Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 11. Jahrgang, Heft 3, September 2011

Schwerpunkt:

Reputation im Internet

Skimming

Tatphasen und Haftung

Dieter Kochheim

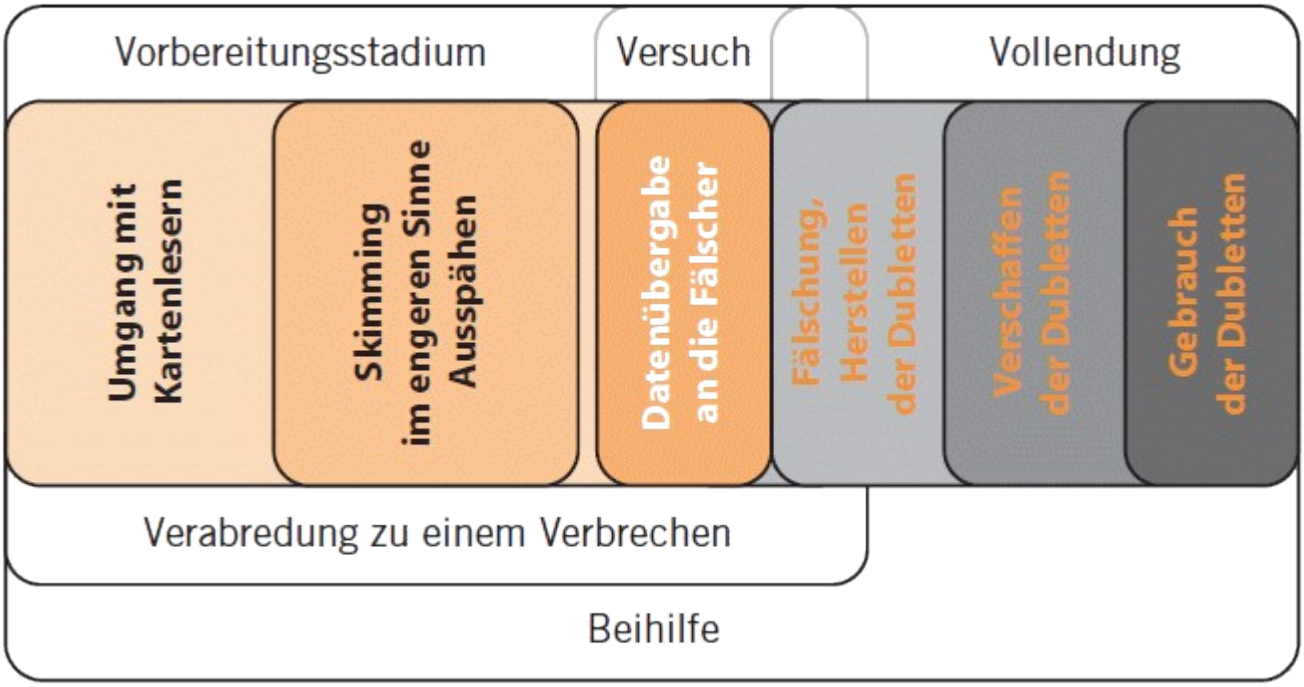
überarbeitete und mit Hyperlinks versehene Version:
#1.01, 25.10.2011

Im September 2011 erschien mein Aufsatz über das Skimming – Tatphasen und Haftung – in der Zeitschrift für Datenrecht und Informationssicherheit, die der Datenschutzbeauftragte des Kantons Basel-Stadt herausgibt.

Ich danke auch an dieser Stelle für die Gelegenheit zur Veröffentlichung.

Der folgende Text ist eine überarbeitete Fassung, in der die Verweise auf die Quellen und zu den Gesetzestexten mit Hyperlinks unterlegt sind.

Dieter Kochheim, 26.10.2011



Das Tatphasenmodell und die ursprüngliche Grafik stammen von mir. Für die Ausgabe bei digma wurde es hervorragend verfeinert. Vielen Dank dafür!

Das Modell stellt die Versuchs- und Vorbereitungsstadien dar, die beim Skimming zu betrachten sind. Nach der Rechtsprechung des BGH kommt dem Versuchsstadium eine ganz besondere Bedeutung zu. Selbst „unabhängige“ Ausspäher, die sich nicht einer Cashing-Bande angeschlossen haben, können als deren Mittäter im Versuchsstadium handeln.


report

Recht

Skimming – Tatphasen und Haftung

Skimming – Tatphasen und Haftung

Von Dieter Kochheim [1]

Unter dem Begriff „Skimming fassen wir eine mehraktige kriminelle Erscheinungsform zusammen, deren strafrechtlicher Schwerpunkt im Fälschen von Zahlungskarten mit Garantiefunktion im Sinne des Verbrechenstatbestandes des § 152b StGB liegt.

Überwiegend sind arbeitsteilige Tätergruppen im Einsatz, die zunächst in Deutschland in Bankfilialen [2] mit Kartenlesegeräten (Skimmer) die Magnetstreifen von Bankkarten [3] auslesen und gleichzeitig die Tastatureingaben der Bankkunden mit geschickt platzierten Kameras oder mit Tastaturaufsätzen beobachten („abgreifen“). Erfahrungsgemäß stehen die „Abgreifer“ im engen Kontakt zu ihren Tatgenossen im Ausland, denen sie die abgegriffenen Daten per E-Mail übermitteln und die das Fälschen besorgen. Überwiegend werden dazu die ausgespähten Magnetstreifendaten auf einfache Rohlinge (WhiteCards) kopiert, die nur aus einer unbedruckten Identitätskarte mit einem Magnetstreifen bestehen [4].

Skimming als Fälschungsdelikt

Der Grundtatbestand des § 152a StGB hat zwei selbständige Fallgruppen, womit das Fälschen der optischen Sicherheitsmerkmale einer Zahlungskarte alternativ dem Fälschen ihrer digitalen Sicherungen gegenüber gestellt werden [5] („oder“). Zu den optischen Merkmalen gehören unter anderem das Druckbild, das Hologramm, das Logo des Zahlungsverbundes, die individuellen Angaben zum Karteninhaber, die Angaben zur Bank und zum Konto, das Unterschriftsfeld mit der Unterschrift und die Prüfziffern. Die digitalen Sicherheitsmerkmale sind vor allem die Persönliche Identfikationsnummer – PIN, die auf dem Magnetstreifen und dem EMV-Chip gespeicherten Daten [6], die verschlüsselten Prüfziffern für die PIN sowie das Modulierte Merkmal – MM [7], das eine Besonderheit bei den von deutschen Banken herausgegebenen Karten ist.

Der erstrebte Taterfolg besteht im erfolgreichen

---

1 Dieter Kochheim ist als Oberstaatsanwalt in Hannover tätig. Dieser Aufsatz fasst die Ergebnisse aus seinem Arbeitspapier Skimming zusammen (Stand: 22.04.2011), siehe: Cyberfahnder.de.

2 Auch andere Terminals für den bargeldlosen Zahlungsverkehr werden angegriffen, zum Beispiel Point of Sale-Handgeräte (PoS-Terminal) im Einzelhandel, Tankstellenautomaten (Castrop Rauxel) und Fahrkartenautomaten.
Siehe auch: CF, Skimming an Fahrkartenautomaten, 23.10.2011

3 Gemeint sind Kredit- und Debitkarten, die von einer Bank herausgegeben und im Zahlungsverkehr von Dritten Erfüllungs halber akzeptiert werden. Mit „Banken“ sind die in § 1 Abs. 1, Abs. 1a Kreditwesengesetz definierten Unternehmen gemeint.

4 Meine Erfahrungen decken sich mit der ausgiebigen und instruktiven Sachverhaltsschilderung bei BGH, Urteil vom 17.02.2011 – 3 StR 419/10.

5 BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn. 11

6 Siehe kartensicherheit.de, EMV-Chip. Das Abgreifen der Daten ist kein Ausspähen im Sinne von § 202a Abs. 1 StGB: BGH, Beschluss vom 18.03.2010 - 4 StR 555/09.

7 Siehe kartensicherheit.de, MM-Merkmal - das Sicherheitsmerkmal in deutschen ec-Karten.

Dazu werden Merkmalstoffe in den Kartenkörper eingebettet, die eine Codierung zulassen. Diese wird von den Geldausgabeautomaten – GAA – in inländischen Banken gegen eine codierte Prüfziffer geprüft, die ebenfalls auf dem Magnetstreifen und dem EMV-Chip gespeichert ist. Das MM führt dazu, dass White Cards mit Daten von deutschen Zahlungskarten nur im Ausland eingesetzt werden können, wo es nicht geprüft wird.

Gebrauchen der Falsifikate an ausländischen GAA. Zu diesem „Cashing“ benötigen die Täter die ausgespähten PIN. Je Datensatz erzielen sie im Erfolgsfall durchschnittlich rund 2.350 Euro [8]. Nach ungesicherten Schätzungen sind 2009 durch das Cashing in Deutschland Schäden in Höhe von rund 40 Mio. Euro entstanden, die sich 2010 auf etwa 60 Mio. Euro erhöht haben sollen.

Autorisierung und Garantiefunktion

Eine Garantiefunktion besteht dann, wenn in einem Dreiecksverhältnis die Karten ausgebende Bank (Bezogene) gegen Vorlage der Zahlungskarte eine Zahlungszusage gibt [9]. Sie muss nicht bedingungslos und unbegrenzt sein, sondern darf auch interne Verfügungsrahmen (Guthaben, Überziehungskredit, Tages-/Wochenlimit) oder sonstige Beschränkungen voraussetzen (keine Auslandsverfügungen). Die Zahlungszusage, die sich ursprünglich im Euroscheck verkörperte [10], ist vom Autorisierungsverfahren abgelöst worden. Dabei werden die am fremden (ausländischen) Terminal eingegebenen Transaktionsdaten (Kartendaten, PIN, Zahlungsbetrag, Gebühren, Terminalkennung, Zeitstempel) im Onlineverfahren bis zum Rechenzentrum der Karten ausgebenden Bank übermittelt und anhand des Verfügungsrahmens und den vorgegebenen Beschränkungen geprüft. Darauf erfolgt eine ausdrückliche Genehmigung durch die Übermittlung des Genehmigungscodes „0“ [11]. Darin verkörpert sich die vom Kartenverbund geforderte Zusage der bezogenen Bank, diese Verfügung im Einzelfall zu bedienen. Wegen des Fälschungstatbestandes kommt es nur darauf an, ob die Originalkarte zu garantierten Zahlungen verwendet werden kann, nicht auch darauf, ob die Fälschung zu einer garantierten Zahlung missbraucht wird [12].

Das Autorisierungsverfahren ist für Kredit- und Debitkarten dasselbe. Sie sind ebenso Zahlungskarten im Sinne von § 152a StGB wie andere Identitätskarten mit Handelsfunktionen, wenn von einem Finanzdienstleistungsverband geldwerte Verrechnungen gewährt werden [13].

Cashing

Das Cashing als finales Ziel der Täter ist strafrechtlich als der Gebrauch von gefälschten Zahlungskarten mit Garantiefunktion (§ 152b Abs. 1 StGB [14]) in Tateinheit mit Computerbetrug (§ 263a StGB) zu bewerten [15], wobei der Betrugsschaden im Rahmen der Autorisierung beim bargeldlosen Zahlungsverkehr beim Bankkunden [16] (Debitkarten) oder bei der Karten ausgebenden Bank (Kreditkarten), also im Inland eintritt (Erfolgsort, § 9 Abs. 1 StGB). Das Fälschungsdelikt unterliegt dem Weltrechtsprinzip (§ 6 Nr. 7 StGB), so dass auch reine Auslandstaten in Deutschland strafbar

---

8 Schätzung auf der Grundlage der Fallzahlen der Polizeilichen Kriminalstatistik für 2009 und den Zahlen von der Deutschen Bundesbank; siehe: Kochheim, Skimming. Code 0, Mai 2011, S. 5.

9 Schon zum Kredit- und Scheckkartenmissbrauch gemäß § 266b StGB: BGH, Urteil vom 12.05.1992 - 1 StR 133/92, Rn. 9.

10 Der papierförmige, bis 2002 verwendete EC verkörperte eine Zahlungsgarantie der ausstellenden Bank bis zu 400 DM.

11 Siehe kartensicherheit.de, Genehmigungsnummer | Authorisation Code: *Die Genehmigungsnummer wird infolge einer Autorisierungsanfrage von der Karten ausgebenden Bank (Issuer) vergeben und wiederum von dem Acquirer an den Händler bestätigt. Ohne diese Genehmigungsnummer hat der Händler für die Transaktion keine Zahlungsgarantie.*

12 Die EC-Karte hat auch dann eine Garantiefunktion, wenn sie im Lastschriftverfahren eingesetzt wird: BGH, Urteil vom 21.09.2000 - 4 StR 284/00.

13 Auch Tankkarten oder solche von Bonussystemen können Zahlungskarten mit Garantiefunktionen sein, wenn der Finanzdienstleister in einem Verbund selbständiger Unternehmen die Verrechnung abwickelt und garantiert.

14 Als Urkundsdelikt tritt die Fälschung beweiserheblicher Daten gemäß § 269 StGB hinter der spezielleren Vorschrift des § 152a Abs. 1 Nr. 1 StGB zurück; Arg. aus: BGH, Beschluss vom 26.01.2005 - 2 StR 516/04.

15 Ständige Rechtsprechung seit BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 17 (Betrug); zuletzt BGH, Beschluss vom 23.06.2010 – 2 StR 243/10, Rn 3 (Tateinheit, deliktische Einheit).

16 Die Stoffgleichheit (siehe jüngst: BGH, Beschluss vom 07.12.2010 - 3 StR 433/10, Rn 10), zeigt sich zunächst in der Verringerung des Verfügungsrahmens des Karteninhabers und schließlich in der Kontobelastung.

sind. In Bezug auf den „Gebrauch“ wird die Tat durch den Einsatz der WhiteCard und der Eingabe der PIN vollendet und das auch dann, wenn die Auszahlung fehl schlägt. Diese vollendete „Fälschung“ (hier: Gebrauch) erfolgt im Versuchsstadium des gleichzeitigen Computerbetruges (unbefugte Nutzung der Kartendaten und PIN), der seinerseits durch die erfolgreiche Auszahlung vollendet wird.

Sowohl das „Abgreifen“ verschiedener Karten- und Zugangsdaten, die Fälschung einer Serie von White Cards und ihr serienmäßiger Einsatz beim Cashing stehen in aller Regel in einem engen räumlichen und zeitlichen Zusammenhang, so dass sie grundsätzlich eine deliktische Einheit bilden (Tateinheit im Sinne von § 52 StGB [17]). Mehrere materielle Taten sind jedoch dann anzunehmen, wenn das Fälschen oder das Cashing in mehreren, deutlich unterbrochenen Tranchen erfolgt, also zu ihrer Fortsetzung ein neuer Willensentschluss erforderlich wird.

Bei arbeitsteiligen Tätergruppen kann man in aller Regel von gewerbsmäßigem Handeln ausgehen, so dass allein wegen des Fälschungsverbrechens eine Freiheitsstrafe von mindestens 2 Jahren droht (§ 152b Abs. 2 StGB), die selbst im Einzelfall bis zur gesetzlichen Höchststrafe von 15 Jahren Freiheitsstrafe reicht (§ 38 Abs. 2 StGB [18]). Dasselbe gilt, wenn sich die arbeitsteiligen Täter zu einer Bande zusammen gefunden haben.

Abgreifen der Kundendaten

Das Abgreifen der Bankkundendaten, also das Skimming im engeren Sinne, ist im Vorbereitungsstadium des Fälschungs- und Betrugsdelikts angesiedelt [19]. Der Versuch der Fälschung beginnt grundsätzlich erst mit der Fälschungshandlung selber [20]. Bei arbeitsteiligen Tätergruppen kann sich der Versuchsbeginn zeitlich vorverlagern. Der BGH erkennt jetzt an, dass die Übermittlung der abgegriffenen Daten an die fälschungswilligen und -bereiten Casher den Versuch auch dann einleitet, wenn die Daten erst noch mit den ausgespähten Tastatureingaben synchronisiert werden müssen [21]. Das führt dazu, dass sich die „Abgreifer“ nicht nur an einer Verbrechensabrede (§ 30 Abs. 2 StGB) beteiligen können, die mit dem Versuch des Fälschens beendet wird, und sich auch nicht nur als Mittäter (§ 25 Abs. 2 StGB) die weiteren Tathandlungen ihrer Komplizen als vollendetes Tatunrecht zurechnen lassen müssen, sondern ungeachtet derer Handlungen eigenhändig den Versuch des Fälschens beginnen.

Der BGH sieht die „Abgreifer“ in arbeitsteiligen Tätergruppen aufgrund ihrer wesentlichen und anspruchsvollen Tatbeiträge grundsätzlich als Mittäter und nicht nur als Gehilfen zu den späteren Fälschungs- und Cashinghandlungen an [22]. Das ist die logische Konsequenz aus den Besonderheiten des Skimmings [23]:

Der Große Senat für Strafsachen hat 2001 davon Abstand genommen, dass Mittäterschaft und Bandenhandeln auf das gemeinsame Vollenden der Tat, also auf die Zusammenarbeit am Tatort beschränkt ist [24]. Logistische Zuarbeiten wie das Beschaffen von besonderen Tatwerkzeugen, das

---

17 BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 17; BGH, Beschluss vom 26.01.2005 - 2 StR 516/04; BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 8; BGH, Beschluss vom 07.03.2008 - 2 StR 44/08; BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 13; BGH, Beschluss vom 23.06.2010 – 2 StR 243/10, Rn 3. Zuletzt lapidar: BGH, Beschluss vom 11.10.2011 - 3 StR 331/11.

18 Die hohe Strafdrohung ist nicht zu beanstanden: BVerfG, Beschluss vom 18.03.2009 - 2 BvR 1350/08. Werden nur wenige Karten gefälscht oder missbraucht, ist ein minder schwerer Fall zu prüfen: BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 12.

19 BGH, Beschluss vom 15.03.2011 - 3 StR 15/11, Rn 6

20 BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn 9

21 BGH, Urteil vom 27.01.2011 - 4 StR 338/10

22 Siehe oben: BGH, Urteil vom 17.02.2011 – 3 StR 419/10.

23 Die Rechtsprechung des BGH zum Skimming hat das Gericht jetzt selber zusammen gefasst: BGH, Beschluss vom 11.08.2011 - 2 StR 91/11. Siehe auch: CF, Skimming im engeren Sinne, 09.10.2011.

Auskunden geeigneter Tatorte und der Abtransport zwischen Vollendung und Beendigung macht diese Handlungen im Licht einer effektiven Strafverfolgung [25] nicht weniger gefährlich als die arbeitsteilige Zusammenarbeit am Tatort selber. Im Einzelfall macht sich deshalb bereits der Komplize als Mittäter strafbar, wenn er einen Firmenmantel beschafft und einrichtet, unter dem seine Komplizen später betrügerische Leasing- und Kaufverträge abschließen [26]. Auch spontan wirkende Tatentschlüsse wechselnder Tatbeteiligter können ihren Ursprung in einem stillschweigenden Tatbegehungskonsenz haben, also auf einer Bandenabrede beruhen [27]. Die neue Ausrichtung des BGH, gefährliche Täterbeiträge in ihrer ganzen zeitlichen Erstreckung zu betrachten, passt besonders auf das mehraktige Tatgeschehen beim Skimming.

Hinzu kommt, dass das Abgreifen beim Skimming keine einfache Hilfeleistung ist. Sie bedarf der Erkundung geeigneter GAA und ihrer Standorte [28], geübtes handwerkliches Geschick bei der Installation und den Gebrauchsprüfungen, handwerkliche Anpassungen der Skimmer und der anderen Geräte und eine gehörige Portion Dreistigkeit, um die Geräte schnell betriebsbereit zu machen und während des Abgreifens zu überwachen. Damit ist das Abgreifen nicht nur eine wesentliche Voraussetzung für das Cashing und als Handlung erheblich anspruchsvoller als das mehr mechanische Beschreiben von WhiteCards sowie ihr geballtes Gebrauchen beim Cashing. Die Abgreifer haben in dieser frühen Tatphase eine ultimative Tatherrschaft. Ohne ihren Tatanteil ist das Cashing ausgeschlossen.

Beteiligung am Versuch des Fälschens

Die Strafbarkeit des Skimmings im Stadium des Abgreifens ist im wesentlichen von dem gemeinsamen Tatplan der Tätergruppe bestimmt. Keiner klaut Daten, um sie sich hinterher an die Wand zu nageln (wie es ein Vorsitzender Richter treffend ausgeführt hat). Auch wenn dem Abgreifen eine ultimative Rolle zukommt und in aller Regel die Abgreifer als Mittäter und Beteiligte an einer Verbrechensabrede anzusehen sind, können sie sich im Einzelfall darauf beschränken, unbestimmten „Nachtätern“ die Daten gegen Entgelt zum selbständigen Missbrauch zu beschaffen. Damit entfiele der gemeinsame, sich auf das Fälschen und Gebrauchen erstreckenden Tatplan und die Abgreifer handelten als akzessorische Gehilfen zum Cashing [29]. Dem ist mit der neuen Rechtsprechung zum Versuchsbeginn ein Riegel vorgeschoben: Wenn bereits mit der Übermittlung der abgegriffenen Daten an die fälschungsbereiten „Nachtäter“ der Versuchs beginnt und eine Freiheitsstrafe von mindestens drei Monaten droht (§§ 152b Abs. 1, 23 Abs. 1, 49 Abs. 1 Nr. 3 StGB), dann haben es die Abgreifer nicht mehr in der Hand, den Unrechtserfolg durch Untätigkeit abzuwenden (§ 24 Abs. 1 S. 2 StGB); sie müssen hingegen aktiv handeln. Spätestens bei der Übermittlung der abgegriffenen Daten kommt es auch nicht mehr auf einen gemeinsamen Tatplan an, weil sich die Abgreifer bereits als Versuchstäter strafbar machen.

Dabei geht es um getrennt arbeitsteilige Operation Groups, die erst bei der Übergabe der ausgespähten Daten täterschaftlich zusammen arbeiten. In dieser Form der Arbeitsteilung handeln die „Abgreifer“ zunächst selbständig mit der Vorstellung, ihre gesammelten Daten auf dem Schwarzmarkt noch unbekannten Cashern anzubieten. Als solche sind sie zunächst Gehilfen und können sich weder an einer Verbrechensabrede noch an

---

[24] BGH, Beschluss vom 22.03.2001 - GSSt 1/00

[25] BVerfG, Beschluss vom 18.03.2009 - 2 BvR 2025/07, Rn 16

[26] BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

[27] BGH, Urteil vom 21.12.2007 - 2 StR 372/07

[28] Die Auswahl richtet sich nach der Bauart der GAA, dem Equipment der Täter und den erforderlichen Anpassungen beim Einbau. Wichtig sind auch, ob eine Kameraüberwachung vorhanden, wie groß das Entdeckungsrisiko und ob die Kundenfrequenz groß genug ist, damit sich das Risiko lohnt.

[29] An der Verbrechensabrede (§ 30 Abs. 2 StGB) können sich nur (mindestens zwei) Mittäter und nicht auch Gehilfen beteiligen: BGH, Urteil vom 04.02.2009 - 2 StR 165/08. Sie ist – wie die Mittäterschaft, Anstiftung und Beihilfe – eine Form der Beteiligung, die mit dem Versuch der Tat beendet ist: BGH, Beschluss vom 14.04.2011 - 1 StR 458/10. Beihilfe zum Versuch ist nicht strafbar.

einer Bande beteiligen. Das ändert sich, sobald sie die ausgespähten Daten an Casher übergeben, die alles zur Fälschung von Zahlungskarten vorbereitet haben. Unter diesen Voraussetzungen machen sich die Ausspäher zu Mittätern der Casher.

Strafbarer Umgang mit Skimming-Geräten

§ 149 StGB stellt bereits den Umgang (Verschaffen, Verwahren usw) mit klassischen Fälschungswerkzeugen und Rohstoffen unter Strafe. Das gilt auch für Computerprogramme und ähnliche Vorrichtungen, die für das Fälschen von Zahlungskarten bestimmt sind (Verweise in den §§ 152a Abs. 5, 152b Abs. 5 StGB), und deshalb für die Lesegeräte (Skimmer), die keinen anderen Verwendungszweck haben können als den, die Daten vom Magnetstreifen oder EMV-Chips abzugreifen [30]. Diese Daten dienen jedenfalls unmittelbar zum Fälschen von Dubletten.

Etwas anderes gilt für die Kameras und Tastaturaufsätze, mit denen die Tastatureingaben und vor allem die PIN abgegriffen werden. Sie dienen zum späteren Gebrauch und dem damit verbundenen Computerbetrug, also ausdrücklich nicht zum Fälschen im engeren Wortsinne.

§ 263a Abs. 3 StGB stellt den Umgang mit Programmen unter Strafe, die zum Computerbetrug eingesetzt werden sollen. Das betrifft nicht die Hardware der Geräte, sondern nur die elektronischen Schaltungen in besonderen Kameravorrichtungen und Tastaturaufsätzen, die für die Aufnahme der PIN und ihr Abspeichern vorgesehen und präpariert werden. Auf die „Werktiefe“ des Programms kommt es nach dem schlichten, aber zweckgerichteten Wortlaut der Strafvorschrift nicht an.

Dieser Tatbestand greift meines Erachtens nicht beim Einsatz von Dual Use-Produkten wie handelsüblichen Digitalkameras und Mobiltelefonen mit Kamerafunktion [31], auch wenn sie zur Tarnung in Rauchmeldern oder anderen Attrappen verbaut oder mit zusätzlichen Stromquellen verbunden werden, wenn die Steuerungen seitens der Hersteller unverändert bleiben. Mit anderen Worten: Dual Use ist strafneutral [32].

Skimming im engeren Sinne

Auch das Abgreifen der Kartendaten und PIN ist noch im Vorbereitungsstadium des Fälschungsverbrechens und des noch späteren Computerbetruges angesiedelt, so dass – mit erhöhtem Handlungsunrecht – die Strafbarkeit auf den §§ 149 und 263a Abs. 3 StGB oder einer Verbrechensabrede gemäß §§ 152b Abs. 1, 2, 30 Abs. 2 StGB beruht [33].

Bei den Skimmern hat der BGH eine Strafbarkeit wegen des Ausspähens von Daten abgelehnt, weil gegen den Lesevorgang keine Schutzvorrichtungen vorgesehen sind [34]. Dasselbe gilt für PIN-

[30] Der BGH lässt die tatbestandliche Frage und die nach der Konkurrenz zur Verbrechensabrede ausdrücklich offen (BGH, Urteil vom 17.02.2011 – 3 StR 419/10, Rn 12), hat aber schon mehrere Verurteilungen nach § 149 StGB kommentarlos „durchgewunken“ (BGH, Beschluss vom 12.05.2011 - 3 StR 101/11). Nach Ansicht des 2. Strafsenats verdrängt die Verbrechensabrede den § 149 StGB (BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 16)

[31] Zum „Hackerparagraphen“ § 202c StGB: BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07 u.a.

[32] Das gilt für Dual Use-Produkte wegen ihrer Strafbarkeit als Beziehungsgegenstand („unerlaubter“ Besitz). In verbauter Form sind sie hingegen ein starkes Beweismittel dafür, dass das Skimming im Rahmen einer Verbrechensabrede geplant gewesen ist. Das Skimming im engeren Sinne ist keine Gelegenheitshandlung. Es bedarf erfahrener und geübter Täter.

[33] Alexander Seidl und Katharina Fuchs (Zur Strafbarkeit des sog. "Skimmings", HRRS 6/2011, S. 265) diskutierten jüngst in Bezug auf PIN-Skimmer eine Strafbarkeit nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1 und Nr. 3 BDSG. Aufgrund seiner allgemeineren Schutzrichtung und seiner geringen Strafdrohung wird die Datenschutz-Straftat von § 263a Abs. 3 StGB verdrängt.

Bei gewerbsmäßigem Bandencomputerbetrug (§§ 263a Abs. 2, 263 Abs. 5 StGB) kommt eine Verbrechensabrede auch wegen des Vermögensdelikts in Betracht.

Siehe auch: CF, Zur Strafbarkeit des sog. "Skimmings", 09.10.2011.

[34] Siehe oben (BGH, Beschluss vom 18.03.2010 - 4 StR 555/09). Das wäre nur der Fall, wenn die Daten auf der Zahlungskarte insgesamt verschlüsselt wären und mit der PIN die Entschlüsselung erfolgen würde.

Skimmer. Sie dienen dem Abgreifen von Daten während des Eingabevorganges und nicht, wie es die Datendefinition in § 202a Abs. 2 StGB vorsieht, dem Ausspähen bereits gespeicherter Daten (§ 202a Abs. 1 StGB) oder dem Abfangen „fließender“ Daten während eines Datenverarbeitungsvorganges (§ 202b StGB).

Bei dem Einsatz von an ihren Steuerungen unveränderten Dual Use-Komponenten kommt hingegen § 303b Abs. 5 StGB in Betracht. Die Computersabotage wird zwar grundsätzlich von dem besonderen Computerbetrug verdrängt, was nichts daran ändert, dass die abgegriffenen PIN schließlich zur schädigenden Beeinflussung fremder Datenverarbeitungen eingesetzt werden sollen, also des bargeldlosen Zahlungsverkehrs im Autorisierungsverfahren. Der Gefährdungstatbestand der Computersabotage verweist auf § 202c StGB und somit auf das Tatbestandsmerkmal „Zugangscodes“, also auch auf die PIN. Die Strafbarkeit beginnt dem Wortlaut der Vorschrift folgend mit dem erfolgreichen Abgreifen von mindestens zwei PIN (Mehrzahl).

Ergebnisse

Das Skimming umfasst als mehraktiges Delikt das Abgreifen von Zahlungskartendaten und PIN im Vorbereitungsstadium, das eigentliche Fälschen von Zahlungskarten mit Garantiefunktion und schließlich deren Gebrauch unter Einsatz der ebenfalls abgegriffenen PIN (Cashing, Gebrauch gefälschter Zahlungskarten mit Garantiefunktion in Tateinheit mit Computerbetrug). Mit dem Fälschen beginnt die Strafbarkeit als vollendetes Verbrechen gemäß § 152b Abs. 1 StGB, wobei aufgrund des logistischen Aufwandes, den die Täter betreiben, grundsätzlich von einem gewerbsmäßigen Handeln und von arbeitsteiligen Bandenstrukturen im Sinne von § 152b Abs. 2 StGB auszugehen ist.

In arbeitsteiligen Tätergruppen beteiligen sich auch die Abgreifer am Versuch der Fälschung, sobald sie die abgegriffenen Daten an ihre fälschungsbereiten Komplizen übermitteln. Bis dahin handeln sie im Vorbereitungsstadium des Fälschungsdelikts und sind als Mittäter die Beteiligten an einer Verbrechensabrede gemäß § 30 Abs. 2 StGB.

Selbständige Abgreifer oder Zwischenhändler, die die abgegriffenen Daten an die fälschungswilligen und -bereiten Casher übermitteln, beteiligen sich bereits am Versuch deren Fälschungsverbrechens. Sie müssen die Casher nicht persönlich kennen und auch keine dauerhafte Beziehung mit ihnen eingehen wollen. Allein die Tatsache der Zulieferung der Daten mit der Vorstellung, dass die Casher bereits auf die Daten warten, reicht dazu aus, dass die Abgreifer und Zwischenhändler zu Mittätern der Fälscher werden (Grunddelikt: § 152b Abs. 1 StGB).

Der Umgang mit Skimming-Geräten ist auch im Vorbereitungsstadium strafbar gemäß §§ 149, 263a Abs. 3 StGB. Eine Ausnahme bilden verbaute Dual Use-Komponenten in PIN-Skimmern, solange keine Veränderungen an ihren Steuerungen vorgenommen wurden. Ihr Einsatz ist strafbar, sobald mindestens zwei PIN aufgenommen wurden (§ 303b Abs. 5 StGB).