Debit Card Fraud: Strafrechtliche Aspekte des sog. „Skimmings“

Von Wiss. Mitarbeiter und Mediator (CVM) **Alexander Seidl**, Passau*

Die Zahl der „Angriffe auf Geldautomaten“ bewegt sich seit Jahren auf hohem Niveau. 2009 wurden laut Bundeskriminalamt (BKA) in Deutschland über 100.000 Menschen Opfer sog. Skimming-Attacken,[1] wobei ein Schaden von etwa 40 Millionen Euro entstand. Ihre bisherige Spitze erreichte die Zahl der Skimming-Attacken mit 190.000 betroffenen Kunden und einem Schaden von schätzungsweise 60 Millionen Euro im Jahr 2010.[2] Für das Jahr 2011 war ein Rückgang im Vergleich zum Vorjahr von rund 50 Prozent festzustellen.[3] Dennoch dürfte der Kampf gegen das Skimming noch nicht endgültig gewonnen sein. Es ist zu befürchten, dass die rückläufigen Zahlen auf eine Phase der Umorganisation der kriminellen Banden zurückzuführen sind.

Im Folgenden soll die Strafbarkeit dieser Form der Geldautomatenkriminalität nach dem StGB näher beleuchtet werden.[4] Insbesondere werden die neueren Entscheidungen der verschiedenen Senate des BGH zum Versuchsbeginn bei der Fälschung von Zahlungskarten mit Garantiefunktion gem. §§ 152b, 22 StGB untersucht.

I. Einführung – Was ist Skimming?

Skimming meint das Abschöpfen von Daten aus einer Debit- (früher: ec-Karte) oder Kreditkarte (zusammengefasst als Zahlungskarten bezeichnet) durch Auslesen und Kopieren des Inhalts des auf der Karte befindlichen Magnetstreifens, um die Informationen anschließend auf einen Kartenrohling zu übertragen und diesen in der Folge gemeinsam mit der ebenfalls ausspionierten zugehörigen persönlichen Identifikationsnummer (PIN) für Geldabhebungen im Ausland zu missbrauchen. Namengebend für diese Form des „Zahlungskartenbetrugs“ sind die dabei zum Einsatz kommenden Kartenlesegeräte, die sog. Skimmer.[5]

Skimming-Angriffe treten in unterschiedlichen Erscheinungsformen auf. So wurden zuletzt nicht nur Geldautomaten mit zusätzlichen Kartenlesegeräten ausgestattet, auch an SB-Tankstellen und Bahnkartenautomaten wurden die Bank- bzw. Kreditkartenterminals auf diese Weise manipuliert.[6] Beim „klassischen“ Fall des Skimmings – auf den sich die folgenden Darstellungen beschränken –, also dem Ausspähen von Zahlungskartendaten an Geldautomaten, wird von den Tätern zunächst ein Miniatur-Kartenleser von außen vor dem Leseschlitz des Geldautomaten befestigt oder aber bereits am Türöffner im Eingangsbereich des betroffenen Kreditinstituts angebracht.[7] Die Zahlungskarte des Kunden wird bei der Benutzung von Automat oder Türöffner unbemerkt durch das zusätzliche Lesegerät gezogen, wobei es zum Auslesen des Inhalts des Magnetstreifens kommt. Für das ungeschulte Auge ist die Manipulation kaum zu erkennen, da der Aufsatz von den Tätern in Farbe und Form dem jeweiligen Geldautomaten bzw. Türöffner angepasst wird. Die abgegriffenen Daten werden gespeichert und nach dem Abbau der Skimming-Vorrichtung auf einen PC übertragen oder gleich per Funk an die Täter übermittelt.[8]

Das Ausspähen der PIN des Karteninhabers kann ebenfalls auf unterschiedliche Weise erfolgen. Meist kommt eine oberhalb des Tastaturfeldes angebrachte Videoleiste zum Einsatz, hinter der sich eine kleine Kamera verbirgt, mittels derer die PIN-Eingabe aufgezeichnet wird. Alternativ verwenden die Täter auch Nachbildungen der Geldautomatentastaturen, die auf die echte Tastatur geklebt werden. Bei Eingabe der PIN werden die Anschläge an die Originaltastatur durchgereicht und dabei protokolliert, während gleichzeitig der Geldautomat störungsfrei bedient wird. Das Ausspähen kann aber auch schlicht durch „Über-die-Schulter-Schauen“ eines Täters erfolgen.

Nach erfolgreicher Kartendaten- und PIN-Beschaffung stellen die Skimming-Täter unter Verwendung von leeren Kartenrohlingen (sog. „White-Plastics“) Dubletten her, mit denen sie nunmehr Abhebungen vornehmen können. Diese erfolgen dabei stets im – in den letzten Jahren vor allem europäischen – Ausland, da Zahlungskarten deutscher Ausgabestellen mit einem besonderen Schutzmechanismus, dem sog. moduliert maschinenfähigen Merkmal (MM-Merkmal) ausgestattet sind, das Abhebungen unter Zuhilfenahme billiger Datenträger unmöglich macht. Seit der zweiten Jahreshälfte 2010 erfolgen die missbräuchlichen Karteneinsätze zunehmend im außereuropäischen Bereich. Grund dafür ist, dass seit Anfang 2011 Transaktionen europäischer Debitkarten im SEPA-Raum EMV-Chip-basiert[9] abgerechnet werden.[10] Da

---

* *Alexander Seidl* ist Assessor und wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht (Prof. *Dr. Dirk Heckmann*) an der Universität Passau. Der *Autor* dankt Herrn KHK *Stephan Ruf*, LKA Bayern, für technische Erläuterungen und Frau StAin *Ulrike Hackler*, Staatsanwaltschaft Traunstein, für die Unterstützung bei der Ausarbeitung des Beitrags.

[1] http://wirtschaft.t-online.de/bka-2009-ueber-100-000-opfer-von-skimming/id_41434792/index (16.8.2012).

[2] Vgl. BKA, Zahlungskartenkriminalität, Bundeslagebild 2010, S. 5.

[3] S. www.ftd.de/unternehmen/finanzdienstleister/:skimming-erfolgreicher-kampf-gegen-datenklau-am-geldautomaten/60146294.html (16.8.2012).

[4] Zur Strafbarkeit auch nach dem Nebenstrafrecht vgl. *Seidl/Fuchs*, HRRS 2011, 265.

[5] *Kochheim*, Skimming – Hintergründe und Strafrecht, Fassung 2.21, Stand: April 2011, S. 4, im Internet abrufbar unter: http://www.kochheim.de/cf/doc/Kochheim-Skimming-2010.pdf (16.8.2012).

[6] BKA (Fn. 2), S. 8 f.

[7] Letztere Variante war allerdings im Jahr 2010 stark rückläufig und machte nur noch 2 % der Fälle aus.

[8] *Bachfeld*, c't 25/2007, 76 (77).

[9] EMV steht für „Europay International (heute MasterCard Europe), MasterCard und Visa“ und ist ein internationaler technischer Standard zur Abwicklung von Chipkartenzahlungen. Vertiefend hierzu *Seidl/Fuchs*, HRRS 2011, 265 (274).

[10] Eine kriminologische Betrachtung des Skimmings findet sich bei *Bachmann/Goeck*, Neue Kriminalpolitik 2011, 153.

viele Banken im Hinblick auf diese Umstellung die Geräte bereits sukzessive umgerüstet haben, wichen die Täter zunehmend in die Nicht-Chip-Länder aus, insbesondere in die Staaten Südafrika, Kenia, USA, Kanada sowie die Dominikanische Republik.[11]

II. Strafrechtliche Würdigung

Um eine strafrechtliche Würdigung des Skimmings vornehmen zu können, ist der Gesamtvorgang „Skimming" zunächst in folgende Tatkomplexe aufzuteilen:

- Herstellung bzw. Verschaffen der Skimming-Ausrüstung,
- Ausspähen von Magnetstreifen und PIN,
- Herstellung der Dubletten,
- Einsatz der Dubletten,
- Verteilung der Beute.

Ihre strafrechtliche Bewertung soll zum besseren Verständnis hier jedoch nicht chronologisch vorgenommen werden.

Dass jedenfalls der Einsatz der Dubletten stets im Ausland erfolgt, ist für die Anwendbarkeit des deutschen Strafrechts unerheblich.[12] Da nämlich für sämtliche Tatbeteiligte Mittäterschaft anzunehmen sein wird,[13] ist aufgrund der hierbei erfolgenden gegenseitigen Anrechnung der Tatbeiträge an jedem Ort, an dem einer der Mittäter gehandelt hat, mithin auch in Deutschland, ein Tatort i.S.d. § 9 Abs. 1 StGB begründet.[14] Damit findet das deutsche Strafrecht gemäß § 3 StGB Anwendung.[15]

1. Strafbarkeit des Ausspähens von Magnetstreifen und PIN

a) Ausspähen der Magnetstreifeninformationen

aa) Strafbarkeit nach § 202a StGB

Das Auslesen des auf der EC-Karte befindlichen Magnetstreifens erfüllt den Tatbestand des § 202a StGB nicht. Zwar handelt es sich bei den auf dem Magnetstreifen einer EC-Karte gespeicherten Informationen, insbesondere Kontonummer und Bankleitzahl, um nicht unmittelbar wahrnehmbar gespeicherte Daten, da sie in einer für eine Datenverarbeitungsanlage erkennbaren Form codiert sind und erst nach einer Transformation mittels technischem Hilfsmittel wahrgenommen werden können, also mithin Daten i.S.d. § 202a StGB.

Die Daten sind auch „nicht für den Täter bestimmt". Für den Täter bestimmt sind sie nur dann, wenn sie nach dem Willen desjenigen, der zum Zeitpunkt der Tat die formelle Verfügungsberechtigung über die Daten innehat, dem Täter zur Verfügung stehen sollen.[16] Maßgeblich ist bei Bank- und Kreditkarten der Wille des kartenausgebenden Kreditinstituts.[17] Dieses wird mit dem Ausspähen der Magnetstreifeninformationen nicht einverstanden sein.

Eine Strafbarkeit nach § 202a Abs. 1 StGB scheitert jedoch am fehlenden Vorliegen einer besonderen Zugangssicherung, zumindest am mangelnden Überwinden einer solchen. Eine besondere Zugangssicherung liegt nur dann vor, wenn Vorkehrungen getroffen sind, um den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Die Zugangssicherung kann dabei sowohl durch mechanische (z.B. Schlösser, Versiegelungen) als auch durch technische, insbesondere systemimmanente Vorkehrungen (z.B. Passwort, biometrische Erkennungsverfahren) erfolgen.[18] Weder die auf dem Magnetstreifen gespeicherte Kontonummer noch die Bankleitzahl werden jedoch durch derartige Schutzmechanismen gesichert. Insoweit scheitert eine Strafbarkeit nach § 202a Abs. 1 StGB also bereits am fehlenden Vorhandensein einer Zugangssicherung.[19] Doch selbst wenn sich auch verschlüsselte Daten auf dem Magnetstreifen befinden sollten,[20] würde der Tatbestand des § 202a Abs. 1 StGB nicht verwirklicht. Zwar wäre in diesem Fall das Vor-

[11] bka.de/nn_227456/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaetPraesentationInternationaleKonferenz,templateId=raw,property=publicationFile.pdf/zahlungskartenkriminalitaetPraesentationInternationaleKonferenz.pdf (16.8.2012).

[12] Ausf. hierzu vgl. *Seidl/Fuchs*, HRRS 2011, 265 (266).

[13] *Braun/Heidberg*, StrafRechtsReport 2010, 89 (93); vgl. auch *Bachmann/Goeck*, JR 2011, 425.

[14] *Eser*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 28. Aufl. 2010, § 9 Rn. 10; *Rotsch*, in: Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, Kommentar, 2011, § 9 Rn. 13.

[15] Sollte eine Anwendbarkeit deutschen Strafrechts nach diesen Vorschriften ausnahmsweise nicht in Betracht kommen, kann sie sich aus § 6 StGB ergeben. Diese Vorschrift nennt Taten (u.a. § 152b und § 149 StGB, s. § 6 Nr. 7 StGB), die nach dem Weltrechtsprinzip ohne Rücksicht auf Tatort, Recht des Tatorts und Staatsangehörigkeit des Täters dem deutschen Strafrecht unterliegen.

[16] *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 14), § 202a Rn. 6.

[17] Vgl. *Seidl/Fuchs*, HRRS 2011, 265 (267).

[18] Vgl. *Weidemann*, in: von Heintschel-Heinegg (Hrsg.), Beck'scher Online-Kommentar, Strafgesetzbuch, Stand: Juni 2012, § 202a Rn. 13.

[19] Dass die Daten magnetisch und damit nicht unmittelbar wahrnehmbar gespeichert sind, stellt keine besondere Sicherung gegen unberechtigten Zugang dar, sondern ist gem. § 202a Abs. 2 StGB vielmehr Voraussetzung dafür, dass es sich überhaupt um Daten i.S.d. Abs. 1 handelt. Daran zeigt sich, dass nicht schon die Art der Speicherung eine besondere Sicherung i.S.d. § 202a Abs. 1 StGB darstellt, sondern dass darüber hinaus Vorkehrungen getroffen sein müssen, die den unbefugten Zugriff auf Daten ausschließen oder zumindest erheblich erschweren, vgl. BGH, Beschl. v. 14.1.2010 – 4 StR 93/09 und BGH, Beschl. v. 6.7.2010 – 4 StR 555/09. So auch *Eisele*, CR 2011, 131 (132).

[20] Vgl. *Richter*, CR 1989, 303 (305); im Beschl. des BGH v. 18.3.2010 – 4 StR 555/09 wird die Frage, ob sich auf dem Magnetstreifen auch verschlüsselte Daten befinden, ausdrücklich offen gelassen. Laut LKA Bayern befinden sich auf dem Magnetstreifen keine verschlüsselten Daten.

liegen einer Zugangssicherung zu bejahen.[21] Beim bloßen Auslesen und Abspeichern der auf dem Magnetstreifen einer Zahlungskarte gespeicherten Daten würde diese jedoch nicht überwunden.[22] Ein Überwinden erfordert eine Vorgehensweise, durch die die jeweilige Zugangssicherung außer Kraft gesetzt oder umgangen wird.[23] Gerade daran würde es jedoch fehlen: Die verschlüsselten Daten würden nicht etwa entschlüsselt, sondern in verschlüsseltem Zustand gespeichert.[24]

bb) Strafbarkeit nach § 263a StGB

Auch eine Strafbarkeit wegen Computerbetrugs durch unbefugte Verwendung von Daten gem. § 263a Abs. 1 Var. 3 StGB scheidet aus.[25] Zwar erfasst § 263a Abs. 1 Var. 3 StGB – im Gegensatz zu den ersten beiden Tatvarianten – gerade die Fälle, in denen der Täter – wie beim Skimming – richtige Daten verwendet.[26] Es fehlt jedoch an der für die Verwirklichung des Tatbestands erforderlichen Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs: Hierfür reicht eine Einflussnahme, die zu keinem abweichenden Ergebnis des Datenverarbeitungsvorgangs führt, nicht aus. Vielmehr muss diese ein Ergebnis hervorgerufen haben, das ohne die Einwirkung entweder überhaupt nicht oder mit anderem Inhalt entstanden wäre.[27] Dies ist hier jedoch gerade nicht der Fall. Nachdem die Zahlungskarte das zusätzlich angebrachte Kartenlesegerät passiert hat und die auf dem Magnetstreifen enthaltenen Informationen mithilfe des Moduls ausgelesen wurden, läuft der im Geldautomaten stattfindende Datenverarbeitungsprozess ordnungsgemäß ab, es kommt also zu keiner Beeinflussung seines Ergebnisses.

cc)Strafbarkeit nach § 303b StGB

Nichts anderes gilt hinsichtlich einer Strafbarkeit gem. § 303b StGB mangels erheblicher Störung einer Datenverarbeitung. Die Datenverarbeitung ist dann erheblich gestört, wenn ihr reibungsloser Ablauf beeinträchtigt wird.[28] Beim Auslesen der Magnetkartendaten durch das zusätzlich angebrachte Kartenlesegerät wird der Ablauf der Datenverarbeitung im Geldautomaten aber gerade nicht beeinträchtigt. Die Datenverarbeitung läuft vielmehr ordnungsgemäß ab.

dd) Strafbarkeit nach § 303a StGB

Auch eine Strafbarkeit nach § 303a Abs. 1 StGB wegen Veränderns der auf dem Magnetstreifen enthaltenen Daten der Originalbankkarte scheidet aus. Dieses ist nämlich nur dann gegeben, wenn eine inhaltliche Umgestaltung der Daten erfolgt und sie deshalb einen anderen Informationsgehalt aufweisen. Das bloße unbefugte Kopieren von Daten wird dagegen nicht vom Tatbestand erfasst.[29]

ee) Strafbarkeit nach § 202b StGB

Eine Strafbarkeit nach § 202b StGB scheitert daran, dass der Skimming-Täter die auf dem Magnetstreifen enthaltenen Informationen – bei denen es sich um nicht für ihn bestimmte Daten i.S.d. § 202b StGB handelt – nicht aus einer nicht öffentlichen Datenübermittlung abfängt.[30] Eine nicht öffentliche Datenübermittlung findet beim Abhebungsvorgang zwar statt, die Magnetstreifendaten werden aber noch im Vorfeld des zwischen Bankkunde und Kreditinstitut erfolgenden Datenübertragungsvorgangs, der erst mit Einlesen der Zahlungskarte durch den Originalkartenleser beginnt, vom Täter abgeschöpft. Im Zeitpunkt des Abschöpfens der Informationen stammen die Daten also gerade nicht aus einer nicht öffentlichen Datenübertragung. Vielmehr wird eine eigene Datenübertragung durch den Täter initiiert, deren Adressat er selbst ist.[31]

ff) Strafbarkeit nach §§ 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB

Indem der unwissende Bankkunde seine EC-Karte in den am Bankautomaten angebrachten Skimming-Aufsatz einführt, macht sich der Täter jedoch wegen Fälschung beweiserheblicher Daten in mittelbarer Täterschaft strafbar. Der vorsatzlos handelnde Bankkunde erfüllt die Tatbestandsvoraussetzungen

[21] Nach h.M. stellen auch Datenverschlüsselungen Sicherungen i.S.v. § 202a StGB dar, vgl. *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 59. Aufl. 2012, § 202a Rn. 9a.

[22] BGH, Beschl. v. 14.1.2010 – 4 StR 93/09, BGH, Beschl. v. 18.3.2010 – 4 StR 555/09 und BGH, Beschl. v. 6.7.2010 – 4 StR 555/09; *Seidl/Fuchs*, jurisPR-ITR 9/2010 Anm. 6; i.E. auch *Tyszkiewicz*, HRRS 2010, 207 (209), die jedoch trotz Bejahung des Vorhandenseins verschlüsselter Daten weniger auf das Überwinden, als vielmehr auf das Fehlen einer ausreichenden Zugangssicherung abstellt; a.A. dagegen *Braun/Heidberg*, StrafRechtsReport 2010, 89 (91), die ohne nähere Erläuterung das Vorhandensein von Schutzvorkehrungen und deren Überwindung bejahen.

[23] *Weidemann* (Fn. 18), § 202a Rn. 17; Eine Datenverschlüsselung schützt nur vor der Erfassung des Bedeutungsgehalts (kryptierter) Daten, nicht aber vor dem bloßen Auslesen und Abspeichern der verschlüsselten Daten auf einem Datenträger des Täters, vgl. BGH, Beschl. v. 18.3.2010 – 4 StR 555/09.

[24] Vgl. auch BGH, Beschl. v. 14.1.2010 – 4 StR 93/09, und BGH, Beschl. v. 18.3.2010 – 4 StR 555/09; a.A. dagegen noch BGH, Urt. v. 10.5.2005 – 3 StR 425/04, die jedoch auf Anfragebeschluss aufgegeben wurde, vgl. BGH, Beschl. v. 6.7.2010 – 4 StR 555/09.

[25] Im Ergebnis ebenso, aber mit anderer Begründung *Eisele*, CR 2011, 131 (134).

[26] „Verwenden“ meint in diesem Zusammenhang die Einführung der Daten in den Datenverarbeitungsprozess, wobei über die Fälle der eigenhändigen Eingabe hinaus auch diejenigen erfasst sind, in denen der Täter sich – wie beim Skimming – für den unmittelbaren Akt der Eingabe einer anderen Person bedient, vgl. *Wohlers*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2007, § 263a Rn. 29.

[27] *Wohlers* (Fn. 26), § 263a Rn. 17.

[28] *Hilgendorf*, JuS 1996, 1082 (1083).

[29] *Weidemann* (Fn. 18), § 303a Rn. 13.

[30] Ebenso *Eisele*, CR 2011, 131 (132).

[31] Vgl. zur ähnlichen Problematik beim Phishing *Seidl/Fuchs*, HRRS 2010, 85 (86).

des § 269 Abs. 1 Alt. 1 StGB, denn er speichert beweiserhebliche Daten so, dass bei ihrer Wahrnehmung eine unechte Urkunde vorliegen würde. Daten sind beweiserheblich, wenn sie dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden.[32] Bei Codekartendaten im Bankautomatenverkehr ist dies der Fall.[33] Ein Speichern der Daten ist gegeben, wenn sie auf einem Datenträger erfasst oder aufbewahrt oder auf ihn kopiert bzw. aufgenommen werden. Durch das Speichern muss ein Falsifikat entstehen, das – von der Wahrnehmbarkeit abgesehen – die Merkmale einer falschen Urkunde aufweist.[34] Die auf dem Magnetstreifen einer EC-Karte gespeicherten Daten beinhalten eine Garantieerklärung der Ausstellerbank zugunsten des berechtigten Karteninhabers. Wer den Magnetstreifen einer solchen Karte kopiert, erzeugt den falschen Anschein einer weiteren Gedankenerklärung der Ausstellerbank und verwirklicht dadurch § 269 StGB.[35] Dieser vom Bankkunden unvorsätzlich herbeigeführte, strafrechtlich verbotene Erfolg wird vom Skimming-Täter vorsätzlich bewirkt, sodass ein klassischer Fall der mittelbaren Täterschaft vorliegt.[36] Der Skimming-Täter handelt darüber hinaus auch mit dem Willen, die erlangten Daten zur fälschlichen Beeinflussung einer Datenverarbeitung zu verwenden, welche gem. § 270 StGB der Täuschung im Rechtsverkehr gleichsteht. Regelmäßig wird zudem der Qualifikationstatbestand des § 267 Abs. 4 StGB, auf den § 269 Abs. 3 StGB verweist und der eine verschärfte Sanktionierung für die gewerbsmäßige Begehung als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263-264 oder 267-269 StGB verbunden hat, vorsieht, verwirklicht sein.[37]

gg) Strafbarkeit nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB

Ferner ist auch der Tatbestand der Vorbereitung der Fälschung von Zahlungskarten mit Garantiefunktion gem. § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB zu bejahen.[38] § 149 Abs. 1 Nr. 1 StGB beschreibt bestimmte Vorrichtungen zur Herstellung von Falsifikaten, die ihrer Art nach zur Begehung der Tat geeignet sein müssen. Neben den explizit erwähnten fallen darunter auch solche, denen schon ihrer Art nach eine spezifische Verwendbarkeit zur Ausführung von Fälschungen innewohnt.[39] Erforderlich ist auch, dass diese „ähnlichen Vorrichtungen" gebrauchsfertig und zum unmittelbaren Einsatz im eigentlichen Fälschungsvorgang geeignet sind.[40] Seit der Aufnahme des Begriffs „Computerprogramme" in den Tatbestand des § 149 Abs. 1 Nr. 1 StGB,[41] mit dem zum Ausdruck kommt, dass sich der Anwendungsbereich der Vorschrift nicht prinzipiell auf körperliche Tatobjekte beschränkt, steht darüber hinaus fest, dass auch nicht körperliche Vorlagen der Vervielfältigungstechnik als „ähnliche Vorrichtungen" von der Vorschrift erfasst werden.[42] Damit fallen auch die mithilfe des Skimmers ausgelesenen Datensätze, die im Anschluss auf die Magnetstreifen der Kartendubletten kopiert werden können und dabei unmittelbar zur Entstehung unechter Zahlungskarten mit Garantiefunktion führen, unter diesen Begriff.[43]

hh) Strafbarkeit nach §§ 152b, 22 StGB in Abgrenzung zu §§ 152b, 30 Abs. 2 Var. 3 StGB

Mehrfach Gegenstand höchstrichterlicher Entscheidungen war zuletzt die Frage, wann – in Fällen, in denen die Manipulationen am Geldautomaten vor Tatvollendung durch Sicherstellung der Skimming-Anbauten verhindert wurde – ein unmittelbares Ansetzen der Täter zum Fälschen von Zahlungskarten mit Garantiefunktion zu bejahen ist.[44]

Nach den allgemeinen Grundsätzen zur Abgrenzung von Vorbereitungshandlungen zum strafbaren Versuch liegt ein unmittelbares Ansetzen nur bei solchen Handlungen vor, die nach Tätervorstellung in ungestörtem Fortgang unmittelbar zur Tatbestandserfüllung führen oder mit ihr in einem unmittelbaren räumlichen und zeitlichen Zusammenhang stehen. Dies ist insbesondere der Fall, wenn der Täter subjektiv die

[32] *Fischer* (Fn. 21), § 269 Rn. 4.
[33] Vgl. *Lackner/Kühl*, Strafgesetzbuch, Kommentar, 27. Aufl. 2011, § 269 Rn. 2.
[34] *Fischer* (Fn. 21), § 269 Rn. 7.
[35] *Hoyer*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, 131. Lfg., Stand: März 2012, § 269 Rn. 16.
[36] *Joecks*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 1, 2. Aufl. 2011, § 25 Rn. 53 ff.
[37] Auf Konkurrenzebene dürfte § 269 StGB jedoch von § 152b StGB verdrängt werden, vgl. *Erb*, in: Joecks/Miebach (Fn. 26), § 269 Rn. 41.
[38] § 149 StGB tritt hinter § 152b StGB zurück, sobald dort ein strafbarer Versuch begangen wird. Ob § 149 StGB auch hinter die Verabredung der gewerbs- und bandenmäßigen Fälschung von Zahlungskarten mit Garantiefunktion gem. §§ 152b, 30 Abs. 2 Var. 3 StGB zurücktritt, ist umstritten. Vom BGH wurde diese Frage zuletzt immer offen gelassen, vgl. bspw. BGH, Beschl. v. 11.8.2011 – 2 StR 91/11, oder BGH, Urt. v. 17.2.2011 – 3 StR 419/10. Teils wird vertreten, § 149 StGB werde wegen seiner geringeren Strafandrohung (Freiheitsstrafe bis zu fünf Jahre) vom Tatbestand des §§ 152b, 30 Abs. 2 Var. 3 StGB, der einen Strafrahmen von sechs Monaten bis zu elf Jahren und drei Monaten eröffnet, verdrängt (so BGH, Urt. v. 13.1.2010 – 2 StR 439/09). Nach a.A. soll Tateinheit zwischen den beiden Delikten möglich sein, da dem Vergehen nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 gegenüber der Verbrechensverabredung nach §§ 152b, 30 Abs. 2 Var. 3 StGB ein eigener Unrechtsgehalt zukomme, vgl. *Fischer* (Fn. 21), § 149 Rn. 12; *Hoyer* (Fn. 35), § 30 Rn. 60.
[39] *Erb* (Fn. 38), § 149 Rn. 3.
[40] *Erb* (Fn. 38), § 149 Rn. 3.
[41] Gesetz v. 22.8.2002 = BGBl. I 2002, S. 3387.
[42] *Erb* (Fn. 38), § 152a Rn. 13.
[43] Vgl. *Erb* (Fn. 38), § 152a Rn. 13; *Stein*, in: Rudolphi u.a. (Hrsg.), 67. Lfg., Stand: Oktober 2006, § 149 Rn. 2; *Puppe*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 3. Aufl. 2010, § 149 Rn. 9; vgl. auch *Eisele*, CR 2011, 131 (134).
[44] Vgl. hierzu schon *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

Schwelle zum „jetzt geht es los“ überschreitet, es eines weiteren Willensimpulses nicht mehr bedarf und er objektiv zur tatbestandsmäßigen Angriffshandlung ansetzt, sodass sein Tun ohne Zwischenakte in die Erfüllung des Tatbestandes übergeht.[45]

Unter Heranziehung dieser Grundsätze haben sowohl der *2.* und der *3.* als auch der *5. Strafsenat* des BGH entschieden, dass ein unmittelbares Ansetzen frühestens dann anzunehmen sei, wenn der Täter mit der eigentlichen Fälschungshandlung, also dem Herstellen der falschen Zahlungskarte, beginne.[46] In den übrigen Fällen liege lediglich die Verabredung der gewerbs- und bandenmäßigen Fälschung von Zahlungskarten mit Garantiefunktion gem. §§ 152b, 30 Abs. 2 Var. 3 StGB vor.

Mit Urteil vom 27.1.2011 entschied der *4. Strafsenat* des BGH,[47] dass spätestens die Weitergabe der ausgelesenen Kartendaten das unmittelbare Ansetzen zur Tatbestandsverwirklichung i.S.d. § 22 StGB darstellt, wenn es der Täter im Rahmen eines Tatplans zur Fälschung von Zahlungskarten mit Garantiefunktion, bei dem die einzelnen Tatbeiträge eng ineinander greifen und schnell aufeinander folgen, übernommen hat, die Daten von Zahlungskarten mittels Skimmings auszuspähen, da dem Täter auf Grund des Tatplans bewusst ist, durch die Weitergabe einen gleichsam automatisierten Ablauf in Gang zu setzen. Der *4. Strafsenat* stellte dabei auf das enge Ineinandergreifen der einzelnen, einem festen Ablaufplan folgenden Tatbeiträge und auf den nach dem Tatplan engen zeitlichen Zusammenhang zwischen dem Tatbeitrag der Angeklagten und dem Beschreiben der Kartenrohlinge durch andere Bandenmitglieder als eigentliche Fälschungshandlung ab. Die dem Auslesen der Daten und der Weitergabe der Speichermedien nachfolgenden Arbeitsschritte bis hin zu den – der Tatbestandsverwirklichung des § 152b StGB nachgelagerten – Abhebungen an den Geldautomaten mussten vonstattengehen, bevor die Manipulation an den Lesegeräten in den Bankfilialen bemerkt wurde. Die schnelle zeitliche Abfolge wurde durch das eingespielte System von Tatbeiträgen gewährleistet, bei dem den im Ausland sitzenden Mittätern die einzelnen Datenübersendungen jeweils avisiert wurden. Diese wussten dadurch bereits im Voraus, dass die Erbringung ihres eigenen Tatbeitrags unmittelbar bevorstand. Es bedurfte mithin keines neuen Willensimpulses bei einem der durch die Bandenabrede verbundenen Mittäter mehr, sondern die Angeklagten setzten mit der Weitergabe der Daten – was ihnen bewusst war – gleichsam einen automatisierten Ablauf in Gang, sodass auch unter dem Gesichtspunkt der konkreten nahen Rechtsgutsgefährdung die Annahme eines unmittelbaren Ansetzens geboten sei. Dass dem Beschreiben der Kartenrohlinge die Auswertung der Speichermedien durch Abgleich von Videoaufzeichnungen und ausgelesenen Kartendaten und die Übersendung der Daten ins Ausland vorausgingen, stellt – nach Ansicht des BGH – bei der gebotenen wertenden Betrachtung keine diese Annahme hindernden Zwischenschritte dar.[48]

Die – nur auf den ersten Blick widersprüchliche – Rechtsprechung der verschiedenen BGH-*Senate* baut konsequent und widerspruchsfrei aufeinander auf.[49] Der *2.*, *3.* und *5. Strafsenat* beziehen sich zu Recht auf die von der Rechtsprechung entwickelten allgemeinen Grundsätze zur Abgrenzung von Vorbereitungshandlungen zum strafbaren Versuch. Deshalb ist auch nach diesen Entscheidungen das Beginnen mit der Fälschungshandlung als Beginnen im Sinne der allgemeinen Definition des unmittelbaren Ansetzens zu verstehen; hiervon sind auch vorgelagerte Handlungsakte umfasst, sofern diese nach der Tätervorstellung in ungestörtem Fortgang unmittelbar zur Tatbestandserfüllung führen oder mit ihr in einem unmittelbaren räumlichen und zeitlichen Zusammenhang stehen. Die drei Entscheidungen stehen mithin der Annahme einer Versuchstat im Fall des *4. Strafsenats* nicht entgegen, denn hier hätte die Weiterleitung der gewonnenen Daten nach der Vorstellung der Angeklagten bei ungestörtem Fortgang unmittelbar zur Tatbestandserfüllung führen sollen.[50]

Zum Versuch des Nachmachens setzt nach diesen Grundsätzen jedoch noch nicht an, wer die aufgezeichneten Datensätze nicht in seinen Besitz bringen und sie deshalb auch nicht an seine Mittäter, die die Herstellung der Kartendubletten vornehmen sollen, übermitteln kann. Das Anbringen einer Skimming-Apparatur an einem Geldautomaten in der Absicht, dadurch Daten zu erlangen, die später zur Herstellung der Kartendubletten verwendet werden sollen, ist als solche lediglich eine Vorbereitungshandlung. Die Tat stellt in diesem Verwirklichungsstadium daher lediglich eine Verabredung zu dem Verbrechen der banden- und gewerbsmäßigen Fälschung von Zahlungskarten dar, §§ 152b, 30 Abs. 2 Var. 3 StGB.[51]

b) Strafbarkeit des Ausspähens der PIN gem. § 202c Abs. 1 Nr. 1 i.V.m. § 202a Abs. 1 StGB

Hinsichtlich des Ausspähens der PIN macht sich der Täter nach § 202c Abs. 1 Nr. 1 i.V.m. § 202a Abs. 1 StGB strafbar, und zwar in der Form des Sichverschaffens eines Passworts. Unter einem Passwort versteht man jede Zeichenkombination, die im Rahmen einer Sicherungsabfrage den Zugang zu Daten ermöglicht, mithin nicht nur Wörter.[52] Ein Sichverschaffen ist gegeben, wenn der Täter in irgendeiner Form eigene Verfügungsgewalt am Tatobjekt begründet.[53] Unabhängig davon, ob das Ausspähen der PIN durch bloßes „Über-die-Schulter-Schauen“ oder mithilfe einer Tastatur-

[45] St. Rspr.; vgl. BGH, Urt. v. 13.1.2010 – 2 StR 439/09, und BGH, Urt. v. 7.11.2007 – 5 StR 371/07.

[46] BGH, Urt. v. 13.1.2010 – 2 StR 439/09; BGH, Beschl. v. 11.8.2011 – 2 StR 91/11; BGH, Urt. v. 17.2.2011 – 3 StR 419/10; BGH, Beschl. v. 14.9.2010 – 5 StR 336/10.

[47] BGH, Urt. v. 27.1.2011 – 4 StR 338/10.

[48] Zur Kritik an der Entscheidung des *4. Senats* vgl. *Bachmann/Goeck*, JR 2011, 425 (428).

[49] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

[50] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

[51] BGH, Urt. v. 13.1.2010 – 2 StR 439/09; BGH, Beschl. v. 14.9.2010 – 5 StR 336/10; BGH, Beschl. v. 11.8.2011 – 2 StR 91/11; *Bachmann/Goeck*, JR 2011, 425 (429).

[52] *Weidemann* (Fn. 18), § 202c Rn. 4.

[53] *Sternberg-Lieben*, in: Schönke/Schröder (Fn. 14), § 146 Rn. 15.

attrappe bzw. Videokamera erfolgt, sind diese beiden Voraussetzungen damit erfüllt.[54] Zu beachten ist, dass hinsichtlich der Frage, ob eine Straftat nach § 202a Abs. 1 StGB vorbereitet wird, nicht auf die auf dem Magnetstreifen befindlichen Daten abzustellen ist, da insoweit eine Strafbarkeit wegen Ausspähens von Daten – wie bereits erwähnt – ausscheidet. Vielmehr ist der Fokus auf die weiteren Kontodaten, insbesondere auf den Kontostand, zu richten. Auch bei diesem handelt es sich um ein Datum i.S.d. § 202a Abs. 2 StGB, welches zudem nur für den Kontoinhaber bestimmt und durch die vorgeschaltete PIN-Abfrage am Geldautomaten darüber hinaus besonders gesichert ist.[55] Mithilfe der erspähten PIN ist es dem Täter später in Kombination mit den manipulierten Kartendubletten nicht nur möglich, Geld abzuheben, sondern auch, den Kontostand am Geldautomaten einzusehen. Für ein Sichverschaffen des Zugangs reicht diese bloße Möglichkeit der Kenntnisnahme aus.[56]

2. Herstellung der Dubletten

a) Strafbarkeit nach § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 1 StGB

Die Herstellung der Kartendubletten erfüllt den Tatbestand des § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 1 StGB – Fälschung von Zahlungskarten mit Garantiefunktion – in der Form des „Nachmachens".[57] Bei herkömmlichen EC-Karten handelt es sich um Zahlungskarten mit Garantiefunktion i.S.d. § 152b Abs. 4 StGB.[58] Unter „nachmachen" versteht man sowohl Manipulationen an bereits verfälschten Tatobjekten, als auch das Herstellen von Totalfälschungen. Der Täter muss dabei zur Täuschung im Rechtsverkehr oder aber zur Ermöglichung einer solchen Täuschung handeln. Aufgrund dieses Erfordernisses wurde früher die Herstellung falsch codierter Magnetstreifen auf unbedruckten Karten – mangels deren Eignung zur Täuschung – für die Verwirklichung des Tatbestandes als nicht ausreichend angesehen. Heute stellt sich die Rechtslage im Hinblick auf § 270 StGB, der die Täuschung im Rechtsverkehr mit der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleichstellt, dagegen anders dar: Soweit es – wie bei Geldautomaten – für die Möglichkeit täuschungsgleicher Beeinflussung von Datenverarbeitungsanlagen allein auf die Codierung und die äußere Form der Karte, nicht aber auf Aufdrucke o.Ä. ankommt, reicht die Herstellung unbeschrifteter Plastikstücke mit codiertem Magnetstreifen zur Tatbestandsverwirklichung aus.[59]

Regelmäßig wird dabei auch die Qualifikation des § 152b Abs. 2 StGB wegen gewerbsmäßiger Begehung oder als Bandenmitglied begangener Straftaten nach § 152b Abs. 1 StGB erfüllt sein.

b) Strafbarkeit nach § 269 StGB

Schließlich erfüllt der Täter noch den Tatbestand des § 269 Abs. 1 StGB, und zwar in der Begehungsform des „Speicherns". Bei den ausgelesenen Magnetstreifeninformationen der Original-EC-Karte handelt es sich um beweiserhebliche Daten i.S.d. § 269 Abs. 1 StGB (s.o.). Der Täter speichert diese Daten auch, da er sie zum Zwecke der weiteren Verwendung auf einen Datenträger – den Kartenrohling – kopiert. Durch diese Speicherung entsteht sodann ein Falsifikat, das – außer der Wahrnehmbarkeit – alle Merkmale einer falschen Urkunde aufweist: Die auf dem Magnetstreifen enthaltenen Kontodaten verkörpern die Erklärung der ausstellenden Bank, der Karteninhaber sei zur Benutzung der Geldautomaten berechtigt. Der Datensatz ist auch geeignet und dazu bestimmt, für die Befugnis des Karteninhabers Beweis zu erbringen und als Aussteller ist in dem Datensatz die kartenausgebende Bank erkennbar, obwohl nicht diese, sondern der Täter die Daten auf das Blankett übertragen hat.[60] Regelmäßig wird zudem die Qualifikation des über § 269 Abs. 3 StGB anzuwendenden § 267 Abs. 4 StGB verwirklicht sein.[61]

3. Einsatz der Dubletten

a) Strafbarkeit nach § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 2 StGB

Der Einsatz der Dubletten zusammen mit den erspähten PINs zur Abhebung von Geldbeträgen ist nach § 152b Abs. 1 i.V.m. § 152a Abs. 1 Nr. 2 StGB in der Tatvariante des „Gebrauchens" strafbar. Bei den Dubletten handelt es sich um nachgemachte Zahlungskarten mit Garantiefunktion (s.o.). Gebrauchen meint die Verwendung der gefälschten Zahlungskarte im Zahlungsverkehr[62] und erfasst damit auch den Einsatz am Geldautomaten. Regelmäßig wird dabei der Qualifikationstatbestand des § 152b Abs. 2 StGB erfüllt sein.

[54] Die Tatbestandsmäßigkeit bejaht auch *Eisele*, CR 2011, 131 (134), der aber das Vorbereiten einer Straftat nach § 202a bzw. § 202b StGB ablehnt.

[55] *Seidl/Fuchs*, HRRS 2010, 85 (88).

[56] *Schumann*, NStZ 2007, 675 (676).

[57] Vgl. *Braun/Heidberg*, StrafRechtsReport 2010, 89 (92).

[58] St. Rspr., vgl. z.B. BGH, Urt. v. 27.1.2011 – 4 StR 338/10; explizit für Maestro-Karten vgl. BGH, Beschl. v. 13.10.2011 – 3 StR 239/11; *Fischer* (Fn. 21), § 152b Rn. 4 f.; a.A. *Heger*, wistra 2010, 281, der die Fälschung von Maestro-Karten mit gewichtigen Argumenten nur unter § 152a StGB subsumieren will. EC-Karten und Maestro-Karten sind beides Debitkarten unterschiedlicher Debitkartenanbieter (MasterCard International bei der Maestro-Karte und die Deutsche Kreditwirtschaft [DK], bis Mitte 2011 Zentraler Kreditausschuss [ZKA], bei der EC-Karte). EC steht dabei seit 2002 für electronic cash und nicht mehr für Eurocheque.

[59] Ausf. hierzu *Eisele*, CR 2011, 131 (134); *Fischer* (Fn. 21), § 152a Rn. 11; *Braun/Heidberg*, StrafRechtsReport 2010, 89 (92); a.A. *Sternberg-Lieben* (Fn. 53), § 152a Rn. 5.

[60] Vgl. *Meier*, JuS 1992, 1017 (1018); *Freund*, JuS 1994, 207 (209 f.).; *Weidemann* (Fn. 18), § 269 Rn. 9; *Hilgendorf*, JuS 1997, 130 (134).

[61] Auf Konkurrenzebene wird § 269 StGB jedoch von § 152b StGB verdrängt, vgl. *Erb* (Fn. 37), § 269 Rn. 41, und *Eisele*, CR 2011, 131 (134).

[62] *Erb* (Fn. 38), § 152a Rn. 11.

b) Strafbarkeit nach § 263a StGB

Durch die Verwendung der Kartendubletten wird zudem der Tatbestand des § 263a Abs. 1 StGB in der Begehungsform „unbefugte Verwendung von Daten“ verwirklicht.[63] Von dieser Variante ist neben der Verwendung einer im Wege verbotener Eigenmacht erlangten Originalkarte durch einen nichtberechtigten Dritten[64] auch die Verwendung von kopierten, gefälschten oder manipulierten Codekarten erfasst, und zwar unabhängig davon, ob die Herstellung bzw. Manipulation durch den Täter selbst oder durch einen Dritten erfolgt ist.[65] Durch die Tathandlung kommt es auch zu einer Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs.[66] Eine Beeinflussung des Ergebnisses liegt vor, wenn das Ergebnis des Datenverarbeitungsvorgangs ohne die Manipulationshandlung entweder anders hätte lauten müssen oder überhaupt nicht hätte ergehen dürfen. Das Ergebnis kann also bereits inhaltlich unzutreffend oder zwar an sich richtig, aber unbefugterweise herbeigeführt sein.[67] Zudem muss die Manipulationshandlung für das Ergebnis zumindest mitursächlich sein und das Ergebnis hat unmittelbar zu einer Vermögensminderung zu führen.[68] Letzteres ist der Fall, wenn die Vermögensminderung ohne weitere wesentliche Zwischenschritte einer natürlichen Person herbeigeführt wird.[69] Die genannten Voraussetzungen sind bei der Verwendung der Dubletten zur Geldabhebung sämtlich erfüllt: Das Ergebnis des im Geldautomaten ablaufenden Datenverarbeitungsvorgangs ist zwar inhaltlich richtig, wurde vom Skimming-Täter aber unbefugterweise herbeigeführt. Die Verwendung der Dubletten – mithin die Manipulationshandlung – ist zudem mitursächlich für dieses Ergebnis, welches sich schließlich in Form der automatisch erfolgenden Geldausgabe auch unmittelbar vermögensmindernd auswirkt.

Problematisch gestaltet sich die Antwort auf die Frage, bei wem der Vermögensschaden eintritt.[70] Die Abhebung des Geldbetrages durch den Skimming-Täter erfolgt – weil ohne bzw. gegen den Willen des Kontoinhabers – ohne dessen Autorisierung i.S.d. § 675j Abs. 1 S. 1, 4 BGB, sodass ihm gem. § 675u S. 2 BGB grundsätzlich ein Anspruch gegen die Bank auf Erstattung des Zahlungsbetrages zusteht. Zu beachten ist jedoch die Regelung des § 675v Abs. 1 und Abs. 2 BGB, wonach die Bank wiederum einen Schadensersatzanspruch gegen den Kontoinhaber hat, wenn der infolge eines nicht autorisierten Zahlungsvorgangs entstandene Schaden aufgrund der missbräuchlichen Verwendung eines Zahlungsauthentifizierungsinstruments entstanden ist und der Kontoinhaber die personalisierten Sicherheitsmerkmale (insbes. die PIN) nicht sicher aufbewahrt hat (§ 675v Abs. 1 S. 2 BGB) oder der Schaden von Letzterem durch grob fahrlässige Verletzung von Pflichten aus § 675l BGB oder von vereinbarten Bedingungen für die Ausgabe und Nutzung von Codekarte und PIN herbeigeführt wurde (§ 675v Abs. 2 Nr. 1 und 2 BGB).[71] Im Falle des § 675v Abs. 1 S. 2 BGB ist der vom Kontoinhaber zu ersetzende Schaden dabei höhenmäßig auf maximal 150 Euro begrenzt und der Anspruch der Bank besteht nach h.M. nur bei Vorliegen eines Verschuldens.[72] Im Falle des § 675v Abs. 2 BGB haftet der Kontoinhaber dagegen unbegrenzt.

In dem Moment, in dem beim Skimming die PIN des Bankkunden vom Skimming-Täter ausgespäht wird, wird diese von Ersterem, der von der am Geldautomaten vorgenommenen Manipulation nichts ahnt, ordnungsgemäß verwendet. Davon, dass er die PIN zu diesem Zeitpunkt „nicht sicher aufbewahrt“, kann daher nicht die Rede sein, sodass eine (begrenzte) Haftung des Bankkunden nach § 675v Abs. 1 S. 2 BGB also nicht in Betracht kommen dürfte. Auch die (unbegrenzte) Haftung nach § 675v Abs. 2 Nr. 1 und 2 BGB scheidet aus: Nach § 675l S. 1 BGB ist der Bankkunde nur dazu verpflichtet, alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Zumutbar sind dabei nur solche Vorkehrungen, die die Nutzung des Zahlungsauthentifizierungsinstruments nicht derart einschränken, dass es seine praktische Brauchbarkeit für die mit ihm bezweckten Einsatzmöglichkeiten verliert. Das Gebot, bei der PIN-Eingabe

[63] Zum Meinungsstreit bzgl. des Merkmals „unbefugt“ vgl. ausf. *Eisele*, CR 2011, 131 (135).

[64] BGHSt 47, 160 (162).

[65] BGHSt 38, 120 (123); 47, 160 (162); *Wohlers* (Fn. 26), § 263a Rn. 27 subsumiert diesen Fall dagegen unter „Verwendung unrichtiger oder unvollständiger Daten“ (Var. 2), *Ranft* (wistra 1987, 78 [84]) unter „unrichtige Programmgestaltung“ (Var. 1).

[66] BGHSt 38, 120 (124). Ob die Einleitung eines Datenverarbeitungsvorgangs schon für sich gesehen als Beeinflussung des Ergebnisses eingestuft werden kann, ist umstritten, richtigerweise aber zu bejahen, da mit dem Auslösen eines Prozesses auf diesen schließlich sogar besonders intensiv Einfluss genommen wird, vgl. BGHSt 38, 120 (121); OLG Köln, Urt. v. 9.7.1991 – Ss 624/90; *Berghaus*, JuS 1990, 981; *Lackner/Kühl* (Fn. 33), § 263a Rn. 22; *Cramer/Perron*, in: Schönke/Schröder (Fn. 14), § 263a Rn. 18; *Fischer* (Fn. 21), § 263a Rn. 20.

[67] BGHSt 38, 120 (124).

[68] *Beckemper*, in: von Heintschel-Heinegg (Fn. 18), § 263a Rn. 37.

[69] *Beckemper* (Fn. 68), § 263a Rn. 39.

[70] Vgl. zur ähnlichen Problematik beim sog. Phishing *Seidl/Fuchs*, HRRS 2010, 85 (88 f.).

[71] Nach § 675l BGB ist der Kontoinhaber dazu „verpflichtet, unmittelbar nach Erhalt eines Zahlungsauthentifizierungsinstruments alle zumutbaren Vorkehrungen zu treffen, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen“ (S. 1) sowie „dem Zahlungsdienstleister […] den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Zahlungsauthentifizierungsinstruments unverzüglich anzuzeigen, nachdem er hiervon Kenntnis erlangt hat“ (S. 2).

[72] *Palandt*, Bürgerliches Gesetzbuch, Kommentar, 71. Aufl. 2012, § 675v Rn. 3; so auch die Gesetzesbegründung BT-Drs. 16/11643, S. 113, die von einem Verschuldenselement spricht.

am Geldautomaten stets die Tastatur abzudecken, um ein mögliches Ausspähen zu verhindern, stellt aber gerade eine solche einschränkende und damit unzumutbare Vorkehrung dar.[73] Kommt es also zu einem Ausspähen der PIN, weil der Skimming-Täter oder die von ihm installierte Kamera mangels Verdecken der Geldautomatentastatur „freie Sicht" auf das Eingabefeld hatte, so ist der Schaden nicht auf eine Pflichtverletzung des Bankkunden zurückzuführen, dessen Haftung nach § 675v Abs. 2 Nr. 1 BGB scheidet mithin aus. Dies gilt erst recht in den Fällen, in denen das Ausspähen mittels einer Tastaturattrappe erfolgt, weil hier ein Verdecken bei der PIN-Eingabe ohnehin zwecklos ist. Daneben dürfte eine Haftung nach § 675v Abs. 2 BGB zudem an fehlender grober Fahrlässigkeit des Bankkunden scheitern: Wie eingangs bereits erwähnt, ist es für einen Laien nahezu unmöglich, von Skimming-Tätern an Geldautomaten vorgenommene Manipulationen zu erkennen. Davon, dass ein argloser Bankkunde bei der Geldabhebung daher die im Verkehr erforderliche Sorgfalt in einem ungewöhnlich hohen Maß verletzt, kann im Regelfall also nicht die Rede sein. Eine Haftung des Kunden kommt folglich regelmäßig nicht in Betracht, sodass der Vermögensschaden aufgrund der Rückerstattungspflicht aus § 675u S. 2 BGB bei der Bank eintritt.[74]

In der Regel wird auch der Qualifikationstatbestand des über § 263a Abs. 2 StGB anwendbaren § 263 Abs. 5 StGB erfüllt sein.

c) Strafbarkeit nach § 269 StGB

Der Skimming-Täter macht sich durch die Benutzung der Dubletten zudem wegen Fälschung beweiserheblicher Daten nach § 269 Abs. 1 StGB in der Begehungsform des „Gebrauchens" strafbar,[75] wobei auch hier die Qualifikation des über § 269 Abs. 3 StGB anzuwendenden § 267 Abs. 4 StGB regelmäßig erfüllt sein dürfte.[76]

d) Strafbarkeit nach § 202a Abs. 1 StGB

Schließlich ist auch der Tatbestand des § 202a Abs. 1 StGB erfüllt. Mithilfe der zuvor erspähten PIN sowie der angefertigten Kartendubletten ist es dem Täter möglich, am Geldautomaten den Kontostand des jeweiligen Kontoinhabers einzusehen.[77] Darin ist ein Sichverschaffen des Zugangs zu nicht für den Täter bestimmten sowie gegen unberechtigten Zugang besonders gesicherten Daten zu sehen, das unter Überwindung einer Zugangssicherung erfolgt.[78]

4. Strafbarkeit der Herstellung bzw. des Verschaffens der Skimming-Ausrüstung

a) Strafbarkeit des Sichverschaffens bzw. der Herstellung des Magnetstreifenlesers nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB

Für das Skimming greifen die Täter auf legal erhältliche,[79] vorgefertigte Magnetstreifen(-durchzugs- oder -einsteck-)lesegeräte aus dem Handel zurück, die sie vor ihrer Verwendung bearbeiten und verändern. Erforderlich ist neben dem Einbau der Geräte in spezielle (zur Tarnung benötigte) Gehäuse die Erweiterung um eine Batterie als Stromquelle für den mobilen Einsatz sowie das Hinzufügen eines Speicher- oder Sendemoduls, um ein Zwischenspeichern bzw. das Versenden der ausgelesenen Magnetstreifeninformationen zu ermöglichen.[80] Durch die Vornahme dieser Manipulationen wird der Tatbestand des § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB in der Begehungsform des Herstellens einer „ähnlichen Vorrichtung" verwirklicht. Die veränderten Kartenlesegeräte erfüllen bei der Herstellung unechter Zahlungskarten mit Garantiefunktion die gleiche Funktion wie Platten, Formen, Druckstöcke etc. für die Herstellung von falschem Geld.[81] Nach Vornahme der genannten Manipulationen wohnt ihnen darüber hinaus auch eine spezifische Eignung zur deliktischen Verwendung inne. Gleichwohl wurde ihre Subsumtion unter § 149 Abs. 1 Nr. 1 StGB früher abgelehnt. Begründet wurde dies damit, dass durch sie die Herstellung von Falsifikaten nicht „unmittelbar ins Werk gesetzt" wird.[82] Das Kriterium der Eignung zur unmittelbaren Herstellung der Falsifikate ist jedoch auf die traditionellen Herstellungsverfahren mit Druckplatten o.Ä. zugeschnitten und bezieht dort seine Berechtigung daraus, dass diese Gegenstände typischerweise erst auf einer sehr späten Stufe des Produktionsprozesses ihre spezifische Tauglichkeit für Fälschungen erlangen.[83] Bei den von den Tätern hergestellten „Skimmern" ist dies jedoch gerade nicht der Fall, da bereits das auf einer frühen Stufe angesiedelte Auslesen der Magnetstreifen zu den hochspeziellen Fälschungsfunktionen gehört.[84] Aus diesem Grunde sind sie unter § 149 Abs. 1 Nr. 1 StGB zu subsumieren, eine Strafbarkeit ist mithin zu bejahen.[85]

---

[73] *Palandt* (Fn. 72), § 675l Rn. 2.

[74] Vgl. auch *Eisele*, CR 2011, 131 (136).

[75] *Hoyer* (Fn. 35), § 269 Rn. 16; vgl. auch *Eisele*, CR 2011, 131 (134), der weniger auf die Daten der Dublette als vielmehr auf die Eingabe der PIN abstellt.

[76] Auf Konkurrenzebene dürfte § 269 StGB jedoch von § 152b StGB verdrängt werden, vgl. *Erb* (Fn. 37), § 269 Rn. 41.

[77] So auch *Bachmann/Goeck*, JR 2011, 425 (426).

[78] S.o. unter II. 1. b) bb); vgl. auch *Tyszkiewicz*, HRRS 2010, 207 (212); a.A. *Eisele*, CR 2011, 131 (136).

[79] A.A. *Puppe* (Fn. 43), § 149 Rn. 7: Legal verfügbare Lesegeräte, die auch von Händlern im Rahmen des POS- oder POZ-Verfahrens eingesetzt werden, seien zum „skimmen" nicht geeignet, da sie vom Zentralausschuss für das Kreditwesen (ZAK) auf Sicherheit hin geprüft würden und autorisiert seien. Bei den von den Skimming-Tätern verwendeten Geräten müsse es sich deshalb um „illegal" erworbene handeln. Dabei wird jedoch verkannt, dass es sich bei den beim Skimming zum Einsatz kommenden Gerätschaften um einfache Durchzugsleser für Magnetstreifen handelt, die in jedem Elektronikfachversand frei erhältlich sind.

[80] *Eckart/Guggenbühl/Pfefferli/Fluri*, Kriminalistik 2003, 547 (551); *Braun/Heidberg*, StrafRechtsReport 2010, 89 (90).

[81] *Puppe* (Fn. 43), § 149 Rn. 7.

[82] BGH, Urt. v. 16.12.2003 – 1 StR 297/03; *Husemann*, NJW 2004, 104 (109).

[83] *Stein* (Fn. 43), § 149 Rn. 2.

[84] *Stein* (Fn. 43), § 149 Rn. 2.

[85] Vgl. *Fischer* (Fn. 21), § 149 Rn. 3; *Puppe* (Fn. 43), § 149 Rn. 7 f.; *Stein* (Fn. 43), § 149 Rn. 2; a.A. *Eisele*, CR 2011,

b) Strafbarkeit des Sichverschaffens des Schreib-/Codiergeräts samt Software

aa) Strafbarkeit nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB

Wie die Lesegeräte sind auch die Schreibgeräte, mit denen die Dubletten beschrieben werden, frei im Handel verfügbar.[86] Damit fehlt auch ihnen grundsätzlich die spezifisch deliktische Eignung, da sie gleichermaßen für legale Zwecke eingesetzt werden können. Im Unterschied zu den Lesegeräten werden die Codiergeräte auch nicht weiterverarbeitet oder irgendwo eingebaut, sie behalten also ihr ursprüngliches Aussehen und erlangen somit auch nicht auf diese Art die erforderliche ausschließlich deliktische Verwendbarkeit. Damit scheidet hinsichtlich der Magnetstreifencodiergeräte eine Strafbarkeit nach § 152b Abs. 5 i.V.m. § 149 Abs. 1 Nr. 1 StGB aus.

bb) Strafbarkeit nach § 202c Abs. 1 Nr. 2 i.V.m. § 202a Abs. 1 StGB

Auch eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 i.V.m. § 202a Abs. 1 StGB in der Form des Sichverschaffens eines Computerprogramms, dessen Zweck die Begehung einer Tat nach § 202a Abs. 1 StGB ist, scheidet aus. Durch die spätere Benutzung der mithilfe des Codiergeräts hergestellten Kartendubletten wird zwar der Tatbestand des § 202a Abs. 1 StGB verwirklicht.[87] Bei der in Kombination mit dem Codiergerät zum Beschreiben der Magnetstreifen der Dubletten verwendeten Software handelt es sich zudem um ein Computerprogramm, welches sich die Täter im Zuge des Erwerbs des Geräts verschafft haben. Eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB setzt aber auch voraus, dass das Computerprogramm mit der Absicht entwickelt oder modifiziert wurde, es zur Begehung der genannten Straftaten einzusetzen und dass sich diese Absicht auch objektiv manifestiert hat.[88] Die bloße Eignung zur Straftatenbegehung reicht dagegen nicht aus. Bei der in Kombination mit dem Magnetstreifencodierer zu verwendenden Software fehlt es jedoch gerade an der erforderlichen deliktischen Zweckbestimmung.

cc) Strafbarkeit nach § 263a Abs. 3 StGB

Eine Strafbarkeit nach § 263a Abs. 3 StGB scheitert bereits an der hierfür erforderlichen deliktischen Zweckbestimmung, an der es der verwendeten Software fehlt.

5. Strafbarkeit nach § 261 Abs. 2 Nr. 1, Abs. 1 S. 2 Nr. 4 lit. a StGB durch Verteilung der Beute

Das Verteilen der Beute erfüllt den Tatbestand der Geldwäsche nach § 261 Abs. 2 Nr. 1, Abs. 1 S. 2 Nr. 4 lit. a StGB, weil sich die Täter Gegenstände verschaffen, die aus der Katalogtat des § 263a StGB herrühren und diese auch gewerbsmäßig bzw. von einem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, begangen worden ist. Allerdings ist § 261 Abs. 9 S. 2 StGB zu beachten, wonach eine Bestrafung von Personen ausscheidet, die wegen Beteiligung an der Vortat strafbar sind. Dieser persönliche Strafausschließungsgrund wird regelmäßig bei allen Bandenmitgliedern, bei denen – wie bereits erwähnt – grundsätzlich Mittäterschaft anzunehmen ist, einschlägig sein.

III. Zusammenfassung und Ausblick

Die Strafbarkeit der Skimming-Täter ist abhängig vom jeweiligen Tatfortschritt. Das Verhältnis mehrerer verwirklichter Tatbestände zueinander ist auf Konkurrenzebene zu entscheiden.[89] Die Rechtsprechung zu den typischen Fallkonstellationen beim Skimming hat sich mittlerweile durch mehrere höchstrichterliche Entscheidungen gefestigt.[90] So werden die Angeklagten bei Tatvollendung in der Regel wegen gewerbs- und bandenmäßiger Fälschung von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbs- und bandesmäßigem Computerbetrug verurteilt.[91] Auch die Fälle, in denen die Täter bei der Tatausführung gestört werden, z.B. wenn die Manipulationen am Geldautomaten entdeckt werden, und die Tatvollendung in der Folge durch Sicherstellung der Skimming-Anbauten durch die Polizei verhindert wird, und die damit zusammenhängende Problematik des unmittelbaren Ansetzens zur Fälschung von Zahlungskarten mit Garantiefunktion sind nunmehr weitgehend höchstrichterlich geklärt.

Spannend bleibt aber, wie es zukünftig im Kampf gegen die Skimming-Kriminalität weitergehen wird. Obwohl die seit 2011 verbindliche Einführung der EMV-Chip-Technologie[92] in den SEPA-Staaten zur Bekämpfung der Skimming-Kriminalität augenscheinlich erfolgreich ist – die Angriffe auf Geldautomaten sind im ersten Halbjahr 2011 im Vergleich zum Vorjahr um 60 %, insgesamt im Jahr 2011 um rund 50 % zurückgegangen –, dürfte der Kampf noch nicht endgültig gewonnen sein.

Es ist zu befürchten, dass die rückläufigen Zahlen auf eine Phase der Umorganisation der kriminellen Banden zurückzuführen sind, die in den neuen Absatzstaaten, in denen sie weiterhin die manipulierten Zahlungskarten zum Geldabheben verwenden können, erst die erforderlichen Strukturen aufbauen müssen.[93] Nach diesem Stadium der Neuausrichtung

131 (134). Eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB scheidet entgegen der Ansicht von *Braun/Heidberg*, StrafRechtsReport 2010, 89 (91), mangels Strafbarkeit des Auslesens der Magnetstreifeninformationen nach § 202a StGB dagegen grundsätzlich aus.

[86] A.A. *Puppe* (Fn. 43), § 149 Rn. 7.

[87] S.o. unter II. 3. d).

[88] BVerfG, Beschl. v. 18.5.2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08 = ZUM 2009, 745 (749).

[89] Vgl. zu den Konkurrenzen beim Skimming *Bachmann/Goeck*, JR 2011, 425 (426 f.).

[90] Vgl. insbes. BGH, Beschl. v. 6.7.2010 – 4 StR 555/09.

[91] Vgl. z.B. BGH, Urt. v. 27.1.2011 – 4 StR 338/10.

[92] Vgl. hierzu *Seidl/Fuchs*, HRRS 2011, 265 (274).

[93] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.

dürften ähnlich hohe Angriffszahlen zu erwarten sein wie bisher.[94]

Dies ist vor allem deshalb der Fall, weil eine Umsetzung des EMV-Standards in diversen außereuropäischen Staaten – wie beispielsweise den USA – nicht geplant ist und sich daher auch auf neu ausgegebenen Karten wieder ein Magnetstreifen befinden wird, um die internationale Einsatzfähigkeit dieser Karten zu sichern.[95] An den EMV-kompatiblen Geldautomaten der SEPA-Staaten werden zwar nur noch die EMV-Chips ausgelesen, die auf dem Magnetstreifen gespeicherten Daten können aber nach wie vor kopiert werden. Ein Abheben mittels Kartendubletten ist innerhalb Europas somit zwar nicht mehr möglich, weil Karten ohne Chip von den Terminals als Fälschung entlarvt werden. Zu einem Versiegen der Skimming-Kriminalität wird dies jedoch nicht führen. Ohne flankierende Maßnahmen werden die Täter lediglich die Verwertung der erlangten Kartendubletten in Nicht-Chip-Länder verlagern, in denen mangels Einsatzes EMV-kompatibler Geldautomaten weiterhin Abhebungen mit Kartendubletten vorgenommen werden können.[96]

Wünschenswert wären also die weltweite Einführung des EMV-Standards und die damit einhergehende Abschaffung der Magnetstreifen. Denkbar wäre aber auch eine „europäische Lösung", wonach die Karten innerhalb Europas nur noch mit EMV-Chips versehen werden, im außereuropäischen Raum dagegen eine zweite, mit Magnetstreifen ausgestattete Karte zum Einsatz kommt.[97]

Am praktikabelsten erscheint jedoch das sog. „Magstripe-Controlling", gemeint sind damit Mechanismen, die eine bewusste Kontrolle von Magnetstreifenumsätzen ermöglichen.[98] Dieses „Magstripe-Controlling" beinhaltet z.B. Maßnahmen wie die Festlegung von Limits für Auslandsabhebungen, die unverzügliche Benachrichtigung von Kunden per SMS bei erfolgten Auslandstransaktionen oder die grundsätzliche Deaktivierung der Karte für den Einsatz in Nicht-SEPA-Staaten.[99] Möchten die Kunden ihre Zahlungskarte dann aber in diesen Ländern einsetzen, müssen sie zuvor den Magnetstreifen ihrer Karte bei ihrer Bank „aktivieren" lassen – ein im Vergleich zum Skimming-Risiko verschmerzbar geringer Aufwand.[100]

---

[94] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.
[95] *Seidl/Fuchs*, HRRS 2011, 265 (274).
[96] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.
[97] *Seidl/Fuchs*, HRRS 2011, 265 (274).
[98] Vgl. hierzu BKA, Gemeinsame Pressekonferenz der EURO Kartensysteme GmbH und des Präsidenten des Bundeskriminalamtes: Aktuelle Zahlen zur Zahlungskartenkriminalität 2010 in Deutschland, S. 4 f., im Internet abrufbar unter: http://www.bka.de/nn_233110/SharedDocs/Downloads/DE/Presse/Pressearchiv/Presse__2011/pm110510__ZahlungskartenkriminalitaetBundeslagebild,templateId=raw,property=publicationFile.pdf/pm110510_ZahlungskartenkriminalitaetBundeslagebild.pdf (16.8.2012).
[99] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.
[100] *Seidl*, jurisAZO-ITR 19/2011 Anm. 2.