44 Das Fallaufkommen dieser außerstaatlichen Judikatur ist marginal und liegt dauerhaft im zweistelligen Bereich (vgl. Jahresberichte unter http://www.fs-arzneimittelindustrie.de/downloads.html – Aufruf v. 13.10..2011). Zur dortigen Judikatur näher KUHLEN (2010), S. 882.
45 KLÜMPER / WALTHER (2010), S. 146, 147.
46 KLÜMPER / WALTHER (2010), S. 147.
47 Vgl. etwa EHLERS (2005), S. 97 f.; für die entsprechende Rechtsberatung stellvertretend PASSARGE (2011), S. 83 f. sowie das Seminarbeispiel unter http://www.ra-wigge.de/Dateien/Veranstaltungen/euroforum10_03_10.pdf (Aufruf v. 13.10.2011).
48 Näher zu den im Anschluss angesprochenen Entwicklungen KÖLBEL (2011b).
49 So setzen manche Strategievarianten auf Kooperationsverträge mit den Kassen und vertriebsförderliche Effekte im Rahmen der sog. Integrierten Versorgung. Der neu gefasste § 140b I Nr. 8 SGB V macht nämlich auch pharmazeutische Unternehmen zu möglichen Vertragspartnern der Krankenkassen. Dass in diesen Versorgungsmodellen das eigene Arzneimittelprodukt keine Rolle spielen soll, mag man nicht ernstlich glauben. Für ein Beispiel einer solchen Kooperation zwischen der AOK Niedersachsen und dem Pharmakonzern Janssen-Cilag vgl. http://www.janssen-cilag.de/news/detail.jhtml?itemname=news_company_83 (Aufruf v. 13.10.2011).
50 Etwa HARMS / GÄNSHIRT / LOSERT (2005), S. 868.
51 Vgl. GLAESKE / SCHUBERT (2006), S. 16.
52 BAUER / HAHN / HAMMERSCHMIDT (2006).
53 Vgl. etwa KHANFAR / POLEN / CLAUSON (2009), S. 451 f.

„Skimming" – Eine kriminologische Betrachtung

Mario Bachmann und Ferdinand Goeck

I. Einleitung

„Geldautomatenmanipulation boomt in Deutschland"[1] – Diese und ähnliche Schlagzeilen sind in jüngster Zeit häufig zu lesen. Gemeint ist das sogenannte Skimming, das in den letzten zehn Jahren ebenso wie andere Formen von Kriminalität im modernen Zahlungsverkehr (z.B. Phishing/Pharming) vermehrt in den Fokus der Öffentlichkeit geraten ist. Hierbei werden durch gezielte Manipulationen an Geldautomaten Daten von Bankkarten ausgespäht, um mit den so erlangten Informationen Dubletten zur späteren Geldabhebung herzustellen. Bisher wurde das Skimming vor allem unter strafrechtsdogmatischen Gesichtspunkten erörtert.[2] Kriminologische Aspekte spielten dabei allenfalls am Rande eine Rolle. Der vorliegende Beitrag will insoweit Abhilfe schaffen und nach einer kurzen Darstellung der technischen Vorgehensweise (II.) sowie einer knappen strafrechtlichen Einordnung (III.) die Phänomenologie in den Blick nehmen (IV.). Im Anschluss daran soll eine Interpretation der statistischen Befunde erfolgen (V.), bevor schließlich nach Präventionsansätzen gefragt wird (VI.).

II. Vorgehensweise

1. Skimming

Um die Vorgehensweise der Täter beim Skimming zu verstehen, ist es zunächst notwendig, sich die Funktionsweise von Zahlungskarten (= Debit- oder Kreditkarten[3]) vor Augen zu führen. So ist zu beachten, dass die für eine Transaktion erforderlichen Daten (Bankleitzahl, Kontonummer, Gültigkeitsdauer der Karte u.a.) sowohl auf dem Chip als auch auf dem Magnetstreifen der Karte gespeichert sind, wobei die Informationen (nur) auf letzterem in unverschlüsselter Form vorliegen.[4] Demgegenüber ist die Geheimzahl des Bankkunden (PIN) nicht auf dessen Zahlungskarte gespeichert, sondern wird bei der Eingabe am Geldautomaten verschlüsselt erfasst und im Regelfall mit sogenannten „PIN-Verify-Keys" im Rechenzentrum der Bank überprüft.[5]

Da Karteninformationen und Geheimzahl somit getrennt voneinander „aufbewahrt" werden, erfolgt das Skimming regelmäßig in zwei Schritten. Zunächst müssen die Täter an die unverschlüsselten Kartendaten des Bankkunden und danach an dessen PIN gelangen. Zum Ausspähen der erstgenannten Informationen werden handelsübliche Lesegeräte verwendet, die bereits für deutlich unter 50 Euro im Handel zu erwerben sind. Diese werden als gewöhnliche Einzugsvorrichtung getarnt und auf den regulären Einzug eines Geldautomaten (oder in Einzelfällen auch auf den Türöffner der Bankfiliale) montiert. Beabsichtigt ein Kunde nunmehr Geld abzuheben, schiebt er die Zahlungskarte in das vermeintliche Einzugsfach und seine Daten werden noch vor ihrer ordnungsgemäßen Bearbeitung im Geldautomaten von den Tätern ausgelesen. Im Anschluss daran wird die Eingabe der PIN – oftmals mittels einer Miniaturkamera[6] – aufgezeichnet oder per Funk direkt übertragen.[7] Alternativ ist es auch möglich, die PIN mittels eines getarnten Aufsatzes auf dem eigentlichen Eingabefeld des Bankautomaten auszuspähen.[8] Dabei werden die Tastenanschläge des Kunden entweder in der Attrappe gespeichert oder direkt per Funk an die Täter übertragen. Das Ausspähen der Kartendaten kann mitunter auch durch einen Kassierer erfolgen, der die EC- oder Kreditkarte eines Kunden beim Bezahlvorgang an der Kasse heimlich durch ein zweites Lesegerät zieht.[9] Ferner ist es möglich, Terminals im POS-Verfahren („point of sale")[10] so zu manipulieren, dass Karteninformationen und PIN gleichzeitig ausgespäht werden können.[11]

Sobald den Tätern alle erforderlichen Daten vorliegen, werden diese auf Kartenrohlinge („white plastics") überspielt, die zusammen mit der Geheimzahl im Ausland zum Geldabheben („cashing") verwendet werden.[12] Mitunter werden die ausgespähten Informationen nicht direkt eingesetzt, sondern über das Internet in Staaten außerhalb Europas verkauft.[13] Beim sogenannten „carding"[14] werden hingegen mit den ausgepähten Daten zunächst Waren bestellt, um diese anschließend über fremde oder eigene Onlineshops weiterverkaufen zu können. In einer Vielzahl von Fällen bedienen sich die Täter zudem des „cardings on demand". Dies bedeutet, dass der Inhaber ausgespähter Kreditkartendaten bei einer anderen Person (dem sogenannten „carder") die gewünschte Ware bestellt und zugleich die erforderlichen Kartendaten übermittelt. Letztere verwendet der carder sodann für die eigentliche Bestellung des Produkts und erhält hierfür in der Regel zwischen 25% und 40% des Realpreises der bestellten Ware. Vorteil einer solchen arbeitsteiligen Handlungsweise dürfte aus Sicht des Bestellers sein vermindertes Entdeckungsrisiko sein, da er die Möglichkeit hat, seine Identität beim Bestellvorgang weitestgehend zu verschleiern. Der carder wiederum wird sich in der Regel auf den Einsatz missbräuchlich erlangter Kreditkarten spezialisiert haben, auf deren Beschaffung er gerade nicht angewiesen ist.

2. Abgrenzung zum Phishing

Ein dem Skimming ähnliches Phänomen, das in der Literatur bisher viel Aufmerksamkeit erfahren hat, ist das sogenannte „Phishing".[15] Hierbei geht es um die Erlangung sensibler Daten (z.B. Kontodaten, E-Mail-Accounts) im virtuellen Bereich. Bedeutsam ist im vorliegenden Zusammenhang vor allem der Umstand, dass mittels Phishing auch Daten von Kreditkarten beschafft werden können. Die „klassische" Vorgehensweise beim Phishing besteht darin, dass die Täter elektronische Mitteilungen versenden, die Internetbenutzer unter falschen Vorwänden zur Preisgabe von Informationen auffordern. Beispielhaft hierfür ist etwa eine gefälschte E-Mail vom „Kundenservice" eines Kreditinstituts, das „zwecks Überprüfung der Kundeninformationen" zur erneuten Übersendung der Kreditkartendaten auffordert. Mitunter werden Bankkunden und Kreditkarteninhaber in einer vermeintlich echten Mitteilung dazu aufgefordert, sich auf einer gefälschten Internetseite des Kreditinstituts oder des Kartenanbieters anzumelden. Die dort seitens des Kunden eingegebenen Informationen werden jedoch von den Tätern eingesehen und anschließend für weitere Transaktionen verwendet. Beispielhaft für die rasante Modifikation des Phishings ist zudem die „Umgehung" des im Jahr 2007/2008 eingeführten i-Tan-Verfahrens[16] im Bereich des Online-Bankings. Hierfür nutzen die Täter nahezu ausschließlich sogenannte „Man-In-The-Middle-" bzw. „Man-In-The-Browser-Attacken".[17] Bei letzteren erfolgt eine Manipulation des Internetbrowsers durch ein Schadprogramm, sodass unbemerkt vom Kunden Informationen an die Täter weitergeleitet werden. Im Gegensatz dazu geschieht das Ausspähen der Daten beim „Man-In-The-Middle"- Angriff durch Manipulation des Kommunikationsweges zwischen dem Kunden und der Bank. Die Täter drängen sich dabei zwischen die beiden Kommunikationspartner, um den Datenverkehr einsehen und umgehend modifizieren zu können (Austausch des Empfängerkontos sowie der Höhe des Betrages).

III. Strafrechtliche Einordnung[18]

In strafrechtlicher Hinsicht ist in der höchstrichterlichen Rechtsprechung inzwischen anerkannt, dass das Skimming nicht den Tatbestand des Ausspähens von Daten (§ 202a StGB) erfüllt, da die auf dem Magnetstreifen gespeicherten Informationen nicht besonders gesichert sind.[19] Eine Strafbarkeit wegen Vorbereitung der Fälschung von Zahlungskarten (§§ 152a Abs. 5, 152b Abs. 5 i.V.m. 149 Abs. 1 Nr. 1 StGB) entfällt ebenfalls, da es sich bei dem Skimming-Equipment (Kamera, Kartenlesegerät) nicht um eine „ähnliche Vorrichtung" im Sinne des § 149 Abs. 1 Nr. 1 StGB handelt.[20] Die Personen, die lediglich an der Manipulation eines Geldautomaten beteiligt waren, können sich jedoch wegen Mittäterschaft oder Beihilfe zu §§ 152a und b StGB (Herstellung der Kartendubletten) bzw. zu § 263a Abs. 1 Var. 3 StGB (Geldabhebung) strafbar machen.

IV. Statistische Befunde zum Skimming

1. Zur Entwicklung der Fälschungskriminalität im Allgemeinen

Blickt man auf die Entwicklung der registrierten Fälschungskriminalität seit 1999 (*Abb. 1*), ist ein deutlicher Anstieg der absoluten Zahlen von 3460 auf rund 10073 Fälle zu verzeichnen.[21] Im selben Zeitraum hat die Zahl der erfassten Fälle der Fälschung von Zahlungskarten (§§ 152a und b StGB) um das 15-fache zugenommen (1999: 439 Fälle; 2010: 6603), wobei der bedeutsamste Zuwachs zwischen 2005 und 2009 stattgefunden hat. Zugleich sank die Zahl der registrierten Fälle von Geld- und Wertzeichenfälschung im letztgenannten Zeitraum von 2779 auf 889. Auch im Hinblick auf das Inverkehrbringen von Falschgeld war von 2005 bis 2008 ein Rückgang zu verzeichnen. Die gemeldeten Zahlen sanken hier von 3265 Fällen im Jahr 2005 auf 1786 in 2008. Seitdem ist jedoch eine steigende Tendenz zu beobachten (2010: 2237 Fälle).

2. Phänomenologie des „Skimmings"[23]

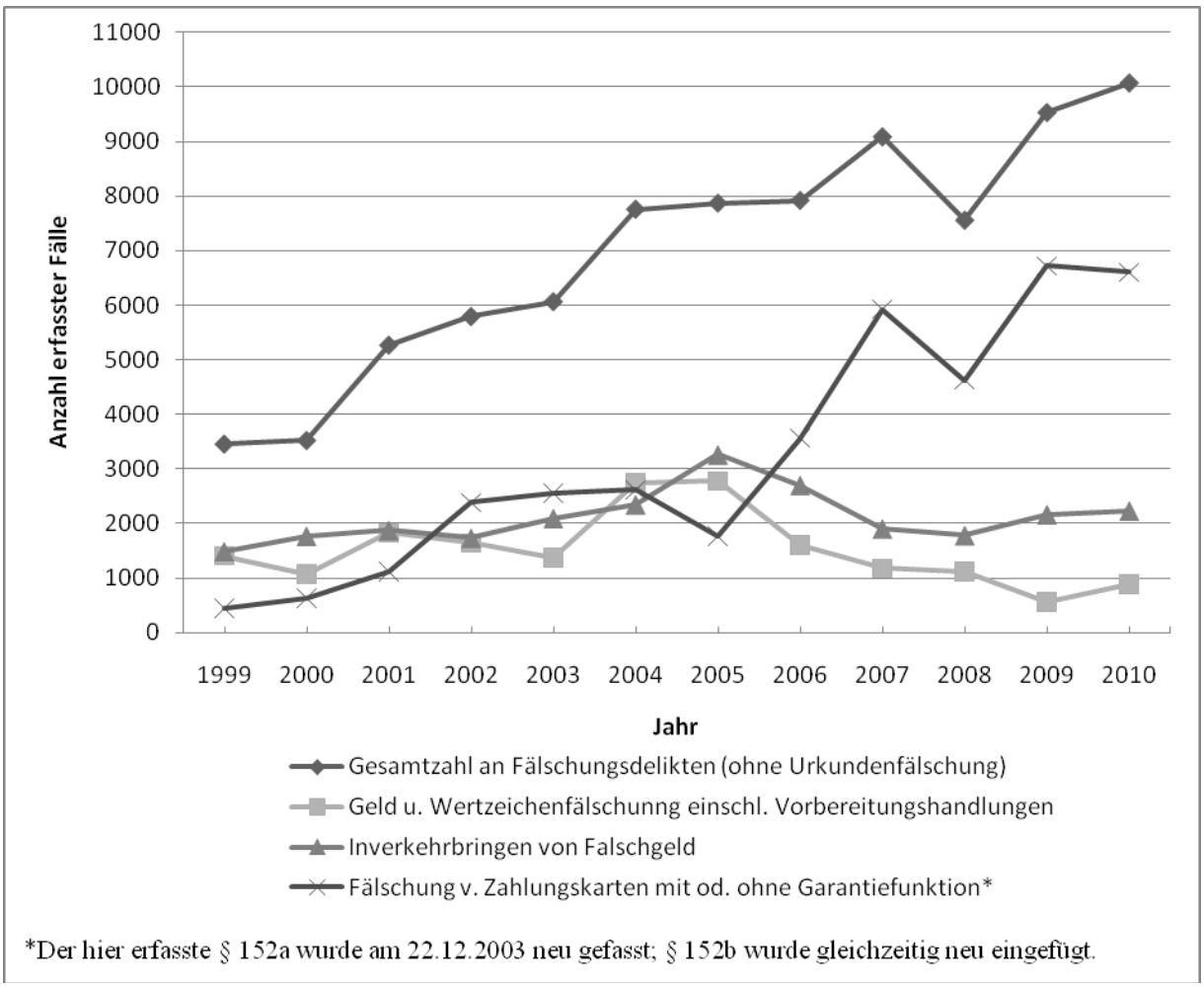
a. Häufigkeit

Im Bereich des Skimmings ist seit Beginn des Jahrtausends eine stetige Zunahme der manipulierten Geldautomaten festzustellen (*Abb.2*). Im Zeitraum von 2001 (28 Fälle) bis 2010 (1765 Fälle) ist es zu einem Anstieg um mehr als das 60-fache gekommen. Allein im vergangenen Jahr war fast eine Verdopplung der gemeldeten Manipulationen von vormals 964 auf 1765 zu verzeichnen. Dabei erfolgte ein Großteil der Manipulationen in der ersten Jahreshälfte, wohingegen im zweiten Halbjahr deutlich weniger Fälle registriert wurden. Wiederum waren vor allem Geldautomaten in hochfrequentierten Bereichen (Fußgängerzonen, Bahnhöfe u.ä.) von mehrfachen Manipulationen betroffen.[24] Die Zahl der Angriffe hat sich seit 2007 (1349 Fälle) weit mehr als verdoppelt (2010: 3183). Lediglich zwischen 2008 und 2009 ist ein leichter Rückgang der gemeldeten Zahlen um ca. 14% festzustellen (2387 bzw. 2058 Fälle). Die große Zahl der Manipulationen an Geldautomaten im ersten Halbjahr 2010 führte dazu, dass bereits Ende Juni nahezu die Fallzahl des Vorjahres (1972 Angriffe) erreicht wurde. Pro Manipulation wurden im Durchschnitt 60 Kartendaten und PIN abgegriffen. Die mit Abstand meisten Angriffe erfolgten im Jahr 2010 auf Geldautomaten in Nordrhein-Westfalen (1144) und Berlin (441). Der Einsatzschwerpunkt gefälschter Debitkarten lag in den letzten Jahren vornehmlich im europäischem Ausland (vor allem Großbritannien, Italien, Niederlande, Bulgarien und Russland). Zudem hat sich der Trend, die Dubletten auch außerhalb Europas einzusetzen im Jahr 2010 fortgesetzt. Dabei spielten vor allem Staaten wie Südafrika, Kenia, USA, Kanada sowie die Dominikanische Republik eine große Rolle. Auffällig ist ferner, dass das Ausspähen von Kartendaten an Türöffnern von Bankfilialen an Bedeutung verloren hat. Während nämlich im Jahr 2009 noch 13% der Manipulationen auf diese Weise erfolgten, waren es im vergangenen Jahr nur noch 2%. Schließlich waren 2010 im Bereich des POS-Skimmings lediglich einige erfolglose Versuche zu verzeichnen.

b. Täter, Opfer und Schadenshöhe

Im Hinblick auf den Täterkreis ist besonders auffällig, dass die registrierten Tatverdächtigen nahezu vollständig südosteuropäischer Herkunft (insbesondere Bulgarien und Rumänien) sind und deutsche Staatsbürger in diesem Zusammenhang nahezu keine Rolle spielen. Häufig ist eine arbeitsteilige Vorgehensweise festzustellen.[25] Die einzelnen Tatbeiträge (Ausspähen der Kartendaten, Herstellung der Dubletten und cashing) werden in der Regel durch jeweils andere Personen(gruppen) durchgeführt. Für den Abgriff der Kartendaten halten sich die Täter mitunter nur relativ kurz an verschiedenen Orten innerhalb Deutschlands auf und agieren zumeist außerhalb der Öffnungszeiten, d.h. vor allem nachts sowie an Wochenenden und Feiertagen, um nicht von Bankmitarbeitern gestört zu werden.[26] Die gefälschten Zahlungskarten kommen dann etwa ein bis zwei Tage nach Ausspähung der

Abb.1: Entwicklung der Fälschungskriminalität nach der PKS im Zeitraum 1999-2010[22]



Kartendaten im Ausland zum Einsatz.

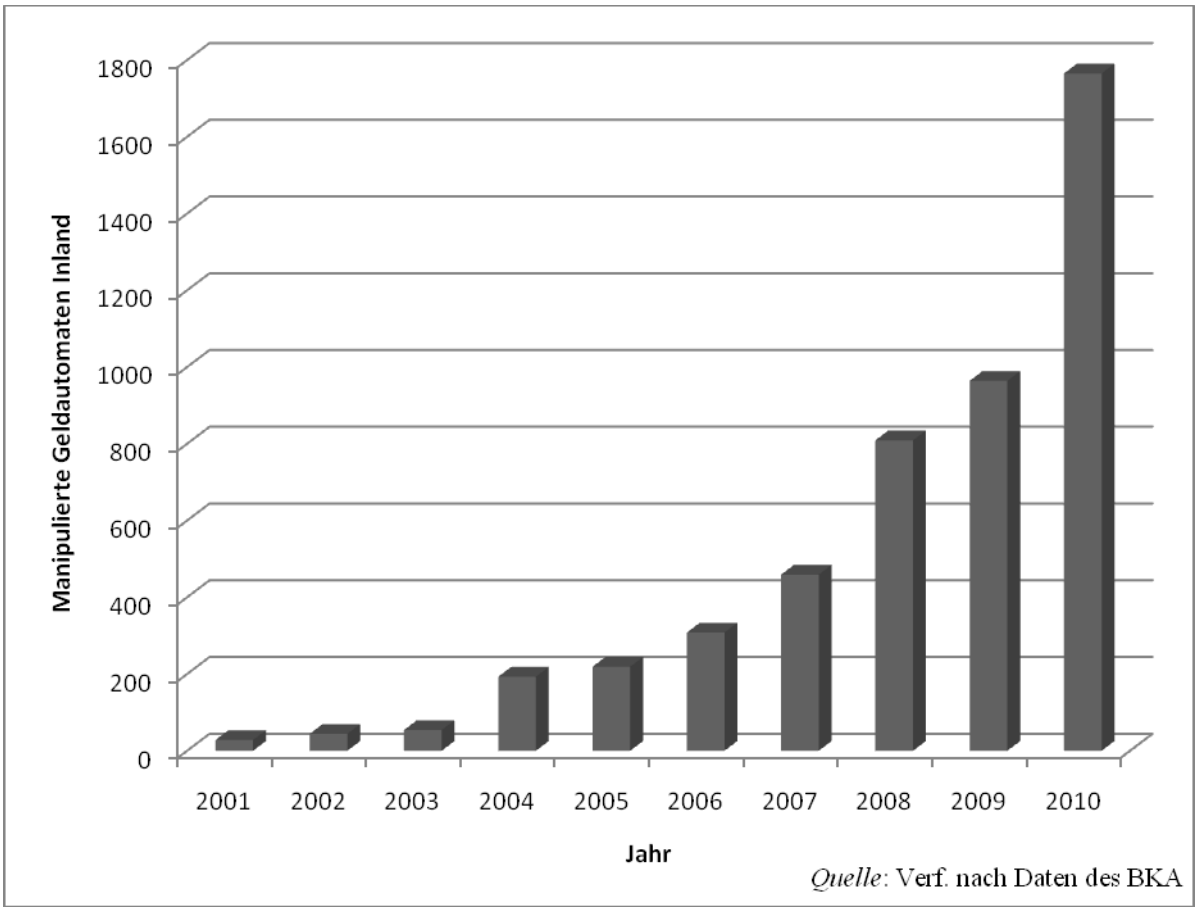
Opfer einer Skimming-Attacke kann grundsätzlich jeder Inhaber einer Zahlungskarte werden. Im Jahr 2009 waren immerhin rund 125 Millionen Debit- und Kreditkarten im Umlauf.[27] Da der Zentrale Kreditausschuss (ZKA) im Jahr 2008 beschlossen hatte, keine Zahlen mehr zur Schadensentwicklung zu veröffentlichen, muss insoweit auf Schätzungen zurückgegriffen werden.[28] Für das Jahr 2010 nimmt das BKA einen Schaden von rund 60 Millionen Euro an (2008 und 2009: jeweils ca. 40 Millionen Euro).[29]

V. Interpretation der statistischen Befunde

Fragt man nach den Ursachen für den beachtlichen Anstieg der Fälschungskriminalität, ist zunächst zu beachten, dass das Jahr 2005 eine Zäsur bedeutet. Bis zu diesem Zeitpunkt liegt die Zunahme darin begründet, dass sowohl die Fälschung von Zahlungskarten als auch diejenige von Geld (einschließlich Inverkehrbringen desselben) an Bedeutung gewonnen hat. Nach 2005 beruht der Zuwachs nur noch auf dem erheblichen Anstieg der statistisch erfassten Fälle von Zahlungskartenfälschungen. Insoweit ist zu berücksichtigen, dass der bargeldlose Zahlungsverkehr im vergangenen Jahrzehnt erheblich an Bedeutung gewonnen hat und die konventionelle Zahlungsweise mittels Bargeld immer mehr verdrängt. So hat sich allein im Zeitraum von 2002 bis 2009 die Zahl der Online-Überweisungen fast verdreifacht, diejenige der Lastschriften nahezu verdoppelt und im Bereich der Zahlungen mit Debitkarte ist ein Anstieg um etwa ein Drittel zu verzeichnen.[30] Damit gehen zugleich zahlreiche Möglichkeiten des Missbrauchs einher, die aus Sicht der Täter gegenüber der Fälschung von Geld nicht unwesentliche Vorteile bringen. Zum einen eröffnet das Nachmachen von Zahlungskarten Zugang zu echten Banknoten, die faktisch risikolos im Zahlungsverkehr eingesetzt werden können. Bei sogenannten „Blüten" besteht hingegen stets die Gefahr der Entdeckung und zwar bei jedem Inverkehrbringen von unechtem Geld aufs Neue. Schließlich ist zu berücksichtigen, dass Inhaber deutscher Zahlungskarten über eine im internationalen Vergleich hohe Bonität verfügen und die Bundesrepublik aufgrund der vorhandenen Infrastruktur (gerade in großstädtisch geprägten Bundesländern wie Nordrhein-Westfalen und Berlin) eine Vielzahl an Tatgelegenheiten bietet.[31]

Da das Skimming in den letzten Jahren erheblich an Bedeutung gewonnen hat und in aller Regel[32] zu dem Zweck erfolgt, mit den hierdurch erlangten Informationen Kartendubletten zur späteren Geldabhebung herzustellen, ist ein Zusammenhang mit dem erläuterten Anstieg der Fälschung von Zahlungskarten unverkennbar. Zwar haben die Kreditinstitute in letzter Zeit vor allem technische Präventionsmaßnahmen ergriffen, um Skimming-Attacken zu unterbinden bzw. zu erschweren. So ist etwa die inzwischen zu beobachtende Bedeutungslosigkeit des Abgriffs von Magnetstreifendaten an Türöffnern von Bankfilialen auf den Abbau bzw. die sicherheitstechnische Aufrüstung der entsprechenden Vorrichtungen zurück-

Abb.2: Entwicklung der Manipulationen an Geldautomaten in Deutschland nach BKA



zuführen.[33] Ungeachtet dessen bieten sich für potenzielle Täter – die ihre Vorgehensweise zudem immer weiter perfektionieren – nach wie vor zahlreiche Möglichkeiten, um mittels Skimming-Attacken an Daten von Bankkunden zu gelangen. So dürfte etwa die Tatsache, dass allein im ersten Halbjahr 2010 fast ebenso viele Skimming-Angriffe zu verzeichnen waren wie im gesamten Jahr 2009, darauf zurückzuführen sein, dass die Täter zahlreiche (allerdings inzwischen ausgetauschte) Geldautomaten älterer Bauart einer bundesweit vertretenen Bank ins Visier genommen hatten.[34] Zudem ist von einem beträchtlichen Dunkelfeld auszugehen, weil ein Großteil der Skimming-Angriffe nicht angezeigt wird, da die Betroffenen den entstandenen Schaden in aller Regel von den Geldinstituten und Kreditkartenorganisationen ersetzt bekommen[35] und letztere aus Reputationsgründen ebenfalls kein großes Interesse daran haben, dass Manipulationen an Geldautomaten publik werden.

Dass die Kartendubletten nicht in Deutschland eingesetzt werden, ist darauf zurückzuführen, dass die Geldabhebung hierzulande ausschließlich über den EMV-Chip der Zahlungskarte erfolgt und nicht über den Magnetstreifen.[36] Seit dem 1.1.2011 gilt dies zudem für den gesamten Euro-Raum. Daher ist zu vermuten, dass außereuropäische Länder zukünftig noch stärker als Einsatzgebiete für gefälschte Zahlungskarten in den Fokus der Täter geraten werden als bisher.[37] Dass Fälle des POS-Skimmings bisher nicht häufiger aufgetreten sind, dürfte vor allem darauf zurückzuführen sein, dass die entsprechenden Geräte nur mit großem Aufwand zu manipulieren sind und unter Umständen mehrere Einbrüche in das jeweilige Geschäft, Restaurant etc. erfolgen müssen (z.B. Entwenden der Originalgeräte; Zurückbringen im präpariertem Zustand).[38] Hinsichtlich des Umstandes, dass das Skimming ganz überwiegend von Angehörigen südosteuropäischer Staaten durchgeführt wird, dürfte von Bedeutung sein, dass sich dort aufgrund der schwierigen wirtschaftlichen Verhältnisse mit relativ wenig Aufwand Personen finden lassen, die bereit sind, für ein geringes Entgelt Manipulationen an Geldautomaten vorzunehmen. Deutlich wird dies, wenn man sich eine jüngst ergangene Entscheidung des BGH[39] zum Skimming vor Augen hält, in der in Bezug auf die Bezahlung der aus Rumänien stammenden Täter festgestellt wird: „*Auch das Tatinteresse der Angeklagten war hoch; denn der Umfang der ihnen zum Teil gezahlten und im Übrigen versprochenen Entlohnung mag zwar nach herkömmlichen mitteleuropäischen Maßstäben eher gering erscheinen; das Entgelt hätte den Angeklagten jedoch in ihrer Heimat für mehrere Monate zum Leben genügt.*" Zudem sehen sich gerade Rumänien und Bulgarien im Zuge der aktuellen Diskussion um den Beitritt beider Länder zum Schengen-Raum u.a. von deutscher Seite dem Vorwurf ausgesetzt, nicht konsequent genug gegen organisierte Kriminalität vorzugehen.[40] Wenn dies tatsächlich zutrifft, wäre auch das ein möglicher Grund dafür, dass gerade aus diesen beiden Ländern heraus die meisten Skimming-Angriffe vorbereitet werden.

VI. Präventionsansätze

Aus präventiver Perspektive ist es zunächst zu begrüßen, dass die Geldabhebung – wie bereits erwähnt – seit Anfang des Jahres im gesamten Euro-Raum nur noch über den EMV-Chip erfolgt. Letzterer bietet nämlich aufgrund des Umstandes, dass er nicht nachgemacht werden kann, eine weitaus höhere Sicherheit.[41] In diesem Zusammenhang ist allerdings darauf hinzuweisen, dass es einer britischen Forschergruppe der Universität Cambridge gelungen ist, die Eingabe der PIN an POS-Terminals trotz EMV-Standards durch eine „man-in-the-middle"-Attacke zu umgehen.[42] Dabei wurden die Terminals derart manipuliert, dass diese irgendeine (zufällig) eingegebene PIN als „richtig" akzeptierten.[43] Nach Auffassung der Forschergruppe ist diese Vorgehensweise nicht auf Geldautomaten übertragbar, so dass insoweit kein Grund zur Besorgnis besteht.[44] Da die Umstellung auf die Chip-Technologie jedoch in vielen Staaten noch nicht erfolgt ist, verdient die Aufforderung des BKA an die Kreditwirtschaft, eine „Zwei-Karten-Strategie" einzuführen,[45] uneingeschränkt Zustimmung. Danach sollen Banken grundsätzlich nur noch Debit- oder Kreditkarten ohne Magnetstreifen ausgegeben, sodass die Ausspähung von Daten nicht mehr möglich ist. Für Transaktionen in Ländern, die noch nicht über den EMV-Standard verfügen (z.B. USA), kann eine zweite Zahlungskarte mit Magnetstreifen beantragt werden, was für etwa 5% der Bankkunden relevant wäre.[46] Bisher haben jedoch nur einzelne Kreditinstitute ihre Ausgabepraxis geändert.[47] Seitens des ZKA wird insoweit vorgebracht, dass die Abschaffung des Magnetstreifens eine Maßnahme darstelle, die vielfältige Auswirkungen habe und beispielsweise die Servicefunktionen der Zahlungskarten einschränkten.[48] Viele Banken behelfen sich daher nach wie vor mit den herkömmlichen Präventionsmaßnahmen und bringen etwa „Anti-Skimming-Module" vor dem Karteneinzug des Geldautomaten an.[49] Dadurch soll u.a. die Befestigung einer Skimming-Apparatur auf dem Kartenschlitz verhindert werden. Manche Geldautomaten sind zudem mit nicht-linearen bzw. ruckelnden Karteneinzügen sowie Magnetfeldstörsendern ausgestattet.[50] Gerade diese technischen Maßnahmen dürften dazu geführt haben, dass Kartendaten – zumindest zeitweise – vermehrt an den Türöffnern der Bankfilialen abgegriffen wurden. Die Anbringung eines Sichtschutzes über dem Eingabefeld des Geldautomaten hat hingegen nur einen geringen präventiven Effekt, da die Miniaturkameras seitens der Täter inzwischen derart geschickt angebracht werden, dass das Ausspähen der Geheimzahl auch weiterhin möglich ist.[51] Auf Seiten der Karteninhaber bestehen kaum effektive Möglichkeiten sich gegen das Skimming zu schützen. Auch ein diesbezüglich sensibilisierter Kunde wird nämlich in aller Regel kaum in der Lage sein, die geschickte Manipulation eines Bankautomaten zu erkennen. In einer Vielzahl von Fällen verhindert selbst das (z.B. mit der Hand) verdeckte Eingeben der PIN nicht ein Ausspähen der Kartendaten. So können die Täter die Kamera etwa flach oberhalb des Eingabefeldes anbringen oder einen Tastaturaufsatz verwenden.[52]

VII. Ausblick

Solange Zahlungskarten mit Magnetstreifen im Umlauf sind, wird das Phänomen des Skimmings weiterhin relevant bleiben. Ähnlich wie beim Phishing findet bereits ein „Katz-und-Maus-Spiel" zwischen technischen Präventionsmaßnahmen auf der einen sowie deren Umgehung auf der anderen Seite statt. Zudem ist das Potenzial an lukrativen Angriffsobjekten – etwa im ländlichen Bereich – aus Sicht der Täter noch längst nicht ausgeschöpft. Bemerkenswert ist zudem, dass im Jahr 2010 erstmals Ticketautomaten der Deutschen Bahn sowie Tankautomaten manipuliert wurden.[53] Es bleibt also abzuwarten, wie weit der Einfallsreichtum der Skimming-Banden zukünftig noch reichen wird.

Der Autor Bachmann ist wiss. Mitarbeiter und Doktorand am Institut für Kriminologie der Universität zu Köln bei Professor Dr. Frank Neubacher M.A. – Mario.Bachmann@uni-koeln.de; der Autor Goeck ist ebendort als stud. Hilfskraft tätig – f.goeck@uni-koeln.de

Fußnoten:

1 So der Titel einer Mitteilung von Spiegel-Online vom 16.7.2010, www.spiegel.de/netzwelt/web/0,1518, 706928,00.html (zuletzt abgerufen am 16.5.2011).
2 **Näher hierzu etwa** *Bachmann/Goeck*: Strafrechtliche Aspekte des Skimmings, in: JR 2011 [im Erscheinen]; *Seidl/Fuchs*: Zur Strafbarkeit des sog. „Skimmings", in: HRRS 2011, 265 ff.; *Eisele:* Payment Card Crime: Skimming, in: CR 2011, 131 ff.; *Tyszkiewicz:* Skimming als Ausspähen von Daten gemäß § 202a StGB, in: HRRS 2010, 207 ff.
3 **Im Gegensatz zu Kredit- belasten Debitkarten** das Konto des Bankkunden direkt. Die in Deutschland gebräuchlichste Debitkarte ist die EC-Karte.
4 **Vgl.** *Tyszkiewicz* (Anm. 2), 207 (209).
5 **Vgl.** *Eisele* (Anm. 2), 131 (131).
6 **Entsprechende Geräte sind ebenfalls vergleichsweise** günstig zu erwerben. Eine z.B. als Feuermelder getarnte Minikamera ist bereits für ca. 80 € erhältlich. Andere Geräte sind bereits ab 40 € verfügbar.
7 **Vgl.** *Eisele* (Anm. 2), 131 (131).
8 **Vgl.** *Tyszkiewicz* (Anm. 2), 207 (208).
9 **Vgl.** *Eisele* (Anm. 2), 131 (131).
10 **Hierbei handelt es sich um Geräte für den bar**geldlosen Zahlungsverkehr, die z.B. an den Kassen von Geschäften, Hotels oder Restaurants eingesetzt werden.
11 **Vgl.** *Eisele* (Anm. 2), 131 (131).
12 **Vgl.** *BKA* (Hrsg.): Zahlungskarten-Kriminalität – Bundeslagebild 2010, S. 5, abrufbar unter http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaet_node.html?_nnn=true.
13 **Vgl.** *Küch:* „Skimming" – Fluch der neuen Technik oder nur Kapitulation vor innovativen Krimminellen, in: Der Kriminalist 2010, Heft 10, 8 (9).
14 **Die folgenden Ausführungen hierzu basieren** – soweit nicht anders angegeben – auf *BKA* (Hrsg.): Cybercrime – Bundeslagebild 2010, S. 12, abrufbar unter http://www.bka.de/nn_233866/DE/Publikationen/Jahresberichte UndLagebilder/Cybercrime/cybercrime_node.html?_nnn=true**15 Vgl. zur Strafbarkeit des** Phishing *Seidl/Fuchs:* Zur Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes, in: HRRS 2010, 85 ff.; *Goeckenjan:* Die Auswirkungen des 41. Strafrechtsänderungsgesetzes auf die Strafbarkeit des „Phishing", in: wistra 2009, 47 ff.
16 Beim i-Tan-Verfahren muss der Kunde für eine Anweisung an seine Bank (z.B. eine Überweisung) eine bestimmte und einmalig verwendbare Nummer – die sog. indizierte Transaktionsnummer – angeben, die er zuvor von der Bank zumeist postalisch erhalten hat.
17 **Vgl. zu den derzeit gebräuchlichen Phishing-**Methoden *BKA* (Anm. 14), S. 10.
18 **Näher zu strafrechtlichen Problemen des Skim**mings *Bachmann/Goeck* (Anm. 2).
19 **Vgl. BGH NStZ 2010, 275; BGH, Beschluss v.** 6.5.2010 – 3 ARs 7/10.
20 **Vgl. BGH wistra 2004, 265 (266);** *Lackner/Kühl*: StGB, 27. Aufl. 2011, § 149 Rn. 2 m.w.N.
21 **Vgl. hierzu im Folgenden die PKS der einzelnen** Jahrgänge, abrufbar unter http://www.bka.de/pks/.
22 **In der Grafik nicht dargestellt sind die Fälle der** gewerbs- und bandenmäßigen Geldfälschung, der Wertpapierfälschung sowie die Fälschung von Geld-/Wertzeichen fremder Währungsgebiete.
23 **Vgl. zu den folgenden Ausführungen** *BKA* (Anm. 12), S. 1 ff.
24 Vgl. Pressemitteilung des BKA vom 21.1.2009, abrufbar unter http://www.bka.de/pressemitteilungen/ 2009/pm090121.html.
25 Beispielhaft hierfür BGH, Urteil v. 17.2.2011, 3 StR 419/10 m. Besprechung *Bachmann/Goeck* (Anm. 2).
26 Vgl. *Kochheim:* Skimming – Hintergründe und Strafrecht, 2. Aufl. 2011, S. 9, abrufbar unter www.kochheim.de/cf/doc/Kochheim-Skimming-2010.pdf (zuletzt abgerufen am 16.5.2011).
27 Der Anteil der Debitkarten beträgt etwa drei Viertel.
28 Vgl. BT-Drs. 17/5659, S. 4.
29 Vgl. Pressemitteilung des BKA vom 21.1.2009, abrufbar unter www.bka.de.
30 Vgl. *Bundesbank* (Hrsg.), Statistik über den Zahlungsverkehr in Deutschland, abrufbar unter www.bundesbank.de/zahlungsverkehr/zahlungsverkehr_statistik.php.
31 Vgl. *BKA* (Anm. 12), S. 5 und 11.

32 Eine Ausnahme hiervon ist vor allem das bereits erwähnte „carding".
33 Vgl. Pressemitteilung des *BKA* vom 10.5.2011, abrufbar unter http://www.bka.de/pressemitteilungen/ 2011/pm110510.html.
34 Vgl. *BKA* (Anm. 33).
35 Vgl. *BKA* (Anm. 12), S. 5.
36 Vgl. *Eisele* (Anm. 2), 131 (131).
37 Vgl. *BKA* (Anm. 12), S. 10.
38 Vgl. *Kochheim* (Anm. 26) , S. 7.
39 Vgl. BGH, Urteil v. 17.2.2011 – 3 StR 419/10 m. Besprechung *Bachmann/Goeck*, in: JR 2011 (Anm. 2).
40 Vgl. *Müller/Boecker*, Schengen-Beitritt Rumäniens und Bulgariens verschoben, 2011, http://www.dradio.de/ dlf/sendungen/hintergrundpolitik/1396158/ (zuletzt abgerufen am 12.5.2011).
41 Vgl. Anm. 28, S. 2.
42 Vgl. *Murdoch/Drimer/Anderson/Bond*: EMV PIN verification „wedge" vulnerability, http://www.cl.cam.ac. uk/research/security/banking/nopin/ (zuletzt abgerufen am 12.5.2011).
43 Vgl. *Murdoch/Drimer/Anderson/Bond* (Anm. 42).
44 Vgl. *Murdoch/Drimer/Anderson/Bond* (Anm. 42).
45 Vgl. hierzu die Nachrichtenmeldung des ZDF *„BKA: Magnetstreifen auf Kredit- und EC-Karten müssen weg"* vom 2.1.2011, abrufbar unter http://www.heute.de/ZDFheute/inhalt/11/0,3672,8182219,00.html.
46 Vgl. Anm. 28, S. 2.
47 Vgl. Anm. 28, S. 6.
48 Vgl. Anm. 28, S. 5.
49 Vgl. *BKA* (Anm. 12), S. 11.
50 Vgl. Spiegel-Online Artikel *„Überfall am Geldautomaten"* vom 10.3.2010, abrufbar unter http:// www.spiegel.de/netzwelt/web/0,1518,682345,00.html.
51 Vgl. *Küch* (Anm. 13), 8 (13).
52 Vgl. *Kochheim* (Anm. 24), S. 6.
53 Vgl. Mitteilung von „Die Welt": „Karten-Gangster suchen sich neue Ziele", abrufbar unter: http://www.welt.de/print/die_welt/finanzen/article13364668/Karten-Gangster-suchen-sich-neue-Ziele.html (zuletzt abgerufen am 16.5.2011).

Rezension von Erhard Blankenburg über

Susanne Baer, Rechtsoziologie – Eine Einführung in interdisziplinäre Rechtsforschung, Nomos Verlag Baden-Baden 2011

Lehrbücher für Rechtssoziologie haben es schwer, ihre Adressaten zu finden. Mangels Lehrstühlen und Studenten richten sie sich meist an ein imaginäres Fachpublikum, erklären den Unterschied zwischen empirischen und normativen Wissenschaften und klappern grosse Theoretiker ab. Sie versuchen mit enzyklopädischer Selbstdarstellung gewichtig zu werden, anstatt eine junge Studentengeneration neugierig zu machen. Aufgeweckte Jurastudenten, die sich aus dem spröden Stoff des Staatsexamens hinauslehnen, mögen nach einer externen Sicht auf die Jurisprudenz verlangen oder gar nach den Realitäten des Rechtsbetriebs fragen. Aber dazu müssen sie zu allererst lernen, Fragen zu stellen. Ihnen bietet sich ein ganzer Kranz von Wissenschaftstraditionen an von der Rechtsphilosophie und Rechtsgeschichte zur Rechtstheorie und juristischen Methodenlehre bis zur Rechtspsychologie und Rechtssoziologie. Susanne Baer klärt kurz, was die Fragestellungen dieser sogenannten Grundlagen- (und für die Studierenden:) Wahlfächer sind, sie verweist auf die zugehörigen Forschungsfelder von interdisziplinärer und empirischer Sozialforschung und illustriert ihren Lernweg mit einem originellen Schnellspurt durch die Rechtsgeschichte. „*Geschichten* statt Geschichte" beginnt klassisch mit Aristoteles, berührt ganz abendländisch Ibn Khaldun, Macchiavelli und Montesquieu um (alles auf zwei Druckseiten) bei Adam Smith, Lorenz von Stein und Tocqueville zu landen. Jetzt wissen die Leser: hier sind wir nicht im Kleingarten der putzigen Nebenfächer, hier wird veränderbares Recht in seinem jeweiligen philosophischen, politischen (und so wird sich zeigen) soziologischen Kontext behandelt.

Man merkt dem Text an, dass die Autorin über etwas politische Praxis verfügt und dass sie sich in den USA bei anderen Rechtsinstitutionen umgetan hat. Sie verhehlt nicht ihre gender-Position, wenn sie mit den Idiotien der politisch korrekten, Sprachregelungen zu Männern, Frauen, Rassen oder Klassen aufräumt: so ersetzt sie – soweit sprachlich auszuhalten – das generische Maskulinum (etwa bei *Studenten, Anwälten*) durch neutrale Substantive (‚*Studierenden*' oder ‚*Anwaltschaft*', nur wenn's nicht anders geht durch ‚*Rechtsanwälte und Rechtsanwältinnen*'.) Im Übrigen schreibt sie so, wie in der Erfahrungswelt der Studierenden geredet wird. Sie verkrampft nicht, um den Existenzbeweis einer akademischen Disziplin zu erbringen, dennoch gelingt es ihr, die Vielfalt der Ansätze empirischer Rechtsforschung sehr leichthin, aber einigermassen erschöpfend darzustellen. Chapeau!

Die rechtsoziologische Umschau beginnt, nachdem sie in den ersten Abschnitten in den Wissenschaften des Rechts eingeordnet ist, mit „Recht als Regulierung". Locker folgt die Darstellung den verschiedenen Typen von Regeln, Normen, Konventionen und Gesetzen zu den Institutionen des positiven Rechts und ‚lebendem Recht'. Von dort geht es zum ‚globalen Recht' und zum Rechtspluralismus. Wo manche Rechtstheoretiker noch immer wortreiche Abschiedsnöte von der Zentriertheit auf den Staat zelebrieren, stellt sie unbeschwert ‚Regelungen' vor von privaten und öffentlichen Akteuren, von internationalen Organisationen und von Märkten. ‚Rechtspluralismus' bei ihr ist immer schon eine freundliche Vielfalt gewesen von alltäglichen Regeln und strikten Vorschriften, die stets mal wieder gebrochen werden.

Das Ausmass der Normbrüche allerdings und das alltägliche Umgehen von Regeln bleiben bei Baer ausser Betracht. Sie nennt die diversen Vorraussetzungen von Wahrnehmung, Psychologie und Semantik für die Interpretation und Konstruktion von Regeln, geht jedoch nicht auf abweichendes Verhalten und seine Konflikte ein. Studenten wissen schliesslich, dass Normen am besten kennen zu lernen sind, wenn man sie mal überschreitet. Hier macht sich schmerzlich bemerkbar, dass Baer die Kriminologie fast völlig ausklammert, obwohl doch Einsicht in die Etikettierungs-Theorie' auch den Zivilrechtlern und Öffentlich-Rechtlern gut tun würde.

Mit der Allgegenwart von ‚Rechtspluralismus' bei ihr bleibt seine Verwendung als juristischer Kampfbegriff von allerlei *Rechten* für Minderheiten, Sprachen oder Traditionalismen politisch noch unbeschwert. Welche Konflikte entstehen, wenn konkurrierende Vorstellungen die Regeln gegeneinander schieben zu einer Inflation von ‚Rechten', dieser Thematik wird erst in späteren Kapiteln der Einführung etwas Dynamik verleihen.

Beim freundlichen Nebeneinander von Baer's Pluralismus bäumen sich Schulen und Theorien oder ‚Ansätze' nicht gegeneinander auf. Wo im rechtstheoretischen Schrifttum Kontroversen ausgefochten werden, stellt Baer kritische Fragen. Sie gibt allenfalls Verweise, wo