strafrechtlich von der *StA Freiburg i.Br.* unter dem Az. 400 Js 4637/07 bearbeitet wurde.

30 *LG Köln* WM 2008, 354, 356.

31 Demgegenüber sieht allerdings das *AG München* ein Kondiktionsanspruch des Phishing-Opfers nach § 812 Abs. 1 Satz 1 2. Alt. BGB als begründet an: CR 2007, 333 m. krit. Anm. *Biallaß*, S. 335.

32 Nr. 8 Abs. 1 AGB-Banken lautet: „Fehlerhafte Gutschriften auf Kontokorrentkonten (z.B. wegen einer falschen Kontonummer) darf die Bank bis zum nächsten Rechnungsabschluss durch eine Belastungsbuchung rückgängig machen, soweit ihr ein Rückzahlungsanspruch gegen den Kunden zusteht (Stornobuchung); der Kunde kann in diesem Fall gegen die Belastungsbuchung nicht einwenden, dass er in Höhe der Gutschrift bereits verfügt hat."

33 *OLG Hamburg* ZIP 2006, 1981 m. Anm. *Borges*; *Bunte*, in: Schimansky/Bunte/Lwowski (o. Fußn. 13), § 13 Rdnr. 14.

liegt eine Leistung des Anweisenden an den Anweisungsempfänger zu Grunde, die über die angewiesene und die gutschreibende Bank vermittelt wird. Fehlt im normalen Überweisungsverkehr der rechtliche Grund für die Leistung, besteht ein vorrangiger Leistungskondiktionsanspruch des Anweisenden gegen den Anweisungsempfänger. Ansprüche der gutschreibenden Bank, die den Anwendungsbereich der Nr. 8 AGB-Banken eröffnen würden, sind dann nicht gegeben.

Im Gegensatz zum Normalfall fehlt es in den Phishing-Fällen aber an einer wirksamen Überweisung, sodass ein vorrangiger Leistungskondiktionsanspruch des Bankkunden gegen den Geldkurier im Ergebnis nicht besteht. Die Frage, ob eine Leistung vorliegt oder nicht, bestimmt sich nach ständiger Rechtsprechung zwar aus der Sicht des Leistungsempfängers.[34] Fehlt es jedoch an einer dem vermeintlich Leistenden zurechenbaren Anweisung, folgt aus dem etwa in § 935 BGB normierten Rechtsgedanken des Veranlassungsprinzips, dass keine Leistung des Bankkunden vorliegt.[35] Insbesondere kann ein etwaiger guter Glauben des Anweisungsempfängers nicht die fehlende Zweck- und Tilgungsbestimmung des Anweisenden überwinden.[36] Folgerichtig lehnt das *LG Bad Kreuznach* einen Kondiktionsanspruch des Bankkunden gegen den Geldkurier ab, schließt dann aber zu Unrecht auf einen Anspruch der Bank aus § 812 Abs. 1 Satz 1 Alt. 1 BGB.[37] Das *Gericht* meint, dass mangels Leistung des Bankkunden an seine Bank nunmehr eine Leistung der Bank an den Geldkurier vorliegen müsse. Auf den ersten Blick scheint dieser Schluss folgerichtig, da die gutschreibende Bank ihrerseits mit dem Geldkurier einen Girovertrag unterhält, aus welchem sie ihren Pflichten nachkommt. Allerdings will sie nicht den tatsächlich gutgeschriebenen Betrag dem Empfänger zuwenden, sondern lediglich die zur Gutschrift führende Dienstleistung. Andere Gerichte lassen auf Grund der Komplexität der bereicherungsrechtlichen Rückabwicklung die Benennung der Anspruchsgrundlage offen und begnügen sich mit einem schlichten Hinweis auf einen Bereicherungsanspruch.[38]

■ Doppelrolle der Bank bei Phishing-Fällen

Zum Verständnis der Problematik ist es hilfreich, sich die für Phishing-Fälle typische Doppelrolle der Bank zu vergegenwärtigen. Sie ist zunächst ausführende Bank des Bankkunden, da sie die Abbuchung vom Konto vornimmt. In zahlreichen Fällen ist die gleiche Bank auch die angewiesene Bank des Geldkuriers. Theoretisch ist hier auch ein Auseinanderfallen der Kreditinstitute denkbar. In der Rolle als vermeintlich angewiesene Bank des Bankkunden steht ihr nach gefestigter Rechtsprechung des *BGH* ein direkter Kondiktionsanspruch gem. § 812 Abs. 1 Satz 1 Alt. 2 BGB zu.[39] Dies folgt daraus, dass der Bankkunde grundsätzlich bei Fehlen einer wirksamen Anweisung einen Rückerstattungsanspruch gegen seine Hausbank hat. Im Ergebnis liegt das Phishing-Risiko deshalb auf Seiten der vermeintlich angewiesenen Bank. Ohne rechtswirksame Anweisung fehlt es an einem Rechtsgrund für die Belastungsbuchung, sodass stets ein Kondiktionsanspruch der Bank dem Grunde nach zu bejahen ist. Die Bank ist ihrerseits Ansprüchen ihres Bankkunden auf Rückgängigmachung der Belastungsbuchung ausgesetzt. Folglich erleidet die Bank bereits mit Ausführung der Überweisung einen Vermögensnachteil, der im Wege der Durchgriffskondiktion zurückverlangt werden kann.

■ Konsequenzen für den Anwendungsbereich der Nr. 8 AGB-Banken

Dieses Ergebnis vor Augen, wird deutlich, dass der Anwendungsbereich der Nr. 8 AGB-Banken nur dann eröffnet ist, wenn die Bank des Bankkunden mit der des Geldkuriers identisch ist. Nur dann hat die anweisende Bank einen bereicherungsrechtlichen Anspruch gegen und gleichzeitig eine girovertragliche Beziehung mit dem Geldkurier.[40] Eine zügige Rückerlangung des fälschlicherweise angewiesenen Betrags im Wege der Stornierung ist daher nur unter zwei Voraussetzungen möglich. Zum einen muss es sich um eine Hausüberweisung handeln, zum anderen darf die Rechnungsperiode noch nicht abgelaufen sein. Fehlt es an einem der Merkmale, bleibt nur der Weg über die Leistungsklage.

Ein Berufen des Geldkuriers auf § 818 Abs. 3 BGB dürfte in den meisten Fällen nicht durchdringen, da eine verschärfte Haftung des Geldkurier nach § 819 Abs. 1 BGB häufig anzunehmen ist. Kenntnis vom fehlenden Rechtsgrund hat nach gefestigter Rechtsprechung des *BGH* auch derjenige, der sich trotz Kenntnis der tatsächlichen Umstände, aus denen sich die Rechtsgrundlosigkeit ergibt, der Einsicht in dieselbe, gemessen an dem normativen Maßstab eines redlich Denkenden, bewusst verschließt.[41] Zumeist hat der Geldkurier diese positive Kenntnis vom fehlenden Rechtsgrund oder es sind ihm die Umstände des beabsichtigten Vorgangs durchaus bekannt.[42] Dabei müssen die dubiosen Umstände, unter denen der Geldkurier zur Teilnahme „überredet" wird, jeden vernünftig Denkenden zumindest misstrauisch machen.[43] Demnach käme man über den Anscheinsbeweis zumindest zu einer Beweislastumkehr hinsichtlich der Voraussetzungen des § 819 Abs. 3 BGB, die sich zu Lasten des Geldkuriers auswirkt.

■ Anspruch aus Delikt

Daneben kommt ein deliktsrechtlicher Anspruch der angewiesenen Bank in Betracht. Ist die Beihilfe zum Computerbetrug als Schutzgesetz des § 823 Abs. 2 BGB im Einzelfall schwer nachzuweisen,[44] stehen an strafrechtlichen Tatbeständen noch § 261 Abs. 2, Abs. 5 StGB und § 54 KWG i.V.m. § 32 Abs. 1 Satz 1 KWG zur Verfügung. Gerade sie gelten als Schutzgesetze i.S.d. § 823 Abs. 2 BGB.[45] Obwohl die Hintermänner beim Abgreifen von Kontozugangsdaten oftmals nicht greifbar sind, wurde gerade der Geldkurier, der sich im Anschluss an die Tat häufig ahnungslos geriert, strafrechtlich zur Verantwortung gezogen. Auch ist davon auszugehen, dass die angewiesene Bank einen Vermögensschaden hat, da gerade sie das Phishing-Risiko trägt.[46] Bei der Frage der Inanspruchnahme des Geldkuriers soll-

34 *BGH* NJW 1999, 1393, 1394.
35 *Schimansky* (o. Fußn. 13), § 50 Rdnr. 6.
36 *BGH* NJW 2003, 583.
37 *LG Bad Kreuznach* MMR 2008, 421.
38 *OLG Hamburg* ZIP 2006, 1981, 1982 m. Anm. *Borges*.
39 *BGH* NJW 1983, 2769; *BGH* NJW 2003, 582, 583; *BGH* NJW 2006, 1965, 1966; *OLG Karlsruhe* WM 2008, 632, 634; *Schimansky* (o. Fußn. 13), § 50 Rdnr. 12.
40 *Löhnig/Würdinger* (o. Fußn. 1), S. 963; offen gelassen von *OLG Karlsruhe* WM 2008, 632, 633: „Soweit darüber diskutiert wird, ob das Stornorecht nach Nr. 8 AGB-Banken auch dann gilt, wenn auf Seiten des Überweisenden und des Überweisungsempfängers zwei verschiedene Banken beteiligt sind, hat dies für den zu entscheidenden Rechtsstreit keine Bedeutung, da es sich um eine Hausüberweisung handelte."
41 *BGH* NJW 1996, 2652.
42 Eine verschärfte Haftung lehnte das *KG* ab: MMR 2010, 128 – in diesem Heft.
43 So auch *LG Bad Kreuznach* MMR 2008, 421.
44 Bejahend: *AG Hamm* CR 2006, 70 f.; differenzierend: *Goeckenjan*, wistra 2008, 128, 133; krit.: *Werner*, CR 2006, 71, 72; abl.: *Popp*, NJW 2004, 3517, 3518; *Graf*, NStZ 2007, 129, 130 f.
45 Für § 261 Abs. 2, Abs. 5 StGB: *LG Köln* WM 2008, 354, 355; *LG Ellwangen* ITRB 2007, 206 m. Anm. *Schiele*; als Schutzgesetz grds. bejahend: *OLG Frankfurt/M.*, U. v. 12.2.2004 – 3 U 123/00, BeckRS 2004 30339044; BGHZ 176, 281; für §§ 54 i.V.m. 32 Abs. 1 Satz 1 KWG: *BGH*, U. v. 11.7.2006 – VI ZR 341/04, BeckRS 2006 10666; *BGH* WM 2005, 1217, 1218; *OLG München* WM 2006, 1765, 1767; differenzierend: *LG Essen* WM 1992, 1224, 1225.
46 Grds. kann die kontoführende Bank ihren Schadensersatzanspruch im Wege der Leistungsklage verfolgen. Ist die fehlerhafte Belastungsbuchung nämlich rückgängig gemacht worden, hat die angewiesene Bank auch einen Schaden. Gleiches gilt, wenn die Täter das Konto in eine bestehende Kreditlinie abgeräumt haben. Selbst in dem Fall, dass die Täter in den Haben-Stand des Kunden abgeräumt haben und die Belastungsbuchung seitens der angewiesenen Bank bislang nicht rückgängig gemacht wurde, liegen die Voraussetzungen für einen ersatzfähigen Schaden i.S.d. § 249 Abs. 1 BGB vor. Dabei kommt es auf eine wirtschaftliche Betrachtungsweise an, bei der eine konkrete Vermögensgefährdung ausreicht. Diese ist bereits durch die Kontoverfügung der Täter eingetreten, vgl. *LG Köln* WM 2008, 354, 356.

te ggf. auch an die Möglichkeit eines Adhäsionsverfahrens gedacht werden.[47]

III. Zusammenfassung und Ausblick

Die aktuellen Fälle des Abfangens von Kontozugangsdaten eröffnen auf Seiten der anweisenden Bank ein deutlich größeres Haftungsrisiko. Dies liegt darin begründet, dass die Täter inzwischen mit technisch ausgereiften Tatmitteln vorgehen. Werden Kontozugangsdaten mit Trojanern ausgespäht, ist dem Bankkunden nur in Ausnahmefällen grobe Fahrlässigkeit als Voraussetzung seiner Haftung anzulasten. Die meisten Computer verfügen heute über vorinstallierte Trojaner- und Virenschutzprogramme, die jedoch keinen hundertprozentigen Schutz bieten.

Die aktuellen Fälle lassen sich längst nicht mehr mit Hilfe des sog. Prima-facie-Beweises lösen, denn den Anscheinsbeweis, dass der Kunde grob fahrlässig seine PIN und TAN preisgegeben habe, gibt es nicht. Das Haftungsrisiko der anweisenden Bank lässt sich nur auf technischer Ebene minimieren, indem die Banken ihre Systeme kontinuierlich dem Stand der Technik anpassen. Ein Erfahrungswert besagt zudem, dass die Täter ihre Handlungen oftmals gerade auf die technisch am wenigsten durchdachten Banksysteme fokussieren. Soweit dieser Befund von der Prämisse ausgeht, dass eine Banktransaktion wenigstens durch eine Transaktionsnummer abgesichert ist, wird zugleich deutlich, wie viel einfacher Systeme – etwa im Versandhandel – ausgeforscht werden können, die nur die Eingabe eines Zugangskennworts und eines Passworts voraussetzen.

Ulrich Schulte am Hülse
ist Rechtsanwalt und Partner von ilex Rechtsanwälte & Steuerberater (Berlin und Potsdam).

Sebastian Klabunde
ist Rechtsreferendar in Berlin.

47 Allerdings machen Gerichte und Staatsanwaltschaften im Strafverfahren oftmals von den Teileinstellungsmöglichkeiten des § 154 StPO Gebrauch. Dies kann dazu führen, dass ein Geschädigter nicht mehr den gesamten Schaden im Adhäsionsverfahren geltend machen kann.