Skimming
Hintergründe und Strafrecht

Dieter Kochheim

Skimming ist eine mehrgliedrige Erscheinungsform der Cybercrime, die sich als sehr anpassungsfähig und lukrativ erwiesen hat.

Die Fragen nach der Strafbarkeit in den verschiedenen Tatphasen sind von der Rechtsprechung weitgehend geklärt.

Dritte überarbeitete Fassung.

Stand: März 2012

Thema:	**Skimming**
Autor:	Dieter Kochheim
Version:	3.04
Stand:	31.03.2012
Cover:	U-Bahn-Station Werderstraße, Hannover (Ausschnitt)
Impressum:	cyberfahnder.de

S. **Inhalt**

Vorwort

Der Begriff ***Skimming*** [1] leitet sich von dem Skimmer [2], also dem Lesegerät ab, mit dem die Magnetstreifen von „Identitätsdokumenten“ [3] ausgelesen werden können. Den Tätern geht es aber nicht um das Ausspähen der Daten auf den Zahlungskarten und der Persönlichen Identifikationsnummern – PIN – von Bankkunden, sondern einzig um die Beute, die sich beim Missbrauch gefälschter Zahlungskarten erzielen lässt.

Das Skimming ist zu einem einträglichen Geschäft geworden, in dem sich gut aufgestellte einheimische und internationale Banden tummeln. 2009 und 2010 entstanden dadurch Schäden von rund 40 bis 60 Millionen € jährlich [4].

Entsprechend wandlungsfähig sind die Täter, indem sie immer wieder neue Sicherungsmaßnahmen umgehen und ihr Vorgehen verändern. Zunächst haben sie nur an Geldausgabeautomaten die Dateneingaben ausgespäht. Seit 2011 sehen sie es vermehrt auf die Eingabegeräte im Einzelhandel (POS-Terminals), die Bezahlautomaten an Tankstellen [5] und Fahrkartenautomaten der Deutschen Bahn ab [6]. In einzelnen Fällen haben sie elektronische Bauteile in den Geldautomaten verbaut, wodurch sie auch den Zugriff auf die Daten in den EMV-Chips erlangen [7].

POS-Skimming: Manipuliertes Eingabegerät (POS-Terminal) aus dem Einzelhandel. Mit einer eingelegten Folie (Bild Mitte) werden die Tastatureingaben abgegriffen und zusammen mit den Kartendaten gespeichert (Bild rechts). Quelle: BKA 2009.

Lukrativer ist hingegen das POS-Skimming [8]. Nach ihren Umbauten gelangen die Täter direkt an die vom Lesegerät erfassten Kartendaten und mittels einer unter der Tastatur platzierten Folie auch an die PIN [9], ohne sie mühsam und mit hoher Fehlerquote mit Kameras ausspähen zu müssen.

Die europäische Finanzwirtschaft hat auf das Skimming unter anderem mit dem verbindlichen Einsatz des EMV-Chips reagiert. Das ist der Grund dafür, dass der Einsatz der gefälschten Karten jetzt fast nur noch in Nord- und Südamerika, Afrika und im Fernen Osten stattfindet, wo noch immer der Magnetstreifen maßgebend ist.

Dieses Arbeitspapier beschreibt das Vorgehen der Täter, die wirtschaftlichen und technischen Hintergründe und die strafrechtlichen Fragen, die sich im Zusammenhang mit dem Skimming stellen. Es soll eine schnelle Orientierung bei den durchaus schwierigen Rechtsfragen geben, die bei der Strafverfolgung wegen des Skimmings auftreten.

---

[1] Die Quellenangaben sind, wenn möglich, mit Hyperlinks zum Internet versehen.

[2] CF, Sicherheitsvorkehrungen, Juli 2007;
CF ist das Kürzel für „Cyberfahnder“.

[3] CF, Überwachungstechnik: Zahlungskarten, 18.05.2008

[4] CF, das Schweigen der L@mmer, 12.09.2010.

[5] CF, Ende der Überfahrt nach 50 Tagen, 28.06.2011 (am Ende).

[6] CF, Skimming an Fahrkartenautomaten, 23.10.2011

[7] Die Postbank ist dazu übergegangen, an ihre Kunden grundsätzlich nur Zahlungskarten mit EMV-Chip und ohne Magnetstreifen auszugeben. Andere Banken sind ihr bereits gefolgt.

Die Tastatureingaben am Geldautomaten werden bereits in der Tastatur verschlüsselt, so dass mit den Bauteilen nur die Daten auf den Zahlungskarten erlangt werden können, nicht aber auch die PIN.

[8] Anhand der veröffentlichten Zahlen für 2009 habe ich errechnet, dass aus einer vollständig ausgespähten Karte im Durchschnitt 2.350 € erlöst werden kann.

[9] Die von den Tätern verbaute Elektronik ist meistens auch mit einem Bluetooth-Modul gekoppelt, so dass die ausgespähten Daten mit einem modernen Mobiltelefon per Nahfunk ausgelesen werden können. Die handwerkliche Qualität dieser Einbauten ist bemerkenswert.

Während ich das Skimming zunächst als ein Randthema zur Cybercrime angesehen habe [10], zeigen der lebhafte Handel mit ausgespähten Daten und technischem Equipment in den Handelsbörsen der Underground Economy, dass sich die Szenen miteinander verbunden haben. Als Ausdruck des Formenwandels sind bereits direkte Angriffe gegen Finanzdienstleister bekannt geworden [11] und wird der Technikeinsatz beim Skimming immer ausgefeilter, der von den Tätern immer mehr Expertenwissen verlangt. Dadurch bilden sie zwar eine eigenständige Gruppe neben den üblichen Cyber-Tätern, die aber aus dem Ensemble der Underground Economy nicht mehr weggedacht werden kann [12].

Seit 2010 hat sich der Bundesgerichtshof – BGH – mehrfach mit der Strafbarkeit des Skimmings beschäftigt und inzwischen fast alle maßgeblichen Fragen geklärt. Das abschließende Cashing, also der Gebrauch gefälschter Zahlungskarten mit Garantiefunktion an Geldautomaten im Ausland, ist ein Verbrechen nach § 152b Abs. 1 StGB und gleichzeitig ein Computerbetrug (§ 263a Abs. 1 StGB), der deshalb als Inlandstat verfolgbar ist, weil hier der Schaden eintritt [13]. Das Ausspähen der Daten [14], also das Skimming im engeren Sinne, ist eine Vorbereitungshandlung zum Cashing [15], deren Strafbarkeit aus anderen Vorschriften abzuleiten ist. Im Januar 2011 hat der BGH das Versuchsstadium des Fälschungsdelikts präzisiert [16]: In arbeitsteiligen Tätergruppen beteiligen sich die „Ausspäher“ bereits am Versuch der Fälschungstat, sobald sie die ausgespähten Daten an ihre zur Fälschung bereit stehenden „Nachtäter“ übermitteln.

Keine ausdrücklichen Worte hat der BGH bislang zu der Frage gesprochen, ***ob*** es sich bei den Kartenlesegeräten [17] (Skimmer) um *Computerprogramme oder ähnliche Vorrichtungen* im Sinne von § 149 Abs. 1 Nr. 1 StGB handelt. Im August 2011 hat das Gericht die Frage auf ganz eigene Art beantwortet [18]: Es lässt die Frage nach dem Konkurrenzverhältnis zwischen der Vorbereitungshandlung (§ 149 StGB) und der gleichzeitigen Verbrechensabrede offen (§ 30 Abs. 2 StGB). Damit hat sich der 2. Strafsenat zwar nicht festgelegt, aber auch keinen Anlass zum Widerspruch gesehen.

Überblick

Die dritte Auflage dieses Arbeitspapier folgt dem Aufbau ihrer Vorgänger. Zunächst werden die Erscheinungsformen des Skimmings beschrieben. Dazu wird zwischen dem Skimming im engeren Sinne, also dem Ausspähen von Kartendaten und Persönlichen Identifiktionsnummern – PIN, und dem Cashing unterschieden, also dem Missbrauch gefälschter Zahlungskarten an Geldautomaten, die den Beginn und den Abschluss des Tatplanes kennzeichnen.

Der zweite Teil widmet sich den finanzwirtschaftlichen Prozessen des bargeldlosen, kartengestützten Zahlungsverkehrs, deren Verständnis für die Rechtsfragen nötig ist. Das gilt besonders für die automatischen Autorisierungs- und Clearingverfahren, die den internationalen Zahlungsverkehr in Echtzeit zulassen. Dabei wird jeder Zahlungsvorgang von dem Rechenzentrum der kartenausstellenden Bank geprüft und schließlich durch die Übermittlung eines Genehmigungscodes die Garantie zur Auszahlung erklärt. Diese Mechanismen machen – neben Kreditkarten –

[10] CF, Cybercrime und IT-Strafrecht, 08.08.2008

[11] CF, Skimming-Coup, 06.02.2009

[12] CF, Mafia, Cybercrime und verwachsene Strukturen, 20.10.2010

[13] Der Schaden tritt zulasten der kartenausgebenden Bank ein. Anders noch: Vorauflage.

[14] Es handelt sich nicht um ein Ausspähen von Daten im Sinne von § 202a Abs. 1 StGB, weil den Zahlungskarten eine Zugangssicherung fehlt.

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

[16] BGH, Urteil vom 27.01.2011 - 4 StR 338/10, CF, Versuch der Fälschung, 21.02.2011.

[17] Die Vorrichtungen zum Ausspähen der Kartendaten und der Tastatureingaben müssen differenziert betrachtet werden, weil § 149 Abs. 1 StGB nur die Fälschung von Zahlungskarten und nicht auch ihren Gebrauch anspricht.

[18] BGH, Beschluss vom 11.08.2011 - 2 StR 91/11

auch Debitkarten zu Zahlungskarten mit Garantiefunktion.

Den umfangreichsten Teil bildet die Auseinandersetzung mit der Strafbarkeit des Skimmings. Ihren Abschluss bildet ein Überblick über die Rechtsprechung zu arbeitsteiligen Tätergruppen, die auch bei der Beteiligung an vorbereitenden Handlungen und an Teilakten des Gesamtplans zur Strafbarkeit am abschließenden Verbrechen führt. Erst im Sommer 2010 sind die Grafiken hinzugekommen, die die Tatphasen veranschaulichen und ihnen die einschlägigen Strafvorschriften zuordnen [19]. Das Beteiligungsmodell wird von einem Phasenmodell begleitet, das die Orientierung verbessert [20].

Das Arbeitspapier schließt mit knappen Anmerkungen zum Strafverfahrensrecht, über kriminalistische Erfahrungen, einer Rechtsprechungsübersicht und einem Glossar.

Hannover, 15.12.2011

[19] CF, Bilderbuch Skimming-Strafrecht, 26.07.2010

[20] CF, Skimming: aktuelles Beteiligungsmodell, 13.03.2011

A. Phänomen Skimming

Das „Skimming“ als kriminelle Erscheinungsform ist etwa seit dem Jahr 2000 bekannt. Seine Vorläufer entstammen dem Trickdiebstahl, bei dem die Täter die Eingabe der Persönlichen Identifikationsnummer – PIN – selber beobachteten und die Zahlungskarte dann stahlen (▸ Lebanese Loop [21]), sowie dem lange vergessen geglaubten ▸ Front Covering, bei dem eine nachgemachte Fassade vor dem Nachtbriefkasten einer Bank installiert wurde, so dass die eingeworfenen Geldbomben nicht in den Tresor, sondern in den Zwischenraum fielen. Seit 2010 ist eine Variante davon bekannt, die „Cash Trapping“ genannt wird: Über den Geldausgabeschlitz kleben die Täter eine Blende, hinter der sich das ausgegebene Geld verfängt. Sobald der entnervte Bankkunde die Filiale verlassen hat, entfernt der Täter die Blende und gelangt an das Geld [22].

Kennzeichnend für das Skimming ist das Auslesen der Magnetstreifen von Kredit- und anderen Zahlungskarten mit einem Kartenlesegerät am Geldautomaten [23] oder einem anderen POS-Terminal [24], also einem Eingabegerät im Einzelhandel, in einem Hotel oder Restaurant, an den Bezahlautomaten an Tankstellen [25] oder an Fahrkartenautomaten der Deutschen Bahn AG [26]. Die für den Einsatz am Geldautomaten angepassten Lesegeräte werden als „Skimmer“ bezeichnet. Das Ausspähen der Kartendaten ist ein notwendiger Schritt zur Fälschung von Zahlungskarten und das Ausspähen der PIN ein weiterer notwendiger Schritt für das finale Ziel der Täter, dem Missbrauch der Zahlungskarten an ausländischen Geldautomaten, wobei sie die Auszahlung

Die Bauteile für das Skimming-Equipment sind zwar frei im Einzelhandel erhältlich. Angepasste Sets – passend für bestimmte Baureihen von Geldautomaten einschließlich Zwischenspeicher und Schreibgerät für die White Cards - gibt es hingegen in öffentlichen Webshops und vor Allem in den einschlägigen Carding-Boards zu kaufen. Die handwerklich hervorragenden Tastaturaufsätze scheinen jedoch aus Bulgarien zu stammen und dort von einer oder sehr wenigen Manufakturen.

Um WhiteCards zu beschreiben, reichen handelsübliche Geräte aus. Schwieriger wird es, originale Bankkarten mit anderen Daten zu überschreiben. Auf den Spuren 1 und 2 auf dem Magnetstreifen befinden sich die Kodierung für die Bank und das Konto befinden.

Solche, eben nicht handelsüblichen Geräte, waren der Grund dafür, dass der 1. Strafsenat des BGH einschränkend zu der Frage Stellung genommen hat, dass das Skimming kein Ausspähen von Daten im Sinne des § 202a StGB ist.

Siehe:
BGH, Beschluss vom 19.05.2010 - 1 ARs 6/10

[21] CF, Proll-Skimming, 18.05.2008

[22] Ich betrachte das „Cash Trapping“ als einen „normalen“ Diebstahl (§ 242 StGB). Diskutiert werden aber auch Betrug (§ 263 StGB) und Unterschlagung (§ 246 StGB). Ein Betrug ließe sich dann annehmen, wenn man eine Vermögensverfügung des „entnervten“ Bankkunden darin sieht, dass er auf den Besitzerwerb am vom Automaten ausgegebenen Geld verzichtet. Das ist aber kein bewusster Akt, weil ihm nicht bekannt ist, dass sich das Geld hinter der aufgesetzten Blende befindet. Eine Unterschlagung scheitert daran, dass der Täter zu keinem Zeitpunkt einen rechtmäßigen Gewahrsam an dem ausgegebenen Geld erlangt.

[23] Geldautomat: Die korrekte, aber umständliche Bezeichnung lautet Geldausgabeautomat – GAA.

[24] POS: Point of Sale.

[25] Im Februar 2011 erfolgte ein Angriff gegen eine frequentierte Tankstelle in Castrop-Rauxel. Mit den dort ausgespähten Daten sollen die Täter nach Presseberichten rund 1 Mio. € Beute erlangt haben.
Skimming-Angriffe an Tankstellensäulen, Heise online 23.02.2010
Thomas Wrycza, Tankkunden in Castrop-Rauxel mit manipuliertem Kartenlesegerät abgezockt, derwesten.de 07.03.2011;
Susanne Linnenkamp, Profis manipulierten SB-Tankstelle in Castrop-Rauxel, ruhrnachrichten.de 10.03.2011

[26] CF, Skimming an Fahrkartenautomaten, 23.10.2011

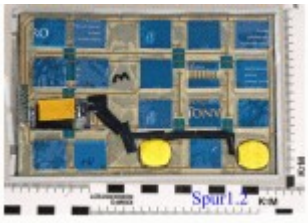
Aufsatz für den Karteneinzugsschacht (Skimmer). Auf der Rückseite befindet sich ein Magnetlesekopf zum Auslesen und die Elektronik zum Speichern. Die Formen der Skimmer wandeln sich je nach der Bauart der GAA.

Immer dann, wenn eine neue Generation von „Mundstücken“ für den Karteneinzug eingeführt wird, häufen sich die Beschädigungen an GAA und Diebstähle dieser Geräte. Nach einiger Zeit tauchen neue Varianten von Skimmern auf, bei denen Original-Teile mit Ausspäh-Technik versehen ist.

In Einzelfällen verbauen die Täter binnen 10 bis 20 Minuten auch elektronische Bauteile in den GAA. An der Platine (links) ist unten eine digitale Kamera angeschlossen, die die Tastatureingaben durch ein stecknadelkopfgroßes Loch im Chasis des GAA aufnimmt. Diese Methode ist noch eher selten.

Am häufigsten werden Kameras zum Ausspähen der Tastatureingaben eingesetzt. Sie werden in Rauchmeldern und anderen Ausstattungsgegenständen verbaut, in Aufsatzleisten, Chasisabdeckungen, Propagandaständern und anderen, unauffällig wirkenden Gegenständen.

Neben elektronischen Bauteilen, die als Unikat zusammengeschraubt und -gelötet werden, kommen ganz häufig auch handelsübliche Digitalkameras und Fotohandys zum Einsatz (Dual Use). Um ihre Laufzeit zu verlängern, werden ihnen gelegentlich weitere Akkus angelötet.



Tastaturaufsätze werden auf das Original aufgelegt und verklebt. Unter jeder Taste befindet sich ein elektronischer Kontakt, der die Eingabe aufnimmt und zum Speicher weiter gibt. Der Tastendruck wird mechanisch an die Tastatur des GAA weiter gegeben. Die handwerkliche Qualität der meisten Tastaturaufsätze ist beachtlich. Es wird vermutet, dass es sich um gestohlene Originalbauteile handelt.

Kameras können überall verbaut werden. Dieses Beispiel zeigt einen Rahmen an der Tastatur, der eigentlich das Beobachten der Eingaben erschweren soll. In ihm ist die Kameratechnik eingebaut. Erkennbar ist nur ein kleines Loch im Chasis des Blendrahmens.

Von hoher handwerklicher Qualität sind auch die Einbauten in POS-Terminals, mit denen die Daten und Tastendrücke gleichzeitig abgegriffen werden. Hier nicht sichtbar ist eine mit Kontakten versehene Folie, mit der die Tastatureingaben abgegriffen werden. Die gespeicherten Daten werden per Nahfunk ausgelesen (Bluetooth).

mit den richtigen Kartendaten und der PIN autorisieren lassen müssen (Cashing).

Die klassischen Skimming-Täter treten in zwei Tatphasen öffentlich auf, beim Ausspähen von Daten und abschließend beim Missbrauch gefälschter Zahlungskarten. Dabei erfolgen auch erfahrungsgemäß die polizeilichen Zugriffe.

Meistens sind arbeitsteilige Tätergruppen aus Südosteuropa im Einsatz, die zunächst in Deutschland mit Kartenlesegeräten verschiedener Bauarten die Magnetstreifen von Bankkarten [27] 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 [28].

Zum Fälschen der Karten genügt ein handelsübliches Gerät, wenn nur die Magnetstreifen von unbedruckten WhiteCards beschrieben werden sollen. Dabei nutzen die Täter meistens nur die zweite der drei vorgesehenen Spuren auf dem Magnetstreifen, auf der die Kontoinformationen (Kennung der Bank und die Kontonummer) sowie die Kartenmerkmale verzeichnet sind [29]. Nur selten kommen auch andere Karten zum Einsatz (Telefon-, Tankkarten ua).

Das Cashing wurde durch den verbindlichen Einsatz des EMV-Chips aus den europäischen Ländern und den beliebten Urlaubszielen am Mittelmeer und auf den Kanaren verdrängt. Die wirklichen Gründe dafür liegen in den Haftungsregeln des europäischen Bankenverbundes: Der Betreiber eines GAA haftet im Rückgriff für den Auszahlungsbetrag, wenn die ausgespähte Karte zwar über einen EMV-Chip verfügt, der GAA sich aber auf die Prüfung des Magnetstreifens beschränkt.

Das hat dazu geführt, dass flächendeckend auf EMV-fähige GAA umgestellt wurde und das Cashing jetzt bevorzugt in Nord- und Südamerika, in West- und Südafrika sowie im Nahen und Fernen Osten erfolgt. Für die hiesigen Banken ist das schmerzhaft, weil sie die eingetretenen Schäden nicht mehr an die Betreiber der GAA abwälzen können.

Wie jede kriminelle Mode wandelt sich auch das Skimming und verfeinern sich die Methoden der Täter. Gegen das Ausspähen der PIN mit einer an der Wand angebrachten Kamera [30] können sich die Bankkunden schützen, wenn sie die Eingabe mit der anderen Hand abdecken. Das funktioniert dann nicht mehr, wenn die Täter eine Kamera flach oberhalb der Tastatur anbringen [31], einen Tastaturaufsatz [32] oder sogar eine vollständige Fassade (Front Covering) einsetzen [33]. Die Verwendung verschiedener Karten für die Zugangskontrolle zu einer Bankfiliale und für den Geldautomaten nützt schon lange nichts mehr, weil die Kartendaten jetzt immer direkt am Geldautomaten ausgelesen werden [34]. Vereinzelt werden auch die EMV-Chips ausgelesen, um die

---

[27] 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.

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

[29] Verschlüsselte Kennziffern für die Karte und das in ihr eingebettete Modifizierte Merkmal – MM.

Die Spuren 1 und 2 der von den Banken enthalten weitgehend gleiche Daten für die Authentifizierung. Die dritte Spur auf den Magnetstreifen ist für variable Daten reserviert (Limits, Fehlversuche).

[30] CF, Kamera, 13.04.2009

[31] CF, Sichtblende mit Kamera, 26.06.2010

[32] CF, Tastaturaufsatz, 13.04.2009; CF, Tastaturblende, 13.04.2009

[33] CF, Skimming, Juli 2007

[34] CF, BKA: Lagebild OK. Zahlungskartenkriminalität, 01.11.2008

Kartendaten anschließend auf die Magnetstreifen von Dubletten zu kopieren. Ihr Einsatz scheitert in aller Regel daran, dass die digitale Kartennummer auf dem Magnetstreifen anders kodiert ist als im EMV-Chip, so dass die Manipulation auffällt.

Erstmals 2008 traten gehäuft Fälle des POS-Skimmings auf [35] (Point of Sale). Gemeint sind die handlichen Terminals an den Kassen im Einzelhandel, die gleichzeitig die Kartendaten auslesen und über ihre Tastatur die PIN aufnehmen [36]. Alle notwendigen Daten durchlaufen diese Geräte. Wenn die Täter es schaffen, sie entsprechend umzurüsten, dann speichern oder senden sie die Dumps [37] an die Täter.

Solche Fälle haben zunächst deutlich nachgelassen, weil die Präparierung der POS-Terminals recht aufwändig ist. Um ihre Schalen nicht zu zerstören, müssen sie mit einer Methode geöffnet werden, bei der sich die innere Elektronik vernichtet. Nur wenn die Täter eine Schalenhälfte richtig zertrümmern, gelangen sie an die intakte Elektronik. Hierzu mussten die Täter in die Einzelhandelsgeschäfte einbrechen, um die POS-Terminals zunächst zu stehlen, die umgebauten Geräte wieder zu installieren und um nach einiger Zeit die ausgespähten Daten wieder auszulesen.

Die Kameraüberwachung aus einem Baumarkt zeigt, dass die Täter jetzt anderes vorgehen. Einer von ihnen lässt sich bei Geschäftsschluss einschließen, stiehlt die Terminals und reicht sie seinen Mittätern nach draußen. Nach wenigen Stunden werden sie ihm wieder ausgehändigt und er installiert sie wieder an den Kassen. Da die manipulierten Geräte über ein Bluetooth-Modul verfügen, können die ausgespähten Daten mit einem Smartphone oder einem ähnlichen Gerät im Bereich der Kassenzone ausgelesen werden [38].

Bis 2010 konnte die durchgängige Erfahrung gemacht werden, dass die ausgespähten Daten äußerst schnell zum Cashing verwendet wurden. Im Einzelfall lagen nur einige Stunden und meistens nur wenige Tage dazwischen. Für dieses Vorgehen sprechen zwei Motivationen: Die Täter haben ein starkes Interesse an schneller Beute und je länger sie warten, desto größer ist die Gefahr, dass die Daten nicht mehr aktuell sind.

In jüngerer Zeit tauchen immer häufiger betagte Daten auf, die schon vor mehreren Monaten ausgespäht wurden. Über die Gründe dafür lässt sich nur spekulieren. Denkbar ist, dass der verstärkte Druck der Strafverfolgung und die verbindliche Einführung des EMV-Chips das Cashing verhinderte, weil die Täter zunächst eine neue Logistik mit ausführenden Komplizen in Übersee aufbauen mussten. Vorstellbar ist auch, dass sich die Szene aufgeteilt hat und getrennte Gruppen für die Beschaffung der Daten und das Cashing zuständig sind, obwohl das nicht zwingend zu einem verzögerten „Umschlag“ führen muss. Schließlich kann es auch sein, dass die Täter schlicht auf die Methoden der Strafverfolgung reagieren: Wenn die Tatsache, dass ein Skimmingangriff erfolgt ist, erst mit monatelanger Verzögerung bekannt wird, dann gibt es keine Verkehrsdaten und keine Aufzeichnungen von Kameraüberwachungen mehr, mit denen sie überführt werden könnten. Außerdem dürften auch die Journale aus den Geldautomaten nicht mehr zur Verfügung stehen, die Auskunft über die Bankkunden, Störungen während des Einbaus der Skimmingapparaturen und dem Einsatz von Testkarten geben.

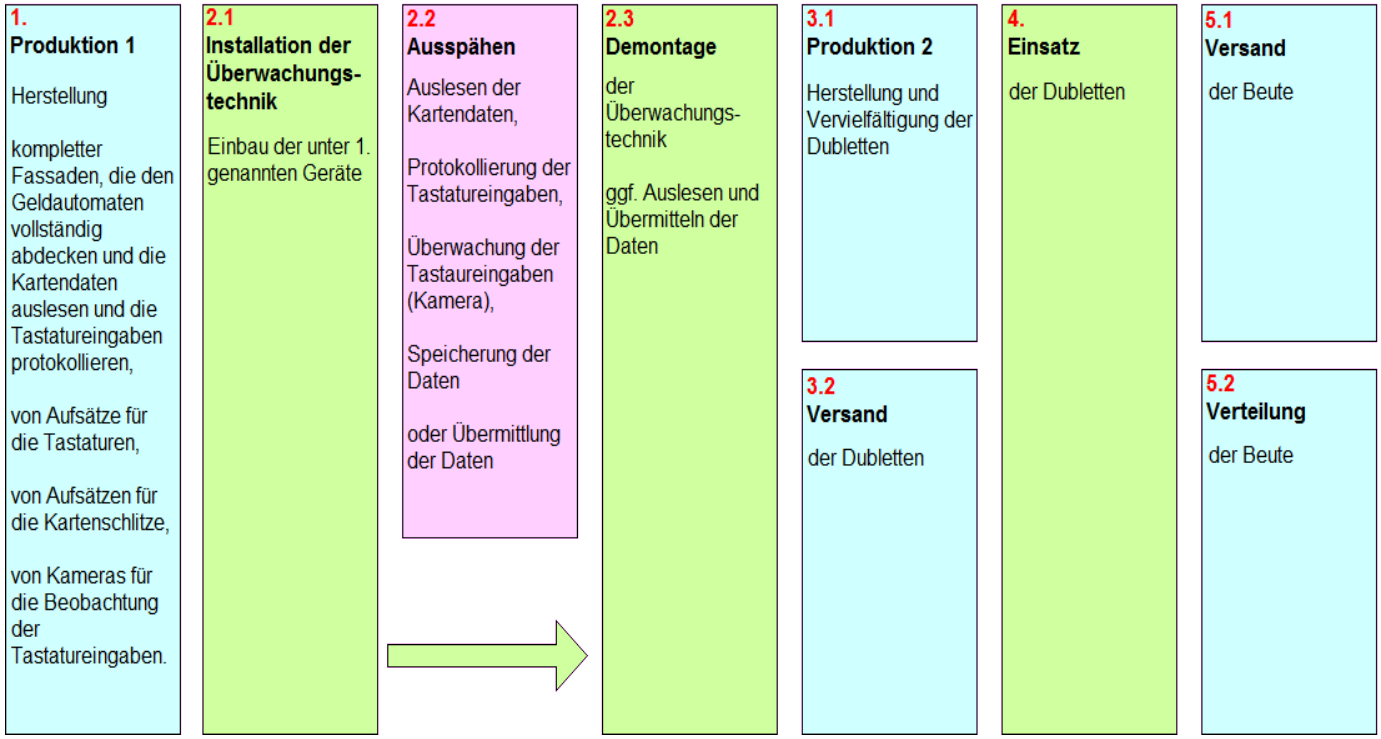
Der Wandel bei den Erscheinungsformen des Skimmings im engeren Sinne belegt, dass die Quelle für die missbrauchten Daten beliebig ist. Betroffen sind alle Gelegenheiten, bei denen sich

[35] CF, POS-Skimming, 18.05.2008; CF, Datenklau und -missbrauch, 19.08.2008

[36] CF, BKA: Lagebild OK. Manipulation von POS Terminals, 01.11.2008

[37] Vollständige Kartendaten einschließlich PIN; CF, Fachworte, April 2007

[38] Die Reichweite des Nahfunks wird meistens durch Wände der Bebauung begrenzt, so dass sich die Täter bis auf einige Meter an das sendende Gerät zubewegen müssen.



Die Arbeitsteilung beim Skimming kann als Organisationsmodell mit einer einheitlichen Struktur angesehen werden. Es ist aber nicht zwingend.

Dagegen sprechen, was die „Produktion“ anbelangt, die immer ausgefeilteren Geräte, die zum Einsatz kommen und spezialisierte Zulieferer erwarten lassen. Auch die „Abgreifer“ spezialisieren sich zunehmend. Mussten sie zunächst „nur“ Anpassungen an der fertigen Hardware vornehmen, so müssen sie jetzt beim POS-Skimming auch den Einbau der Elektronik in kurzer Zeit bewerkstelligen. Sie mögen die Elektronik nicht selber herstellen, müssen mit ihr aber fachkundig umgehen und sie einbauen können.

Hinzu kommt die Erfahrung, dass viele „Abgreifer“ und ihre persönlichen Spuren seit mehreren Jahren Immer wieder auftauchen. Das spricht dafür, dass sie in stabilen Zusammenhängen agieren und sich laufend fortbilden.

Über die Nähe zwischen den Tätern beim Abgreifen und beim Cashing ist wenig bekannt. Solange es noch in Europa stattfand, sind direkte Telefonkontakte zwischen ihnen und teilweise auch die Beteiligung der Abgreifer am Cashing selber belegt.

Für die Frage, ob sie eine einheitliche Bande bilden, kommt es darauf nicht an. Sie müssen sich nicht kennen und auch keine Kommunikation führen, wenn sie durch dieselben Hinterleute miteinander verbunden werden. Dafür sprechen die Erfahrungswerte, dass häufig dieselben Telefonkontakte erfolgen und das Cashing zwar in Übersee stattfindet, aber bevorzugt in denselben Orten.

die Authentifizierungsmerkmale von Karteninhabern abgreifen lassen. Sie sind zwar ausschlaggebend für den Taterfolg, am Ende zählt aber das erbeutete Geld und nicht die Methode, mit der die Täter an die Daten gelangten.

Zunächst wurden 2009 in Russland die Geldautomaten selber gehackt, um die Dateneingabe vollständig aufzuzeichnen [39]. In jüngerer Zeit tauchten auch hierzulande elektronische Bauteile auf, die in die Geldautomaten eingebaut werden können. Sie lassen das Auslesen der Kartendaten unmittelbar aus der Elektronik des Gerätes zu, ohne dass irgendeine äußere Veränderung erkennbar wird und enthalten gelegentlich auch die Kameraelektronik für die Beobachtung der Tastatureingaben. Diese Daten lassen sich noch nicht aus der Elektronik des Geldautomaten abgreifen, weil sie unmittelbar in der Tastatur verschlüsselt werden.

Besonders heimtückisch gingen die Hacker vor, die Ende 2008 in die Datenhaltung einer US-amerikanischen Bank eindrangen und die Kartendaten einschließlich PIN von 100 Kunden ausspähten [40]. Gleichzeitig erhöhten sie deren Auszahlungslimit. Am 08.11.2008 wurden weltweit und gleichzeitig an 130 Geldautomaten in 49 Städten die gefälschten Zahlungskarten eingesetzt und damit 9 Millionen US-$ erbeutet.

Dieses Beispiel zeigt, wie sich die Methoden der Cybercrime in den Formen des Hackings, des Ausspähens und des Verfälschens von Daten mit denen anderer Formen der Cybercrime vermengen.

Das übliche Skimming im engeren Sinne verlangt nach besonderen handwerkliche Fertigkeiten bei der Herstellung der eingesetzten Geräte, besonderes Wissen wegen der Auswahl der Geldautomaten und Standorte, die sich einer-

„Abgreifer“, aufgenommen von einer im GAA eingebauten Kamera (Januar 2011). Verfremdung mit Schnee-Effekt.

seits zum Ausspähen der erstrebten Daten und andererseits zum Missbrauch der gefälschten Zahlungskarten eignen, sowie logistisches Geschick bei der Installation der Überwachungshardware [41]. Die verschiedenen Arbeitsschritte im Tatplan, ihre wechselnden Anforderungen an die Fähig- und Fertigkeiten der Täter [42] und die grenzüberschreitende Logistik des Gesamtplans sprechen in aller Regel für eine Arbeitsteilung mit einer zentralen planenden und steuernden Instanz.

Die bisher gemachten Erfahrungen zeigen, dass Skimmer [43] und Casher [44] überwiegend zu zweit oder dritt auftreten und gelegentlich auch mehrere Gruppen gleichzeitig handeln. Aus den Bildern von Überwachungskameras ist bekannt, dass die Täter noch am Tatort mobil telefonieren. Sie berichten dann offenbar über den Erfolg ihres Einsatzes und stimmen sich untereinander ab.

In den Journalen von angegriffenen Geldautomaten werden auch Stromunterbrechungen protokolliert, wenn Lesegeräte ausgewechselt wur-

[39] CF, Skimming an der Quelle, 20.03.2009

[40] CF, Skimming-Coup, 06.02.2009

[41] Das hat jetzt auch der BGH hervorgehoben: BGH, Urteil vom 27.01.2011 - 4 StR 338/10, Rn. 8

[42] CF, Grafik, Juni 2008. Wegen der Herstellung von Skimmern (Kartenlesegeräte) fehlt noch der Hinweis auf § 149 StGB. Die Diskussion um die Strafbarkeit wegen des Umgangs mit diesen Geräten wurde erst ab Herbst 2008 öffentlich.

[43] Skimmer: siehe Glossar.

[44] Casher: siehe Glossar.

den. Inzwischen schalten sich in einem solchen Fall die Geldautomaten einfach ab.

Im Journal werden auch alle Karteneinsätze dokumentiert, so dass auch der wiederholte Einsatz einer Testkarte erkennbar wird. Sie wird dazu genutzt, um die Funktionsbereitschaft des Geldautomaten und die Passgenauigkeit des Skimmers zu prüfen. Außerdem eignen sie sich dazu, Marken im Protokoll des Skimmers zu setzen, die den Tätern die Zuordnung der Kartendaten zu den mit einer Kamera ausgespähten PIN-Eingaben erleichtert [45]. Andere Bilder haben eindrucksvoll gezeigt, wie Casher beim Einsatz von WhiteCards [46] mit ihren Handys telefonieren und sich dabei offenbar die PIN übermitteln lassen.

Die bevorzugten Zeiten für das Ausspähen liegen außerhalb der Banköffnungszeiten, also ganz besonders ab Freitag Mittag bis über das Wochenende hinweg. Das verbindet die Skimming-Täter mit denen beim klassischen (überholten) Phishing. Beiden geht es darum, den störenden Eingriff der Bankmitarbeiter zu unterlaufen. Beim Phishing [47] soll dadurch die Transaktion mit den ausgespähten Daten des Onlinebankings abgesichert und beim Skimming das Entdeckungsrisiko verringert werden.

Auch das Cashing findet vor Allem am Wochenende und während der Nacht statt. Nachts haben die Casher die wenigsten Störungen durch Bankkunden, Publikum und Sicherheitspersonal zu befürchten. Um 0:00 Uhr wird auch in aller Regel das Tageslimit für die Zahlungskarten umgestellt. Das bedeutet, dass die Täter zwei Tageshöchstbeträge ergaunern können, wenn sie die gefälschte Karte vor und nach Mitternacht missbrauchen. Aus diesen Gründen bevorzugen sie auch das Wochenende und die Feiertage. Hinzu kommt, dass in der Nacht von Freitag auf Samstag meistens auch das Wochenlimit storniert wird [48], so dass am Samstag Morgen das neue Wochenlimit angegriffen werden kann.

Dank des maschinenlesbaren Merkmals, das aber nur deutsche Zahlungskarten enthalten müssen, können Fälschungen mit inländischen Magnetstreifendaten nur im Ausland zum Cashing eingesetzt werden. Im europäischen Ausland haben sich weitgehend die Geldautomaten durchgesetzt, die statt des Magnetstreifens den EMV-Chip der Zahlungskarte prüfen, den die Fälscher bislang nicht nachmachen können. Das führt dazu, dass das Cashing fast nur noch im außereuropäischen Ausland stattfindet.

[45] Als Testkarte eignet sich jede Magnetkarte, also auch Telefon- oder Tankkarten. Wichtig ist den Tätern nur, dass sie anhand der ihnen bekannten Eigenschaften der Testkarte den Zeitpunkt und die Reihenfolge der ausgespähten Daten überprüfen und den gesondert beobachteten PIN zuordnen können.

[46] White Cards, auch White Plastics: siehe Glossar.

[47] Mit „klassischem Phishing“ ist die Verbreitung von Spam-Mails gemeint, die die Empfänger zur Preisgabe ihrer Kontozugangsdaten bewegen sollen. Zu den jetzt üblichen Methoden: CF, Phishing mit Homebanking-Malware, 22.10.2008.

[48] Zum Beispiel HypoVereinsbank, HVB Cashkarte. Denn Zeit ist Geld!, S. S. 2.

B. bargeldloser, kartengestützter Zahlungsverkehr

1. Fälschungssicherung

Die in Deutschland herausgegebenen Zahlungskarten [49] verfügen über mehrere Vorrichtungen gegen das Fälschen der Karte selber [50]. Neben dem Unterschriftsfeld, den Merkmalen des Aufdrucks und des für die Individualdaten verwendeten Schrifttyps (OCR-B [51]) sind das besonders der EMV-Chip, die digitale Prüfziffer - CVV - und das Maschinenlesbare Merkmal – MM.

Das MM ist eine Besonderheit, die es nur in Deutschland gibt. Dabei handelt es sich um einen im Kartenkörper eingebettete Merkmalstoffe, der eine individuelle Codierung der Karte zulassen [52]. Diese Codierung wird im Geldautomaten mit einer Prüfsumme abgeglichen, die auf dem Magnetstreifen und dem EMV-Chip der Zahlungskarte gespeichert ist. Es wird jedoch (noch) nicht von allen Handgeräten im Einzelhandel geprüft (POS-Terminal), so dass hier zum Cashing verfälschte Zahlungskarten eingesetzt werden können, bei denen der Magnetstreifen der Originalkarte mit fremden Kontodaten beschrieben ist [53].

Der EMV-Chip wird von den großen Verbünden für grenzüberschreitend einsetzbare Zahlungskarten gefordert und ist bereits weit verbreitet [54]. Das Kürzel geht auf „**E**lectronic Cash – **M**aster/Maestro – **V**isa“ zurück [55]. Der Chip ist programmierbar [56], verspricht, nicht manipulierbar sein [57] und eine verschlüsselte Datenkommunikation zu ermöglichen [58].

In Europa wird inzwischen flächendeckend der EMV-Chip für die Autorisierung der Auszahlungen an den GAA benutzt. Nur in Übersee (Amerika, Afrika, Südasien) beschränken sich die GAA noch auf noch auf das Auslesen des Magnetstreifens, dessen Daten verhältnismäßig leicht kopiert und übertragen werden können.

2. bargeldloser Zahlungsverkehr

Beim klassischen Euroscheck verkörperte die Bank des Kunden ihre Zahlungsgarantie in Papierform, also durch den Euroscheck selber [59]. In Verbindung mit der EC-Karte erfolgte die Autorisierung durch den Akzeptanten. Parallel dazu entwickelte die Finanzwirtschaft das System der bargeld- und papierlosen Zahlungen, die unter dem Begriff Point of Sale – POS – zusammengefasst werden. Es kennt zwei Ausprägungen, die bankwirtschaftlich entstanden sind und ihre rechtliche Anerkennung erhalten haben: Die Lastschrift und der Abbuchungsauftrag [60].

---

[49] Es handelt sich um standardisierte Identitätsdokumente nach ISO/IEC 7810 (Wikipedia).

[50] CF, Zahlungskarten, 18.05.2008

[51] CF, Zeichensatz OCR-B, Juli 2007

[52] CF, Sicherheitsmerkmale und Merkmalstoffe, 06.02.2010

[53] Der Magnetstreifen verfügt über drei Spuren, wovon die dritte Spur überschreibbar ist (zum Beispiel: Zahl der Fehlversuche).

[54] Kartensicherheit.de, EMV-Chip

[55] CF, Zahlungskarten mit Garantiefunktion, 13.04.2009

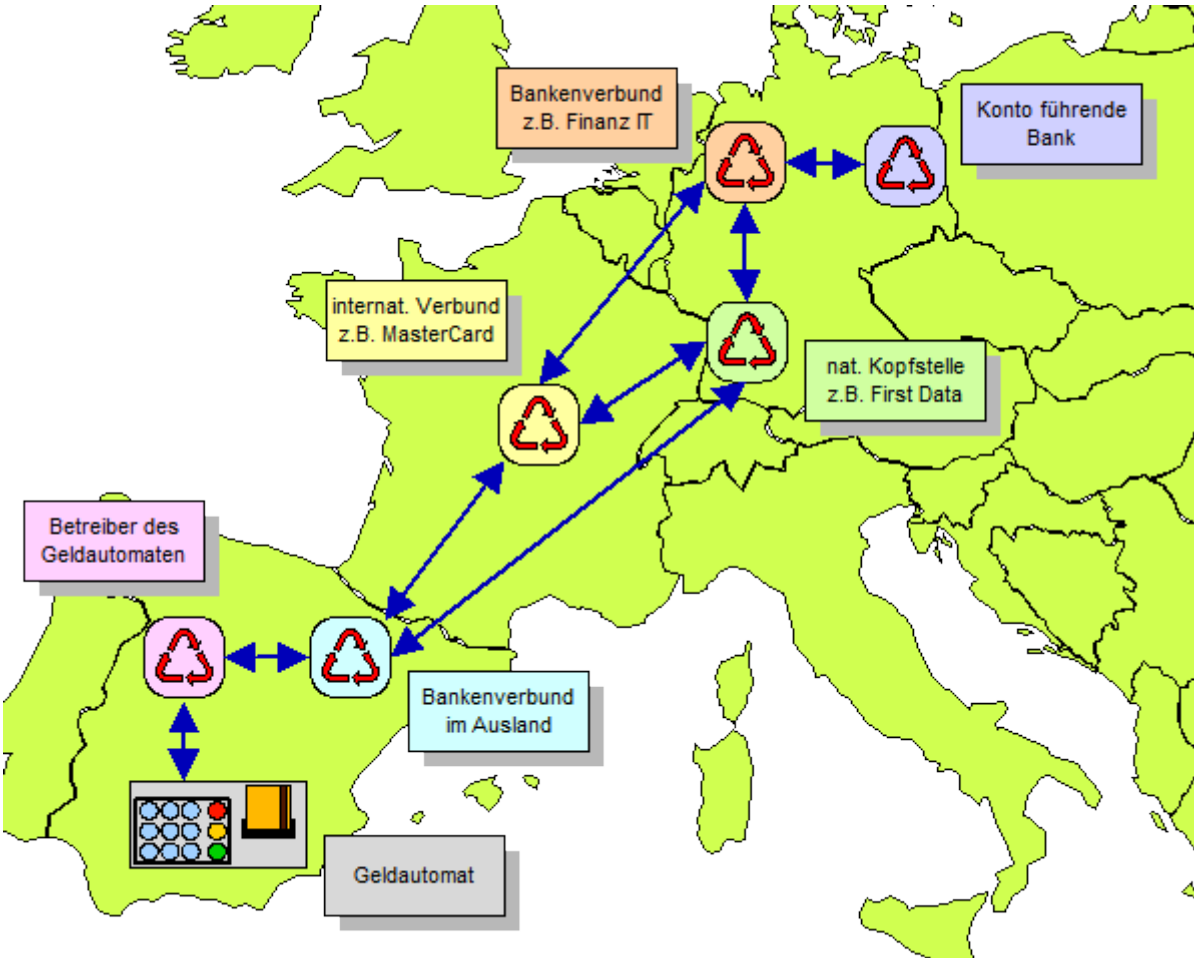
[56] CF, Turbulenzen beim bargeldlosen Zahlungsverkehr, 06.02.2010

[57] Mehrere Meldungen lassen daran Zweifel aufkommen:
PIN-Prüfung im EMV-Verfahren bei EC-und Kreditkarten ausgehebelt, Heise online 12.02.2010;
Bericht: PIN-Prüfung bei EC- und Kreditkarten unsicherer als angenommen, Heise online 19.01.2010;
Daniel Bachfeld, Phish & Chips, Angriff auf das EMV-Verfahren bei Bezahlkarten, c't 6/2010

[58] EC-Karten-Update soll Fehler beheben, c't 3/2010, S. 53; Update für EC-Karten, c't 4/2010, S. 54.

[59] Die Garantie war auf 400 DM beschränkt. Auch höhere Beträge konnten mit dem EC angewiesen werden, der überschießende Betrag war dann aber nicht von der Garantie der Bank umfasst.

[60] CF, Einzugsermächtigung und Lastschriftverfahren, 2007



Online-Verfahren beim bargeldlosen Zahlungsverkehr im Ausland. Der Geldautomat im Ausland übernimmt die Kartendaten, die PIN und den Auszahlungsbetrag und verbindet diese Daten mit der Gebühr, seiner eigenen Kennung und einem Zeitstempel zu einem Datensatz. Dieser Datensatz wird über die Bank, die den GAA betreibt und deren ausländischen Bankenverbund direkt, über einen internationalen Kartenverbund oder über die deutsche Kopfstelle (First Data) bis zum Rechenzentrum der kartenausgebenden Bank gesandt.

Das Rechenzentrum ist für die **Autorisierung** zuständig. Es prüft zunächst die Verfügungsberechtigung (**Authentifizierung**: Übereinstimmung zwischen Kartendaten, Prüfziffern und PIN) und dann die Validität des Kontos des Karteninhabers. Dazu gehört das Guthaben (Debitkarten, zum Beispiel bei Maestro), den Kreditrahmen und andere Verfügungsbeschränkungen (Tages- und Wochenlimit, Zulässigkeit von Auslandsverfügungen).

Zur Genehmigung der Transaktion sendet das Rechenzentrum den Code „0“. Damit garantiert das Rechenzentrum, dass die Auszahlung akzeptiert wird und frei von Beschränkungen im Innenverhältnis zwischen Bank und Karteninhaber ist.

Mit einem gewissen zeitlichen Verzug erfolgt das **Clearing**. In diesem Verfahren verrechnen die Kopfstellen und Bankenverbünde untereinander die saldierten Forderungen und Verbindlichkeiten. Dieser Prozess wurde schon im SWIFT-Verfahren durchgeführt und ist auch vom Roaming bei der mobilen Telefonie bekannt, wobei Clearinghouses die gegenseitigen Forderungen der Mobifunkunternehmen verrechnen.

Anschließend folgt im europäischen Verbund der Schadensausgleich. Dabei geht es darum, die Beteiligten mit geringeren Sicherheitsstandards zum Schadenersatz heranzuziehen. Wenn die Karte, deren Daten missbräuchlich verwendet wurden, zwar über einen EMV-Chip verfügt, der Betreiber des auszahlenden GAA aber nur den (gefälschten) Magnetstreifen prüft, dann trägt der Betreiber allein den Schaden für die Auszahlung.

Dieser Prozess hat zu dem wirtschaftlichen Druck geführt, dass die Betreiber von GAA in Süd- und Osteuropa jetzt flächendeckend Geräte einsetzen, die den EMV-Chip auslesen. Für die Cashing-Täter bedeutet das, dass sie nach Übersee ausweichen müssen. Irgendwann werden sie wahrscheinlich lernen, auch Falsifikate mit EMV-Chip herzustellen.

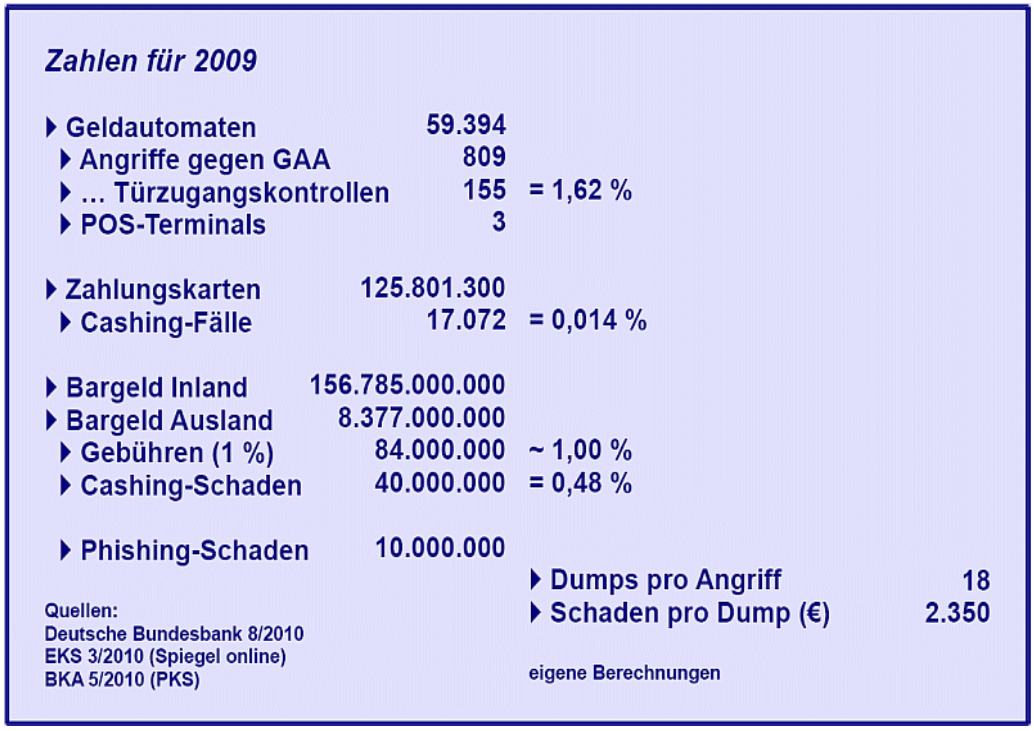


Schaubild links: Das Volumen des bargeldlosen Zahlungsverkehrs verdeutlicht, dass die Finanzwirtschaft auf ihn nicht mehr verzichten kann. Die jedenfalls in der Vergangenheit durch Cashing entstandenen Schäden sind zwar schmerzhaft, gegenüber dem Verkehrsvolumen und den erfolgten Personaleinsparungen jedoch eher als Erdnüsse zu betrachten.

Bei der Lastschrift verbleibt das Risiko bei dem Akzeptanten. Das Lastschriftverfahren ist noch immer im Einzelhandel vertreten, wenn zwar die Zahlungskarte des Kunden ausgelesen und geprüft wird, er jedoch mit seiner Unterschrift die Zahlung anweist [61].

Die heute übliche Autorisierung fußt auf dem Abbuchungsauftrag, der dem Akzeptanten eine höhere Auszahlungssicherheit gibt [62]. Im Alltag zeigt sich die Autorisierung darin, dass nicht nur die Zahlungskarte geprüft wird, sondern auch die PIN eingegeben werden muss. Die damit ausgelöste Prüfung erfolgt bei der kartenausgebenden Bank, der die Transaktionsdaten im elektronischen Onlineverfahren übermittelt werden und die einen Genehmigungscode zurückmeldet (Code „0“). Der Genehmigungscode ersetzt die im Euroscheck verkörperte Garantiefunktion und enthält eine Auszahlungsgarantie der kartenausgebenden Bank. Sie erklärt damit verbindlich, dass die Zahlungskarte akzeptiert wird und der geforderte Betrag zur Verfügung steht.

Der EMV-Chip lässt zwei weitere Autorisierungsverfahren zu [63]. Bei dem einen übermittelt der Chip eine kodierte Fassung der in ihm gespeicherten PIN, die im Terminal mit der Ziffernfolge verglichen wird, die per Tastatur eingegeben wurde. In dem anderen Fall übergibt das Terminal dem EMV-Chip die eingegebene PIN und der Microcomputer im Chip prüft sie gegen die gespeicherte Ziffernfolge. Am Ende gibt er einen Genehmigungscode an das Terminal zurück.

Für die strafrechtliche Praxis spielt das keine entscheidende Rolle, weil für sie die prinzipiellen Sicherheitsmerkmale und -prozesse ausschlaggebend sind und nicht der kriminelle Einsatz im Einzelfall. Bei der Frage nach der zivilrechtlichen Haftung kann das anders aussehen.

[61] Siehe auch BGH, Urteil vom 21.09.2000 – 4 StR 284/00, Rn 7.

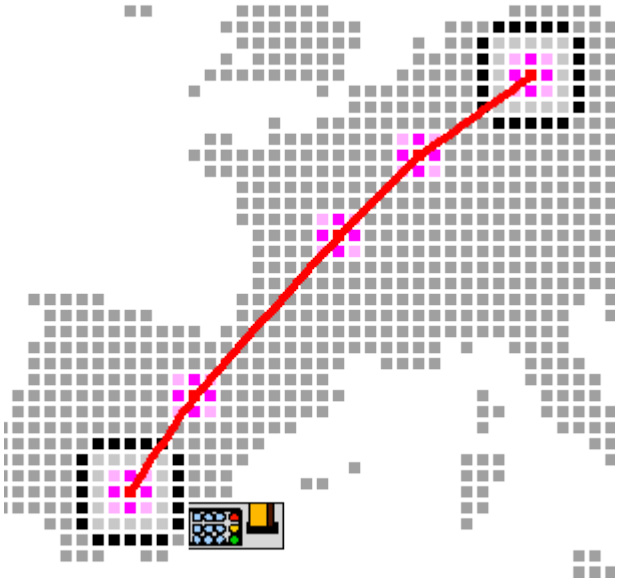
[62] Die Einzugsverfahren sind in das SEPA-Übereinkommen aufgenommen worden und gelten jetzt europaweit; siehe CF, Single Euro Payments Area, 26.01.2008.

[63] CF, eierlegende Wollmilchsau, 20.03.2011

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.

kartensicherheit.de



3. Autorisierung

Die wesentlichen Sicherungen für das Autorisierungsverfahren [64] bestehen in den Sicherheitsmerkmalen der Zahlungskarte, in der PIN und schließlich in dem Genehmigungscode, den die kartenausgebende Bank an den Akzeptanten meldet [65].

Zum Zweck der Autorisierung von Debitkarten [66] liest der ausländische Geldautomaten die Kartendaten aus, kombiniert sie mit der vom Kunden eingegeben PIN, dem Auszahlungsbetrag, der Gebühr, den Individualmerkmalen des Geldautomaten und der Uhrzeit. Der daraus gebildete Datensatz wird über Kommunikationsnetze und durch verschiedene Zwischenstellen (zum Beispiel in Deutschland: First Data Corporation [67], Finanz IT [68]) bis zur kartenausgebenden Bank geleitet [69]. Diese prüft, ob die Karte von ihr ausgestellt und nicht gesperrt ist, die Auszahlung im Ausland erlaubt, das Tages- oder Wochenlimit nicht überschritten sind und schließlich, ob Kontodeckung oder ein Überziehungskredit bestehen. Danach sendet die Bank an den Geldautomaten einen Genehmigungscode zurück [70], der die Auszahlung autorisiert und eine Garantie enthält, dass die autorisierende Bank für den Auszahlungsbetrag bürgt [71] [72].

4. Clearing

Nach der Autorisierung erfolgt bei Debitkarten in aller Regel keine unmittelbare Belastung des Kundenkontos, sondern eine Zwischenbuchung auf einem bankinternen Konto [73]. Nach der Auszahlung erfolgt im Bankenverbund über die Verbindungsstellen das Clearingverfahren, wobei die gegenseitig bestehenden Forderungen der Verbünde und schließlich der Institute unterein-

[64] Wegen der technischen Einzelheiten: ISO 8583 (Wikipedia).

[65] CF, Autorisierung im POS-Verfahren, 13.04.2009

[66] Gemeint sind Zahlungskarten auf Guthabenbasis, wobei als Guthaben auch der gewährte Überziehungskredit gilt.

[67] früher Gesellschaft für Zahlungssysteme - GZS

[68] Rechenzentrum der Sparkassen

[69] Siehe Glossar: Autorisierung, Clearing.

[70] Der Genehmigungscode lautet „0“. Andere Codeziffern belegen Zeitüberschreitungen, Kartensperren, Verwendungsbeschränkungen und andere Ereignisse. Sie führen immer dazu, dass die Transaktion verweigert wird.

[71] Siehe auch das Glossar bei kartensicherheit.de und das Zitat im Kasten oben.

[72] In dem Positionspapier strafbare Vorbereitung und Versuch beim Skimming habe ich noch angenommen, dass die Garantie von einer der zwischengeschalteten Clearingstellen geleistet wird. Das ist falsch. Die Garantie stammt immer von der Bank, die die Zahlungskarte ausgegeben und die einzelne Verfügung autorisiert hat.

[73] Conto pro Diverse – CPD

ander ausgeglichen werden. Am Ende wird die Zwischenbuchung der Hausbank gegen das Konto des Kunden aufgelöst.

Diese Buchung ist ein interner Vorgang, der die Verrechnung zwischen Bank und ihrem Kunden betrifft. Auf den Eintritt des Schadens im Sinne von § 263a StGB [74] hat sie keine Auswirkung.

5. Schadensausgleich

Beanstandet der Kunde eine Kontobelastung und ist diese auf den Einsatz einer gefälschten Zahlungskarte zurückzuführen, wird grundsätzlich ein Schadensausgleich durchgeführt, bei dem zunächst die Hausbank des Kunden die Belastung gegenbucht und diese Forderung bei der EURO Kartensysteme - EKS [75] - zum Ausgleich anmeldet. Stellt sich dabei heraus, dass der ausländische Geldautomat von einer Karte, deren Original mit einem EMV-Chip ausgestattet ist, nur den Magnetstreifen geprüft hat, dann haftet im europäischen Bankenverbund die ausländische Bank für den Schaden. Auf diese Weise wird ein wirtschaftlicher Druck auf die Betreiber von Geldautomaten aufgebaut, der sie zur Modernisierung ihrer Geräte und zur Verbesserung der Sicherheitsstandards drängt. Solange jedoch die Schäden aus dem Skimming das Gebührenaufkommen weit unterschreiten, bleibt der Druck für die Betreiber erträglich, muss man vermuten [76].

Dieser Anpassungsdruck funktioniert dann nicht mehr, wenn sich das Cashing in das entfernte Ausland verlagert, was zunehmend geschieht. Die Finanzwirtschaft wird dafür neue Formen der Sicherung und des Schadensausgleiches entwickeln müssen.

[74] Wegen der Einzelheiten: CF, Der Eingehungsschaden löst den Gefährdungsschaden ab, 16.02.2011.

[75] Siehe auch EKS – Analyse.

[76] CF, das Schweigen der L@mmer, 12.09.2010

6. Ergebnisse

Der erfolgreiche Missbrauch einer Zahlungskarte im Ausland, der sich in einer Kontobelastung beim deutschen Bankkunden äußert, belegt zugleich, dass eine erfolgreiche Autorisierung stattgefunden und die inländische Bank eine Auszahlung wegen ihres Gegenwertes garantiert hat (Autorisierung).

Daraus folgt ferner, dass im Ausland eine gefälschte Zahlungskarte, die gegen Fälschung besonders geschützt ist (Fälschungssicherung), mit Garantiefunktion verwendet wurde. Das qualifiziert die Tat zu einem Verbrechen gemäß § 152b Abs. 2 StGB mit einer Mindeststrafe von 2 Jahren Freiheitsstrafe, wobei ein gewerbsmäßiges Handeln in diesen Fällen grundsätzlich anzunehmen ist.

Der finanzwirtschaftliche Schadensausgleich hat dazu geführt, dass die durch das Skimming bei den Bankkunden eingetretenen Schäden im Bankenverbund ausgeglichen wurden. Dieses System wird jetzt einer besonderen Belastungsprobe ausgesetzt, weil sich das Cashing in das außereuropäische Ausland verlagert.

7. Innenverhältnis [77]

Zwischen der Bank als Zahlungsdienstleister – ZD – und dem Kunden als Zahlungsdienstnutzer besteht ein entgeltlicher Geschäftsbesorgungsvertrag (§ 675 BGB) in einer besonderen Ausgestaltung für Zahlungsdienste (§ 675c BGB). Daraus entsteht der Bank ein Anspruch auf Aufwendungsersatz (§§ 675c iVm 670 BGB) und auf das vereinbarte Entgelt (§ 675f BGB) [78].

Darauf beruht der Grundsatz, dass wegen Zahlungsvorgänge zunächst die Bank in Einstand tritt und ihr daraus eine Forderung gegen ihren Kunden erwächst. Für das Cashing bedeutet

[77] Dieses Kapitel ist neu in die dritte Auflage eingeführt worden. Es begründet die Abkehr von der Position in den Vorauflagen, wo noch davon ausgegangen wurde, dass der Schaden beim Bankkunden eintritt.

[78] Siehe im Ergebnis auch schon: BGH, Urteil vom 05.10.2004 - XI ZR 210/03.

das, dass der Schaden zum Nachteil der Karten ausgebenden Bank eintritt. Sie garantiert die Auszahlung gegenüber dem ausländischen GAA-Betreiber und wird nicht unverzüglich frei von der Zahllast [79].

Voraussetzung für den Anspruch ist die erfolgreiche Autorisierung der Anweisung durch den ZD (§ 675j Abs. 1 BGB) und die Mitteilung an den Kunden (§ 675d BGB). Der ZD haftet wegen unautorisierter Zahlungen und hat in diesen Fällen das Zahlungskonto wieder auf den vorigen Stand zu bringen (§ 675u BGB).

Das hat eine besondere Bedeutung dann, wenn Zahlungsautorisierungsinstrumente – ZAI – zum Einsatz kommen (§ 675l BGB). Dahinter verbergen sich keine anderen Techniken als die, die von den Zahlungskarten bekannt sind: Das sind die Kartendaten auf dem Magnetstreifen und dem EMV-Chip auf Kredit- und Debitkarten sowie die PIN (Kundenkennung, § 675r Abs. 1 BGB), die dem Kunden ausgehändigt werden. Während das Übersendungsrisiko dem ZD obliegt (§ 675m BGB), hat der Kunde für den Schutz der ZAI „alle zumutbaren Vorkehrungen“ zu treffen (§ 675l BGB).

Die Haftungsverhältnisse werden besonders deutlich anhand der Haftungszuweisungen beim Verlust und Diebstahl der ZAI: Solange der Kunde den Verlust nicht angezeigt hat, kann er bis zu 150 € je autorisierter Verfügung haften (§ 675v Abs. 1 S. 1 BGB), nach der Meldung (§ 675l S. 2 BGB) haftet er nicht mehr (§ 675v Abs. 3 S. 1 BGB). Zusätzlich muss der ZD die Authentifizierung nachweisen (§ 675w BGB), wozu allein der Nachweis, dass ein ZAI genutzt wurde, nicht genügt (§ 675w S. 3 BGB). Im Streit ist der ZD nachweispflichtig (§ 676 BGB).

Die verschiedenen Haftungszuweisungen lassen erkennen, dass durch die Verrechnung zulasten des Kundenkontos noch keine schadensverhindernde Kompensation eintritt. Diese wird angenommen, wenn durch die Verfügung – hier: Autorisierung der Bank – zugleich auch ein wertgleicher Anspruch erwächst. Dabei kann es sich zum Beispiel um eine Ausfallversicherung oder einen Pfand handeln [80]. Der Anspruch der Bank ist hingegen nicht einwendungsfrei, wie zum Beispiel der Erstattungsanspruch des „Zahlers“ belegt (§ 675x BGB). Die spätere Kompensation durch den Bankenverbund verhindert den Schadenseintritt nicht [81].

Im Zusammenhang mit dem Cashing, also dem Gebrauch gefälschter Zahlungskarten mit Garantiefunktion in Tateinheit mit Computerbetrug (§§ 152b Abs. 1, 263a Abs. 1 StGB), erleidet der Kunde nicht etwa dadurch einen Schaden, dass sein Verfügungsrahmen beschränkt wird. Insoweit handelt es sich nur um eine Einschränkung der Dispositionsfreiheit, mit der kein vermögensrechtlicher Schaden verbunden ist [82].

Die praktische Konsequenz für die Ermittlungen ist, dass wegen des Schadens das Augenmerk auf die betroffenen Banken zu richten ist. Es kommt deshalb nicht darauf an, ob die Bank direkt gegen das Kundenkonto bucht oder zunächst gegen ein CPD (conto pro diverse), sondern nur darauf, dass sie das missbrauchte ZAI authentifiziert und die Auszahlung autorisiert hat. Ermittlungen gegenüber den Bankkunden zum Nachweis des Schadenseintritts sind deshalb nicht erforderlich. Sie müssen allenfalls wegen der eigenen Geldabhebungen befragt werden, um das Skimming im engeren Sinne nachzuweisen (Ausspähen der Kartendaten und der PIN). Dazu geben die Journale aus den Geldautomaten im Zusammenhang mit der Tatsache, dass die ZAI später missbraucht wurden, bereits hinreichend Beweis.

Die weitere Konsequenz daraus ist, dass zwischen Kredit- und Debitkarten kein Unterschied gemacht werden muss. Diese Vertragsverhältnisse betreffen nur das Innenverhältnis zwischen

[79] Es tritt keine schadensverhindernde Kompensation ein. Darauf wird weiter unten eingegangen.

[80] Fischer, § 263 StGB, Rn 111

[81] Fischer, § 263 StGB, Rn 111a

[82] BGH, Beschluss vom 14.04.2011 – 1 StR 458/10, Rn 33;
BGH, Urteil vom 24.06.2010 – 3 StR 90/10, Rn 18 [Untreue].

Ins Gewicht fällt vielmehr, dass die Täter *vor Ort bezüglich des gesamten Ausspähens der Daten beim Einbau, der Kontrolle sowie den Abbau der erforderlichen Geräte auf sich allein gestellt waren und damit über einen längeren Zeitraum jedenfalls teilweise durchaus komplexe, besondere Kenntnisse und Fähigkeiten erfordernde Handlungen zu verrichten hatten, die zudem für sie mit einem im Vergleich zu den übrigen Beteiligten besonderen Entdeckungsrisiko verbunden waren.*

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.

BGH, Urteil vom 17.02.2011 – 3 StR 419/10, Rn 4

Ich habe meine Tante im Krankenhaus besucht. Sie hat es ja schwer an den Beinen und kann nur hier in Deutschland richtig behandelt werden. Irgendwann bin ich dann runter vor die Tür, um eine Zigarette zu rauchen. Plötzlich stand so ein Typ im grünen Kittel neben mir, rauchte hastig auch 'ne Zigarette und sprach davon, dass er üblen Stress habe. Die OP würde kein Ende nehmen und der nächste Patient läge bereits im anderen OP.

Dann schaute er mich direkt an und sagte, Mensch, ich könne ihm helfen, das sei ganz einfach. Ich müsse nur ein Skalpell nehmen, den Bauch aufschneiden, den Blinddarm raus nehmen und dann würde mir die OP-Schwester dabei helfen, alles wieder zuzunähen.

Das habe ich dann gemacht, ich bin ja Kumpel, und der Typ hat mir nachher 50 Euro gegeben.

Glosse aus dem Schlussvortrag zu: LG Hannover, Urteil vom 17.11.2009 - 6403 Js 43834/09

der Bank und ihrem Kunden. Wegen des Cashings kommt es hingegen nur darauf an, dass die Bank im Rahmen ihrer Garantiefunktion gegenüber dem (dritten) Betreiber eines GAA den Forderungsausgleich zusagt und damit die Zahllast für den Auszahlungsbetrag trägt.

Das gilt auch für das Phishing im Zusammenhang mit dem Onlinebanking-Betrug. Die Bank als ZD trägt das Verfügungsrisiko. Der Anscheinsbeweis beim Einsatz von ZAI (Kontozugangsdaten und TAN) spricht für eine Verfügung ihres Kunden (Anscheinsbeweis). Dagegen kann er aber wirksam einwenden, dass die Verfügung ungewöhnlich ist für sein Zahlverhalten. Damit geht das Beweisrisiko wieder auf die Bank über [83].

Einen Unterschied gibt es nur wegen der Lastschrift. Das Risiko trägt allein der Akzeptant (zum Beispiel: Einzelhändler), der seine Forderung ohne Autorisierung im Onlineverfahren einzieht.

[83] Wegen der tatsächlichen Abläufe siehe: Dieter Kochheim, IuK-Strafrecht, Oktober 2011.

8. arbeitsteilige Handlungen beim Skimming

Das Skimming ist geprägt von verschiedenen Tathandlungen, die in der Grafik auf Seite 12 wegen ihrer wesentlichen Merkmale zusammengefasst werden.

Am Anfang steht die Herstellung der Ausspähtechnik. Dazu gehören Kartenlesegeräte, die später am Geldautomaten, an der Eingangskontrolle oder am Kontoauszugsdrucker installiert werden. Für das Ausspähen der PIN werden entweder Kameras, Tastaturaufsätze oder elektronische Bauteile verwendet.

Alle Geräte müssen so getarnt werden, dass sie den Kunden auf dem ersten Blick nicht auffallen. Die Täter müssen deshalb zunächst auskundschaften, welche Geldautomaten und Umgebungen für den Einsatz ihrer Geräte geeignet sind. Die Baureihen der Geldautomaten lassen sich verschiedenen Bankverbünden zuordnen, so dass häufig zunächst eine Recherche im Internet erfolgt. Zur Vorbereitung und während der Installation der technischen Geräte müssen gelegentlich Anpassungen am Geldautomaten oder am kriminellen Gerät vorgenommen werden, die auf ein erhebliches Fach- und Erfahrungswissen der Installateure schließen lassen.

Zwei Tatphasen finden in der Öffentlichkeit statt. Das ist zunächst das eigentliche Ausspähen der Zugangsdaten, für das sich der Begriff des Skimmings (im engeren Sinne) eingebürgert hat. Es umfasst die Installation der Ausspähtechnik, das Ausspähen selber und den Abbau der (wertvollen) Geräte. Entsprechend der eingesetzten Technik müssen die Geräte während des Ausspähens überprüft werden. Besonders dann, wenn der Abgriff der Kartendaten nicht direkt am Geldautomaten erfolgt, müssen die ausgespähten Kartendaten und PIN synchronisiert werden. Das erfolgt häufig in der Weise, dass die Täter Testkarten einsetzen, deren Merkmale ihnen geläufig sind, und damit Marker in ihr Listenwerk setzen.

Die Übermittlung der ausgespähten Daten erfolgt in aller Regel per E-Mail oder anderen Kommunikationstechniken des Internets. Das erklärt auch, warum zwischen dem Ausspähen und dem Cashing häufig nur wenige Stunden vergehen [84].

Je nach dem Erfolg des Ausspähens werden die Kundendaten einer oder mehrerer Skimmingangriffe zusammengefasst und mit ihnen Dubletten angefertigt. Es handelt sich meistens um unbedruckte WhiteCards, die nur über einen Magnetstreifen verfügen und damit den einfachsten Anforderungen der ISO-Norm für Identitätsdokumente genügen. Die dazu erforderliche Technik und das Zubehör sind im Einzelhandel erhältlich.

Die zweite Tatphase in der Öffentlichkeit wird als das Cashing bezeichnet. Dabei werden die Dubletten „gebraucht“, um Auszahlungen an Geldautomaten zu bewirken.

Die in Deutschland üblichen Sicherheitsmerkmale, das sind vor allem das im Kartenkörper eingebrachte Maschinenlesbare Merkmal – MM – und der EMV-Chip, machen es erforderlich, dass die Dubletten im Ausland eingesetzt werden, wo die Geldautomaten sie nicht prüfen. Das zeigt, dass auch das Cashing selber die Auskundschaftung geeigneter Geldautomaten erfordert.

Die gewandelten Erscheinungsformen beim Ausspähen zeigen, dass diese Kriminalitätsform Wandlungen unterworfen ist, die besonders das Ausspähen selber betreffen. Verfeinerte Prüfungen der Sicherheitsmerkmale und der beschriebene Schadensausgleich lassen vermuten, dass sich das Cashing in immer weiter entfernte Länder und Kontinente verlagern wird.

Das Cashing ist aus krimineller Sicht ein äußerst effektives Instrument der Beuterealisierung. Es ist zu erwarten, dass es uns noch lange erhalten bleibt.

9. EMV-Chip

Besonders die deutsche Finanzwirtschaft hat einige mächtige Anstrengungen unternommen, um die Sicherheit der Zahlungskarten für den bargeldlosen Zahlungsverkehr zu erhöhen.

Das gilt in erster Linie für das modulierte Merkmal – MM. Die Merkmalstoffe im Plastikkörper der Karte lassen sich anhand ihrer physikalischen Eigenschaften messen und bilden damit einen Code, der einem Code entsprechen muss, der verschlüsselt auf dem Magnetstreifen und im EMV-Chip gespeichert ist [85]. Dieses Prüfverfahren, das verlässlich das Cashing mit inländischen Kartendaten im Inland ausschließt, wird leider nur in Deutschland eingesetzt.

Ihm vergleichbar ist die digitale Kartenprüfnummer – CVV, die mit unterschiedlichen Kodierungen auf dem Magnetstreifen und im EMV-Chip gespeichert ist [86]. Sie wird im förmlichen Autorisierungsverfahren geprüft und verhindert durch ihre unterschiedliche Kodierung, dass aus dem EMV-Chip ausgelesene Daten mit einer White Card missbraucht werden können, die nur über einen Magnetstreifen verfügt.

Die Postbank ist 2011 dazu übergegangen, ihren Kunden nur noch Zahlungskarten mit EMV-Chip und ohne Magnetstreifen auszuliefern. Europa und die beliebtesten Urlaubsgebiete sollen darauf bereits eingestellt sein. Wenn der Kunde in die USA oder ein anderes Land reisen will, das den EMV-Chip nicht flächendeckend akzeptiert,

[84] Siehe jetzt: BGH, Urteil vom 17.02.2011 – 3 StR 419/10

[85] CF, Sicherheitsmerkmale und Merkmalstoffe, 06.02.2010

[86] CF, Quellenkritik an Heise, 09.04.2011

dann kann er eine weitere Karte mit Magnetstreifen erhalten.

Der Umstieg ist ziemlich lautlos erfolgt. Es war vor Allem der Einzelhandel, der an POS-Terminals festgehalten hat, die noch 2010 überwiegend nur den Magnetstreifen auslesen konnten.

Die Skimming-Täter haben ihre Probleme mit den Umstellungen und das Cashing ist im ersten Halbjahr 2011 zunächst zurück gegangen und hat sich auf das außereuropäische Ausland verlagert. Das ist schmerzhaft für die hiesige Finanzwirtschaft, weil dort die Regeln des europäischen Bankenverbundes für den Schadensausgleich nicht gelten. Er hat zur technischen Aufrüstung geführt und die europäischen Geldautomaten fast flächendeckend EMV-fähig gemacht.

Die Carding-erprobten Täter werden aufrüsten, sich zunächst auf das Auslesen der EMV-Chips und dann darauf konzentrieren, sie nachzumachen. Andere werden den Missbrauch ausgespähter Zahlungsverkehrsdaten verstärkt im Zusammenhang mit Online-Transaktionen anwenden, wo die physischen Sicherheitsmerkmale nicht greifen.

Den künftigen EMV-Cashern wird ein Geburtsfehler des EMV-Chips helfen: Er kann zu viel und lässt zu viele Ausnahmen zu [87]. Mehrere Laborversuche haben gezeigt, dass die Schwächen der Terminals (Geldautomat, POS-Terminal) die eigentlich starken Sicherheitsmechanismen im EMV-Chip aushebeln können. So ist es prinzipiell möglich, dass die PIN unverschlüsselt aus dem Chip ausgelesen oder an den Chip vermittelt werden kann. Unter Sicherheitsaspekten fatal ist, dass der EMV-Chip umprogrammierbar ist und eine On-Board-Autorisierung zulässt. Hierbei prüft der Chip mit der ihm eingebauten Elektronik („Intelligenz“) die eingegebene PIN gegen die, die in ihm gespeichert ist. Das Terminal wartet dann nur noch auf den Genehmigungscode "0x9000", den jeder Man-in-the-Middle oder eine spezialisierte Malware vortäuschen kann.

[87] CF, eierlegende Wollmilchsau, 20.03.2011

C. Strafbarkeit

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 [88] („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 [89], die verschlüsselten Prüfziffern für die PIN sowie das Modulierte Merkmal – MM [90], das eine Besonderheit bei den von deutschen Banken herausgegebenen Karten ist. Die von § 152b StGB geforderte Garantiefunktion verbirgt sich jetzt in dem Autorisierungsverfahren und die mit ihm verbundene Genehmigung der kartenausstellenden Bank gegenüber der Zahlstelle im POS-Verfahren [91]. Es ist an die Stelle der früher üblichen Euroschecks getreten.

Der erstrebte Taterfolg besteht im erfolgreichen 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 [92]. 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.

1. arbeitsteiliges Vorgehen

Der Tatplan beim Skimming umfasst bei einer groben Unterteilung drei Arbeitsschritte:

1) Ausspähen von PIN und Kartendaten

2) Fälschung von Zahlungskarten

3) Missbrauch der gefälschten Zahlungskarten

Vor dem Arbeitsschritt 1) ist die Herstellung der teilweise handwerklich anspruchsvollen Skimming-Hardware angesiedelt und nach dem Arbeitsschritt 3) die Beuteverteilung, wenn es sich – wie üblich – um eine arbeitsteilig aufgestellte Gruppe von Tätern handelt.

Das arbeitsteilige und wiederholte Vorgehen beim Skimming rechtfertigt regelmäßig die Annahme die Mittäterschaft und das gewerbsmäßige Handeln [93]. Einzeltäter, die alle Arbeitsschritte persönlich ausüben, treten allenfalls vereinzelt auf. In aller Regel haben wir es mit Tätergruppen zu tun, die sich nur deshalb zusammentun, um eine dauerhafte Einnahmequelle zu haben. Das wird auch von den Schäden durch Cashing-Aktionen belegt, bei denen mehrere Täter gleichzeitig handeln und binnen weniger Tage mehrere Zehntausend Euro erbeutet haben.

---

[88] BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn. 11

[89] 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.

[90] 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.

[91] Siehe Glossar: POS

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

[93] Siehe Zitat im Kasten oben rechts: BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5.

*Nach § 27 Abs. 1 StGB macht sich wegen **Beihilfe** strafbar, wer (vorsätzlich) einem anderen zu dessen (vorsätzlich begangener) rechtswidriger Tat Hilfe leistet. Nach ständiger Rechtsprechung (...) ist als Hilfeleistung in diesem Sinne grundsätzlich jede Handlung anzusehen, die die Herbeiführung des Taterfolges durch den Haupttäter objektiv fördert oder erleichtert; dass sie für den Eintritt dieses Erfolges in seinem konkreten Gepräge in irgendeiner Weise kausal wird, ist nicht erforderlich (...). Es genügt, dass ein Gehilfe die Haupttat im Vorbereitungsstadium fördert, wenn die Teilnahmehandlung mit entsprechendem Förderungswillen und -bewusstsein vorgenommen wird (...). Beihilfe zu einer Tat kann schließlich schon dadurch geleistet werden, dass der Gehilfe den Haupttäter in seinem schon gefassten Tat-entschluss bestärkt und ihm ein erhöhtes Gefühl der Sicherheit vermittelt* (...).

BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09

***Mittäter** nach § 25 Abs. 2 StGB ist, wer nicht nur fremdes Tun fördert, sondern einen eigenen Beitrag derart in eine gemeinschaftliche Tat einfügt, dass dieser als Teil der Tätigkeit des anderen und umgekehrt dessen Tun als Ergänzung seines eigenen Tatanteils erscheint. Ob ein Beteiligter ein so enges Verhältnis zur Tat hat, ist nach den gesamten Umständen, die von seiner Vorstellung umfasst sind, in wertender Betrachtung zu beurteilen (...). Wesentliche Anhaltspunkte können der Grad des eigenen Interesses am Taterfolg, der Umfang der Tatbeteiligung und die Tatherrschaft oder wenigstens der Wille zur Tatherrschaft sein; Durchführung und Ausgang der Tat müssen somit zumindest aus der subjektiven Sicht des Tatbeteiligten maßgeblich auch von seinem Willen abhängen. Dabei deutet eine ganz untergeordnete Tätigkeit schon objektiv darauf hin, dass der Beteiligte nur Gehilfe ist (st. Rspr. ...).*

BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09

***Gewerbsmäßig** handelt, wer sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen will. Liegt diese Absicht vor, ist bereits die erste Tat als gewerbsmäßig begangen einzustufen, auch wenn es entgegen den ursprünglichen Intentionen des Täters zu weiteren Taten nicht kommt. Eine Verurteilung wegen gewerbsmäßiger Deliktsbegehung setzt daher schon im Grundsatz nicht notwendig voraus, dass der Täter zur Gewinnerzielung mehrere selbstständige Einzeltaten der jeweils in Rede stehenden Art verwirklicht hat. Ob der Angeklagte gewerbsmäßig gehandelt hat, beurteilt sich vielmehr nach seinen ursprünglichen Planungen sowie seinem tatsächlichen, strafrechtlich relevanten Verhalten über den gesamten ihm anzulastenden Tatzeitraum (...). Erforderlich ist dabei stets, dass sich seine Wiederholungsabsicht auf dasjenige Delikt bezieht, dessen Tatbestand durch das Merkmal der Gewerbsmäßigkeit qualifiziert ist.*

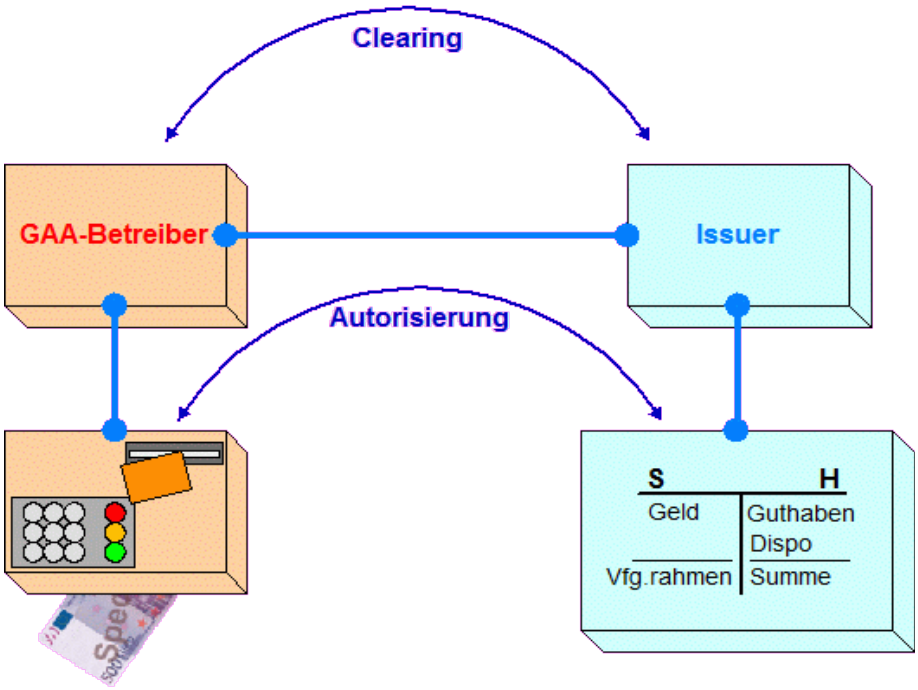
BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5

*Eine **Bande** ist danach gekennzeichnet durch den Zusammenschluss von mindestens drei Personen, die sich mit dem Willen verbunden haben, künftig für eine gewisse Dauer mehrere selbstständige, im Einzelnen noch ungewisse Straftaten zu begehen; ein gefestigter Bandenwille und ein Tätigwerden in einem übergeordneten Bandeninteresse sind demgegenüber nicht mehr erforderlich (...). Nach deutschem Recht ist indes allein die Mitgliedschaft in einer Bande nicht strafbar; vielmehr führt das Handeln als Bandenmitglied (lediglich) dazu, dass der Täter nicht nur einen strafrechtlichen Grundtatbestand erfüllt, sondern ein Qualifikationsmerkmal. … Die Mitgliedschaft in einer Bande ist deshalb kein strafbegründendes, sondern ein strafschärfendes Merkmal.*

BGH, Urteil vom 03.12.2009 - 3 StR 277/09, S.18

***Bedingt vorsätzliches Handeln** setzt voraus, dass der Täter den Eintritt des tatbestandlichen Erfolges als möglich und nicht ganz fern liegend erkennt, ferner, dass er ihn billigt oder sich um des erstrebten Zieles willen mit der Tatbestandsverwirklichung zumindest abfindet. Da die Schuldformen des bedingten Vorsatzes und der bewussten Fahrlässigkeit im Grenzbereich eng beieinander liegen, müssen bei der Annahme bedingten Vorsatzes beide Elemente der inneren Tatseite, also sowohl das Wissens- als auch das Willenselement, umfassend geprüft und gegebenenfalls durch tatsächliche Feststellungen belegt werden.*

BGH, Urteil vom 28.01.2010 - 3 StR 533/09, Rn 5



Die Genehmigung im Rahmen der Autorisierung verpflichtet die Karten ausgebende Bank (Issuer) zur Zahlung an den Akzeptanten. Bei ihr tritt der Betrugsschaden wegen des Auszahlungsbetrages und der Gebühren ein.

Die anschließende Buchung gegen das Konto des Kunden oder ein CPD verringert zwar den Verfügungsrahmen, stellt aber nur eine Beschränkung der Dispositionsfreiheit dar, die nicht als vermögensrechtlicher Schaden angesehen wird.

2. einschlägige Normen und Konkurrenzen

Das Fälschen von Zahlungskarten und ihren Gebrauch hat der Gesetzgeber neben die Vorschriften über das Fälschen von Geld und Wertzeichen gestellt (§§ 146 ff. StGB). Die Strafvorschriften dienen der Sicherheit und Funktionsfähigkeit des bargeldlosen Zahlungsverkehrs [94]. Die hohen Mindestfreiheitsstrafen, mit denen die §§ 152b Abs. 1, Abs. 2 StGB drohen, sind von Verfassungs wegen nicht zu beanstanden [95].

Die Missbrauchshandlung beim Skimming (Cashing) ist im Grunddelikt der Gebrauch falscher inländischer oder ausländischer Zahlungskarten gemäß § 152a Abs. 1 Nr. 2 StGB [96]. In Tateinheit [97] damit steht der Computerbetrug gemäß § 263a StGB [98], dessen Vollendung mit der Auszahlung am Geldautomaten eintritt [99].

Die Fälschung von Zahlungskarten mit Garantiefunktion ist ein selbständiger Verbrechenstatbestand (§§ 152b Abs. 1, 12 Abs. 1 StGB), der immer auch die Strafbarkeit des Versuchs umfasst (§ 23 Abs. 1 StGB). Unter der Voraussetzung der Gewerbsmäßigkeit erhöht sich die Mindeststrafe auf 2 Jahre Freiheitsstrafe (§ 152b Abs. 2 StGB).

Der Computerbetrug im Zusammenhang mit dem Cashing ist ein besonders schwerer Fall, der sich vom Grundtatbestand des § 263a Abs. 1 StGB in aller Regel durch das weitere Merkmal der Gewerbsmäßigkeit abhebt. Er ist auch in dieser Form als Vergehen zu behandeln (§ 12 Abs. 1 StGB), so dass das Gesetz die Strafbarkeit des

[94] BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 11.

[95] BVerfG, Beschluss vom 18.03.2009 - 2 BvR 1350/08; siehe auch CF, Fälschung von Zahlungskarten, 01.05.2009.

[96] Strafrahmen: Geldstrafe bis 5 Jahre Freiheitsstrafe.

[97] Zur Tateinheit zwischen dem Gebrauch gefälschter Zahlungskarten (§ 152a StGB) und Betrug (§ 263 StGB): BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 17.

[98] Fallgruppe: Unbefugte Verwendung von Daten. BGH, Urteil vom 10.05.2005 – 3 StR 425/04, S. 8. Siehe auch: BGH, Beschluss vom 13.01.2010 - 4 StR 378/09.

[99] Tateinheit: BGH, Beschluss vom 23.06.2010 – 2 StR 243/10, Rn 3. In der Entscheidung wird kommentarlos die falsche Strafvorschrift wegen der Fälschung von Zahlungskarten mit Garantiefunktion angewendet, nämlich § 152a StGB anstelle von § 152b StGB. Das scheint auch der Staatsanwaltschaft Aachen entgangen zu sein, die das Urteil mit seiner sowieso schon *milde(n) Gesamtfreiheitsstrafe von drei Jahren* (BGH, Rn 7) nicht angegriffen hat.

Versuchs besonders anordnen muss (§ 23 Abs. 1 StGB). Das erfolgt in § 263 Abs. 2 StGB, auf den der § 263a Abs. 2 StGB ausdrücklich verweist.

Dagegen tritt die Fälschung beweiserheblicher Daten gemäß § 269 StGB hinter der spezielleren Vorschrift des § 152a Abs. 1 Nr. 1 StGB zurück [100]. Das mit ihr verbundene „Speichern" realisiert sich nur bei der Fälschung selber und nicht auch beim Missbrauch der gefälschten Zahlungskarten.

Bei genauer Betrachtung greifen auch die Datendelikte nach § 202a und § 202b StGB im Zusammenhang mit dem Skimming nicht.

2.1 Ausspähen von Daten

§ 202a Abs. 1 StGB kommt wegen des Ausspähens der Daten auf den Magnetstreifen der Zahlungskarten der betroffenen Bankkunden nicht in Betracht, weil ihm eine besondere Sicherungsfunktion fehlt [101]. Die gespeicherten Daten können in aller Regel mit handelsüblichen Lesegeräten und Komponenten ausgelesen werden können. Andere Senate des Gerichts sind dem inzwischen beigetreten, der 1. Strafsenat jedoch mit der Einschränkung, *dass die Voraussetzungen des § 202a StGB ... dann nicht gegeben sind, wenn die zum Auslesen benutzte Software auch im regulären Handel erhältlich ist* [102].

2.2 Abfangen von Daten

Die ausgespähten Kartendaten werden zum Fälschen von Zahlungskarten benötigt und die PIN zum später einsetzenden Gebrauch. § 149 Abs. 1 StGB beschränkt den Anwendungsbereich für die Haftung im Vorbereitungsstadium auf die Fälschung und bezieht nicht auch den Gebrauch mit ein. Daraus folgt, dass keine Strafbarkeit wegen des Umgangs mit Geräten zum Ausspähen der PIN aus § 149 StGB abgeleitet werden kann.

Wegen des Ausspähens der PIN greift auch das Hackerstrafrecht nicht, wenn es unmittelbar angewendet wird. Es handelt sich dabei weder um ein Ausspähen von Daten gemäß § 202a Abs. 1 StGB noch um ein Abfangen von Daten gemäß § 202b StGB., auf die § 202c StGB ausdrücklich anspricht. Verantwortlich dafür ist auch die Definition von „Daten" in § 202a Abs. 2 StGB. Das sind nur solche Daten, die bereits gespeichert sind oder übermittelt werden. Das Übermitteln setzt jedoch eine vorherige Speicherung voraus.

Beim Skimming wird die PIN aber bei der ***Eingabe*** ausgespäht. Dieser Vorgang ist der Speicherung und der Übermittlung vorgelagert.

2.3 PIN-Skimming und Computersabotage

Das Cashing ist bei der Eingabe von Daten mit dem Ziel verbunden, einem Anderen Nachteil zuzufügen, und deshalb auch ein Anwendungsfall der Computersabotage gemäß § 303b Abs. 1 Nr. 2 StGB [103]. Diese Strafvorschrift wird im Zusammenhang mit dem Cashing vom Computerbetrug als dem spezielleren und schwereren Vorwurf verdrängt.

§ 303b Abs. 5 StGB erweitert jedoch die Strafbarkeit auch auf das Vorbereitungsstadium, indem er auf § 202c StGB verweist. Dadurch werden nicht nur Computerprogramme geschützt, sondern ausdrücklich auch Passwörter und

---

[100] Grundsätzlich zum Verhältnis zwischen Urkunden- und Zahlungsmittelfälschung: BGH, Beschluss vom 26.01.2005 - 2 StR 516/04.

[101] BGH, Beschluss vom 18.03.2010 - 4 StR 555/09, CF, Ausspähen von Daten und das Skimming, 14.05.2010;
überholte Auffassung: BGH, Urteil vom 10.05.2005 – 3 StR 425/04, S. 7

[102] BGH, Beschluss vom 19.05.2010 - 1 ARs 6/10; CF, Ausspähen von Magnetstreifen, 02.07.2010

[103] Dieser Tatbestand ist auch deshalb außergewöhnlich, weil er die Tathandlungen nicht auf das Schadensereignis bezieht, sondern auf die Zuleitung und Eingabe vorverlagert. Weitere Einzelheiten:
Dieter Kochheim, IuK-Strafrecht, 29.10.2011, S. 37.

sonstiger Sicherungscode (§ 202c Abs. 1 Nr. 1 StGB). Der Umgang mit ihnen mit dem Ziel, sie zum Cashing zu verwenden, steht unter Strafe [104] und wird mit einer Höchststrafe von einem Jahr Freiheitsstrafe bedroht.

Die Schutzrichtung dieser Normen beschränkt sich jedoch auf Computer***programme*** einerseits und PIN (als Passwörter) andererseits, nicht aber auch auf die zum Ausspähen genutzten Geräte als Hardware.

Das Sich-Verschaffen von PIN ist somit gemäß § 303b Abs. 5 StGB in Verbindung mit § 202c StGB strafbar. Es verlangt nach dem Nachweis, dass tatsächlich PIN ausgespäht wurden.

2.4 natürliche Handlungseinheiten

Aus dem Begriff „dieselbe Tat“ (§ 52 Abs. 1 StGB) leitet die Rechtsprechung die ***natürliche Handlungseinheit*** ab, wobei *mehrere Verhaltensweisen von einem einheitlichen Willen getragen werden und räumlich-zeitlich so eng miteinander verbunden sind, dass das gesamte Tätigwerden objektiv als ein einheitliches und zusammengehöriges Tun erscheint* [105]. Sie darf nicht mit der fortgesetzten Handlung verwechselt werden, womit von der Rechtsprechung gleichartige Taten mit weitem räumlich-zeitlichem Zusammenhang zusammengefasst wurden. Die Handlungsform der fortgesetzten Handlung hat der BGH 1994 aufgegeben [106], nicht zuletzt deshalb, weil sie erhebliche Nachteile für die Angeklagten barg [107].

Eine besondere Ausprägung der Handlungseinheit hat der BGH im Zusammenhang mit Betäubungsmittelstraftaten entwickelt. Insoweit spricht er von einer ***Bewertungseinheit*** und fasst damit alle Veräußerungshandlungen des Täters zusammen, wenn das Rauschgift aus derselben Quelle stammt, also aus einer einmaligen Erwerbstat [108].

Wenn die Kartendaten an verschiedenen Geldautomaten und an verschiedenen Tagen ausgespäht werden, dann besteht grundsätzlich Tatmehrheit [109]. Das gilt jedenfalls dann, wenn die gefälschten Karten zeitnah zum Cashing eingesetzt wurden.

Im Zusammenhang mit dem Skimming spricht der BGH von ***deliktischen Einheiten***, die einerseits zwischen dem Gebrauchen nachgemachter Zahlungskarten und dem damit verbundenen Betrug und andererseits zwischen den Tathandlungen des Nachmachens und des Gebrauchens im Sinne von § 152a Abs. 1 StGB bestehen, soweit sie räumlich-zeitlich eng verbunden und von einem einheitlichen Vorsatz umschlossen sind [110]. Solche deliktischen Einheiten können auch die gleichzeitig Fälschung mehrerer Karten [111] und ihren Gebrauch beim Cashing bilden [112].

Die praktische Konsequenz daraus ist, dass als eine materielle Tat alle Fälschungen, alle Missbräuche von Zahlungskarten und alle unmittelbar aufeinander folgenden Ausspähungen von Kontozugangsdaten zu einer materiellen Tat zusammengefasst werden müssen, soweit sie einen engen Zusammenhang miteinander haben [113].

---

[104] CF, Ausspähen der PIN, 06.12.2008

[105] lexexakt.de, natürliche Handlungseinheit

[106] BGH, Großer Senat, Beschluss vom 03.05.1994 - GSSt 2/93, 3/93; zum Steuerstrafrecht:

[107] Siehe BGH, Urteil vom 20.06.1994 - 5 StR 595/93; wenn verschiedene Handlungen (Steuererklärungen) durch den Fortsetzungszusammenhang zusammen gefasst werden, dann beginnt ihre Verjährung erst mit der letzten Tathandlung (§ 78a StGB). Das hat dazu geführt, dass Steuerstraftaten über Jahrzehnte hinweg bestraft werden konnten, wenn sie dieselbe Steuerart betrafen.

[108] BGH, Beschluss vom 19.12.2000 - 4 StR 503/00, mwN.

[109] BGH, Urteil vom 07.03.2012 - 1 StR 656/11

[110] BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 17; BGH, Beschluss vom 26.01.2005 - 2 StR 516/04; BGH, Beschluss vom 07.03.2008 - 2 StR 44/08

[111] BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 13; BGH, Beschluss vom 23.06.2010 – 2 StR 243/10, Rn 3.

[112] BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 8.

[113] Weitere Einzelheiten: CF, Angleichung des Rechts beim Falschgeld und Rauschgift, 13.03.2011;

Das ist zum Beispiel der Fall, wenn die Skimmer ihre technischen Geräte installieren, ihre Funktionstüchtigkeit gelegentlich überprüfen und die Geräte schließlich wieder abbauen. Das Ausspähen bildet dabei einen einheitlichen Handlungsrahmen, wobei der Vorsatz der Täter darauf gerichtet ist, möglichst viele Kundendaten bei ihrem Angriff zu erlangen. Auch wenn die Täter über mehrere Tage hinweg dieselbe Bankfiliale ausspähen und die Technik nur während der Bankgeschäftszeiten abbauen und anschließend wieder einrichten [114], kann eine deliktische Einheit bestehen [115].

Dasselbe gilt wegen des Cashings, wenn die Täter mit engem zeitlichen Zusammenhang handeln. Eine Zäsur kann jedoch dann angenommen werden, wenn die Täter ihr Handeln unterbrechen, um sich zum Beispiel mit weiteren Dubletten zu versorgen [116].

Im Zusammenhang mit dem Nachmachen und Gebrauchen von Zahlungskarten ist jedenfalls dann das Vorliegen eines minder schweren Falles zu prüfen, wenn es um eine geringe Stückzahl von Karten geht [117].

3. Fälschungssicherheit

Von der Rechtsprechung des BGH ist anerkannt, dass sich die Fälschung auch alleine auf die Daten auf dem Magnetstreifen beschränken kann [118]. In Bezug auf Zahlungskarten hat der BGH 2010 ausgeführt [119]:

„Falsch sind Zahlungskarten (mit Garantiefunktion), wenn sie fälschlicherweise den Anschein erwecken, sie seien von demjenigen ausgegeben worden, auf den die lesbaren Angaben auf der Karte oder die auf ihr unsichtbar gespeicherten Informationen als Aussteller hinweisen. Optische Wahrnehmungsmöglichkeit und digitale Maschinenlesbarkeit müssen nicht gleichzeitig gegeben sein, so dass eine "falsche" Karte nicht die kumulative Nachahmung beider Komponenten voraussetzt. Es genügt, dass die Fälschung entweder nur die Urkundenfunktion zum Gegenstand hat - was etwa bei einer gefälschten Kreditkarte der Fall ist, die nur in ihrem äußeren Erscheinungsbild einer echten Kreditkarte entspricht, aber keinen funktionsfähigen Magnetstreifen oder Mikrochip enthält - oder ein Magnetstreifen bzw. ein Mikrochip zwecks ausschließlicher Verwendung an Automaten gefälscht und auf ein unbedrucktes Stück Plastik oder Pappe geklebt ist ...“

§ 152a Abs. 4 Nr. 2 und § 152b Abs. 4 Nr. 2 StGB verlangen gleichermaßen nach einer besonderen Sicherung gegen die Nachahmung durch Ausgestaltung oder Codierung, wobei der Gesetzeswortlaut unklar lässt, ob sie unterschiedliche Sicherheitsmerkmale meinen. Dafür könnte sprechen, dass bei gleichem Wortlaut § 152a StGB das Verfälschen und Nachmachen und § 152b StGB die Garantiefunktion in den Vordergrund stellen.

Die allgemeine „Ausgestaltung“ der Zahlungskarten wird von den Aufdrucken, Hologrammen, der erhabenen Kartennummer und der Prüfnummer (bei Kreditkarten) sowie dem Unterschriftsfeld

BGH, Beschluss vom 02.02.2011 - 2 StR 511/10.

[114] BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 9.

[115] BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 14, leitet das daraus ab, dass *verschiedene Vorbereitungshandlungen, die sich auf denselben Gegenstand erstrecken, nur eine Tat darstellen*. Die Abgrenzung zwischen Vorbereitungs- und Versuchsstadium beim Skimming wird unten angesprochen.

[116] Siehe: BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 9.

[117] BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn. 12.

[118] Zur Verfälschung einer echten Zahlungskarte: BGH, Urteil vom 21.09.2000 - 4 StR 284/00.

[119] BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn. 11

und dem Vorhandensein des Magnetstreifens oder des EMV-Chips geprägt. Als besondere Sicherungen im Hinblick auf die Kodierung sind an erster Stelle das Maschinenlesbare Merkmal, die Prüfwerte auf dem Magnetstreifen und die Sicherungsmechanismen im EMV-Chip zu nennen (codierte Kartennummern, CVV), der zudem einen verschlüsselten Datenverkehr ermöglicht.

Im Hinblick auf die Garantiefunktion kommt als gestaltendes Element eine besondere Bedeutung dem Label zu, das die Karte als eine solche ausweist, die am Onlineverfahren zur Autorisierung und Genehmigung teilnimmt. Die besonderen Sicherheitsmerkmale in Bezug auf die Garantiefunktion sind dieselben, die auch zur allgemeinen Kartensicherheit dienen. Das sind vor allem die Prüfwerte auf dem Magnetstreifen und die Sicherungsmechanismen im EMV-Chip. Von besonderer Bedeutung ist insoweit die PIN, die im Autorisierungsverfahren geprüft wird. Im Zusammenhang mit § 152b Abs. 4 Nr. 2 StGB kommt auch den Verschlüsselungsmechanismen im EMV-Chip eine besondere Bedeutung zu [120].

4. Garantiefunktion

§ 152a Abs. 1 StGB schützt inländische und ausländische Zahlungskarten und geldwerte Wertpapiere (Schecks, Wechsel) vor ihrer Fälschung, wenn sie von einem Kredit- oder Finanzdienstleistungsinstitut herausgegeben wurden (§ 152a Abs. 4 Nr. 1 StGB) und durch ihre Ausgestaltung oder Codierung besonders gegen Nachahmung gesichert sind (§ 152a Abs. 4 Nr. 2 StGB) [121]. Diese Voraussetzungen liegen angesichts der beschriebenen Sicherheitsmerkmale bei den üblichen von Banken herausgegebenen Karten vor [122] und der BGH hat Ende 2011 ausdrücklich auch die Debitkarten zu Zahlungskarten mit Garantiefunktion erklärt [123].

Eine Garantiefunktion besteht dann, wenn in einem Dreiecksverhältnis die Karten ausgebende Bank (Bezogene) gegen Vorlage der Zahlungskarte eine Zahlungszusage gibt [124]. 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 [125], 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“ [126]. 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 Zahlun-

[120] Falsch programmierte EMV-Chips haben Anfang 2010 zu erheblichen Irritationen geführt. Im Onlineverfahren zeigt die Kodierung des Magnetstreifens an, dass die Karte über einen EMV-Chip verfügt. Damit soll das POS-Terminal angewiesen werden, den Chip auszulesen und dessen Sicherheitsfunktionen zu nutzen. Mit einfachem Klebeband ließ sich der Chip jedoch abdecken, so dass die Terminals ihn als defekt betrachteten. Darauf beschränkten sie sich auf die Prüfung des Magnetstreifens.

[121] CF, Skimming und Fälschungsrecht, 13.04.2009

[122] Siehe oben **Fälschungssicherung**.

[123] BGH, Beschluss vom 13.10.2011 - 3 StR 239/11, Rn 3 (Maestro); siehe auch: CF, BGH zum Skimming, 01.03.2012.

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

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

[126] 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.*

gen verwendet werden kann, nicht auch darauf, ob die Fälschung zu einer garantierten Zahlung missbraucht wird [127].

Die Garantiefunktion wird darin gesehen, *dass das die Karte ausgebende Unternehmen ... sich gegenüber Vertragsunternehmen* <verpflichtet>, *deren Forderungen gegen den Kartenbenutzer zu bezahlen* [128]. Diese Definition nimmt § 152b Abs. 4 StGB auf und definiert die Zahlungskarten mit Garantiefunktion als Kredit-, Euroscheck- und sonstige Karten, die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu veranlassen [129]. Die Modalitäten des Forderungsausgleiches zwischen der Bank und ihrem Kunden wirken sich darauf nicht aus.

In Literatur und Rechtsprechung bestehen an der Garantiefunktion keine Zweifel, wenn es sich um Kreditkarten handelt, bei denen der Auszahlungsbetrag gegen ein eigenes Konto des Kartenausstellers erfolgt. Die bekanntesten Kreditkartenverbünde sind die von American Express, Master und Visa [130]. Die Autorisierung im Onlineverfahren und die damit verbundene Genehmigung, ohne die keine Verfügung akzeptiert wird, ist bei Kredit- und Debitkarten jedoch identisch [131], so dass auch die Debitkarten, die an dem Autorisierungsverfahren teilnehmen können, Karten mit Garantiefunktion sind [132]. Für die Strafbarkeit nach § 152b StGB kommt es nur darauf an, dass die Garantiefunktion besteht, und nicht auch darauf, dass der Täter sie in Anspruch nehmen will [133].

Bereits dem Schutz des § 152a StGB unterliegen auch andere Zahlungskarten von Finanzdienstleistungsinstituten oder Tank- und Telefonkarten. Dienen sie auch zur Legitimation gegenüber Dritten, können sie ebenfalls über eine Garantiefunktion verfügen. Das ist eine Frage des Einzelfalls [134].

Die vom Gesetzestext genannten Euroschecks und -karten gibt es seit 2002 nicht mehr. An ihre Stelle ist das (auch vorher schon praktizierte) Autorisierungsverfahren getreten. Wie beim EC-Verfahren [135] geht es ihm um die Garantie des Ausstellers wegen der Auszahlung, nur dass die durch den Euroscheck verbürgte und von der EC-Karte autorisierte Garantie übergegangen ist zum Genehmigungscode, den der Aussteller in jedem POS-Verfahren übermittelt, wenn er die Verfügung genehmigt. Das EC-Verfahren hat dadurch eine neue Ausprägung erfahren. Während das klassische Modell eine frühe Autorisierung bei der Ausgabe der Schecks durchgeführt hat, erfolgt sie jetzt in Echtzeit durch die Übermittlung des Genehmigungscodes. Nicht anders als im alten Verfahren erfolgt die Buchung der Forderung gegen die Bank zunächst auf einem ihrer Zwischenkonten [136], was der Ausgabe der Euroschecks gleich kommt. Das zeigt auch, dass die

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

[128] BGH, Urteil vom 12.05.1992 - 1 StR 133/92, Rn. 9. Die Entscheidung betrifft den Kredit- und Scheckkartenmissbrauch gemäß § 266b StGB und unterscheidet deshalb zwischen Einziehungsverfahren und Lastschriftverfahren. Im Lastschriftverfahren trägt das Ausfallrisiko der Akzeptant, so dass die Karten ausstellende Bank nicht geschädigt wird (ebenda).

[129] Für die EC-Karte hat der BGH anerkannt, dass sie auch dann eine Garantiefunktion hat, wenn sie im Lastschriftverfahren eingesetzt wird: BGH, Urteil vom 21.09.2000 - 4 StR 284/00

[130] Siehe die Übersicht und Erklärungen bei kartensicherheit.de – Zahlungsverfahren.

[131] In BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 4, spricht das Gericht unklar von falschen "Kreditkarten mit Garantiefunktion", meint jedoch Kreditkarten als solche, die nach Art der ausstellenden Banken bedruckt und mit den Labeln von Visa oder Master versehen waren.

[132] Siehe oben **Autorisierung**.

[133] BGH, Beschluss vom 17.06.2008 - 1 StR 229/08.

[134] Wenn die Karte ausschließlich zur Forderungsabrechnung zwischen Aussteller und Inhaber verwendet werden soll, handelt es sich um eine schlichte Zahlungskarte. Karten für Akzeptanz-Verbünde (zum Beispiel DKV) garantieren dem Akzeptanten die Abrechnung und Vergütung im Dreiecksverhältnis und verbürgen deshalb eine Zahlungsgarantie

[135] Das Markenzeichen „EC“ wurde als „electronic cash“ fortgeführt und wird auf neu ausgegebenen Karten nicht mehr verwendet.

[136] Siehe oben **Clearing**

autorisierende Bank die buchhalterische Haftung für die betreffende Forderung übernimmt.

5. Tatorte und deutsche Gerichtsbarkeit

Das Cashing im Ausland unterliegt gemäß § 6 Nr. 7 StGB dem deutschen Strafrecht. Das Ausspähen im Inland bildet für den Mittäter einen eigenen Tatort (§ 9 Abs. 1 StGB) und für den Teilnehmer greifen § 9 Abs. 2 S. 1, S. 2 StGB. Wegen des im Ausland vollendeten Computerbetruges tritt der Taterfolg zunächst bei der kartenausgebenden Bank [137], so dass der Erfolgsort gemäß § 9 Abs. 1 StGB im Inland liegt.

Das Cashing – ob im Ausland mit inländischen oder im Inland mit ausländischen Kartendaten und PIN - stellt sich deshalb als die Vollendung des gewerbsmäßigen Gebrauchs gefälschter Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbsmäßigem Computerbetrug gemäß §§ 152a Abs. 1 Nr. 2, 152b Abs. 1, 2, 263a Abs. 1, 2, 263 Abs. 3 Nr. 1, 52 StGB dar [138].

Eine Ausnahme bilden die vollständigen Auslandstaten, in denen das Cashing im Ausland mit ebenfalls ausländischen Kartendaten erfolgt. Sie haben keinen inländischen Handlungs- oder Erfolgsort, so dass das Weltrechtsprinzip gemäß § 6 Nr. 7 StGB unmittelbar greift, wenn die ausländischen Täter im Inland ergriffen werden (§ 9 StPO) oder sich hier niedergelassen haben (§ 8 StPO). Die Täter können deshalb wegen des Gebrauchs gefälschter Zahlungskarten verfolgt werden, nicht aber wegen Computerbetruges, für den das Weltrechtsprinzip nicht gilt [139].

5.1 Erfolgsort beim Computerbetrug

Im Zusammenhang mit dem Kontoeröffnungsbetrug verlangt der BGH nach einer genauen Bezeichnung des Schadens und dessen, der für ihn einsteht [140]. Anlass geben ihm dazu die Fälle, *wenn der Täter unter Vorlage eines gefälschten Personalausweises und Täuschung über seine Zahlungswilligkeit bei einer Bank ein Konto eröffnet und ihm - antragsgemäß - eine EC-Karte (Eurocheque-Karte) und Schecks ausgehändigt werden*. Bereits darin kann ein vollendeter Betrug bestehen, wenn die Bank eine Auszahlung garantiert oder eine Rückbelastung nicht möglich ist [141].

Der BGH spricht damit das POZ-Verfahren an [142], das Ende 2006 eingestellt wurde [143], aber im Lastschriftverfahren noch immer praktiziert wird. Seine praktische Konsequenz ist, dass nicht die kartenausstellende Bank, sondern der Akzeptant (Einzelhändler) das Ausfallrisiko trägt.

Derartige Zweifel können im Zusammenhang mit dem Cashing nicht auftreten, weil das Autorisierungsverfahren die Eintrittspflichten standardisiert. Mit der Übermittlung des Genehmigungscodes „0“ unterwirft sich die kartenausgebende Bank der Einstandspflicht gegenüber dem Betreiber des POS-Terminals wegen der Summe seiner Forderung [144]. Damit stellt sie den Betreiber

---

[137] Das BVerfG verlangt seit 2010 nach einem bezifferten Schaden. Entgegen der Vorauflage tritt der Schaden beim Cashing zulasten der Karten ausgebenden Bank ein.
Zum Schadensbegriff: BVerfG, Beschluss vom 23.06.2010 - 2 BvR 2559/08, 105/09, 491/09; CF, BVerfG: Bezifferter Gefährdungsschaden, 15.08.2010;
CF, Der Eingehungsschaden löst den Gefährdungsschaden ab, 16.02.2011;
BGH, Beschluss vom 07.12.2010 - 3 StR 433/10.

[138] Das Landgericht Hannover ist bereits am 17.11.2009 meinen rechtlichen Auffassungen gefolgt (rechtskräftig seit Ende April 2010):
CF, Skimming-Rechtsprechung, 18.11.2009

[139] Wegen der Strafverfolgung Deutscher und solcher Ausländer, die nicht abgeschoben werden können, siehe § 7 Abs. 2 StGB.

[140] BGH, Beschluss vom 18.11.2009 - 4 StR 485/08; siehe auch CF, Betrug mit Zahlungskarten auf falschem Namen, 28.01.2009.

[141] Siehe jetzt auch: BGH, Beschluss vom 14.10.2010 - 2 StR 447/10; CF, vom Kontoeröffnungsbetrug zum Identitätsglibber, 03.12.2010.

[142] Point of Sale ohne Zahlungsgarantie – POZ.

[143] Zentraler Kreditausschuss, Kreditwirtschaft stellt POZ-Verfahren Ende 2006 ein, 15.10.2004

[144] Bei Geldautomaten ist das der Auszahlungsbetrag einschließlich der Gebühr.

als Dritten wegen der zivilrechtlichen Störungen im Innenverhältnis frei. Sie kann zwar in aller Regel auf den Karteninhaber und dessen Vermögen zurückgreifen, haftet jedoch im Außenverhältnis in eigener Person. Auch im ▸ Innenverhältnis ist die Verrechnung nicht frei von Einwendungen und die Haftung des Kunden bei missbräuchlicher Nutzung von Zahlungsautorisierungsinstrumenten begrenzt.

Im Zuge des Clearingverfahrens werden die gegenseitigen Forderungen der Banken und ihrer Verbünde verrechnet. Spätestens dabei werden nach dem Einsatz einer Debitkarte der Auszahlungsbetrag und die Gebühr vom CPD der Bank gegen das Girokonto des Kunden gebucht.

5.2 Schaden

Die unbezifferte schadensgleiche Vermögensgefährdung [145] wurde jüngst von der Rechtsprechung des BGH in Frage gestellt, weil sie die konkreten Gefährdungsdelikte des Vermögensstrafrechts den abstrakten Gefährdungsdelikten annähert [146] und deshalb vom 1. [147] und vom 3. Strafsenat des BGH [148] tendenziell abgelehnt wird. Auch das BVerfG verlangt seit 2010 immer nach einer Berechnung und Bezifferung des eingetretenen Schadens [149].

Eine erfreuliche Klärung lieferte der 3. Strafsenat im Januar 2011, weil er an die Stelle der schadensgleichen Vermögensgefährdung den Eingehungsschaden setzt [150]. Er ergibt sich aus der rechnerischen Gegenüberstellung der wirtschaftlichen Werte der gegenseitigen vertraglichen Ansprüche beim Vertragsabschluss selber. Gemeint ist der Vergleich der wirtschaftlichen Werte aus den beiderseitigen Vertragspflichten nach einer noch abstrakten Berechnung. Stehen sie in einem deutlichen Missverhältnis zueinander, ist der Betrug vollendet.

Im ▸ Innenverhältnis zwischen der Bank und ihrem Kunden besteht ein entgeltlicher Geschäftsbesorgungsvertrag, der die Bank zur Vorleistung verpflichtet und ihr nur einen Anspruch auf Aufwendungsersatz (§§ 675c iVm 670 BGB) und auf das vereinbarte Entgelt (§ 675f BGB) verschafft. Beim Einsatz von Zahlungsautorisierungsinstrumente – ZAI (§ 675l BGB) – muss sie die kontrollierte Authentifizierung beweisen und nicht nur darauf verweisen, dass die ZAI vollständig eingesetzt wurden. Der Einwand des Kunden, seine Authentifizierungsdaten seien missbraucht worden, führen zunächst zur Beweislast bei der Bank [151]. Hinter dem Begriff ZAI verbergen sich keine anderen Techniken als die, die von den Zahlungskarten bekannt sind: Das sind die Kar-

[145] Bestätigt vom BVerfG: Beschluss vom 10.03.2009 - 2 BvR 1980/07

[146] CF, Schaden und schadensgleiche Vermögensgefährdung, 31.01.2010

[147] BGH, Beschluss vom 18.02.2009 - 1 StR 731/08

[148] BGH, Urteil vom 13.08.2009 - 3 StR 576/08

[149] BVerfG, Beschluss vom 23.06.2010 - 2 BvR 2559/08, 105/09, 491/09; CF, BVerfG: Bezifferter Gefährdungsschaden, 15.08.2010.

[150] BGH, Beschluss vom 07.12.2010 - 3 StR 433/10; die Entscheidung ist vom Gegenstand her identisch mit BGH, Beschluss vom 07.12.2010 - 3 StR 434/10. Siehe auch: CF, Der Eingehungsschaden löst den Gefährdungsschaden ab, 16.02.2011.

[151] Eine Beweislastumkehr eröffnet der Anscheinsbeweis (siehe zum Beispiel: BGH, Urteil vom 05.10.2004 - XI ZR 210/03). Bei ihm geht es um logische Prozesse und statistische Wahrscheinlichkeiten, die dem behaupteten Anspruch – hier des Bankkunden – entgegen stehen. Wenn das PIN-Verfahren als sicher gilt, dann ist der Anscheinsbeweis gestattet, dass der Kunde die PIN nicht sicher verwahrt hat. Durch die kriminellen Erscheinungsformen des Skimmings und des Phishings ist dieser Anscheinsbeweis hingegen erschüttert. Dasselbe gilt für die Sicherheit des EMV-Chips. Durch Laborversuche ist belegt, dass die PIN prinzipiell abgegriffen werden kann (vom EMV-Chip und bei einer ausnahmsweise unverschlüsselten Eingabe am Terminal). Nicht möglich ist es hingegen, in Deutschland ausgespähte Kartendaten mit Falsifikaten im Inland zu missbrauchen. Dagegen spricht das Maschinenlesbare Merkmal – MM, das die Täter bislang nicht nachmachen können. Dasselbe gilt für den EMV-Chip: Seine solide Grundkonstruktion wurde von den finanzwirtschaftlichen Vorgaben dermaßen perforiert, dass er überschrieben und manipuliert werden kann. Dadurch rächt sich die Forderung nach wirtschaftlicher Beliebigkeit an der informationstechnischen Stabilität, die der EMV-Chip hätte leisten können.

Erfüllt ein Mittäter hinsichtlich aller oder einzelner Taten der Serie sämtliche Tatbestandsmerkmale in eigener Person oder leistet er für alle oder einige Einzeltaten zumindest einen individuellen, nur je diese fördernden Tatbeitrag, so sind ihm diese Taten - soweit nicht natürliche Handlungseinheit vorliegt - als tatmehrheitlich begangen zuzurechnen. Allein die organisatorische Einbindung des Täters in ein betrügerisches Geschäftsunternehmen ist nicht geeignet, die Einzeldelikte der Tatserie rechtlich zu einer Tat im Sinne des § 52 Abs. 1 StGB zusammenzufassen. Erbringt er dagegen im Vorfeld oder während des Laufs der Deliktsserie Tatbeiträge, durch die alle oder mehrere Einzeldelikte seiner Mittäter gleichzeitig gefördert werden, so sind ihm die gleichzeitig geförderten einzelnen Straftaten als tateinheitlich begangen zuzurechnen, da sie in seiner Person durch den einheitlichen Tatbeitrag zu einer Handlung im Sinne des § 52 Abs. 1 StGB verknüpft werden. Ob die übrigen Beteiligten die einzelnen Delikte gegebenenfalls tatmehrheitlich begangen haben, ist demgegenüber ohne Bedeutung

BGH, Beschluss vom 07.12.2010 - 3 StR 433/10

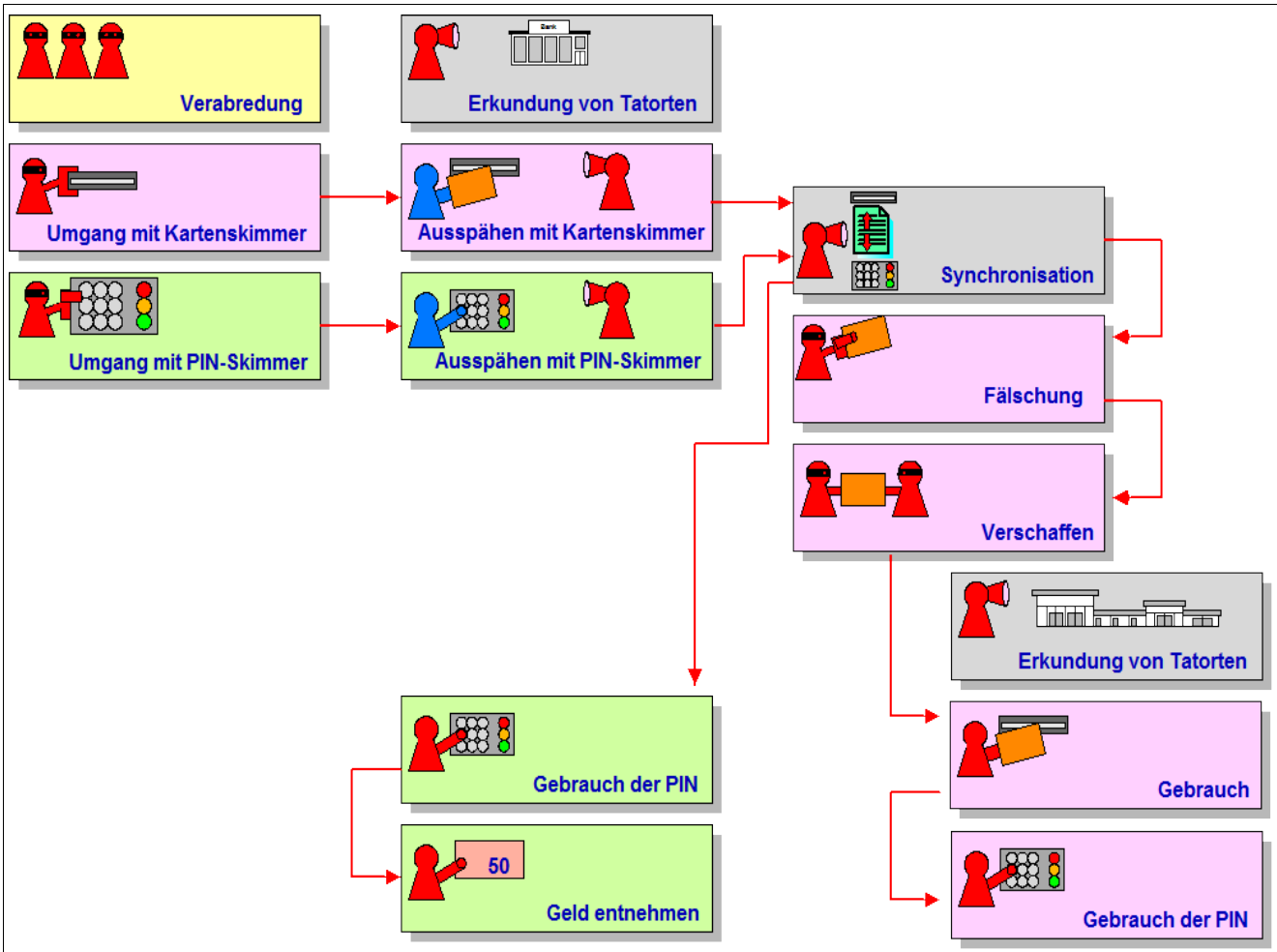
Bereits die Verabredung der Verbrechen ist der Beginn des Rechtsgutsangriffs (...); daher ist für das Verhältnis der Taten zueinander darauf abzustellen, was verabredet ist. Für die Verwirklichung des Tatbestands des § 152 b Abs. 2 StGB kommen verschiedene Möglichkeiten in Betracht, auch die gleichzeitige und sich (teilweise) überschneidende Herstellung mehrerer oder sogar aller Falsifikate unter Verwendung der in dem sichergestellten Päckchen befindlichen Rohlinge.

BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn 13

tendaten auf dem Magnetstreifen und dem EMV-Chip auf Kredit- und Debitkarten sowie die PIN (Kundenkennung, § 675r Abs. 1 BGB), die dem Kunden ausgehändigt werden. Während das Übersendungsrisiko dem ZD obliegt (§ 675m BGB), hat der Kunde für den Schutz der ZAI „alle zumutbaren Vorkehrungen“ zu treffen (§ 675l BGB).

Mit jeder missbräuchlichen Verfügung des Cashers wird auch der Verfügungsrahmen des Kontoinhabers um den Auszahlungsbetrag und die Gebühr für die Auszahlung verringert – und zwar unabhängig davon, ob die Verfügung zunächst gegen ein bankinternes CPD oder gleich gegen das Konto des Kunden gebucht wird. Dabei handelt es sich um eine Einschränkung der Dispositionsfreiheit, die nicht als vermögensrechtlicher Schaden angesehen wird.

Die dem Clearing anschließende Schadensverrechnung über die EURO-Kartensicherheit – EKS - ist ein versicherungsähnlicher Prozess, der dem Schadensausgleich zwischen den beteiligten Banken dient. Sie ist Verfahrensregeln unterworfen und keine Schadensfreistellung, die gleichzeitig mit der schädigenden Vermögensverfügung eintreten müsste.



Das Schaubild stellt die Tathandlungen beim Skimming und beim Cashing in Bezug auf das Fälschungsdelikt (rot unterlegt) und den Computerbetrug dar (grün unterlegt). Der Gebrauch der gefälschten Zahlungskarte wird mit der Eingabe der PIN vollendet und der Computerbetrug mit der Entnahme des Geldes.

Entgegen der Auffassung der Revision beruhen die Feststellungen zur nur vorübergehenden Zurückstellung der Tatausführung auf hinreichenden tatsächlichen Anhaltspunkten, stellen sich also nicht als bloße Vermutung dar. Die Begehung von Straftaten wie das „Skimming" bedarf eines erheblichen organisatorischen Aufwands, insbesondere müssen Geräte zur Herstellung der Zahlungskarten-Doubletten zur Verfügung stehen. Dass Täter, die schon über längere Zeit … mit der Vorbereitung der Tat befasst waren, nur wegen des Versagens der Stromversorgung eines technischen Hilfsmittels, für das Ersatz beschafft werden kann, von der weiteren Ausführung des Vorhabens endgültig absehen, ist eine lebensfremde Annahme.

Eine Ersatzbeschaffung erforderte entgegen der Auffassung der Revision … keinen neuen Tatentschluss, sondern stellte nur einen von vielen Handlungsschritten bis zur Herstellung der Zahlungskarten-Doubletten dar. Dass die Strafkammer mangels Anhaltspunkten für einen endgültigen Tatabbruch davon ausgegangen ist, dass ein solcher von dem Angeklagten und seinen Mittätern nicht gewollt war und schon deshalb ein Verhindern der Tat noch ein Bemühen darum festzustellen waren, ist ein nicht nur möglicher, sondern ausgesprochen naheliegender Schluss. Somit schied ein Rücktritt von der Verabredung eines Verbrechens gemäß § 31 StGB aus.

Generalbundesanwalt, Stellungnahme vom 09.12.2009 zu 3 StR 539/09

5.3 Vollendung

Die Tatvollendung erfolgt beim Cashing in zwei Schritten. In der Schlussphase steckt der Täter zunächst die gefälschte Zahlungskarte in den Geldautomaten und gibt die ausgespähte PIN ein. Bis zu diesem Moment kann er den Vorgang noch abbrechen und damit vom Versuch des Gebrauchens zurücktreten (§ 24 Abs. 1 S. 1 StGB). Sobald er jedoch die Taste „Bestätigung" drückt, ist ihm der Abbruch und der Rücktritt verwehrt. Der Gebrauch einer Zahlungskarte mit Garantiefunktion ist damit vollendet.

Etwas anderes gilt für den gleichzeitig begangenen Computerbetrug [152]. Sein Erfolg tritt erst ein, sobald sich der Täter einen Vermögensvorteil verschafft hat. Das ist der Fall, wenn der Geldautomat das angeforderte Geld zur Entnahme präsentiert und der Täter es nimmt. Zu diesem Zeitpunkt ist ein bezifferbarer Schaden bei der kartenausgebenden Bank eingetreten. Die Bank garantiert für die Deckung des Auszahlungsbetrages und der fremden Gebühr und der Verfügungsrahmen des Kunden hat sich um die Summe beider Beträge verringert.

[152] BGH, Beschluss vom 23.06.2010 – 2 StR 243/10, Rn 3.

6.1 Beginn des Versuchsstadiums

§ 22 StGB verlangt für den Versuchsbeginn, dass der Täter nach seiner Vorstellung von der Tat zur Verwirklichung des Tatbestandes unmittelbar ansetzen muss. Nach gefestigter Rechtsprechung beginnt das Versuchsstadium, sobald der Täter nach seinen Vorstellungen vom konkreten Tatplan eines von mehreren Tatbestandsmerkmalen erfüllt oder seine Handlung unmittelbar in die Tatbestandsverwirklichung einmündet. Der BGH hat das treffend mit dem Wortbild bezeichnet: ***„Jetzt geht es los!"*** [153]

Das Ausspähen der Daten auf den Magnetstreifen von Zahlungskarten ist im Vorbereitungsstadium des Fälschens von Zahlungskarten gemäß § 152b StGB angesiedelt [154]. Der Versuch in einer arbeitsteiligen Organisation beginnt erst, wenn der Skimmer (Ausspäher) die Daten an den Fälscher weiter gibt [155]. Nach dieser Klarstel-

[153] BGH, Beschluss vom 07.11.2007 - 5 StR 371/07, Rn 17.

[154] BGH, Beschluss vom 15.03.2011 - 3 StR 15/11, Rn 6

[155] BGH, Urteil vom 27.01.2011 - 4 StR 338/10; CF, Versuch der Fälschung, 21.02.2011.
Noch unsicher: BGH, Beschluss vom 14.09.2010 - 5 StR 336/10, Rn. 4.

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 nur eine als solche straflose Vorbereitungshandlung. <Rn 9>

Zum Versuch des Nachmachens setzt daher noch nicht an, wer - wie hier - 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. <Rn 9>

Die Tat stellt hier daher lediglich eine Verabredung zu dem Verbrechen der banden- und gewerbsmäßigen Fälschung von Zahlungskarten dar. <Rn 9>

Ob daneben der Tatbestand der Vorbereitung der Fälschung von Zahlungskarten mit Garantiefunktion gemäß § 152a Abs. 5, § 152b Abs. 5, § 149 Abs. 1 Nr. 1 StGB erfüllt ist (...), kann hier dahinstehen. Teils wird vertreten, § 149 StGB werde wegen seiner geringeren Strafandrohung (Freiheitstrafe bis zu fünf Jahren) von dem Tatbestand des § 30 Abs. 2 3. Var., § 152a Abs. 1, § 152b Abs. 1 und 2 StGB, der einen Strafrahmen von sechs Monaten bis zu elf Jahren und drei Monaten eröffnet, verdrängt (...). <Rn 10

Soweit nach a.A. Tateinheit zwischen beiden Delikten möglich sein soll (...), da dem Vergehen nach § 152a Abs. 5, § 152b Abs. 5, § 149 Abs. 1 Nr. 1 StGB gegenüber die Verbrechensverabredung nach § 152a Abs. 1, § 152b Abs. 1 und 2 StGB ein eigener Unrechtsgehalt zukomme, sind die Angeklagten wegen der Nichtverurteilung auch nach § 149 Abs. 1 Nr. 1 StGB nicht beschwert. <Rn 10>

Soweit das Landgericht in den Fällen, in denen es zu Geldabhebungen mittels nachgemachter Zahlungskarten gekommen ist, nicht zudem einen tateinheitlich verwirklichten banden- und gewerbsmäßigen Computerbetrug nach § 263a Abs. 1 und Abs. 2 StGB erwogen hat (...), beschwert dies die Angeklagten nicht. <Rn 13>

Zusammenfassung der aktuellen Skimming-Rechtsprechung bei:

BGH, Beschluss vom 11.08.2011 - 2 StR 91/11

lung des BGH gilt jetzt: In einer arbeitsteiligen Skimming-Bande setzen die nur mit dem Ausspähen von Kartendaten und PIN befassten Mittäter bereits zum Versuch des Fälschens von Zahlungskarten mit Garantiefunktion (§ 152b StGB) an, sobald sie nicht nur die zum Ausspähen verwendeten Geräte gesichert und die gespeicherten Daten ausgelesen haben, sondern diese Daten an ihre (auch unbekannten) Mittäter (hier: in Norditalien) im Ausland übermittelten. Das erfordert jedoch, dass die Skimmer ("Ausspäher") damit rechnen, dass die Fälscher nach Erhalt der Daten ohne weiteres Zuwarten die ausgespähten Daten einander zuordnen (Kartendaten und PIN) und sogleich mit der Fälschung beginnen.

Diese Entscheidung folgt konsequent der zunächst einschränkenden Spruchpraxis [156]:

„Zum Versuch des Nachmachens setzt hingegen noch nicht an, wer sich lediglich – wie hier – darum bemüht, Kartenrohlinge ausgehändigt zu erhalten, um zu einem nicht festgestellten späteren Zeitpunkt mit der Manipulation zu beginnen“.

In diesem Fall hatten die Kartenrohlinge noch keine Individualmerkmale (Kundenname, Kontonummer, Hologramm usw.), so dass sie tatsächlich den Gegenständen vergleichbar sind, die schon von § 149 StGB angesprochen werden (Druckstöcke, Papiere).

[156] BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn 9. Der BGH verweist u.a. auf OLG Thüringen (Jena), wistra 2009, 204; der Lebenssachverhalt ist in beiden Fällen derselbe.

6.2 Versuch des Computerbetruges

Auch § 263a Abs. 3 StGB schafft einen Gefährdungstatbestand im Vorfeld des strafbaren Versuchs (§ 263a Abs. 2 i.V.m. § 263 Abs. 2 StGB). Er beschränkt sich jedoch auf die „Computerprogramme“ und bezieht die „ähnlichen Vorrichtungen“, die in § 149 Abs. 1 StGB genannt werden, nicht mit ein. Das folgt einerseits aus § 263a Abs. 4 StGB, der nur auf die Rücktrittsregeln der Absätze 2 und 3 des § 149 StGB verweist, und andererseits aus § 149 Abs. 1 StGB, der nur die Fälschung selber der Strafbarkeit im Vorbereitungsstadium unterwirft. Das betrifft die Herstellung gefälschter Zahlungskarten, nicht aber auch ihren Gebrauch.

Die Folge davon ist, dass wegen der Ausspähgeräte für PIN-Eingaben nur solche „Programme“ zur Strafbarkeit im Vorbereitungsstadium führen, die für den besonderen Zweck des Ausspähens installiert oder eingerichtet werden. Das ist bei allen Geräten der Fall, die aus Einzelteilen gebaut und dabei eine eigene Elektronik eingebaut bekommen, also bei Tastaturaufsätzen und selbst gebauten getarnten Kameras. Dort, wo Mobiltelefone oder digitale Kameras verwendet werden, ohne deren Elektronik zu verändern, greift die Rechtsprechung des BVerfG zum Hackerstrafrecht. Es handelt sich bei ihnen um strafneutrale Dual Use-Produkte [157].

Zwischen dem Ausspähen der PIN und ihren missbräuchlichen Einsätzen liegen mehrere Arbeitsschritte. Zunächst müssen die ausgespähten Daten synchronisiert und die Zahlungskarten gefälscht werden. Nur wegen des reinen Fälschungsvorganges sieht der BGH jetzt keine „hemmenden Zwischenschritte“ mehr in der Übermittlung und Synchronisation der Daten [158]. Der Computerbetrug ist jedoch kein Bestandteil der Fälschung, sondern des abschließenden Cashings. Das führt dazu, dass im Zusammenhang mit dem Computerbetrug das Ausspähen der PIN, ihre Synchronisation mit den ausgespähten Kartendaten und ihr Transport zwischen den beteiligten Mittätern noch im Vorbereitungsstadium angesiedelt ist.

6.3 Rücktritt vom Versuch

In arbeitsteiligen Täterverbünden machen sich auch der Mittäter und der Gehilfe strafbar, wenn die Tatbestandsvollendung – aufbauend auf ihren Vorleistungen im Vorbereitungs- oder Versuchsstadium - erst durch andere Tatgenossen erfolgt.

Sobald das Versuchsstadium erreicht ist, kann der vollendend handelnde Tatgenosse nur dann strafbefreiend vom Versuch zurücktreten (§ 24 StGB), wenn er Anstrengungen unternimmt, die Tatvollendung wirklich zu verhindern. Deshalb neigt der Generalbundesanwalt zu einer zurückhaltenden Anwendung der Rücktrittsregeln und lässt vorübergehende technische Störungen, die behoben werden können [159], und das Abbauen der Ausspähgeräte zur Vermeidung der Entdeckung nicht ausreichen. Das passt zur Entscheidungspraxis des BGH, der dem Täter nicht ohne Not die Straffreiheit des Rücktritts zubilligt [160]. Im Zusammenhang mit dem Skimming hat das Gericht bei mehrtägigem Ausspähen je nach den Umständen Tatmehrheit (§ 53 StGB) und Tateinheit (§ 52 StGB) angenommen [161].

In arbeitsteiligen Skimmingstrukturen endet die Tatherrschaft des Skimmers, sobald er die ausgespähten Daten an die „Nachtäter“ der Organisation meldet. Er bleibt nur dann straffrei, wenn er sich ernsthaft gegen den Taterfolg wendet (§ 24 Abs. 2 StGB), die Nachtäter auf die geplante Vollendung verzichten oder die Tat ohne seinen Tatbeitrag ausführen. Im Zusammenhang mit dem arbeitsteiligen Skimming bedeutet das, dass

[157] BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07, 1151/08, 1524/08; siehe auch CF, Klarstellungen zum Hackerstrafrecht, 20.06.2009.

[158] BGH, Urteil vom 27.01.2011 - 4 StR 338/10, Rn 8, 11.

[159] Siehe oben, Kasten vor **2.1 Ausspähen von Daten**.

[160] BGH, Urteil vom 20.05.2009 - 2 StR 576/08, Rn 6; siehe auch CF, Grenzen des Rücktritts, 12.07.2009.

[161] BGH, Urteil vom 10.05.2005 – 3 StR 425/04, S. 9.

sie zwar das Fälschen und das Cashing durchführen, aber nur mit anderen Kartendaten als die, die vom Skimmer (Ausspäher) stammen.

6.4 Zusammenfassung und Strafzumessung

Das Skimming im engeren Sinne, also das Ausspähen von Magnetkartendaten und PIN der Bankkunden am Geldautomaten oder an anderen Eingabegeräten, ist vollständig im Vorbereitungsstadium zum anschließenden Fälschen von Zahlungskarten mit Garantiefunktion gemäß § 152b Abs. 1 StGB angesiedelt. Ihm schließt sich das strafbare Fälschen und der ebenfalls strafbare Gebrauch von gefälschten Zahlungskarten mit Garantiefunktion in Tateinheit mit Computerbetrug an (§§ 152b Abs. 1, 263a Abs. 1, 2, 52 StGB).

§ 152b Abs. 1 StGB ist ein Verbrechenstatbestand, so dass der Versuch stets strafbar ist (§§ 12 Abs. 1, 23 Abs. 1 StGB). Dagegen ist § 263a Abs. 1 ein Vergehenstatbestand, bei dem die Strafbarkeit des Versuchs ausdrücklich bestimmt ist (§§ 12 Abs. 2, 23 Abs. 1 StGB, 263a Abs. 2, 263 Abs. 2 StGB).

Der Versuch des Fälschens von Zahlungskarten mit Garantiefunktion beginnt in arbeitsteiligen Skimmerbanden nach der geklärten Rechtsprechung des BGH frühestens dann, wenn der Skimmer (Ausspäher) die Daten an seine Komplizen übermittelt und dabei die Vorstellung hat, dass diese unverzüglich mit dem Fälschen beginnen [162]. Daraus folgt, dass zwar das Ausspähen als solches nicht unmittelbar in die Tatbestandsverwirklichung mündet (§ 22 StGB), wohl aber die abschließende Handlung des Skimmers, das Übermitteln, bei dem er, wenn auch nur kurzfristig, auch die vollständige Tatherrschaft hat (Mittäter im Sinne von § 25 Abs. 2 StGB).

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 [163]. Dem ist mit der neuen Rechtsprechung zum Versuchsbeginn ein Riegel vorgeschoben: Wenn bereits mit der Übermittlung der abgegriffenen Daten an die fälschungsbereiten „Nachtäter“ der Versuch 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.

Die folgenden Handlungen, das Fälschen sowie das Gebrauchen gefälschter Zahlungskarten und Computerbetrug (Cashing [164]) bilden ungeachtet der Anzahl der Fälschungen und ihrer Einsätze in aller Regel eine deliktische Einheit [165], so dass sie zu einer materiellen Tat verschmelzen [166].

---

[162] CF, Versuch der Fälschung, 21.02.2011

[163] 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. Die Beihilfe zum Versuch ist nicht strafbar.

[164] CF, Cashing, 26.07.2010

[165] Siehe oben: **6.4 natürliche Handlungseinheiten**

[166] Siehe auch: CF, keine deliktische Einheit, 24.10.2010

Spätestens mit dem Herstellen der Dubletten ist die Fälschungstat vollendet. Das hat für den Skimmer zur Folge, dass er als Täter zu bestrafen ist (§ 25 Abs. 2 StGB). Während der kurzen Spanne zwischen der Übermittlung und dem Fälschen greifen die Strafzumessungskriterien wegen des Versuchs. Zu der Frage, ob ein gemilderter Strafrahmen gesetzt werden muss, hat der BGH ausgeführt [167]:

… Dies genügt den Anforderungen an die Strafrahmenwahl bei einem Versuch nicht. Dabei hat das Tatgericht neben der Persönlichkeit des Täters die Tatumstände im weitesten Sinne und dabei vor allem die versuchsbezogenen Gesichtspunkte, namentlich insbesondere die Nähe der Tatvollendung, die Gefährlichkeit des Versuchs und die eingesetzte kriminelle Energie, in einer Gesamtschau umfassend zu würdigen.

Wegen der Nähe zur Tatvollendung ist darauf abzustellen, dass das Fälschen eine einaktige Handlung ist und im Hinblick auf die Gefährlichkeit jedenfalls beim Skimming die Fälschung einer Vielzahl von Zahlungskarten geplant ist. Die kriminelle Energie bezieht sich auf die eigenhändigen Handlungen des Skimmers. Dabei sind der Aufwand für die Vorbereitung, Installation und Kontrolle der Geräte zu berücksichtigen und das Vorgehen des Skimmers bei der Tatausführung.

Die qualifizierenden Merkmale des Handelns "als Mitglied einer Bande" oder "gewerbsmäßig" im Sinne von § 152b Abs. 2 StGB sind besondere persönliche Merkmale im Sinne von § 28 Abs. 2 StGB [168] und müssen in der eigenen Vorstellung des Täters verwirklicht sein.

7. Vorbereitungshandlungen

§ 149 StGB stellt im Vorfeld der Geld- und Wertpapierfälschung den Umgang, also die Herstellung von, den Verkehr mit (Sich-Verschaffen, einem anderen Verschaffen, feilbieten) und das Verwahren von besonderen Fälschungsgrundstoffen und Werkzeugen unter Strafe. Die §§ 152a Abs. 5 und 152b Abs. 5 StGB verweisen auf diese Vorschrift, so dass jedenfalls seit 2003 auch der Umgang mit Programmen und ähnlichen Vorrichtungen mit Strafe bedroht ist [169]. Auch § 263a Abs. 3 StGB schafft einen entsprechenden Gefährdungstatbestand, soweit es um den Umgang mit Programmen geht, die besonders für den Computerbetrug geschaffen wurden oder eingesetzt werden sollen [170]. Schließlich erweitert § 303b Abs. 5 StGB unter Verweis auf § 202c StGB die Strafbarkeit der Computersabotage im Vorbereitungsstadium auf den Umgang mit dazu bestimmten Computerprogrammen (§ 202c Abs. 1 Nr. 2 StGB) sowie ausdrücklich auf Passwörter und sonstige Sicherungscodes (§ 202c Abs. 1 Nr. 1 StGB) [171]. Diese drei unterschiedlichen Gefährdungstatbestände führen dazu, dass bereits der Umgang – hier in den Formen des Sich-Verschaffens und Verwahrens – für die meisten zum Skimming eingesetzten Ausspähgeräte mit geringen Strafen bedroht ist.

Eine noch offene Frage ist die, ob die von § 263a Abs. 3 StGB angesprochenen Programme nur beim Computerbetrug selber eingesetzt werden dürfen oder auch solche umfassen, die zum Ausspähen von PIN dienen [172]. Die ältere Rechtsprechung zu den Fälschungswerkzeugen [173] hat jedenfalls den § 149 StGB restriktiv ausgelegt und

[167] BGH, Beschluss vom 28.09.2010 - 3 StR 261/10, Rn 3

[168] CF, Gehilfe in einer Bande, 11.11.2010

[169] Siehe auch oben **6.1 Versuch der Kartenfälschung**.

[170] Siehe auch oben **6.2 Versuch des Computerbetruges**.

[171] Siehe auch oben **2.3 PIN-Skimming und Computersabotage**.

[172] Unklar ist zudem die geforderte „Werktiefe“ der Computerprogramme. Bislang werden ersichtlich keine besonderen Anforderungen daran gestellt.

[173] Siehe unten **7.1 Kartenlesegeräte**.

nur solche Werkzeuge gelten lassen, die unmittelbar zum Fälschen bestimmt sind. § 263a Abs. 3 StGB setzt nur voraus, dass es der Zweck des Programms sein muss, einen Computerbetrug zu begehen. Dieser Wortlaut enthält keine Beschränkung darauf, dass das Programm nur bei der Tatvollendung eingesetzt werden darf. Unter Berücksichtigung der besonderen Bedeutung, die die Rechtsprechung jetzt dem Ausspähen im Gesamtplan des Skimmings beimisst, schließe ich, dass auch die Computerprogramme umfasst sind, die mur für das Ausspähen erstellt werden.

Wenn hier zwischen Karten-Skimmern und PIN-Skimmern unterschieden wird, so bildet ihr zeitgleicher Einsatz eine Tateinheit (§ 52 StGB).

Die Verabredung zu einem Verbrechen ist ebenfalls im Vorbereitungsstadium angesiedelt. Auf sie wird im Anschluss an die Ausführungen zur Mittäterschaft und zur Bande eingegangen.

7.1 Kartenlesegeräte

Noch 2003 hat der BGH den Umgang mit Skimmern, also mit Kartenlesegeräten, als nicht strafbar im Sinne von § 149 StGB angesehen [174]. Ausschlaggebend dafür war, dass die Regelbeispiele dieses Gefährdungstatbestandes (Druckstöcke und Papiere für die Fälschung von Banknoten) zur unmittelbaren Herstellung der Fälschungen dienen, nicht aber, wie das Kartenlesegerät, zur Vorbereitung der Fälschungen. Der Tatbestand ist vergleichbar mit einer Kamera und ihrem Foto, mit dem das Abbild einer Note oder eines Wertpapiers angefertigt wird, um dieses auf Druckstöcke oder Papiere zu übertragen.

Mit Wirkung vom 30.08.2003 wurde § 149 Abs. 1 Nr. 1 StGB geändert und umfasst jetzt auch „Computerprogramme oder ähnliche Vorrichtungen, die ihrer Art nach zur Begehung der Tat geeignet sind“. Der Generalbundesanwalt hat aus der Gesetzesänderung mehrfach gefolgert, dass jetzt jedenfalls auch der Umgang mit Skimmern im Vorbereitungsstadium strafbewehrt ist [175]. Während der BGH in diesen Fällen die Revisionen der verurteilten Skimmer ohne Begründung verworfen hat, ließ er diese Frage in einer aktuellen Entscheidung ausdrücklich offen [176].

Greift diese Auslegung durch, dann sind Vorrichtungen im Sinne von § 149 StGB jedenfalls die Lesegeräte (Skimmer), die zum Zweck des Skimmings mit einem digitalen Speicher oder einer Funkeinrichtung [177] ausgestattet, also gebaut oder umgebaut wurden. „Vorrichtungen“ sind insoweit die Stromversorgung, das Lesemodul, der Speicher und die Hardware für die kleine Computerlogik, die die Komponenten verbindet. Das „Programm“ sind die verbindenden Computerroutinen.

Danach ist der Umgang mit Skimmern mit Strafe bis zu 5 Jahren Freiheitsstrafe bedroht.

Auf der inneren Tatseite setzt § 149 StGB voraus, dass der Täter *eine Geldfälschung vorbereitet*. Ist das nicht der Fall, senkt sich die Strafdrohung auf 3 Jahre Freiheitsstrafe im Höchstmaß. Denselben Fall spricht auch § 127 OWiG an, der die Zahlungskarten aus den §§ 152a, 152b StGB ausdrücklich benennt (§ 127 Abs. 3 OWiG). Die Ordnungswidrigkeit ist mit einer Geldbuße bis 10.000 Euro bedroht.

7.2 Kameras

Eine übliche Methode zum Ausspähen der PIN ist die Installation einer Kamera, die auf das Tastaturfeld ausgerichtet wird. Die PIN wird jedoch nicht für das Nachmachen der eingesetzten Zahlungskarten benötigt, sondern nur zu ihrem Gebrauch und vor allem zum geplanten Computerbetrug. Deshalb kann ein strafbarer Umgang mit

[174] BGH, Urteil vom 16.12.2003 - 1 StR 297/03.

[175] Stellungnahmen des GBA zu BGH, Beschluss vom 09.09.2008 - 1 StR 414/08, und BGH, Beschluss vom 26.01.2010 - 3 StR 539/09 (unveröffentlicht). Siehe auch Fischer, § 149 StGB Rn 3.

[176] BGH, Urteil vom 17.02.2011 - 3 StR 419/10, Rn 12

[177] Die Funktechnik wurde zunächst selten beobachtet, taucht seit 2011 aber vermehrt beim POS-Skimming auf.

Kameras nicht aus § 149 StGB abgeleitet werden, der sich auf den Vorgang des Fälschens beschränkt, sondern nur aus den beiden anderen Gefährdungsdelikten mit Bezug zum Computerbetrug und zur Computersabotage.

§ 263a Abs. 3 StGB beschränkt die strafrechtliche Haftung im Vorbereitungsstadium auf den Umgang mit Programmen und schließt nicht auch auf die aus § 149 StGB bekannten „ähnlichen Vorrichtungen“ mit ein. Er zielt nur auf die Software, nicht aber auch auf die Hardware, und verlangt nach einer differenzierten Betrachtung der bekannten Kamerainstallationen zum Skimming.

Eine ältere Form besteht in dem Einbau von elektronischen Bauteilen in einen Halter für Werbematerial, der an die Innenwand des Geldautomaten geklebt wird. Hierbei werden Kamera, Stromversorgung und Speicher verwendet, die mit Hilfe eines Schaltung zusammengeführt werden. Diese Schaltung kann als Programm im Sinne von § 263a Abs. 3 StGB angesehen werden. Dasselbe gilt für den jüngst bekannt gewordenen Einbau in einen vorgetäuschten Sichtschutz für die Tastatur [178] oder die elektronischen Bauteile mit Kamerafunktion, die hinter dem Chasis des Geldautomaten verbaut werden.

In Rauchmeldern und Kameraleisten werden in aller Regel handelsübliche Digitalkameras oder Mobiltelefone mit Kamerafunktion eingebaut. Zum Betrieb werden ihre internen Speicher und Steuerungen verwendet, so dass sie als Dual Use-Komponenten zu betrachten und der Umgang mit ihnen im Anschluss an die Rechtsprechung des BVerfG als straflos anzusehen sind [179]. Besondere Computerprogramme kommen dabei nicht zum Einsatz. Rein technische Veränderungen wie das Anlöten weiterer Akkus für die länger dauernde Stromversorgung werden vom Wortlaut des § 263a Abs. 3 StGB nicht erfasst.

Sobald handelsübliche Geräte erfolgreich eingesetzt werden, also spätestens die Eingabe der PIN eines zweiten Kunden ausgespäht wurde, kommt die Strafbarkeit im Hinblick auf die Computersabotage zum Zuge (§§ 303b Abs. 5, 202c StGB), weil sich die Täter damit Passwörter verschafft haben.

Die Einschränkung, dass mindestens zwei PIN ausgespäht sein müssen, folgt aus der Formulierung des § 202c StGB, der die Mehrzahl verwendet. Im Zusammenhang mit dem Fälschen von Zahlungskarten verwendet des Gesetz ebenfalls die Mehrzahl. Dem entgegen hat der BGH bereits die Fälschung ***einer*** EC-Karte genügen lassen [180], weil er die Gefährlichkeit bereits einer einzelnen Tathandlung als ausreichend angesehen hat. Das lässt sich angesichts der geringen Strafdrohung von einem Jahr Freiheitsstrafe im Höchstmaß nicht auf das Ausspähen von PIN übertragen.

7.3 Tastaturaufsätze

Ein Tastaturaufsatz ist ein handwerklich gefertigtes Einzelstück, das die Tastatur eines Geldautomaten täuschend nachahmt und eine Stromversorgung, ein Speichermodul sowie eine elektronische Steuerung aufweist, so dass die Tasteneingaben gespeichert werden. Diese Steuerung kann als Programm im Sinne von § 263a Abs. 3 StGB angesehen werden.

Dasselbe gilt für vollständige Fassaden (Front Covering), die den Geldautomaten mit Ausnahme des Bildschirms vollständig abdecken. Die dabei eingesetzten Tastaturen müssen über ein Programm verfügen, das für die Speicherung der Eingaben sorgt.

[178] CF, Sichtblende mit Kamera, 26.06.2010

[179] BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07, 1151/08, 1524/08; siehe auch oben **6.2 Versuch des Computerbetruges**.

[180] BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 11.

8. Mittäter und Bande

Arbeitsteilig handelnde Täter sind Mittäter (§ 25 Abs. 2 StGB), wenn sie nach einem gemeinsamen Tatplan handeln, der mehrgliedrig ist und in dessen einzelner Phase der Täter nach seiner Vorstellung Tatherrschaft ausübt. Ihn unterstützen kann der Gehilfe (§ 27 Abs. 1 StGB), der keine Tatherrschaft ausübt, sondern sich dem Täter unterordnet [181]. Er hat keine Tatherrschaft und übt in aller Regel eine *"ganz untergeordnete Tätigkeit"* aus [182].

Der Beurteilungsmaßstab ist stark subjektiv geprägt: *„Mittäterschaft liegt ... dann vor, wenn ein Tatbeteiligter nicht bloß fremdes Tun fördern will, sondern seinen Beitrag als Teil der Tätigkeit des anderen und umgekehrt dessen Tun als Ergänzung seines eigenen Tatanteils will. Ob ein Beteiligter dieses enge Verhältnis zur Tat hat, ist nach den gesamten von seiner Vorstellung umfassten Umständen in wertender Betrachtung zu beurteilen. Wesentliche Anhaltspunkte hierfür können gefunden werden im Grad des eigenen Interesses am Erfolg der Tat, im Umfang der Tatbeteiligung und in der Tatherrschaft oder wenigstens im Willen zur Tatherrschaft, so dass Durchführung und Ausgang der Tat maßgeblich von seinem Willen abhängen“* [183].

Die bisher gemachten Erfahrungen und die Rechtsprechung [184] lassen für arbeitsteilig handelnde Skimming-Täter grundsätzlich den Schluss zu, dass sie in allen Tatphasen als Mittäter in fest gefügten Strukturen dauerhaft zusammenarbeiten.

8.1 arbeitsteilige Tätergruppen

Der überholte Bandenbegriff setzte ein Zusammenwirken der Täter am Tatort und bei der Tatvollendung voraus. 2001 hat der große Senat des BGH am Beispiel des Bandendiebstahls (§ 244 Abs. 1 Nr. 2 StGB) die vom gemeinsamen Tatplan geprägte Zusammenarbeit von Mittätern neu gewürdigt und auf das mittelbare Zusammenwirken in verschiedenen Tatphasen erweitert [185]. Er trägt damit der besonderen Gefährlichkeit der arbeitsteiligen und gleichzeitig spezialisierten Tätergruppen Rechnung, ohne damit ein neues Organisationsstrafrecht zu schaffen [186]. Allerdings genügt seither das arbeitsteilige Zusammenwirken in einem Gesamtplan, also *"wenn ein Bandenmitglied die Tat aufgrund seiner Ortskenntnisse oder besonderer Organisationsmöglichkeiten plant, ein anderes die erforderlichen Vorbereitungen trifft, indem es die notwendigen Werkzeuge oder Transportmittel besorgt, während wieder ein anderes Bandenmitglied - möglicherweise wegen seiner besonderen Kenntnisse und Fähigkeiten - die Sache wegnehmen soll und ein weiteres Bandenmitglied für den Abtransport und die Sicherung der Beute Sorge trägt. Eine derartige Arbeitsteilung, die vor allem für organisierte und spezialisierte Diebesbanden typisch ist, ist zumindest genauso gefährlich wie die Arbeitsteilung am Ort der Wegnahme selbst".*

Diese Grundsätze sind auch auf die reine Mittäterschaft übertragbar [187]. Er muss sich die Tatvollendung und den kriminellen Erfolg zurechnen lassen (§ 25 Abs. 2 StGB), auch wenn er an den abschließenden Tathandlungen nicht mehr beteiligt war, wenn die „Nachtäter“ seinen Tatbeitrag nutzen [188], ihr krimineller Erfolg vorhersehbar ist und sich die Beteiligten im Tatplan halten [189]. Der BGH begründet das damit, dass die arbeitsteilige

[181] Siehe zur Abgrenzung BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09 und die Zitate in den Kästen oben sowie auf der Folgeseite. Weitere Zitate werden bei CF, Mittäterschaft und strafrechtliche Haftung, 25.12.2009 diskutiert.

[182] BGH, Beschluss vom 02.02.2010 - 3 StR 4/10 (Bunkerhalter und Kurier beim BtM-Handel).

[183] BGH, Beschluss vom 13.01.2010 - 5 StR 506/09, Rn 5

[184] BGH, Urteil vom 17.02.2011 – 3 StR 419/10

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

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

[187] CF, Tatanteile des Mittäters, 16.02.2011; BGH, Beschluss vom 07.12.2010 - 3 StR 433/10.

[188] BGH, Beschluss vom 13.08.2002 - 4 StR 208/02.

[189] BGH, Beschluss vom 16.09.2009 - 2 StR 259/09, Rn 4 (Mittäterexzess).

Täterschaft und Beteiligung ebenso gefährlich sind wie die Zusammenarbeit mehrerer Täter bei der Tatvollendung. Die Täter müssen sich nicht untereinander kennen, solange nur jeder den Willen hat, sich zur künftigen Begehung von Straftaten mit (mindestens) zwei anderen zu verbinden [190].

Diese Betrachtung hat der BGH auf die Beschaffung eines Firmenmantels, unter dessen Struktur die Komplizen selbständig betrügerische Geschäfte begehen [191], und sogar auf spontan wirkende Zusammenschlüsse übertragen, wenn sie gleichartige Straftaten einer umgrenzbaren Tätergruppe betreffen [192].

Der sozusagen vorbereitend tätige Mittäter gibt sich in die Hände seiner „Nachtäter", sobald er die Tatherrschaft wegen der (weiteren) Tatausführung an sie abgibt. Vollenden sie schließlich die Tat, so treffen auch ihn die Folgen der vollendeten Tat wegen der drohenden Strafe und des dabei verursachten Schadens [193]. Bei der Strafzumessung gemäß § 46 Abs. 2 StGB sind auch ihm *„die verschuldeten Auswirkungen der Tat"* zuzurechnen.

Verzichten die „Nachtäter" auf die geplante Tatvollendung, so kommt das auch dem vorbereitend tätigen Mittäter zugute [194]. Er haftet zunächst nur für die konkreten Handlungen, die er ausgeübt hat, wenn sie selbständig strafbar sind. Deshalb verlangt der BGH wegen der Tatbeiträge arbeitsteilig handelnder Täter und ihrer rechtlichen Bewertung eine genaue Betrachtung des einzelnen Täters, eine genaue Bezeichnung seiner Handlungen und Feststellungen dazu, wie sie sich in den Gesamtplan einfügen [195]. Mit anderen Worten: *"Sind an einer Deliktsserie mehrere Personen als Mittäter, mittelbare Täter, Anstifter oder Gehilfen beteiligt, ist die Frage, ob die Straftaten tateinheitlich oder tatmehrheitlich zusammentreffen, nach ständiger Rechtsprechung des Bundesgerichtshofs für jeden der Beteiligten gesondert zu prüfen und zu entscheiden."* [196]

Mittäter und Gehilfen können eine Bande bilden, wenn sie sich „für eine gewisse Dauer" mit dem Willen verbinden, bestimmte Formen von Straftaten gemeinsam – wenn auch in wechselnden Beteiligungen – zu begehen. Insoweit ist der Zusammenschluss als Bande keine selbständige Straftat, sondern erst die Ausführung einer konkreten Tathandlung, die vom Bandenwillen umfasst ist, wobei die bandenmäßige Begehung dort, wo der Gesetzgeber es vorsieht [197], ein Qualifizierungsmerkmal ist [198], das zu einer schärferen Strafdrohung führt [199].

Die Hinterleute in arbeitsteiligen Täterstrukturen sind in aller Regel keine Mittäter, weil ihnen die Tatherrschaft fehlt. Sie können als Anstifter zu

---

[190] BGH, Urteil vom 16.06.2005 - 3 StR 492/04, S. 8.

[191] BGH, Beschluss vom 29.04.2008 - 4 StR 125/08; siehe auch CF, Mittäterschaft und strafrechtliche Haftung, 25.12.2009.
Das kann dazu führen, dass die ausführenden Täter mehrere materiellen Taten begehen, der (den Firmenmantel) beschaffende Täter aber nur eine, die alle Taten seiner Mittäter umfasst.

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

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

[194] Der BGH wendet sich gegen eine ausufernden Anwendung seiner Rechtsprechung: BGH, Beschluss vom 29.07.2009 - 2 StR 160/09, Rn 5.

[195] BGH, Beschluss vom 13.08.2002 - 4 StR 208/02

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

[197] Siehe CF, Bandenstraftaten, 17.01.2010 (mit einer Aufstellung der vom Gesetzgeber qualifizierten Tatbestände – Bandenliste).

[198] Der besonders schwere Fall bereichert den Grundtatbestand um weitere Tatbestandsmerkmale mit der Folge, dass sich nur der Strafrahmen verändert. Der Typ des Grunddelikts bleibt dadurch erhalten, es wird zu keinem Verbrechen und es gelten die Beteiligungs- und Verjährungsvorschriften für das Grunddelikt. Durch die Qualifizierung wird hingegen ein selbständiger Tatbestand geschaffen, der häufig ein Verbrechen ist und das auch dann, wenn er weitgehend auf die Tatbestandsmerkmale des Grunddelikts verweist.

[199] Im Gegensatz zur Bande ist die Mitgliedschaft in einer kriminellen Vereinigung (§ 129 StGB) ein selbständiges Organisationsdelikt. Mit der Abgrenzung setzt sich BGH, Urteil vom 03.12.2009 - 3 StR 277/09 - (S.18 ff.) auseinander. Siehe auch schon CF, Bande. Vereinigung, 2008.

einer konkreten Straftat (§ 26 StGB), als „Bestimmer“ im Zusammenhang mit einer Verbrechensabrede (§ 30 Abs. 1 StGB) oder als mittelbare Täter (§ 25 Abs. 1 StGB) *„in Fällen mafiaähnlich organisierten Verbrechens in Betracht kommen, bei denen der räumliche, zeitliche und hierarchische Abstand zwischen der die Befehle verantwortenden Organisationsspitze und den unmittelbar Handelnden gegen arbeitsteilige Mittäterschaft spricht“* [200].

8.2 Tatvollendung durch Cashing

Beim Cashing wird der gewerbsmäßige Gebrauch gefälschter Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbsmäßigem Computerbetrug gemäß §§ 152a Abs. 1 Nr. 2, 152b Abs. 1, 2, 263a Abs. 1, 2, 263 Abs. 3 Nr. 1, 52 StGB vollendet. Dabei bilden die verschiedenen Missbräuche von gefälschten Zahlungskarten eine deliktische Einheit, wenn sie in einem engen räumlich-zeitlichen Zusammenhang erfolgen [201]. Allein die Tatsache, dass dabei Karten verwendet werden, deren Originale eine Garantiefunktion haben, führt zu einer Strafdrohung von 1 bis 10 Jahre Freiheitsstrafe.

Allein aus der Tatsache, dass das Cashing über Tage oder Wochen wiederholt wird, kann nicht schon auf die Gewerbsmäßigkeit geschlossen werden [202]. Dazu müssen andere persönliche Merkmale herangezogen werden, die sich aus der Vorbereitung des Skimmings, des (professionellen) Ablaufs der Angriffe, den Investitionen in Technik und Training und anderen Fakten ergeben können.

Handeln die Täter aber gewerbsmäßig oder als Bande, erhöht sich der Strafrahmen auf 2 bis 15 Jahre Freiheitsstrafe (§§ 152b Abs. 2, § 38 Abs. 2 StGB).

Das Cashing unterliegt der deutschen Gerichtsbarkeit unabhängig davon, wo es begangen wird und woher die Kartendaten stammen, die dabei missbraucht werden [203]. Nur bei vollständigen Auslandstaten – begangen im Ausland mit ausländischen Kartendaten – entfällt die tateinheitliche Strafbarkeit wegen Computerbetruges.

8.3 Tatbeteiligung des Skimmers

Dieselbe Strafdrohung trifft den Skimmer, wenn sein Handlungsbeitrag als der eines Mittäters anzusehen ist [204] und die Casher (auch) die von ihm ausgespähten Daten erfolgreich missbrauchen. An anderer Stelle hat der BGH trotz eines recht zügigen Beginns des Cashing – zwei Tage nach dem Ausspähen – nur eine Beihilfe der ausspähenden Skimming-Täter zu den Taten der Cashing-Täter angenommen [205].

Im Einzelfall schwierig zu beantworten sind die Fragen nach den Vorstellungen des Skimmers vom Tatplan und seiner eigenen Tatbeteiligung (innere Tatseite). Das sind die Fragen danach, ob er die abschließende Tatvollendung als eigene (Täterschaft, § 25 StGB [206]), er *sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen* [207] (Gewerbsmäßigkeit) und sich einem Bandenwillen anschließen will (Bande). Diese Fragen werden immer nur im Rahmen einer individuellen Gesamtwürdigung beantwortet werden können, bei der das

---

[200] BGH, Urteil vom 26.07.1994 - 5 StR 98/94, Rn. 84; weitere Einzelheiten: CF, Der Hintermann als Täter, 03.01.2010.

[201] Siehe oben **2.4 natürliche Handlungseinheiten**.

[202] CF, Angleichung des Rechts beim Falschgeld und Rauschgift, 13.03.2011;
BGH, Beschluss vom 02.02.2011 - 2 StR 511/10.

[203] Siehe oben **5. Tatorte und deutsche Gerichtsbarkeit**.

[204] Arbeitsteilige Skimming-Täter handeln grundsätzlich als Mittäter: BGH, Urteil vom 27.01.2011 - 4 StR 338/10, Rn. 8.

[205] BGH, Beschluss vom 13.10.2011 - 3 StR 239/11, Rn 7.

[206] BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09

[207] BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5.

Verhalten bei der Tat, ihre Vorbereitung und das Nachtatverhalten, die darin zum Ausdruck kommenden kriminellen Erfahrungen des Täters und Häufigkeit seiner Taten im Vordergrund stehen.

Die damit verbundenen Schwierigkeiten sind der Rechtsprechung bekannt. Der BGH verlangt deshalb auch im Zusammenhang mit dem Zweifelsgrundsatz – in dubio pro reo [208] – das Vorliegen von tatsächlichen Anhaltspunkten, um zum Beispiel dem Täter einen strafbefreienden Rücktritt vom Versuch zuzubilligen [209], und wendet sich damit gegen eine unkritische Auseinandersetzung mit den von Verteidigungsstrategien gefärbten Einlassungen [210].

Von besonderer Bedeutung bei der Auseinandersetzung mit der inneren Tatseite ist, dass es keinen legalen Verwendungszweck für ausgespähte Kartendaten und PIN gibt. Sie lassen sich nur an noch unbekannte Casher verkaufen oder in einer bereits organisierten Bandenstruktur verwerten. Im ersten – erfahrungsgemäß seltenen, aber nicht ganz auszuschließenden Fall – handeln die Skimmer grundsätzlich als Gehilfen und im zweiten als Mittäter. Beachtlich ist dabei auch die besondere Gefährlichkeit ihres Handelns, die bereits in der hohen Strafdrohung des § 152b Abs. 2 StGB zum Ausdruck kommt [211]. Sie lässt in der Parallelwertung der Skimmer erwarten, dass sie jedenfalls mit bedingtem Vorsatz die Tatvollendung billigen [212].

In den Fällen, in denen es nicht zur Vollendung durch Mittäter kommt, stellt sich die Frage nach dem Beginn des Versuchsstadiums, die jetzt in Bezug auf arbeitsteilige Skimmingbanden geklärt ist. Daraus folgt auch: Wenn die Fälscher erkennbar fälschungsbereit sind und sozusagen „Gewehr bei Fuß stehen“, dann beteiligen sich die Datenlieferanten, egal, ob sie selber die Daten abgegriffen haben oder als Zwischenhändler handeln, am Versuch des Fälschens. Diese Konsequenz zu ziehen hätte ich mir ohne die klarstellende Entscheidung des BGH nicht getraut [213].

Im übrigen verbleibt es bei einer Strafbarkeit wegen der aufgeführten Vorbereitungshandlungen [214], die in Tateinheit mit einer Verbrechensabrede stehen können [215].

---

[208] *„Im Zweifel für den Angeklagten“.* Der Zweifelssatz ist aber keine Beweisregel, sondern eine Entscheidungsregel, wie der BGH jüngst wiederholt hat: BGH, Urteil vom 12.10.2011 - 2 StR 202/11, Rn 10.

[209] BGH, Urteil vom 20.05.2009 - 2 StR 576/08, Rn 6

[210] Zur (unbeachtlichen) Verteidigererklärung: BGH, Urteil vom 20.06.2007 - 2 StR 84/07; siehe auch CF, Prozesserklärung unbeachtlich, 05.09.2007.

[211] Darauf weist auch das BVerfG hin, das auch die besonders schwere Strafdrohung in § 152b Abs. 2 StGB nicht beanstandet: BVerfG, Beschluss vom 18.03.2009 - 2 BvR 1350/08

[212] Siehe Kasten bei 8.1.

[213] BGH, Urteil vom 27.01.2011 - 4 StR 338/10

[214] Siehe oben **7. Vorbereitungshandlungen**.

[215] GBA, Stellungnahme vom 09.12.2009 zu 3 StR 539/09. Offen gelassen: BGH, Urteil vom 17.02.2011 - 3 StR 419/10, Rn 12.

9. Verabredung zu einem Verbrechen

Nicht der gewerbsmäßige Computerbetrug, wohl aber das Fälschen und Gebrauchen von Zahlungskarten mit Garantiefunktion sind nach der Bewertung des Gesetzgebers ein Verbrechen (§ 12 Abs. 1 StGB). Das führt dazu, dass bereits die Verabredung im Vorbereitungsstadium, Skimming zu begehen, oder die Anstiftung dazu gemäß § 30 StGB strafbar sind.

Das gilt auch dann für den Computerbetrug, wenn er nicht nur gewerbs-, sondern gleichzeitig auch bandenmäßig ausgeführt werden soll, weil § 263 Abs. 5 StGB, auf den § 263a Abs. 2 StGB verweist, als selbständiger Verbrechenstatbestand ausgelegt ist. Darin unterscheidet er sich vom „nur“ gewerbsmäßigen Betrug, der einen besonders schweren Fall des Grundtatbestandes bestimmt (§ 263 Abs. 3 StGB).

An der Verbrechensabrede können sich nur Anstifter und Mittäter beteiligen [216], nicht auch Gehilfen. Erst jüngst hat der BGH einige Grundsätze für die Verbrechensabrede im Zusammenhang mit dem Nachmachen von Zahlungskarten mit Garantiefunktion entwickelt, die jedoch nicht den üblichen Fall des arbeitsteiligen Skimmings betreffen [217]. Zu betrachten ist deshalb der Tatbeitrag, den der einzelne an der Abrede Beteiligte leisten soll und will (siehe unten). Nicht der besonders gefährliche Täter als solcher soll der Strafdrohung aus dem § 30 StGB unterliegen, sondern besonders gefährliche Straftaten sollen durch ihre ins Vorbereitungsstadium vorverlagerte Strafbarkeit verhindert werden.

Für den Rücktritt vom Versuch der Beteiligung gelten vereinfachte Regeln (§ 31 StGB), die jedoch nicht bei jedem Scheitern zur Straffreiheit führen [218].

[216] BGH, Urteil vom 04.02.2009 - 2 StR 165/08; siehe auch CF, Verbrecher muss Mittäter sein, 25.04.2009.

[217] BGH, Urteil vom 13.01.2010 – 2 StR 439/09.

[218] Siehe oben **6.3 Rücktritt vom Versuch**.

10. Beteiligungsmodell beim arbeitsteiligen Skimming

Der typische Tatplan beim arbeitsteiligen Skimming [219] liefert das Modell für die Betrachtung der Strafbarkeit in Bezug auf die Verabredung zu einem Verbrechen (§ 30 StGB) und im Vorbereitungsstadium. Das dreistufige Modell muss dazu um eine vorausgehende Stufe erweitert werden:

1) Umgang mit Skimming-Geräten

2) Ausspähen von PIN und Kartendaten

3) Fälschung von Zahlungskarten

4) Missbrauch der gefälschten Zahlungskarten

Die Stufen 3) und 4) betreffen Verbrechen. Allein das Fälschen von Zahlungskarten mit Garantiefunktion ist gemäß § 152b Abs. 1 StGB strafbar (Stufe 3). Der Missbrauch (Stufe 4), also das Cashing, stellt sich als der Gebrauch von gefälschten Zahlungskarten mit Garantiefunktion dar, also ebenfalls als Verbrechen, und in Tateinheit damit als Computerbetrug gemäß § 263a StGB. Der Computerbetrug ist dann ein Verbrechen, wenn er gewerbs- und bandenmäßig betrieben wird (§§ 263a Abs. 2 i.V.m. 263 Abs. 5 StGB).

Die Rechtsprechung verlangt nach der Betrachtung des Tatbeitrages und –willens jedes einzelnen an der Abrede Beteiligten. Die Handlungen in den Stufen 3) und 4) zielen unmittelbar auf die Begehung eines Verbrechens, so dass sie im Vorbereitungsstadium von § 30 StGB direkt angesprochen sind.

Die Stufe 2) birgt erhebliche rechtliche Probleme. In ihr geht es zunächst nur um die Beschaffung der Daten von den Magnetstreifen auf Zahlungskarten mit Garantiefunktion von Bankkunden und ihrer PIN. Ich fasse hier beide als „Kartendaten“ zusammen.

Es stellt sich die Frage, welche Schlüsse aus der Tathandlung des Ausspähens in Bezug auf den Gesamtplan zu ziehen sind. Bei der Beurteilung sind zwei Gesichtspunkte besonders wichtig:

[219] Siehe oben **1. arbeitsteiliges Vorgehen**.

- Das Ausspähen kann keinen anderen finalen Zweck haben als den, die notwendigen Voraussetzungen für das Cashing zu schaffen. Für das Ausspähen gibt es keinen neutralen Zweck, der nicht in eine Straftat münden soll.

- Skimmer können sich auf das Ausspähen spezialisiert haben und das Ziel verfolgen, nicht selber oder durch Mittäter das Cashing durchzuführen, sondern die ausgespähten Daten gewinnbringend abzusetzen. Anhaltspunkte dafür sind eine gewisse Sesshaftigkeit (Verbleib im Inland) und ein hinreichender zeitlicher Abstand zwischen dem Ausspähen und dem Cashing, während die Verkaufsverhandlungen mit noch unbekannten Abnehmern geführt werden. Je kürzer diese Zeit ist, desto wahrscheinlicher ist es, dass die Skimmer das Cashing selber ausführen oder dass das Cashing von anderen Mittätern ausgeführt wird.

10.1 Abrede einschließlich eigenhändiges Cashing

„Wir wollen wiederholt Kartendaten ausspähen und anschließend zum Cashing einsetzen."

Hierbei umfassen der Tatplan und der Vorsatz das Fälschen und den Missbrauch von gefälschten Karten beim Cashing. Die an der Abrede Beteiligten wollen die Tatherrschaft über den Gesamtplan ausüben, der sowohl im Hinblick auf das Fälschen wie auch in Bezug auf den Missbrauch in ein Verbrechen münden sollen. Das „wiederholte … Cashing" bestimmt zudem die Gewerbsmäßigkeit. Die Tat ist deshalb seit der Abrede als Verabredung zum gewerbsmäßigen Fälschen von Zahlungskarten mit Garantiefunktion gemäß §§ 30, 152b Abs. 2 StGB zu bewerten. Der Strafrahmen verringert sich jedoch infolge der §§ 30 Abs. 1 S. 2, 49 Abs. 1 Nr. 2, Nr. 3 StGB auf Freiheitsstrafe zwischen 6 Monate und 11 Jahre 3 Monate.

Sind am Tatplan drei oder mehr Personen beteiligt, dürften sie als Bande handeln. Das ändert in Bezug auf § 152b Abs. 2 StGB nichts, wohl aber im Hinblick auf den bei Cashing begangenen Computerbetrug, der sich zum Verbrechen qualifiziert, wenn er gewerbs- und bandenmäßig betrieben wird. Die Tat ist unter diesen Voraussetzungen als Verabredung zum gewerbs- und bandenmäßigen Fälschen und Gebrauch von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbs- und bandenmäßigem Computerbetrug zu bewerten.

10.2 Abrede einschließlich Cashing durch Mittäter

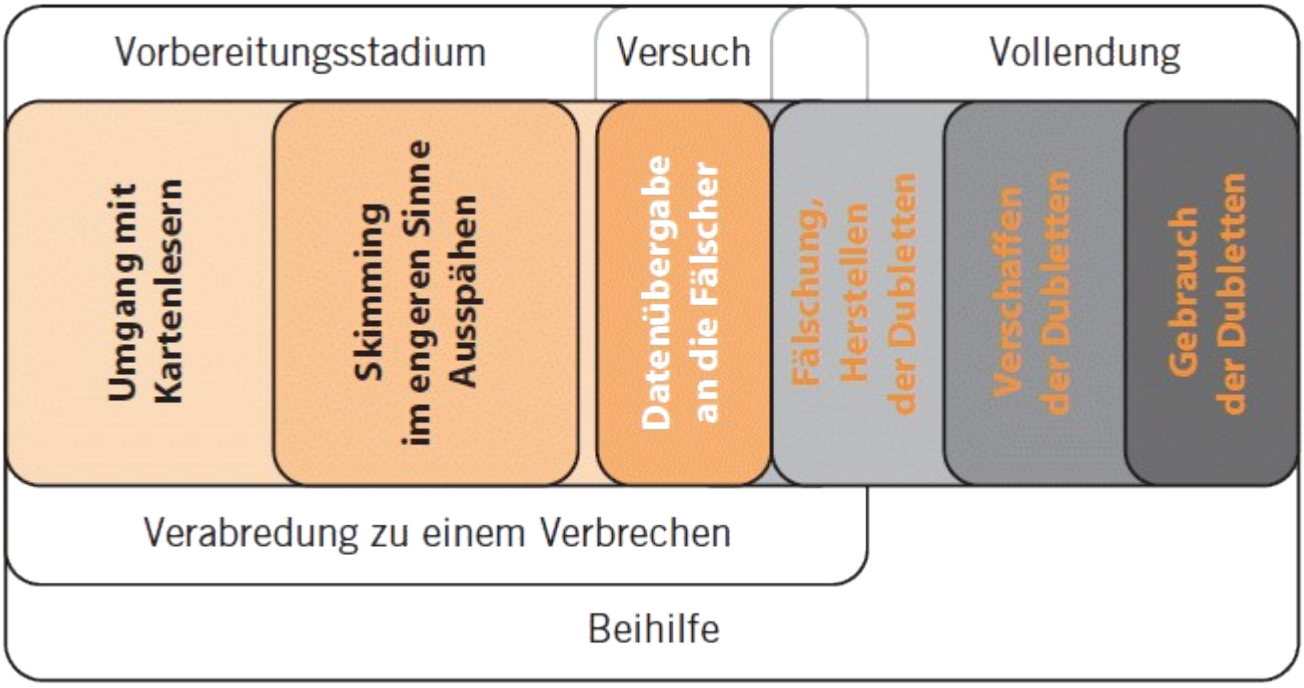
„Wir wollen Geld damit verdienen, dass wir wiederholt Kundendaten ausspähen, um diese an unsere Leute weiter zu geben, die damit das Cashing betrieben."

Die Einbindung in eine mittäterschaftliche und in aller Regel bandenmäßige Struktur führt dazu, dass die reinen Skimming-Täter zu Mittätern in Bezug auf das Cashing werden. Ihnen ist der Taterfolg und der beim Cashing verursachte Schaden gemäß § 25 Abs. 2 StGB zuzurechnen. Auch unter diesen Voraussetzungen ist die Tat als Verabredung zum gewerbs- und bandenmäßigen Fälschen und Gebrauch von Zahlungskarten mit Garantiefunktion in Tateinheit mit gewerbs- und bandenmäßigem Computerbetrug zu bewerten.

10.3 Abrede mit Absatzabsicht

„Wir wollen Geld damit verdienen, dass wir wiederholt Kundendaten ausspähen, um diese an noch unbestimmte Interessenten zu verkaufen."

Bei dieser Konstellation entfällt die Täterschaft oder Mittäterschaft in Bezug auf die Verbrechen in den Stufen 3) und 4). Wenn die Verbrechen in diesen beiden Stufen vollendet werden, so haben die Skimmer zwar eine notwendige Voraussetzung dazu geleistet, allerdings nicht als Täter, sondern als Gehilfen. Als Gehilfe können sie sich jedoch nicht an einer Verbrechensabrede im Sinne von § 30 StGB beteiligen. Ihr Handeln stellt



Tatphasen beim Skimming und beim Cashing.

Den Schwerpunkt der Strafbarkeit bilden das Fälschen, das Sich-Verschaffen und schließlich der Gebrauch der gefälschten Dubletten. Sie unterliegen der Strafbarkeit als Verbrechen gemäß § 152b StGB (rechts im Schaubild).

Der Versuch des Fälschens beginnt spätestens mit der Verwirklichung des ersten Tatbestandsmerkmals der Fälschung. In arbeitsteiligen Tätergruppen beteiligen sich aber auch die „Abgreifer“ von Kartendaten und PIN am Versuch der Fälschung, sobald sie die ausgespähten Daten an ihre „Nachtäter“ versenden. Die Voraussetzung dafür ist, dass die „Nachtäter“ nach der Vorstellung der „Abgreifer“ unmittelbar mit der Fälschung beginnen wollen. Dass die ausgespähten Daten erst noch synchronisiert werden müssen, ist nach der jüngsten Rechtsprechung des BGH unbeachtlich.

Auch wenn das Ausspähen der begehrten Daten im Vorbereitungsstadium des Fälschungsverbrechens angesiedelt ist, hat diese Rechtsprechung weitreichende Konsequenzen. Alle Täter, die als Abgreifer oder Zwischenhändler (Datenhehler) die begehrten Daten an die tatbereiten Fälscher weiter geben, beteiligen sich am Versuch des Fälschungsverbrechens. Schon während der Verhandlungen über die Datenübergabe beteiligen sie sich auch an einer Verbrechensabrede (§ 30 Abs. 2 StGB) mit einer empfindlichen Strafdrohung.

Das Skimming im engeren Sinne ist im Vorbereitungsstadium des Fälschungsverbrechens angesiedelt. In diesem Stadium greifen im Wesentlichen zwei konkurrierende Strafvorschriften. Das ist einerseits § 149 Abs. 1 Nr. 1 StGB, der den Umgang mit Kartenlesegeräten unter Strafe stellt, und andererseits die Verabredung zu einem Verbrechen (§ 30 Abs. 2 StGB), wenn mindestens zwei Täter beteiligt sind, die sich nicht nur als Gehilfen zum Taterfolg der Fälscher beitragen wollen. In Anbetracht der handwerklichen Qualität, die von den „Abgreifern“ verlangt wird, und ihrem wesentlichen Tatbeitrag zum späteren Fälschen ist grundsätzlich von Mittäterschaft auszugehen.

Die §§ 149 Abs. 1 Nr. 1 und 263a Abs. 3 StGB sind auch auf den Umgang mit Skimminggeräten anzuwenden, die für das Ausspähen von Kartendaten und PIN hergerichtet sind, ohne dass die Abgreifer bereits mit dem Ausspähen begonnen haben. Das gilt für PIN-Skimmer mit der Einschränkung, dass handelsübliche Dual Use-Technik ohne Veränderungen an ihrer elektronischen Steuerung von der Strafbarkeit ausgenommen sind. Das gilt etwa für Digitalkameras und Fotohandys, die ohne Veränderungen an ihrer Elektronik in Attrappen verbaut werden.

10.4 Umgang mit Skimming-Geräten

In der Stufe 1) geht es um die Beschaffung, Herstellung und Aufbewahrung von Skimming-Geräten. Dabei ist zu unterscheiden nach:

10.4.1 Kartenlesegeräte (Skimmer): Sie dienen zum Auslesen der Daten aus den Magnetstreifen und damit unmittelbar dazu, Zahlungskarten mit Garantiefunktion zu Fälschen. Das führt zur Strafbarkeit gemäß § 149 Abs. 1 StGB. In den Fällen 10.1 bis 10.3 sind die Taten auch in Tateinheit als „Verabredung und Vorbereitung“ der genannten Beteiligungsformen zu bewerten.

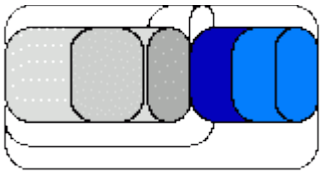
10.4.2 Spezialgeräte zum Ausspähen der PIN: Dabei handelt es sich um Tastaturaufsätze oder getarnte Kameras, die unter Verbindung elektronischer Bauteile für den besonderen Zweck hergestellt wurden, Tastatureingaben an Geldautomaten auszuspähen und aufzuzeichnen. Sie dienen nicht zum Fälschen von Zahlungskarten mit Garantiefunktion, sondern nur zu deren Gebrauch und dem damit einhergehenden Computerbetrug. Das schließt die Anwendung von § 149 StGB aus, dessen Wortlaut sich nur auf das Fälschen selber bezieht. Es handelt sich bei ihnen jedenfalls um „Programme“ im Sinne von § 263a Abs. 3 StGB, wenn sie zu ihrem besonderen Zweck aus elektronischen Bauteilen mit einer eigenen Steuerung für das Ausspähen und Aufzeichnen zusammengebaut wurden. Auch insoweit stehen die Taten in den Fällen 10.1 bis 10.3 in Tateinheit als „Verabredung und Vorbereitung“ wegen der genannten Beteiligungsformen.

10.4.3 Attrappen mit handelsüblichen Kameras zum Ausspähen der PIN: Insoweit kommen vor allem Mobiltelefone mit Kamerafunktion und handelsübliche Digitalkameras zum Einsatz, die mit ihrer eigenen, nicht umgebauten Elektronik zur Steuerung betrieben werden. Es handelt sich um Dual-Use-Komponenten, die im Hinblick auf § 263a Abs. 3 StGB strafneutral sind. Erst der erfolgreiche Einsatz solcher Geräte führt zu einer strafbaren Vorbereitung der Computersabotage gemäß § 303b Abs. 5 in Verbindung mit § 202c StGB. Bei den ausgespähten PIN handelt es sich auch um Passwörter, die beim Cashing auch zum Zugriff auf Daten dienen.

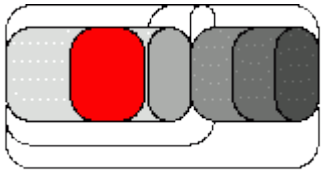
Anhang:
Grafiken zum Beteiligungsmodell

Grafiken erklären häufig mehr als viele Worte. Die Schaubilder in diesem Anhang fassen die wesentlichen Aussagen zur strafrechtlichen Beurteilung des Skimmings aus dem Beteiligungsmodell zusammen [220].

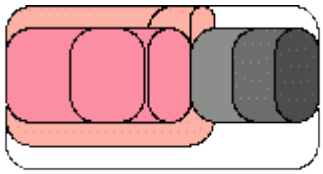
Dem liegt das oben gezeigte Phasenmodell zugrunde [221]:



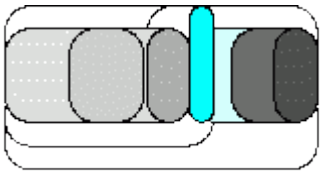
Das Grunddelikt ist das Fälschen von Zahlungskarten im Sinne der §§ 152a, 152b StGB (dunkelblau). Gleichrangige (aber nachfolgende) Tathandlungen sind das Sich-Verschaffen und das Gebrauchen von falschen Zahlungskarten (marineblau).



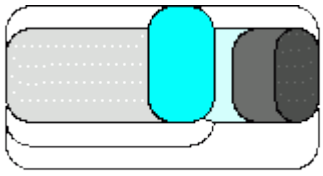
Das Skimming im engeren Sinne, also das Ausspähen der Kartendaten und PIN (rot), ist im Vorbereitungsstadium des Fälschungsdelikts angesiedelt. Es ist kein Erfolgsdelikt, also vor allem kein Ausspähen von Daten im Sinne von § 202a StGB [222].



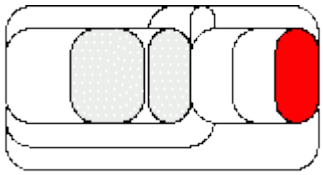
Das Vorbereitungsstadium beim Skimming reicht von der Herstellung von Skimmern (Kartenlesegeräten), über ihren Einsatz (Skimming im engeren Sinne) bis zum Beginn der Fälschung von Zahlungskarten. Strafrechtlich wird es erfasst vom Vorbereiten der Fälschung von Zahlungskarten (§ 149 Abs. 1 Nr. 1 StGB) und der Verabredung zu einem Verbrechen (§ 30 Abs. 2 StGB), an der sich aber nur Mittäter (§ 25 Abs. 2 StGB), nicht aber auch Gehilfen beteiligen können (§ 27 Abs. 1 StGB).



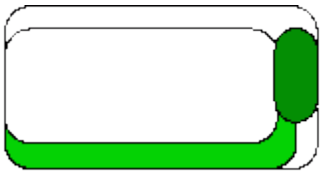
Bei ganz strenger Betrachtung beginnt der Versuch (§ 22 StGB) nach der Verwirklichung eines der Tatbestandsmerkmale des Grunddelikts. Der Täter müsste also beim Skimming mit dem Fälschen von Zahlungskarten beginnen.



In arbeitsteiligen Tätergruppen beteiligen sich die „Abgreifer“ bereits am Versuch des Fälschens, sobald sie die ausgespähten Daten an die fälschungsbereiten Mittäter übermitteln und sie die Vorstellung haben, dass die Mittäter mit der Fälschung unverzüglich beginnen [223].



Mit dem Einsatz der gefälschten Zahlungskarten und der ausgespähten PIN wird tateinheitlich auch ein Computerbetrug begangen (§ 263a StGB).



Alle Unterstützungshandlungen, die am Ende Beute bringen, sind als Beihilfehandlungen strafbar. Das gilt auch für den Umgang mit PIN-Skimmern, wenn sie besondere Schaltungen ("Programme") enthalten, die auf den Computerbetrug spezialisiert sind.

---

[220] CF, Bilderbuch Skimming-Strafrecht, 26.07.2010

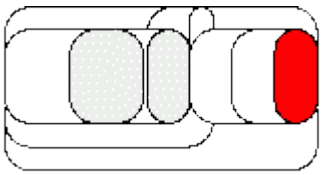
[221] CF, Skimming: aktuelles Beteiligungsmodell, 13.03.2011

[222] CF, Ausspähen von Daten und das Skimming, 14.05.2010

[223] CF, Versuch der Fälschung, 21.02.2011; BGH, Urteil vom 27.01.2011 - 4 StR 338/10.

Cashing

Grafik 1: Cashing



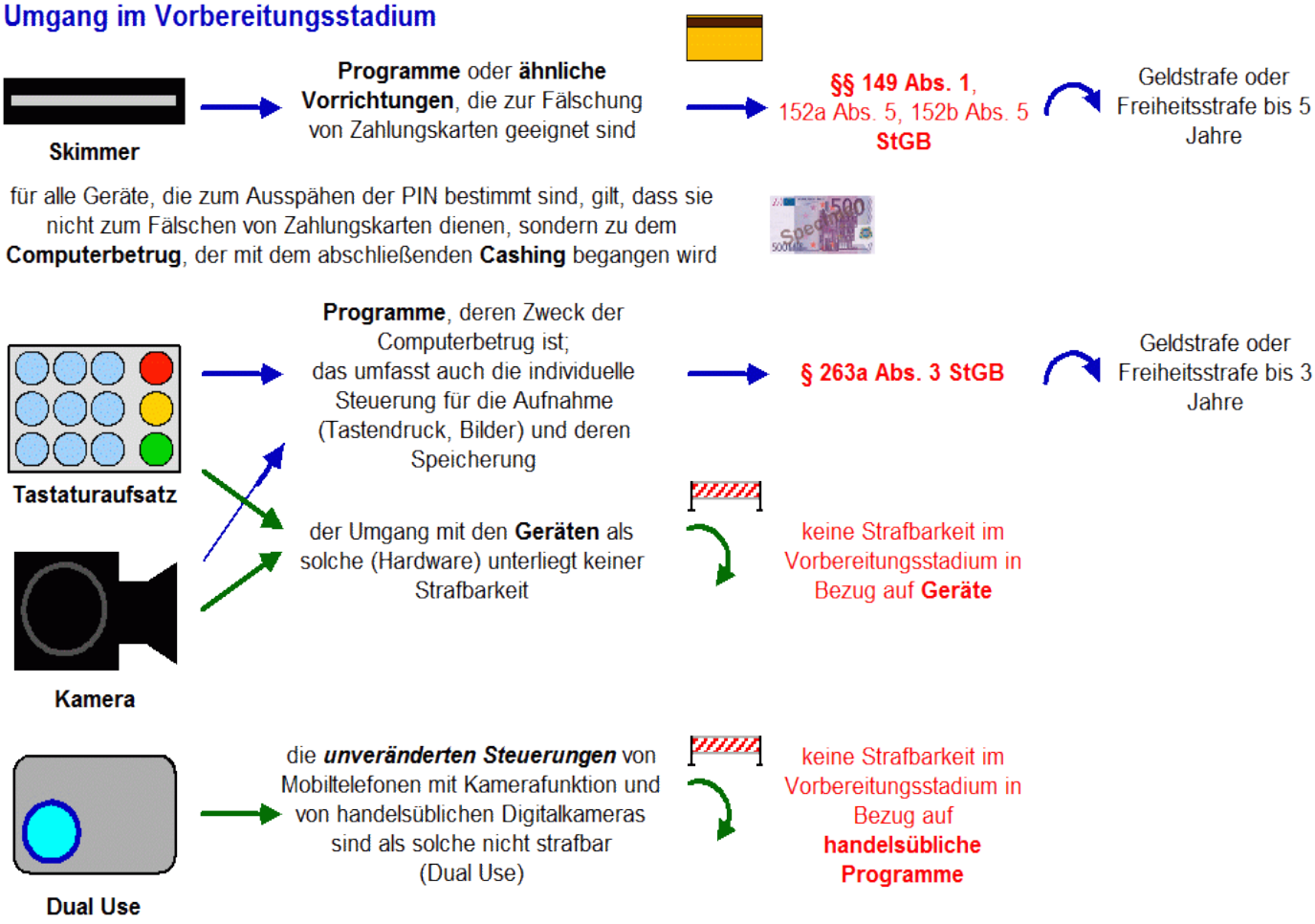
Das finale Ziel des Skimmings, das Cashing, ist am einfachsten darzustellen.

Bereits mit der Fälschung von Zahlungskarten mit Garantiefunktion wird das Verbrechen des § 152b Abs. 1 StGB vollendet.

Der abschließende Akt beim Skimming ist das Cashing, wobei die gefälschten Zahlungskarten an Geldautomaten eingesetzt werden. Es handelt sich dabei um den Gebrauch falscher Zahlungskarten mit Garantiefunktion in Tateinheit mit Computerbetrug.

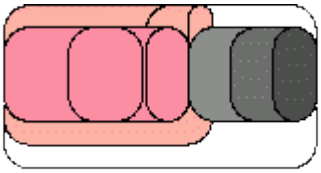
Die Qualifikation des gewerbsmäßigen Handelns wird grundsätzlich vorauszusetzen sein, so dass sich der Strafrahmen auf Freiheitsstrafe von 2 bis 15 Jahre erhöht (§ 152b Abs. 2 StGB).

Umgang im Vorbereitungsstadium



Grafik 2:

Umgang mit Skimminggeräten im Vorbereitungsstadium



Im Zusammenhang mit dem Skimming sind bereits im Vorbereitungsstadium verschiedene Handlungen strafbar (Gefährdungsdelikte)

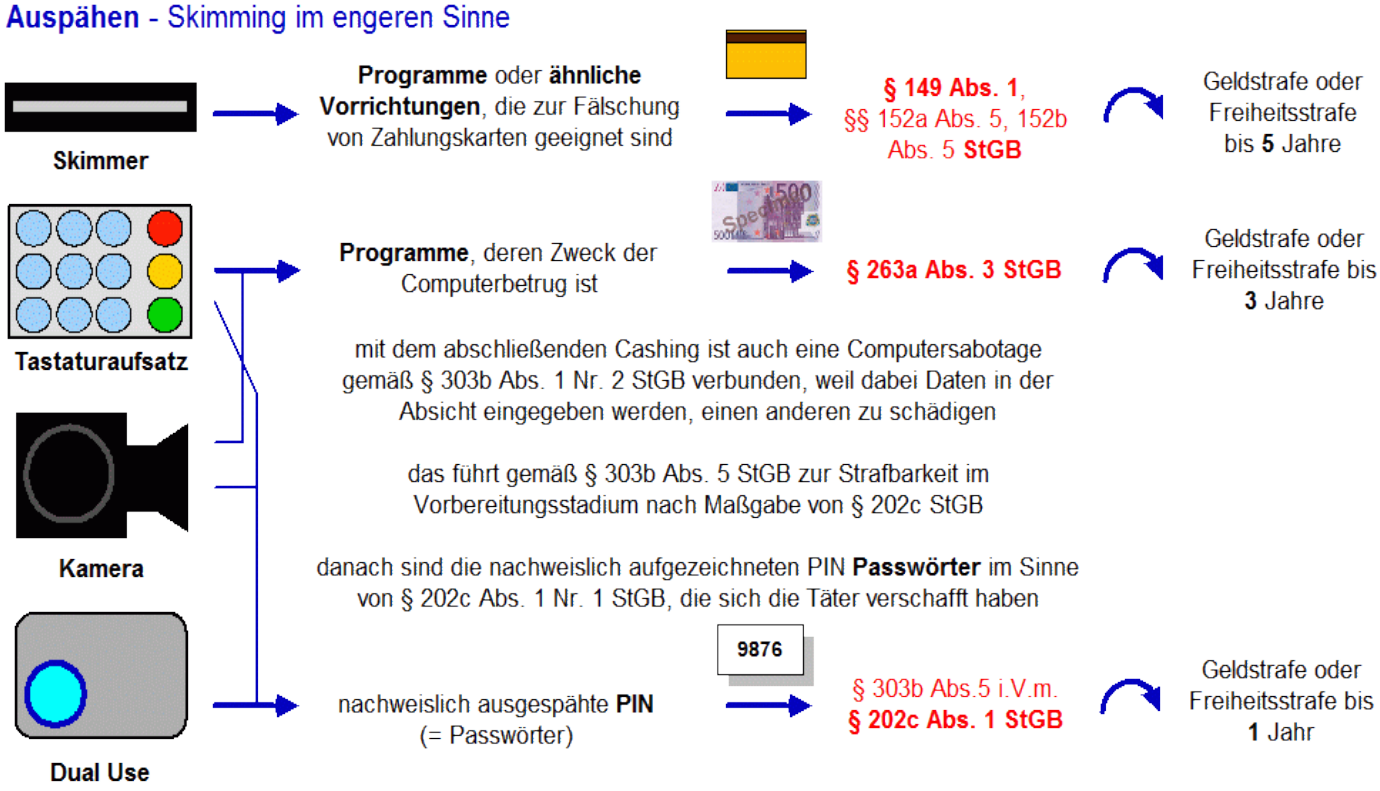
Das gilt besonders für die zum Ausspähen angepassten Kartenlesegeräte (Skimmer), die als „Programme oder ähnliche Vorrichtungen“ von § 149 Abs. 1 StGB genannt werden.

Die Geräte, die zum Ausspähen der PIN bestimmt sind, werden von dieser Vorschrift nicht erfasst, weil sie nicht zur Fälschung von Zahlungskarten dienen, sondern zu dem abschließenden Computerbetrug beim Cashing. Insoweit richtet sich die Strafbarkeit nach § 263a Abs. 3 StGB, die sich jedoch auf die Programme beschränkt, die zum Computerbetrug bestimmt sind. Das ist allein die Steuerung, die das Aufzeichnen und Speichern der PIN-Eingabe bewirkt.

Die Geräte zum Ausspähen der PIN als solche unterliegen deshalb nicht der Strafbarkeit bei der Vorbereitung des Computerbetruges.

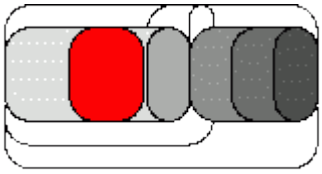
Eine weitere Einschränkung ergibt sich beim Einsatz handelsüblicher Mobiltelefone mit Kamerafunktion und digitaler Kameras, die ohne Änderung der werksseitigen Steuerung verbaut werden. Sie sind Dual Use-Produkte und sind deshalb strafneutral.

Auspähen - Skimming im engeren Sinne



Grafik3:

Einsatz von Skimminggeräten



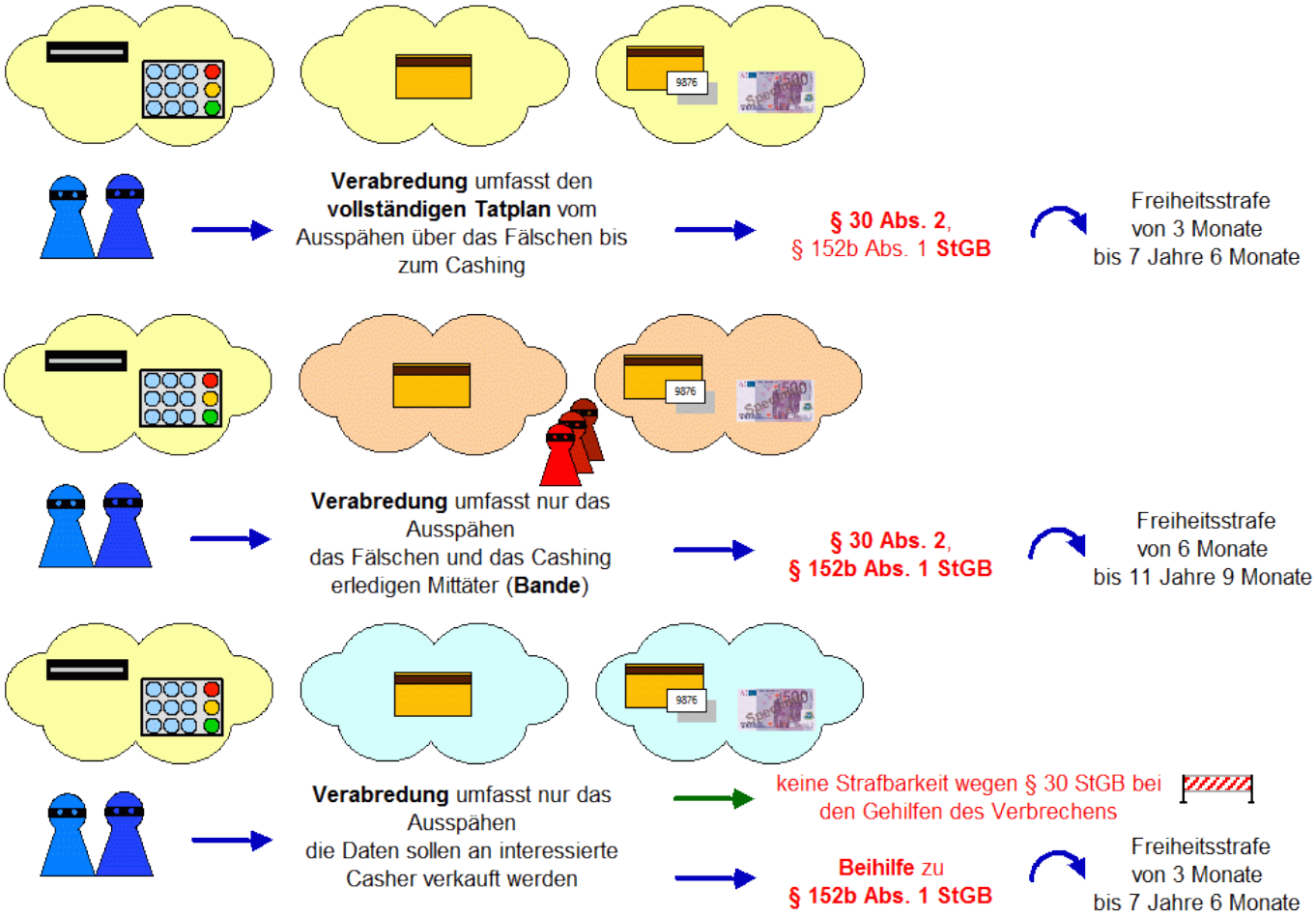
Mit dem Einsatz der Skimminggeräte ändert sich wegen der Kartenlesegeräte und der in den Attrappen verbauten Programmen nichts (Grafik 2).

Sobald jedoch jedoch erfolgreich zwei PIN ausgespäht wurden, greift auch die Computersabotage gemäß § 303b StGB. Auch sie kennt eine strafrechtliche Haftung im Vorbereitungsstadium, wobei § 303b Abs. 5 StGB auf den „Hackerparagraphen“ § 202c StGB verweist.

Danach ist es auch strafbar, sich Passwörter zu verschaffen, die zu schädlichen Dateneingaben verwendet werden sollen. Die Tathandlung ist nicht der Umgang mit den Ausspähgeräten, sondern der mit ihrem Einsatz verbundene Erfolg.

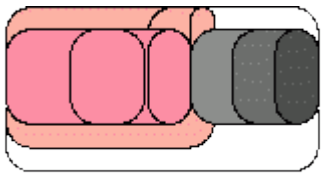
Bei strenger Auslegung müssen mindestens zwei PIN ausgespäht werden, bis die Strafbarkeit eintritt (Gesetzeswortlaut in Mehrzahl).

Verabredung zu einem Verbrechen



Grafik 4:

Verabredung zu einem Verbrechen



Die Strafbarkeit der Verabredung zu einem Verbrechen (§ 30 Abs. 2 StGB) verlangt nach einer Betrachtung des Täterwillens. Wenn mindestens zwei Täter das Skimming mit allen drei Tatphasen ausführen wollen, dann planen sie damit die Verbrechen des Fälschens und des Gebrauchs von Zahlungskarten mit Garantiefunktion.

Die vorgestellten Varianten orientieren sich an dem oben ausgeführten Beteiligungsmodell.

Planen die Täter, sich auf das Ausspähen zu beschränken, um die Daten dann an ihnen bekannte oder auch unbekannte Mittäter weiter zu geben, die das Cashing ausführen, müssen sie sich als Mittäter des abschließenden Verbrechens behandeln lassen. Auch sie machen sich bereits im Vorstadium nach § 30 StGB strafbar.

Anders sieht es jedoch bei den Tätern aus, die sich von vornherein auf das Ausspähen beschränken und die erlangten Daten an spezialisierte Casher verkaufen wollen. Die Skimmer sind zwar am Ende auch als Gehilfen des Gebrauchs von Zahlungskarten und des Computerbetruges strafbar. Gehilfen können sich jedoch nicht an einer Verbechensabrede beteiligen.

In diesen Fällen sind die Täter nicht wegen § 30 Abs. 2 StGB strafbar.

11. Nichtanzeige des geplanten Skimmings

Nicht Täter und Gehilfen, sondern die Mitwisser, die aus familiären oder sonstigen Loyalitätsgründen die Fälscher und Gebraucher kennen und möglicherweise unterstützen, werden von § 138 StGB mit Freiheitsstrafe bis 5 Jahre bedroht, wenn sie die geplante Straftat des Nachmachens oder Gebrauchens von Zahlungskarten mit Garantiefunktion nicht der Polizei oder der Staatsanwaltschaft anzeigen.

Noch schärfer kann das Strafrecht nicht reagieren.

12. Prüfungsschema

Kaum eine Kriminalitätsform kennt eine so breite Ausgestaltung der anwendbaren Vorschriften und der Beteiligungsformen wie das arbeitsteilige Skimming. Ich schlage deshalb ein grobes Prüfungsschema vor, das bei der Orientierung helfen soll.

12.1 vollendetes Cashing

① ***Kartenqualität***

①① *Zahlungskarte*

①② *Kredit- oder Finanzdienstleistungsinstitut*

①③ *Sicherheitsmerkmale*

Die Bejahung von ①① bis ①③ führt zur Anwendung des § 152a StGB.

①④ *Garantiefunktion*

①⑤ *Sicherheitsmerkmale*

Die zusätzliche Bejahung von ①④ und ①⑤ führt zur Anwendung von § 152b Abs. 1 StGB. Für alle 5 Prüfungsmerkmale gilt die Faustformel, dass der erfolgreiche Missbrauch gefälschter Karten mit erfolgreicher Autorisierung die Originale als Zahlungskarten mit Garantiefunktion ausweist. Wurde die verfälschte Karte im Lastschriftverfahren eingesetzt, so ändert das nichts an der Fälschungshandlung, sondern nur im Zusammenhang mit dem missbräuchlichen Einsatz zum Schadenseintritt beim Akzeptanten (Einzelhändler) und nicht beim Bankkunden. Die Sicherheitsmerkmale i.S.v. ①⑤ können dieselben wie bei ①③ sein.

② ***Fälschung***

②① *Verfälschen*
Manipulation des Magnetstreifens

②② *Nachmachen*
Herstellung von WhiteCards

Die Alternativen von ②① und ②② führen zur Strafbarkeit wegen des Herstellens von Zahlungskarten.

③ ***Gewahrsam***

Derjenige, der ver- oder gefälschte Karten bei sich führt, hat sie sich zumindest verschafft.

④ ***Gebrauch***

④① *Einstecken der Karte* in das Lesegerät.

④② *Eingabe der PIN*

④③ *„Bestätigung“*

④④ *Entnahme des Geldes*

Spätestens mit ④① beginnt auch der Versuch des Computerbetruges. Mit ④③ ist der Gebrauch der Zahlungskarte vollendet. Mit ④④ ist auch der Computerbetrug vollendet. Alle weiteren Missbrauchshandlungen führen zu einer deliktischen Einheit, wenn sie in einem engen räumlich zeitlichen Zusammenhang geschehen.

⑤ ***Qualifizierung***

⑤① *gewerbsmäßiges Handeln*

⑤② *arbeitsteiliges Handeln*

⑤②① *Zusammenarbeit beim Cashing*

⑤②② *Zusammenarbeit mit Hinterleuten*

⑤②③ *Zusammenarbeit mit Skimmern*

⑤③ *bandenmäßiges Handeln*

Die Bejahung von ⑤① oder ⑤③ führt zur qualifizierten Strafbarkeit gemäß § 152b Abs. 2 StGB. ⑤③ setzt den Zusammenschluss von mindestens 3 Tätern voraus, so dass nach der delikti-

schen Abrede und der Beteiligung anderer Täter gefragt werden muss (⑤②). Die Qualifizierungen durch ⑤① oder ⑤③ führen auch zu einem besonders schweren Fall des Computerbetruges gemäß §§ 263a Abs. 2, 263 Abs. 3 Nr. 1 StGB als Vergehen (§ 12 Abs. 3 StGB). Wenn ⑤① und ⑤③ vorliegen handelt es sich um ein selbständiges Verbrechen nach §§ 263a Abs. 2, 263 Abs. 5 StGB.

12.2 Ausspähen von Karten und PIN bei vollendetem Cashing

⑥ *Tatplan der Skimmer*

Während ⑤②③ nach der inneren Tatseite der Casher fragt, geht es bei ⑥ um den Vorsatz der Skimmer. Die Erfahrungen mit arbeitsteiligen Skimmingtätern lassen grundsätzlich eine qualifizierte (⑤①, ⑤③) Mittäterschaft erwarten, durch die sich die Skimmer den deliktischen Taterfolg der Casher nach § 25 Abs. 2 StGB zurechnen lassen müssen. Die Skimmer, die ihre ausgespähten Daten an beliebige Casher verkaufen oder verkaufen lassen, machen sich als deren Gehilfen strafbar (§ 27 StGB).

12.3 Ausspähen von Karten und PIN ohne Cashing

❶ *Mittäterschaft*

Im mittäterschaftlichem Verbund stellt sich besonders die Frage nach dem Beginn des Versuchs. Das Ausspähen der Kartendaten erfolgt im Vorbereitungsstadium. Mit dem Versuch des Fälschens beginnen die „Ausspäher“ frühestens, sobald sie die ausgespähten Daten an ihre Hinterleute oder direkt an die Casher übermitteln, wenn sie die Vorstellung haben, dass die Empfänger dann unverzüglich mit dem Fälschen beginnen. Scheitert die weitere Tatausführung aus technischen Gründen oder weil Dritte die Tat vereiteln, bleiben sie strafbar wegen eines fehlgeschlagenen Versuchs.

Bei strenger Betrachtung des Versuchsbeginns ergeben sich noch andere Folgen:

❷ *Verbrechensabrede*

Die Strafbarkeit der Verbrechensabrede zwischen Skimmer und Casher beginnt bereits im Vorbereitungsstadium unmittelbar mit der Verabredung und dauert bis zur geplanten Vollendung durch die Casher an. War die Abrede auf Handlungen nach ⑤① oder ⑤③ ausgerichtet, so ergibt sich die Strafbarkeit der Skimmer in Bezug auf eine Tat nach § 152b Abs. 2 StGB, wobei der Strafrahmen gemäß §§ 30 Abs. 1 S. 2, 49 StGB gemildert werden muss. Er umfasst dann 6 Monate bis 11 Jahre 9 Monate Freiheitsstrafe. Der Umgang mit Skimmern (Kartenlesegeräte) führt dabei zu einer tateinheitlichen Handlung, wobei alle einzelnen Täterhandlungen zu einer materiellen zusammenfallen.

Bei einer gewerbs- und bandenmäßigen Abrede kommt tateinheitlich auch der Computerbetrug hinzu. Unter diesen Voraussetzungen besteht auch Tateinheit mit dem verbotenen Umgang bezüglich zum Computerbetrug bestimmten Programmen [224].

❸ *selbständiges Skimming*

Fehlt es sowohl an dem Cashing, am strafbaren Versuch wie auch an der Verbrechensabrede, so greifen ausschließlich die strafbaren Vorbereitungshandlungen [225].

Der Umgang mit Skimmern, also den präparierten Kartenlesegeräten [226], ist gemäß § 149 StGB mit Geldstrafe oder Freiheitsstrafe bis zu 5 Jahren bedroht.

Der Umgang mit Tastaturaufsätzen zum Ausspähen der PIN setzt den Einsatz von Programmen voraus, die für den Computerbetrug bestimmt sind. Das reicht zur Strafbarkeit im Vorbereitungsstadium gemäß § 263a Abs. 3 StGB mit ei-

[224] Siehe oben **7.2 Kameras** und **7.3 Tastaturaufsätze**.

[225] Siehe oben **7. Vorbereitungshandlungen**.

[226] Siehe oben **7.1 Kartenlesegeräte**.

nem Strafrahmen von Geldstrafe bis 3 Jahre Freiheitsstrafe aus.

Der Umgang mit Kameras zum Ausspähen der PIN ist differenziert zu betrachten. Werden sie mit besonderen, zum Ausspähen bestimmten Programmen ausgestattet, gilt für sie dieselbe Strafbarkeit wie für Tastaturaufsätze.

Werden zum Beispiel Kameraleisten oder präparierte Rauchmelder eingesetzt, in denen handelsübliche Dual Use-Komponenten ohne verbindendes Programm verbaut werden, dann entfällt eine Strafbarkeit gemäß § 263a Abs. 3 StGB. Sobald jedoch mindestens zwei PIN ausgespäht wurden, greift der Gefährdungstatbestand im Vorfeld der Computersabotage (§§ 303b Abs. 5, 202c StGB) und droht mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr [227].

13. Fazit

Gegen Fälscher hat der Gesetzgeber mit § 152b Abs. 1 StGB und gegen Fälscherbanden mit § 152b Abs. 2 StGB schwere Geschütze aufgefahren und Verbrechenstatbestände geschaffen. Das arbeitsteilige Skimming lässt sich damit gut erfassen, sobald Karten gefälscht und missbräuchlich eingesetzt werden. Das Leitbild des Gesetzgebers ist die Fälscherwerkstatt, in der Banknoten gefälscht werden. Die dabei genutzten Rohstoffe und Werkzeuge haben Eingang in den § 149 StGB gefunden. Ihre Herstellung und der Umgang mit ihnen ist mit Strafe bedroht.

In das Leitbild vom Fälscher hat der Gesetzgeber die modernen Zahlungsmittel und namentlich die Zahlungskarten nur mühsam eingefügt und dabei die Erscheinungsform des Skimmings nur unvollständig erfasst. Präparierte Kartenlesegeräte können gerade noch als Programme und ähnliche Vorrichtungen angesehen werden und die gleichermaßen gefährlichen PIN-Skimmer überhaupt nicht. Die Verweise auf strafbare Vorbereitungshandlungen aus dem Computerbetrug und der -sabotage beschränken sich auf Teilaspekte wie Programme und Zugangscodes und leiden unter gesetzessprachlichen Mängeln, was die Verwendung der Mehrzahl in § 202c StGB und der unerwartete Verweis aus § 303b StGB auf diese Vorschrift belegen. Die Klarheit, mit der das Gesetz die Tathandlungen beim Computerbetrug benennt (§ 263a StGB), fehlt im übrigen vollständig. Das führt zum Beispiel dazu, dass die Fälschung beweiserheblicher Daten (§ 269 StGB) als Anwendungsfall des Identitätsdiebstahls [228] auch unter juristischen Fachleuten kaum verbreitet ist und leicht übersehen wird.

Die wechselnden Erscheinungsformen der Cybercrime, zu der ich inzwischen auch das Skimming zähle, lassen eine Revision des Cyber-Strafrechts geraten erscheinen, das, wie beim Computerbetrug, allgemeine Handlungsformen benennt und damit allen Adressaten, Laien wie Fachleuten, klare und verständliche Richtlinien gibt. Der juristische Zickzacklauf, den die Verweise aus § 303b Abs. 5 StGB und § 263a Abs. 3 StGB verlangen, ist für alle Beteiligten unwürdig. Für den Gesetzgeber, für den Bürger, der keine Chance hat, das Richtige oder Falsche seines Handelns im Gesetz zu finden, und für die Polizei und die Justiz, die dieselben Probleme haben, um ihre Werkzeuge anzuwenden.

Der BGH hat immer wieder und bemerkenswert klare Linien gezogen. Dabei gilt der alte Grundsatz von Larenz, dass die Grenze der Auslegung vom Wortlaut des Gesetzes bestimmt wird. Demzufolge hat das Gericht recht, wenn es das Ausspähen von Kartendaten nicht als ein Ausspähen von Daten im Sinne von § 202a Abs. 1 StGB ansieht. Den Magnetstreifen fehlt ein Zugangsschutz in Form von Dongles oder Passwörtern für die Leseberechtigung.

Den vom Skimming betroffenen Bürgern ist das egal. Sie fühlen sich vom Skimming bedroht und verängstigt, weil sie ihren Kontoabrechnungen misstrauen, sie prüfen und beanstanden müssen. Die Finanzwirtschaft unternimmt beachtliche Anstrengungen und die Durchsetzung des MM

[227] Siehe oben **2.3 PIN-Skimming und Computersabotage**.

[228] Siehe CF, Missbrauch fremder Identitäten. Carding, 22.11.2008.

und des Schadensausgleiches fordern Respekt. Warum aber hapert es an der Einführung des EMV-Chips, warum wird dessen Programmierung nicht richtig geprüft und warum erfährt man nichts von international wirksamen Bemühungen, dem Cashing-Spuk ein Ende zu bereiten? Statt dessen erfährt man nebenbei, dass EMV-Chips von Geldautomaten umprogrammiert werden können. Ein wirksamer Lese- und Schreibschutz würde nach einer festen Verdrahtung nach dem Vorbild von Risk-Prozessoren verlangen. Solche Komponenten bilden eine physikalische Einheit und könnten nicht manipuliert, aber auch nicht softwaremäßig repariert werden. Kombiniert mit dem MM und einer Verfeinerung der Autorisierung bestände so gut wie gar keine Chance, Dubletten anzufertigen. Heute reichen hingegen schlichte WhiteCards dazu, mehrere Tausend Euro Schaden zu verursachen!

D. Strafverfahren

1. geheime Ermittlungen

Sowohl der gewerbsmäßige Computerbetrug gemäß § 263a Abs. 2 i.V.m. § 263 Abs. 3 Nr. 1 StGB wie auch die Fälschung von Zahlungskarten gemäß § 152a Abs. 1 i.V.m. § 152b Abs. 1, Abs. 2 StGB sind Katalogstraftaten im Sinne von § 100a Abs. 2 Nr. 1. lit e), lit n) StPO. Der Gesetzgeber betrachtet beide Kriminalitätsformen als besonders schwere Kriminalität, die nach der Definition des BVerfG dadurch gekennzeichnet ist [229], dass die angedrohte Höchststrafe mehr als 5 Jahre Freiheitsstrafe beträgt. Zuletzt im Zusammenhang mit den Verkehrsdaten hat das BVerfG ausgeführt [230]:

„Der Gesetzgeber hat in § 100a Abs. 2 StPO die dort benannten Straftaten als so schwer eingestuft, dass sie nach seiner Einschätzung eine Überwachung der Telekommunikation rechtfertigen … der in § 100a Abs. 2 StPO enthaltene Straftatenkatalog <liefert> *eine Leitlinie dafür, welche Straftaten der Gesetzgeber als so schwerwiegend bewertet, dass sie auch gewichtige Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG rechtfertigen können.“*

Demzufolge stehen für die Ermittlungen auch die geheimen Maßnahmen im Sinne von § 101 StPO zur Verfügung, wenn die Voraussetzungen auch im Einzelfall vorliegen (siehe vor Allem § 100a Abs. 1, § 100g StPO und § 163f sowie § 100h Abs. 1 Nr. 2 StPO).

2. Organisierte Kriminalität

Das Skimming ist jedenfalls dann Organisierte Kriminalität, wenn es von arbeitsteilig aufgestellten Tätergruppen ausländischer Herkunft ausgeübt wird. Es gehört zum Kriminalitätsfeld „Fälschung und Missbrauch unbarer Zahlungsmittel“, die als ein Schwerpunkt der Organisierten Kriminalität angesehen werden [231]. Die bisher bekannten Erscheinungsformen im Zusammenhang mit Tätergruppen ausländischer Herkunft lassen zudem geschäftsähnliche Strukturen erkennen [232].

Das führt dazu, dass die Strafverfolgungsbehörden besonders eng zur Bekämpfung dieser Kriminalitätsform zusammen arbeiten sollen. Die Staatsanwaltschaft ist berechtigt, die Strafverfolgung von Nebenbeteiligten zunächst zurück zu stellen, um die Haupttäter dingfest zu machen [233].

[229] BVerfG, Urteil vom 03.03.2004 - 1 BvR 2378/97, 1 BvR 1084/99

[230] BVerfG, Beschluss vom 11.03.2008 - 1 BvR 256/08

[231] Nr. 2.3 der Anlage E zu den RiStBV.

[232] Nr. 2.1 der Anlage E zu den RiStBV.

[233] Nr. 4.2.4 der Anlage E zu den RiStBV.

E. kriminalistische Erfahrungen

Obwohl bislang nur wenige Skimmingtäter gefasst werden konnten und ihre Verurteilungen noch rar sind [234], lassen sich bereits einige Erfahrungswerte formulieren, die für die Bewertung in anderen und neuen Verfahren herangezogen werden können [235].

1. Programm

Das Ziel des Skimmings ist der Missbrauch von Zahlungs- und Kreditkarten, um Beute zu machen.

Diese programmatische Aussage unterliegt einer Einschränkung. Es ist denkbar, dass Skimmer in der Absicht handeln, die ausgespähten Daten nicht selber zu missbrauchen oder durch Mittäter missbrauchen zu lassen. Wenn sie sie verkaufen wollen, dann wissen sie, dass der Käufer nur deshalb bezahlt, weil die Daten einen kriminellen Marktwert haben und den haben sie nur, wenn sie auch missbraucht werden. In diesem Bewusstsein machen sie sich zu Beihilfetätern zum finalen Cashingangriff, auch ohne die daran beteiligten Täter zu kennen.

Die kurzen Zeiten, die jetzt zwischen dem Skimming und dem Cashing liegen, lassen jedoch gut strukturierte Banden erwarten (siehe unten).

2. Garantiefunktion

Aus der Tatsache, dass das Cashing mit Dubletten von Debitkarten im Ausland erfolgreich war, lassen sich mehrere sichere Schlüsse ziehen:

Es liegt eine Debitkarte zugrunde, die am Point of Sale-Verfahren teilnimmt.

Die Transaktion hat das Autorisierungsverfahren erfolgreich durchlaufen. Dem Geldautomaten ist der Genehmigungscode übermittelt worden.

Die Genehmigung im Rahmen der Autorisierung ist der Kern der Garantiefunktion, die der Ursprungskarte inne wohnt.

Es wurde eine gefälschte Zahlungskarte mit Garantiefunktion genutzt.

Die vier abgeleiteten Aussagen fußen auf der Norm ISO 8583 und der Annahme, dass kein Institut, das einen Geldautomaten betreibt, Geld an jedermann verschenken, sondern Gewinn in Höhe der Gebühr erzielen will.

3. Ausspähen

Den Skimmingvorgang als solchen habe ich lange unterschätzt. Das Ausspähen setzt voraus, dass die eingesetzte Hardware zu den Geldautomaten passt, die Umgebung stimmt und die Täter vor Ort in kürzester Zeit handwerkliches Geschick beweisen, um ihre Hardware an die Umgebung anzupassen. Das ist kein Job für Anfänger!

3.1 Vorerkundung

Vor dem Skimming müssen die Örtlichkeiten und die geeigneten Geldautomaten ausbaldowert werden.

Es mag spontane Skimmingangriffe geben. An den Täter, der 'mal so locker Freitag Nachmittag durch die Gegend streift, um geeignete Geldautomaten zu finden, glaube ich hingegen nicht.

Alle Anzeichen sprechen vielmehr dafür, dass in Vorbereitung des Skimmings entweder die Späher oder gut eingeweihte Beteiligte die Umgebung von Banken erkunden, die sich zum Skimming lohnen.

---

[234] Jüngst: Urteil des Landgerichts Hannover vom 17.11.2009 gegen zwei Skimmer, die zu langjährigen Freiheitsstrafen verurteilt wurden; siehe CF, Skimming-Rechtsprechung, 18.11.2009

[235] Siehe CF, Erfahrungswerte wegen des Skimmings, 29.11.2009

3.2 Spezialisten

Skimmer haben in der kriminellen Organisation eine besonders vertrauensvolle Rolle. Die eingesetzten Geräte sind wertvoll, sollen weiter verwendet und müssen pfleglich behandelt werden.

Die Geräte, die die Skimmer verwenden, verlangen nach einer gewissen Anerkennung, soweit es um ihre handwerkliche Gestaltung geht. Dies vorausgesetzt: Mit solchen Teilen lässt man keine Anfänger in der Gegend herumlaufen.

Auch Skimmer brauchen Lehrlinge. Sie müssen das Geschäft unter der Anleitung von Fachleuten lernen. Eine Skimmergruppe, die nur aus angelernten Dilettanten besteht, gibt es jedoch nicht.

Daraus folgt:

Die Installation der Ausspähgeräte erfordert Erfahrung, handwerkliches Geschick und die Anpassung der Geräte an die örtlichen Begebenheiten.

Und:

Skimmer arbeiten arbeitsteilig.

Für die zweite Aussage gibt es hinreichende Belege, die zeigen, dass es Fachleute für die Einrichtung der Kartenlesegeräte und andere für die Ausspähtechnik im Übrigen gibt (Tastaturaufsatz, Kamera). Darüber, ob die Zuständigkeit unter den Tätern auch wechseln kann, gibt es keine hinreichenden Erfahrungen.

3.3 Einsatz

Je nach der Art des Angriffs müssen - jedenfalls beim Kartenlesegerät - Marker für die Synchronisation der ausgespähten Daten gesetzt werden.

Eine schwierige Aufgabe ist es, die ausgespähten Kartendaten und PIN zu einem Dump zu synchronisieren. Nur synchronisierte Dumps können erfolgreich missbraucht werden.

In vielen Fällen hat es sich gezeigt, dass dazu am Skimmer Testkarten eingesetzt werden. Mit ihnen und ihren bekannten Daten lassen sich die Zeitphasen beim Ausspähen segmentieren und präzisieren.

Daraus folgt auch:

Skimmer beobachten den Tatort und kontrollieren zwischenzeitlich die Geräte (Funktionstüchtigkeit, Akkuladung).

Der Einsatz von Testkarten und die Funktionsprüfung des Ladezustandes der verwendeten Kameras oder anderer Geräte erfordern es, dass die Skimmer den Einsatzort kontinuierlich beobachten und zur Kontrolle betreten.

Dieses Vorgehen ist durch Kameraaufnahmen belegt.

4. Abstimmung und Bericht

Skimmer benutzen am Tatort Mobiltelefone, um sich mit ihren Mittätern und Hinterleuten abzustimmen und den Beginn, Verlauf und Abschluss der Maßnahme zu melden.

Überraschend viele Belege gibt es dafür, dass die Skimming-Täter, Skimmer wie auch Casher, Mobiltelefone am Tatort oder in seiner unmittelbaren Nähe nutzen. Sie zeigen, dass diese kleinen Tätergruppen mit anderen Beteiligten in Verbindung stehen, sich mit ihnen abstimmen und Bericht erstatten. Bei den Cashern kommt hinzu, dass Fotos belegen, dass sie während des Karteneinsatzes telefonieren. Daraus lässt sich schließen, dass sie sich die PIN übermitteln lassen.

Ein weiteres Ergebnis dieser Erfahrungen ist, dass beim Skimming in aller Regel fest gefügte Banden im Einsatz sind.

5. Banden

Für mittäterschaftliche und Bandenstrukturen im Zusammenhang mit Skimmingtaten sprechen verschiedene Erfahrungen.

Sowohl für das Skimming als auch für das Cashing müssen die geeigneten Standorte und

Geldautomaten erkundet werden. Das ist eine gute Aufgabe für „Repräsentanten“, die die Logistik für die aktiven Täter zur Verfügung stellen und deren Einsätze vorbereiten.

Jedenfalls die Skimmer „fliegen“ zu ihren Einsätzen ein und halten sich nur kurzfristig im Inland auf. Sie quartieren sich bei Bekannten oder in Billig-Hotels ein, leihen sich Autos und skimmen nacheinander an mehreren, aber wenigen lukrativ erscheinenden Tatorten. Danach verlassen sie wieder das Inland.

Skimming-Täter sind rege Telefonierer. Ich halte sie aber nicht für stressresistent, so dass nicht zu erwarten ist, dass sie liebreizende Gespräche mit ihren Freundinnen führen. Sie dürften sich eher mit ihren Mittätern und Hinterleuten abstimmen.

Die kürzesten Abstände zwischen Skimming und Cashing betragen inzwischen zwei Tage. Allein diese kurze Spanne spricht für schlagkräftige Organisationen, die in der Lage sind, binnen kürzester Zeit gefälschte Zahlungskarten herzustellen und Casher damit auszustatten.

Anhang 1: Rechtsprechungsübersicht

Die in diesem Arbeitspapier angesprochene Rechtsprechung im Überblick:

Ausspähen von Daten (§ 202a Abs. 1 StGB)
BGH, Beschluss vom 18.03.2010 - 4 StR 555/09
BGH, Beschluss vom 14.01.2010 – 4 StR 93/09
BGH, Urteil vom 10.05.2005 – 3 StR 425/04

Bande
BGH, Beschluss vom 22.03.2001 - GSSt 1/00

Bande, Abgrenzung zur **Vereinigung**
BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

Bande, Firmenmantel (Vorbereitungsstadium)
BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

Bande, kein Organisationsstrafrecht
BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

Bande, Qualifikationsmerkmal
BGH, Urteil vom 03.12.2009 - 3 StR 277/09

Bande, spontaner Tatentschluss
BGH, Urteil vom 21.12.2007 - 2 StR 372/07

Bande, unbekannte Beteiligte
BGH, Urteil vom 16.06.2005 - 3 StR 492/04

Bande, Zurechnung
siehe Mittäter, Grenzen der Zurechnung

bedingter Vorsatz
BGH, Urteil vom 28.01.2010 - 3 StR 533/09

Bewertungseinheit (BtM)
BGH, Beschluss vom 19.12.2000 - 4 StR 503/00

Cashing, Tateinheit bei mehreren Handlungen (§ 52 StGB)
BGH, Urteil vom 10.05.2005 - 3 StR 425/04

Cashing, Tatmehrheit (§ 53 StGB)
BGH, Urteil vom 10.05.2005 - 3 StR 425/04

Computerbetrug (Tateinheit)
BGH, Beschluss vom 23.06.2010 – 2 StR 243/10

deliktische Einheit (§ 152a StGB)
BGH, Urteil vom 21.09.2000 - 4 StR 284/00
BGH, Beschluss vom 26.01.2005 - 2 StR 516/04
BGH, Beschluss vom 07.03.2008 - 2 StR 44/08

Dual Use
siehe Hackerstrafrecht

Eingehungsschaden
BGH, Beschluss vom 07.12.2010 - 3 StR 433/10

Fälschung, optische und digitale **Merkmale** von Zahlungskarten
BGH, Urteil vom 13.01.2010 – 2 StR 439/09

Fälschung, minder schwerer Fall
BGH, Urteil vom 21.09.2000 - 4 StR 284/00

Fälschung, Schutzzweck (§ 152a StGB)
BGH, Urteil vom 21.09.2000 - 4 StR 284/00

Fälschung, Tateinheit bei mehreren Handlungen (§ 52 StGB)
BGH, Beschluss vom 07.03.2008 - 2 StR 44/08
Fälschung, Versuchsbeginn (§ 152a StGB)
BGH, Urteil vom 13.01.2010 – 2 StR 439/09
OLG Thüringen (Jena), wistra 2009, 204

fortgesetzte Handlung
BGH, Großer Senat, Beschluss vom 03.05.1994 - GSSt 2/93, 3/93
BGH, Urteil vom 20.06.1994 - 5 StR 595/93

Garantiefunktion (§ 266b StGB)
BGH, Urteil vom 12.05.1992 - 1 StR 133/92

Garantiefunktion bei Verwendung im **Lastschriftverfahren**
BGH, Urteil vom 21.09.2000 - 4 StR 284/00

Garantiefunktion, Täterwille
BGH, Beschluss vom 17.06.2008 - 1 StR 229/08

Gefährdungsschaden
BVerfG, Beschluss vom 23.06.2010 - 2 BvR 2559/08, 105/09, 491/09

BGH, Beschluss vom 18.11.2009 - 4 StR 485/08

Gehilfe (§ 27 StGB)
BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09

gewerbsmäßiges Handeln
BGH, Beschluss vom 01.09.2009 - 3 StR 601/08

Hackerstrafrecht, Dual Use (§ 202c StGB)
BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07, 1151/08, 1524/08

Hintermann
BGH, Urteil vom 26.07.1994 - 5 StR 98/94

Konkurrenz zwischen Zahlungsmittel- und Urkundenfälschung
BGH, Beschluss vom 26.01.2005 - 2 StR 516/04

Kontoeröffnungsbetrug, Geschädigter (POZ)
BGH, Beschluss vom 18.11.2009 - 4 StR 485/08

Kreditkarte (§ 152b StGB)
BGH, Urteil vom 13.01.2010 - 2 StR 439/09

mafiöse Struktur
siehe Hintermann

Mittäter (§ 25 Abs. 2 StGB)
BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09
BGH, Beschluss vom 13.01.2010 - 5 StR 506/09

Mittäter, Einzelbetrachtung der Beteiligten
BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

Mittäter beim Skimming
BGH, Urteil vom 17.02.2011 – 3 StR 419/10
BGH, Urteil vom 27.01.2011 - 4 StR 338/10

Mittäter, Zurechnung der Vollendung, Schaden
BGH, Beschluss vom 13.08.2002 - 4 StR 208/02
BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

Mittäter, Grenzen der Zurechnung
BGH, Beschluss vom 29.07.2009 - 2 StR 160/09

Mittäterexzess
BGH, Beschluss vom 16.09.2009 - 2 StR 259/09

mittelbare Täterschaft
siehe Hintermann

natürliche Handlungseinheit
siehe deliktische Einheit

Prozesserklärung
siehe Verteidigererklärung

Rücktritt vom Versuch, Anhaltspunkte (§ 24 StGB)
BGH, Urteil vom 20.05.2009 - 2 StR 576/08

schadensgleiche Vermögensgefährdung
BverfG, Beschluss vom 10.03.2009 - 2 BvR 1980/07
BGH, Beschluss vom 18.02.2009 - 1 StR 731/08
BGH, Urteil vom 13.08.2009 - 3 StR 576/08

Skimmer, Umgang (§ 149 StGB)
BGH, Urteil vom 16.12.2003 - 1 StR 297/03

Skimming, Tateinheit bei mehreren Handlungen (§ 52 StGB)
BGH, Urteil vom 10.05.2005 - 3 StR 425/04
BGH, Beschluss vom 07.12.2010 - 3 StR 433/10
BGH, Beschluss vom 02.02.2011 - 2 StR 511/10

Strafdrohung (§ 152b StGB)
BVerfG, Beschluss vom 18.03.2009 - 2 BvR 1350/08

Tateinheit; **Gebrauch** (§ 152a StGB) und **Betrug** (§ 263 StGB)
BGH, Urteil vom 21.09.2000 - 4 StR 284/00

Tateinheit, **Gebrauch** (§ 152a StGB) und **Computerbetrug** (§ 263a StGB)
BGH, Beschluss vom 23.06.2010 – 2 StR 243/10
BGH, Urteil vom 10.05.2005 – 3 StR 425/04
BGH, Beschluss vom 13.01.2010 - 4 StR 378/09

Verabredung zu einem Verbrechen (§ 30 StGB), ausschließlich **Mittäter**
BGH, Urteil vom 04.02.2009 - 2 StR 165/08

Verabredung zu einem Verbrechen mit **mehreren Handlungen**
BGH, Urteil vom 13.01.2010 - 2 StR 439/09

Verfälschung einer Zahlungskarte
BGH, Urteil vom 21.09.2000 - 4 StR 284/00

Versuch, Strafmaß
BGH, Beschluss vom 28.09.2010 - 3 StR 261/10

Versuch, vorgelagerte Handlungen
BGH, Urteil vom 09.03.2006 – 3 StR 28/06

Versuchsbeginn (Fälschung)
BGH, Urteil vom 27.01.2011 - 4 StR 338/10

BGH, Beschluss vom 14.09.2010 - 5 StR 336/10

Versuchsbeginn („jetzt geht es los!“)
BGH, Beschluss vom 07.11.2007 - 5 StR 371/07

Verteidigererklärung
BGH, Urteil vom 20.06.2007 - 2 StR 84/07

Vertraulichkeit und Integrität informationstechnischer Systeme
BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07

Zahlungskarte, EC-Karte
BGH, Urteil vom 21.09.2000 - 4 StR 284/00

Anhang 2: Glossar

Siehe auch das ▸ Glossar kartensicherheit.de.

Autorisierung: Automatisches Genehmigungsverfahren im bargeldlosen, kartengestützten Zahlungsverkehr.

Carder: Auf den Missbrauch von Karten spezialisierter Täter.

Casher: Am Cashing beteiligter Täter.

Cashing: Missbrauch ausgespähter Kartendaten und PIN mit gefälschten Karten an Geldautomaten.

Clearing: Automatisches Verrechnungsverfahren zwischen den Banken und Verrechnungsstellen im bargeldlosen Zahlungsverkehr.

CPD: Conto pro Diverse. Bankinternes Konto zur Buchung unbestimmter oder vorläufiger Zahlungsbewegungen, zum Beispiel zwischen Autorisierung und Clearing.

Debitkarte: Zahlungskarte auf Guthabenbasis. Als Guthaben gilt auch der eingeräumte Überziehungskredit.

Dump: Vollständiger Datensatz von einer Karte einschließlich PIN. Bei der Kreditkarte gehört auch die Prüfnummer dazu.

EMV-Chip: Im Kartenkörper integrierter Speicherchip, der die Autorisierungsdaten und weitere Informationen enthält (zum Beispiel über Guthaben auf der Karte). Das Kürzel leitet sich von **E**uroCard, **M**aster und **V**isa ab.

EURO Kartensysteme - EKS: Deutscher Dachverband, der den Schadensausgleich ausführt und die Kartensicherheit standardisiert.

Euroscheck: Papiergebundene Auszahlungsgarantie der ausgebenden Bank, die sich in dem Euroscheck verkörperte. Die Autorisierung erfolgte dezentral anhand der EC-Karte. Das System endete 2001. Das Kürzel **EC** wird weiter verwendet für „electronic cash“.

Front Covering: Vollständige Fassade vor einem Geldautomaten mit eingebautem Skimmer und Tastauraufsatz.

Garantiefunktion: Auszahlungsgarantie des Kartenausstellers für Debit- und Kreditkarten im Rahmen der Autorisierung.

Geldautomat: Kurzform für Geldausgabeautomat, der von einem Finanzdienstleister betrieben wird und am grenzüberschreitendem Autorisierungsverfahren teilnimmt.

IT: Informationstechnik. Oberbegriff für vernetzte elektronische Informations- und Kommunikationsdienste.

Kameraleiste: Auspähhardware mit integrierter Kamera zum Beobachten der PIN-Eingabe.

Karte: Kreditkarten und Zahlungskarten.

Kopfstelle: Regionale (Rechenzentrum eines Bankenverbundes, z. B. Finanz IT der Sparkassen),
nationale (z. B. First Data Corporation) oder internationale Kontaktstelle für die Autorisierung und das anschließende Clearing (z.B. MasterCard International).

Kreditkarte: Karte mit einer (auch limitierten) Zahlungsgarantie vom Kartenaussteller. Die Verfügungen werden gegen ein selbständiges Kreditkonto des Kunden gebucht

Magnetstreifen: Datenträger auf einer beliebigen Karte, auch White Card. In dem hier verstandenen Sinne enthält der M. die für die Autorisierung nötigen Kartendaten.

Maestro: Debitkartendienst von MasterCard International.

MasterCard: Internationale Dachgesellschaft für Kreditkarten (neben American Express, Diners Club und Visa).

Merkmalstoff: siehe MM

MM: Maschinenlesbares Merkmal; besondere Fälschungssicherung. Es handelt sich um einen in den Kartenkörper eingebetteten Merkmalstoff, der codiert werden kann. Die Codierung wird vom Geldautomaten anhand eines Prüfwertes geprüft, der sich auf dem Magnetstreifen befindet. Das Verfahren wird nur in Deutschland angewendet.

Persönliche Identifikationsnummer – PIN: Vom Kartenaussteller bestimmte Ziffernfolge zur Autorisierung des Karteninhabers.

Phishing: Kriminalitätsform, bei der die Daten des Online-Bankings ausgespäht und zu Kontomanipulationen missbraucht werden.

POS: Point of Sale. Einsatzort einer Karte am Geldautomaten oder im Einzelhandel.

POS-Skimming: Skimming unter Einsatz manipulierter POS-Terminals.

POS-Terminal: Kombiniertes Eingabegerät für Karten und PIN über ein Tastenfeld (Einzelhandel).

Skimmer: a) Ausspähhardware für Geldautomaten. Zum Speichern oder Weiterleiten präpariertes Kartenlesegerät, das die Magnetstreifen von Karten ausliest.

Skimmer: b) Täter, der Ausspähhardware installiert, betreibt und überwacht.

Skimming: a) Im engeren Sinne: Ausspähen von Kartendaten und PIN durch Einsatz von Ausspähhardware.

Skimming: b) Im weiteren Sinne: Kriminalitätsform, die sich zum Missbrauch gefälschter Karten ausgespähter Daten bedient.

Tageslimit: Täglicher Höchstbetrag, der bei der Autorisierung zugelassen wird.

Tastaturaufsatz: vollständige Abdeckung der Tastatur am Geldautomaten zur Prokollierung der PIN.

Testkarte: Magnetstreifenkarte, mit der der Skimmer die Funktion des Lesegeräts prüft und mit der er Marker in der Liste der ausgespähten Kartendaten setzt (zur Zuordnung der ebenfalls ausgespähten PIN).

White Card, White Plastic: Unbedruckter Kartenrohling mit Magnetstreifen.

Wochenlimit: Wöchentlicher Höchstbetrag, der bei der Autorisierung zugelassen wird.

Zahlungskarte: Debitkarte für Verfügungen auf Guthabenbasis einschließlich Überziehungskredit oder Kreditkarte. Beide Karten sind für das Autorisierungsverfahren geeignet.

Anhang 3:
Cybercrime und Strafverfolgung

Die Webseite ▸ cyberfahnder.de widmet sich seit 2007 der Cybercrime, ihren Erscheinungsformen und ihrer Strafverfolgung. Dazu gehören die technischen Grundlagen, soweit sie zum Verständnis nötig sind, die Auseinandersetzung mit den einschlägigen Gesetzen und der Rechtsprechung. Die Arbeitspapiere fassen die wesentlichen Aufsätze, Beiträge und Meldungen zusammen.

Im Juli 2010 ist das ▸ Arbeitspapier Netzkommunikation erschienen, das sich mit den Grundlagen der Telekommunikation und des Internets befasst. Von der Adressierung in den Netzen führt das Arbeitspapier über das Routing und die Verschlüsselung zu den Manipulationen im Internet, zu den Schurkenprovidern und schließlich zu der Feststellung, dass wir uns in einer Phase des Kalten Cyberwars befinden. Wenn das zunächst noch eine kühne These war, so wurde sie dennoch von den weiteren Ereignissen seit dem Sommer 2010 immer wieder bestätigt. Das bezeugt zunächst das ▸ Arbeitspapier Eskalationen aus dem Februar 2011, das sich mit den zielgenauen Angriffen seit 2010, mit WikiLeaks, der neuen Qualität des Hacktivismus und dem Schutz Kritischer Infrastrukturen auseinander setzt.

Das ▸ Arbeitspapier Cybercrime erschien im Mai 2010 und fasst die seit 2007 entstandenen Beiträge und Aufsätze über die Erscheinungsformen und Strukturen der Cybercrime zusammen. Es ist dadurch zu einer Art Grundwerk geworden, auf denen die neueren Ausarbeitungen aufbauen.

Das gilt zunächst für zwei kleinere Arbeitspapiere: Im März 2010 gab McAfee eine Studie von Paget über die mafiösen Erscheinungsformen der Cbercrime und dem Hacktivismus heraus [236], die mich wegen ihrer Materialfülle und Betrachtungsweise begeistert hat. Der Text ist jedoch nur in englischer Sprache erschienen, so dass ich ihn im Oktober 2010 in freier Form nacherzählt und gelegentlich kommentiert habe [237]. Das Faktenmaterial von Paget habe ich schließlich angereichert und zu einer Zeitgeschichte der Cybercrime verarbeitet [238].

Im Oktober 2011 erschien schließlich das ▸ Arbeitspapier zum IuK-Strafrecht, das bis einschließlich November 2011 860 Mal abgerufen wurde. Es beschreibt typische Erscheinungsformen der Cybercrime und stellt ihnen die einschlägigen Straftatbestände zur Seite. Das gilt besonders für die Verbreitung von Malware und ihre besonderen Ausprägungen als Onlinebankingtrojaner und zur Steuerung von Zombies in Botnetzen.

Die Auseinandersetzung mit der Strafbarkeit der kriminellen Erscheinungsformen zeigt, dass zwar einzelne Strafbarkeitslücken bestehen, im Ganzen betrachtet aber ein differenziertes System von Strafnormen besteht, das die Strafverfolgung möglich macht. Sie bestätigt auch die Erfahrung, die ich bei der Befassung mit dem Skimming gemacht habe: Die wirkliche Dimension der Strafbarkeit erschließt sich erst, wenn man den zugrunde liegenden Tatplan vollständig erfasst. Dann erweisen sich nämliche viele Formen der Cybercrime als Verbrechen, deren Verfolgung bereits in einem frühen Stadium der Tatplanung und -ausführung möglich ist [239].

---

[236] François **Paget**, Cybercrime and Hacktivism, McAfee Labs 15.03.2010

[237] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010

[238] Dieter **Kochheim**, Eine kurze Geschichte der Cybercrime, 03.11.2010

[239] Verabredung zu einem Verbrechen (§ 30 Abs. 2 StGB).

Zuerst habe ich mich mit dem Skimming in der Form eines Arbeitspapiers im Mai 2009 befasst [240]. Es erörtert vor allem sich mit den Fälschungstatbeständen (§§ 152a, 152b StGB) und den verschiedenen Haftungsnormen für das Vorbereitungsstadium (§§ 30, 149 Abs. 1, 263 Abs. 3 StGB). Daraus entstand im Dezember 2009

das ▸ erste Arbeitspapier Skimming, das erstmals vertieft auf den bargeldlosen Zahlungsverkehr, die Autorisierung und das Clearingverfahren eingeht. Darin habe ich den Beginn des Versuchs der Fälschung sehr früh und im Stadium des Skimmungs im engeren Sinne angesetzt, wovon ich im Sommer 2010 abgerückt bin, um danach vom BGH quasi überholt zu werden. Das Gericht geht jetzt davon aus, dass jedenfalls in arbeitsteiligen Tätergruppen, bei denen die Fälscher sozusagen „Gewehr bei Fuß-stehen“, um die Fälschungen und vor allem das Cashing auszuführen, sich die „Ausspäher“ bereits am Versuch des Fälschens beteiligen, sobald sie die ausgespähten Daten an ihre Komplizen übermitteln.

Anfang 2010 nahm der BGH in mehreren Entscheidungen Stellung zum Skimming, was eine gründliche Überarbeitung nötig machte und im April 2010 zum ▸ Abeitspapier Skimming #2 führte. Es wurde im Sommer 2010 um das Beteiligungsmodell erweitert, das genauer nach den einzelnen Tatphasen und den Grad der Arbeitsteilung zwischen den Tätern unterscheidet. Bis Mai 2011 wurde es mehrfach aktualisiert und wurde mit fast 3.500 Downloads das begehrteste vom Cyberfahnder herausgegebene Arbeitspapier.

Die jetzt präsentierte dritte Auflage wurde nötig, weil eine neuere Entscheidung des BGH mir das Problem vergegenwärtigt hat, dass Einschränkungen der Dispositionsfreiheit kein vermögensrechtlicher Schaden sind, und die 2009 in Kraft getretenen Vorschriften über Zahlungsdienstleistungen sowie die im BGB eingeführten Risiko- und Beweislastregeln zunächst spurlos an mir vorüber gegangen sind. Das hat Anlass dazu gegeben, das Arbeitspapier erneut gründlich zu überarbeiten und meinen zwischenzeitlich bei digma veröffentlichten Aufsatz einzuarbeiten [241].

Die Schriftenreihe wird abgerundet von dem ▸ Arbeitspapier über die Ermittlungen im Internet. Es erschien im Juli 2011 und befasst sich vor allem mit den Recherchen im Internet und dem Einsatz Verdeckter Ermittler. Die angesprochen Themen stießen auf reges Interesse, so dass das Arbeitspapier nach gut vier Monaten mehr als 2.200 Mal abgefordert wurde.

[240] Dieter **Kochheim**, Skimming. Erscheinungsformen und Strafbarkeit, 16.05.2009

[241] Dieter **Kochheim**, Skimming. Tatphasen und Haftung, digma September 2011