



*Dieter Kochheim*  
***Skimming***  
*Hintergründe und Strafrecht*



Zweite überarbeitete Fassung,  
Stand: 22.04.2011

**Erscheinungsformen und  
Strafbarkeit des Skimmings**

mit **Glossar** und **Rechtsprechungsübersicht**

### Cybercrime im Cyberfahnder

Die Webseite [cyberfahnder.de](http://cyberfahnder.de) widmet sich seit 2007 der Cybercrime, ihren Erscheinungsformen und ihrer Strafverfolgung. Dazu gehören die technischen Grundlagen, soweit sie zum Verständnis nötig sind, sowie 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](#) mit neuen Texten 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 von Schurkenprovidern und anderen Netzbetreibern. Den Abschluss bildet eine Auseinandersetzung mit den miteinander verflochtenen Formen der Cybercrime und des Cyberwar.



Sozusagen das Grundwerk ist das [Arbeitspapier Cybercrime](#) aus dem Mai 2010. Es berichtet über die wichtigsten Erscheinungsformen der Cybercrime und befasst sich mit Angriffspunkten gegen die Informations- und Kommunikationstechnik, die Nummertricks, Malware, Botnetze, den Identitätsdiebstahl und die Methoden des Social Engineering. Der letzte Teil widmet sich der Underground Economy, den Schurkenprovidern und den kriminellen Strukturen, die sich im Zusammenhang mit der Internetkriminalität erkennen lassen. Das Arbeitspapier fußt auf den seit 2007 im Cyberfahnder erschienenen Beiträgen, die überarbeitet, aktualisiert und ergänzt wurden.



Mit einem verwandten Thema beschäftigt sich [Die Kurze Geschichte der Cybercrime](#) (November

2010). Sie liefert die Fakten nach und stellt sie geschichtlich nebeneinander



Als erstes Arbeitspapier in dieser Reihe erschien im Dezember 2009 das [Arbeitspapier Skimming](#). Mehrere wichtige Entscheidungen des Bundesgerichtshofes machten gründliche Überarbeitungen nötig. Die zweite Fassung ist Ende Februar 2010 erschienen und wird seither fortgeschrieben und aktualisiert.



Zuletzt erschien im Februar 2011 das [Arbeitspapier Eskalationen](#), das sich mit den zielgenauen Angriffen seit 2010, mit WikiLeaks, der neuen Qualität des

Hacktivismus und dem Schutz Kritischer Infrastrukturen auseinandersetzt.

Hannover, Februar 2011

---

Thema:	<b>Skimming</b>
Autor:	Dieter Kochheim
Version:	2.21
Stand:	22.04.2011
Cover:	U-Bahn-Station Werderstraße, Hannover
Impressum:	<a href="http://cyberfahnder.de">cyberfahnder.de</a>

S. **Inhalt**

4 **Vorwort**

6 **A. Phänomen Skimming**

11 **B. bargeldloser, kartengestützter  
Zahlungsverkehr**

11 1. Fälschungssicherung

11 2. bargeldloser Zahlungsverkehr

13 3. Autorisierung

13 4. Clearing

14 5. Schadensausgleich

14 6. Ergebnisse

14 7. arbeitsteilige Handlungen beim Skimming

16 8. EMV-Chip

18 **C. Strafbarkeit**

18 1. arbeitsteiliges Vorgehen

18 2. einschlägige Normen und Konkurrenzen

20 2.1 Ausspähen von Daten

20 2.2 Abfangen von Daten

20 2.3 PIN-Skimming und Computersabotage

21 2.4 natürliche Handlungseinheiten

22 3. Fälschungssicherheit

23 4. Garantiefunktion

24 5. Tatorte und deutsche Gerichtsbarkeit

24 5.1 Erfolgsort beim Computerbetrug

25 5.2 schadensgleiche Vermögensgefährdung

26 5.3 Vollendung

27 6.1 Beginn des Versuchstadiums

27 6.2 Versuch des Computerbetruges

28 6.3 Rücktritt vom Versuch

28 6.4 Zusammenfassung und Strafzumessung

29 7. Vorbereitungshandlungen

30 7.1 Kartenlesegeräte

31 7.2 Kameras

31 7.3 Tastaturaufsätze

32 8. Mittäter und Bande

33 8.1 arbeitsteilige Tätergruppen

35 8.2 Tatvollendung durch Cashing

36 8.3 Tatbeteiligung des Skimmers

37 9. Verabredung zu einem Verbrechen

37 10. Beteiligungsmodell beim arbeitsteiligen  
Skimming

38 10.1 ... einschließlich eigenhändiges Cashing

38 10.2 ... einschließlich Cashing durch Mittäter

39 10.3 ... mit Absatzabsicht

39 10.4 Umgang mit Skimming-Geräten

40 Anhang: **Grafiken zum Beteiligungsmodell**

46 11. Nichtanzeige des geplanten Skimmings

46 12. Prüfungsschema

46 12.1 vollendetes Cashing

47 12.2 Ausspähen von Karten und PIN bei  
vollendetem Cashing

47 12.3 Ausspähen von Karten und PIN ohne  
Cashing

48 13. Fazit

50 **D. Strafverfahren**

50 1. geheime Ermittlungen

50 2. Organisierte Kriminalität

51 **E. kriminalistische Erfahrungen**

51 1. Programm

51 2. Garantiefunktion

51 3. Ausspähen

51 3.1 Vorerkundung

52 3.2 Spezialisten

52 3.3 Einsatz

52 4. Abstimmung und Bericht

52 5. Banden

54 **Rechtsprechungsübersicht**

56 **Glossar**

## Vorwort

Das **Skimming**<sup>1</sup> leitet sich ab von dem Skimmer<sup>2</sup>, also dem Lesegerät, mit dem die Magnetstreifen von „Identitätsdokumenten“<sup>3</sup> 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 Millionen € jährlich<sup>4</sup>.

Dieses Arbeitspapier beschreibt ihr Vorgehen, die wirtschaftlichen und technischen Hintergründe und die strafrechtlichen Fragen, die sich im Zusammenhang mit dem Skimming stellen.

## Das Thema Skimming im Cyberfahnder

Mit dem Thema „Skimming“<sup>5</sup> befasst sich der Cyberfahnder seit dem Sommer 2007. Die erste Fassung des Aufsatzes wurde zum beliebtesten der Webseite. Im Mai 2008 wurde der Beitrag neu gefasst<sup>6</sup> und im November 2009 erschien die erste Fassung dieses Arbeitspapiers<sup>7</sup>.

Das Skimming als Kriminalitätsform war zunächst ein Randthema und ich habe es nicht als einen Teil der Cybercrime<sup>8</sup> im engeren Sinne angesehen. Das sehe ich inzwischen anders,

<sup>1</sup> Die Quellenangaben sind, wenn möglich, mit Hyperlinks zum Internet versehen.

<sup>2</sup> CF, Sicherheitsvorkehrungen, Juli 2007; CF ist das Kürzel für „Cyberfahnder“.

<sup>3</sup> CF, Überwachungstechnik: Zahlungskarten, 18.05.2008

<sup>4</sup> CF, das Schweigen der L@mmen, 12.09.2010.

<sup>5</sup> CF, Skimming, Juli 2007

<sup>6</sup> CF, arbeitsteiliges Skimming, 18.05.2008

<sup>7</sup> CF, Zwischenbilanz: Skimming, 14.11.2009

<sup>8</sup> CF, Cybercrime und IT-Strafrecht, 08.08.2008

weil sich die Formen, in denen sich die Kriminellen der Informationstechnik – IT – und des Internets bedienen, immer mehr annähern und Mischformen bilden<sup>9</sup>. Dieser Trend setzt sich unvermindert fort<sup>10</sup> und wird dazu führen, dass sich die „klassische“ und die Cyberkriminalität wegen ihrer Methoden und Vorgehensweisen kaum noch unterscheiden werden<sup>11</sup>.

Dieses Arbeitspapier ist ein selbständiges Werk. Seine Aufgabe ist es vor allem, eine schnelle Orientierung in Bezug auf die durchaus schwierigen Rechtsfragen zu geben, die bei der Strafverfolgung wegen des Skimmings auftreten.

## Zweite Auflage, Stand 2011

Seit 2010 hat sich der Bundesgerichtshof – BGH – intensiv mit dem Fälschen von Zahlungskarten mit Garantiefunktion befasst. Das Arbeitspapier wurde deshalb mehrfach aktualisiert, insgesamt überarbeitet zuletzt im April 2011. Die wesentlichen Rechtsfragen sind jetzt geklärt.

Das Auslesen der Magnetstreifen von Zahlungskarten ist kein Ausspähen von Daten im Sinne von § 202a Abs. 1 StGB<sup>12</sup>, weil es den Karten an einer besonderen Zugangssicherung fehlt. Die frühere Auffassung des BGH<sup>13</sup> ist damit vom Tisch.

Im Januar 2011 hat der BGH den Beginn des Versuchs beim Skimming geklärt<sup>14</sup>. Der 5. Strafsenat hatte zunächst im Herbst 2010 erwogen, dass der Versuch erst in unmittelbarer zeitlicher und räumlicher Nähe zum eigentlichen Fälschen

<sup>9</sup> CF, Skimming-Coup, 06.02.2009

<sup>10</sup> CF, Mafia, Cybercrime und verwachsene Strukturen, 20.10.2010

<sup>11</sup> CF, Eskalationen in der dualen Welt, 19.02.2011

<sup>12</sup> BGH, Beschluss vom 18.03.2010 - 4 StR 555/09, BGH, Beschluss vom 14.01.2010 - 4 StR 93/09, S. 4, CF, Ausspähen von Daten und das Skimming, 14.05.2010.

<sup>13</sup> BGH, Urteil vom 10.05.2005 - 3 StR 425/04

<sup>14</sup> BGH, Urteil vom 27.01.2011 - 4 StR 338/10, CF, Versuch der Fälschung, 21.02.2011.

beginnen könne<sup>15</sup>. Das hat der 4. Strafsenat jetzt präzisiert: In einer arbeitsteiligen Skimming-Bande setzen die nur mit dem Ausspähen von Kartendaten und PIN befassten Mittäter zum Versuch des Fälschens von Zahlungskarten mit Garantiefunktion (§§ 152a, 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 unbekannt)en Mittäter im Ausland übermitteln. Das erfordert jedoch, dass die Skimmer ("Ausspäher") damit rechnen, dass die Fälscher nach dem Erhalt der Daten ohne weiteres zuwarten die ausgespähten Daten einander zuordnen (Kartendaten und PIN) und sogleich mit der Fälschung beginnen.

Diese Position wird von mir bereits seit dem Juli 2010 vertreten; das musste einmal gesagt werden.

Das Skimming im engeren Sinne findet im Vorbereitungsstadium des eigentlichen Fälschens von Zahlungskarten statt. Das bedeutet, dass in diesem Stadium

→ der „Umgang“ mit modifizierten Kartenlesegeräten nach § 149 StGB strafbar ist und

→ dass grundsätzlich alle Mitglieder in einer arbeitsteiligen Skimming-Bande als Mittäter und nicht nur als Gehilfen zu behandeln sind.

→ Das gilt besonders auch für die „Ausspäher“, die am Fälschen und am Cashing nicht beteiligt sind und doch einen überaus wesentlichen Tatbeitrag leisten. Deshalb können sie sich auch grundsätzlich an einer Verabredung zu einem Verbrechen (§ 30 StGB) beteiligen, also dem Fälschen von Zahlungskarten mit Garantiefunktion (§ 152b StGB) und

→ müssen sich die Tatvollendung ihrer Mittäter beim Cashing zurechnen lassen (§ 25 Abs. 2 StGB).

<sup>15</sup> BGH, Beschluss vom 14.09.2010 - 5 StR 336/10, CF, Versuch beim Skimming, 02.10.2010.

## Überblick

Zunächst werden die aktuellen Erscheinungsformen des Skimmings beschrieben. Dazu wird zwischen dem Skimming im engeren Sinne, also dem Ausspähen von Kartendaten und Persönlichen Identifikationsnummern – 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 das automatische Autorisierungs- und Clearingverfahren, die den internationalen Zahlungsverkehr in Echtzeit zulassen. Dabei wird jeder Zahlungsvorgang von der kartenausstellenden Bank geprüft und schließlich durch die Übermittlung eines Genehmigungs-codes die Garantie zur Auszahlung erklärt. Diese Mechanismen machen – neben Kreditkarten – 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<sup>16</sup>. Das Beteiligungsmodell wird jetzt von einem Phasenmodell begleitet, das die Orientierung verbessert<sup>17</sup>.

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

Hannover, 21.04.2011

<sup>16</sup> CF, Bilderbuch Skimming-Strafrecht, 26.07.2010

<sup>17</sup> CF, Skimming: aktuelles Beteiligungsmodell, 13.03.2011

## A. Phänomen Skimming

Das „Skimming“ als kriminelle Erscheinungsform ist etwa seit dem Jahr 2000 bekannt. Seine früheren Vorläufer entstammen dem Trickdiebstahl, bei dem die Täter die Persönliche Identifikationsnummer – PIN – ausspähten und die Zahlungskarte stahlen (► [Lebanese Loop](#)<sup>18</sup>), sowie dem lange vergessen geglaubten ► [Front Covering](#), bei dem eine nachgemachte Fassade vor den Nachtbriefkasten einer Bank installiert wurde, so dass die eingeworfenen Geldbomben nicht in den Tresor, sondern in den Zwischenraum fielen.



Kennzeichnend für das Skimming ist das Auslesen der Magnetstreifen von Kredit- und anderen Zahlungskarten mit einem Kartenlesegerät am Geldautomaten oder einem anderen POS-Terminal<sup>19</sup>, also einem Eingabegerät im Einzelhandel, in einem Hotel, bei einer Tankstelle oder anderswo. Die für den Einsatz am Geldautomaten angepassten Lesegeräte werden als „Skimmer“ bezeichnet.

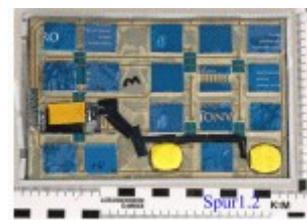
Das Ausspähen der Kartendaten ist ein notwendiger Schritt zur Fälschung von Zahlungskarten und das Ausspähen der PIN ein weiterer notwendiger Schritt für das finale Ziel der Täter, dem Missbrauch der Zahlungskarten an ausländischen Geldautomaten, wobei sie die Auszahlung mit den richtigen Kartendaten 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 von Zahlungskarten. Dabei erfolgen auch erfahrungs-



gemäß die polizeilichen Zugriffe.

Die Fälschung der Zahlungskarten erfolgt entweder im osteuropäischen Ausland, wo die Hinterleute zu vermuten sind, oder durch die Casher, die bereits im Ausland auf die ausgespähten Daten und auf ihren Einsatz warten.



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<sup>20</sup> können sich die Bankkunden schützen, wenn sie eine Hand über die andere halten, mit der sie gerade die Ziffernfolge eingeben. Das funktioniert dann nicht mehr, wenn die Täter eine Kamera flach oberhalb der Tastatur anbringen<sup>21</sup>, einen Tastaturaufsatz<sup>22</sup> oder sogar eine vollständige Fassade (Front Covering) einsetzen<sup>23</sup> (Bild oben: Rückseite eines Tastaturaufsatzes). Die Verwendung verschiedener Karten für die Zugangskontrolle zu einer Bankfiliale und für den Geldautomaten nützt schon lange nichts mehr, weil die Kartendaten in aller Regel direkt am Geldautomaten ausgelesen werden<sup>24</sup>. Inzwischen werden häufiger auch die EMV-Chips ausgelesen, um die Kartendaten auf die Magnetstreifen von Dubletten zu kopieren. Ihr Einsatz scheitert in aller Regel daran, dass die digitale Kartenummer auf dem Magnetstreifen anders kodiert ist als im EMV-Chip, so dass die Manipulation auffällt.

<sup>20</sup> CF, Kamera, 13.04.2009

<sup>21</sup> CF, Sichtblende mit Kamera, 26.06.2010

<sup>22</sup> CF, Tastaturaufsatz, 13.04.2009; CF, Tastaturblende, 13.04.2009

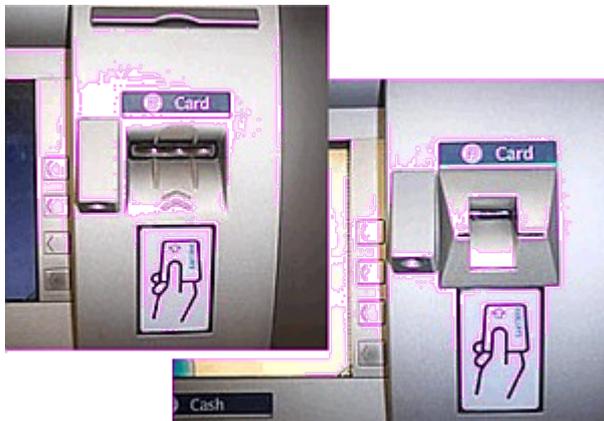
<sup>23</sup> CF, Skimming, Juli 2007

<sup>24</sup> CF, BKA: Lagebild OK. Zahlungskartekriminalität, 01.11.2008

<sup>18</sup> CF, Proll-Skimming, 18.05.2008

<sup>19</sup> POS: Point of Sale.

Zunächst wurden 2009 in Russland die Geldautomaten selber gehackt, um die Dateneingabe vollständig aufzuzeichnen<sup>25</sup>. 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 Elektronik 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.



Auch das klassische Front Covering erlebte jüngst mit dem „Cash Trapping“ eine Wiedergeburt: Mit einer Blende wird einfach nur der Geldausgabeschacht überdeckt, so dass die Geldscheine in den Zwischenraum hinter der Blende rutschen, wo sie mit Klebstoff „festgehalten“ werden. Sobald die enttäuschten Bankkunden die Filiale verlassen haben, können die Täter die Geldscheine in Ruhe bergen<sup>26</sup>. Das erfordert

<sup>25</sup> CF, Skimming an der Quelle, 20.03.2009

<sup>26</sup> Die rechtliche Beurteilung dieses Vorgehens ist noch streitig. 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 scheidet daran, dass der Täter zu keinem Zeitpunkt einen rechtmäßigen Gewahrsam an dem ausgegebenen



eine ständige Beobachtung des Geldautomaten und bringt nicht den beachtlichen Gewinn von durchschnittlich etwa 2.350 Euro je gefälschter Karte<sup>27</sup>, die beim Cashing erzielt werden. Die Methode hat jedoch den Vorteil, dass die Täter die Beute sofort erzielen<sup>28</sup>.

2008 traten gehäuft Fälle des POS-Skimmings auf<sup>29</sup> (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<sup>30</sup>. Alle notwendigen Daten durchlaufen diese Geräte. Wenn die Täter es schaffen, sie entsprechend umzurüsten, dann speichern oder senden sie die Dumps<sup>31</sup> an die Täter. Solche Fälle haben deutlich nachgelassen, weil die Präparierung der POS-Terminals recht aufwändig ist. Um ihre Schalen heile zu behalten, müssen sie mit einer Methode geöffnet werden, bei der sich die innere Elektronik vernichtet. Nur wenn die Täter eine Schalenhälfte richtig zertrümmern, dann gelangen sie an die intakte Elektronik. Außerdem müssen sie mindestens zweimal in denselben Markt einbrechen,

→ um die Original-Geräte zu stehlen,  
Geld erlangt.

<sup>27</sup> Eigene Berechnung anhand der für 2009 veröffentlichten Zahlen.

<sup>28</sup> Jedenfalls in einem Fall weiß ich davon, dass ein bekannter Skimmingtäter auf das Cash Trapping umgestiegen ist – wahrscheinlich um sich seinen täglichen Lebensbedarf zu sichern.

<sup>29</sup> CF, POS-Skimming, 18.05.2008; CF, Datenklau und -missbrauch, 19.08.2008

<sup>30</sup> CF, BKA: Lagebild OK. Manipulation von POS Terminals, 01.11.2008

<sup>31</sup> vollständige Kartendaten einschließlich PIN; CF, Fachworte, April 2007

- die präparierten Geräte zu installieren und
- die ausgespähten Daten auszulesen.

Das lohnt sich nur, wenn die präparierten Geräte länger im Einsatz bleiben. Das hingegen führt zu überalteten Daten, die überholt und wertlos sein können.

Seit 2010 sind Fälle bekannt, bei denen das Ausspähen von Kartendaten und PIN nicht an Geldautomaten stattfand, sondern an den fest verbauten POS-Terminals von Tankstellen<sup>32</sup>. Ein erster Höhepunkt dieser Variante wurde im März 2011 bekannt, nachdem an einer unbewachten Automaten-Tankstelle in Castrop-Rauxel mindestens 50 Dumps ausgespäht und damit ein Schaden von mindestens 100.000 Euro ange richtet wurde<sup>33</sup>.

Die Beispiele zeigen, dass die Beschaffung der Kartendaten und PIN auf vielen Wegen erfolgen kann. Sie sind zwar wichtig für den Taterfolg, am Ende zählt aber das erbeutete Geld und nicht die Methode, mit der die Täter an die Daten gelangten. Die Arbeitsteilung bei dieser Kriminalitätsform lässt auch spezialisierte „Subunternehmer“ zu, die sich auf die Beschaffung der Daten beschränken und ihre „Rohstoffe“ an andere Spezialisten verkaufen, die sich um das Fälschen und das Cashing kümmern.

Besonders heimtückisch gingen die Hacker vor, die Ende 2008 in die Datenhaltung einer US-amerikanischen Bank eindringen und die Kartendaten einschließlich PIN von 100 Kunden ausspähten<sup>34</sup>. 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

<sup>32</sup> [Skimming-Angriffe an Tankstellensäulen](#), Heise online 23.02.2010

<sup>33</sup> [Thomas Wrycz, Bankkunden in Castrop-Rauxel mit manipuliertem Kartenlesegerät abgezockt](#), DerWesten 07.03.2011

<sup>34</sup> [CF, Skimming-Coup](#), 06.02.2009

*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 White Cards zu beschreiben, reichen handelsübliche Geräte aus. Schwieriger wird es, originale Bankkarten mit anderen Daten zu überschreiben. Die Spuren 1 und 2 auf dem Magnetstreifen, auf denen sich die Kodierung für die Bank und das Konto befinden, sind besonders stark magnetisiert. Sie können nicht mit handelsüblichen Schreibgeräten überschrieben werden, sondern nur mit speziellen Geräten.*

*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](#)

Ausspähens und des Verfälschens von Daten mit denen anderer Kriminalitätsformen vermengen.

Das übliche Skimming verlangt nach besonderen handwerkliche Fertigkeiten bei der Herstellung der eingesetzten Geräte, besonderes Wissen wegen der Auswahl der Geldautomaten und Standorte, die sich einerseits zum Ausspähen der erstrebten Daten und andererseits zum Missbrauch der gefälschten Zahlungskarten eignen, sowie logistisches Geschick bei der Installation der Überwachungshardware<sup>35</sup>. Die verschiedenen Arbeitsschritte im Tatplan, ihre wechselnden Anforderungen an die Fähig- und Fertigkeiten

<sup>35</sup> Das hat jetzt auch der BGH hervorgehoben: [BGH, Urteil vom 27.01.2011 - 4 StR 338/10](#), Rn. 8

der Täter <sup>36</sup> 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 <sup>37</sup> und Casher <sup>38</sup> 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 wurden. 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 <sup>39</sup>. Andere Bilder haben eindrucksvoll gezeigt, wie Casher beim Einsatz von White Cards <sup>40</sup> mit ihren Handys telefonieren und sich dabei offenbar die PIN übermitteln lassen.

<sup>36</sup> 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.

<sup>37</sup> Skimmer: siehe Glossar.

<sup>38</sup> Casher: siehe Glossar.

<sup>39</sup> Als Testkarte eignet sich jede Magnetkarte, also auch Telefonkarten 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.

<sup>40</sup> White Cards, auch White Plastics: siehe Glossar.

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 <sup>41</sup> 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 <sup>42</sup>, 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 Magnetstreifen 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.

<sup>41</sup> 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.

<sup>42</sup> Zum Beispiel HypoVereinsbank, HVB Cashkarte. Denn Zeit ist Geld!, S. S. 2.



## B. bargeldloser, kartengestützter Zahlungsverkehr

### 1. Fälschungssicherung

Die in Deutschland herausgegebenen Zahlungskarten<sup>43</sup> verfügen über mehrere Vorrichtungen gegen das Fälschen der Karte selber<sup>44</sup>. Neben dem Unterschriftsfeld, den Merkmalen des Aufdrucks und des für die Individualdaten verwendeten Schrifttyps (OCR-B<sup>45</sup>) 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 Merkmalstoff, der eine individuelle Codierung der Karte zulassen<sup>46</sup>. Diese Codierung wird im Geldautomaten mit einer Prüfsumme abgeglichen, die auf dem Magnetstreifen der Zahlungskarte gespeichert ist. Es wird jedoch 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<sup>47</sup>.

Der EMV-Chip wird von den großen Verbänden für grenzüberschreitend einsetzbare Zahlungskarten gefordert und ist bereits weit verbreitet<sup>48</sup>. Das Kürzel geht auf „Electronic Cash – Master/Maestro – Visa“ zurück<sup>49</sup>. Der Chip ist programmierbar<sup>50</sup>, verspricht, nicht manipuliert

<sup>43</sup> Es handelt sich um standardisierte Identitätsdokumente nach ISO/IEC 7810 (Wikipedia).

<sup>44</sup> CF, Zahlungskarten, 18.05.2008

<sup>45</sup> CF, Zeichensatz OCR-B, Juli 2007

<sup>46</sup> CF, Sicherheitsmerkmale und Merkmalstoffe, 06.02.2010

<sup>47</sup> Der Magnetstreifen verfügt über drei Spuren, wovon die dritte Spur überschreibbar ist (zum Beispiel: Zahl der Fehlversuche). Die Spuren 1 und 2 sind besonders stark magnetisiert und können deshalb nicht mit handelsüblichen Geräten überschrieben werden

<sup>48</sup> Kartensicherheit.de, EMV-Chip

<sup>49</sup> CF, Zahlungskarten mit Garantiefunktion, 13.04.2009

bar sein<sup>51</sup> und eine verschlüsselte Datenkommunikation zu ermöglichen<sup>52</sup>.

In den meisten west- und nordeuropäischen Staaten erfolgt die Autorisierung anhand der Chip- und nicht mehr anhand der Daten auf dem Magnetstreifen. Viele Geldautomaten in Teilen Süd- und Osteuropas beschränken sich jedoch immer 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<sup>53</sup>. 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<sup>54</sup>.

<sup>50</sup> CF, Turbulenzen beim bargeldlosen Zahlungsverkehr, 06.02.2010

<sup>51</sup> Mehrere Meldungen lassen daran Zweifel aufkommen:

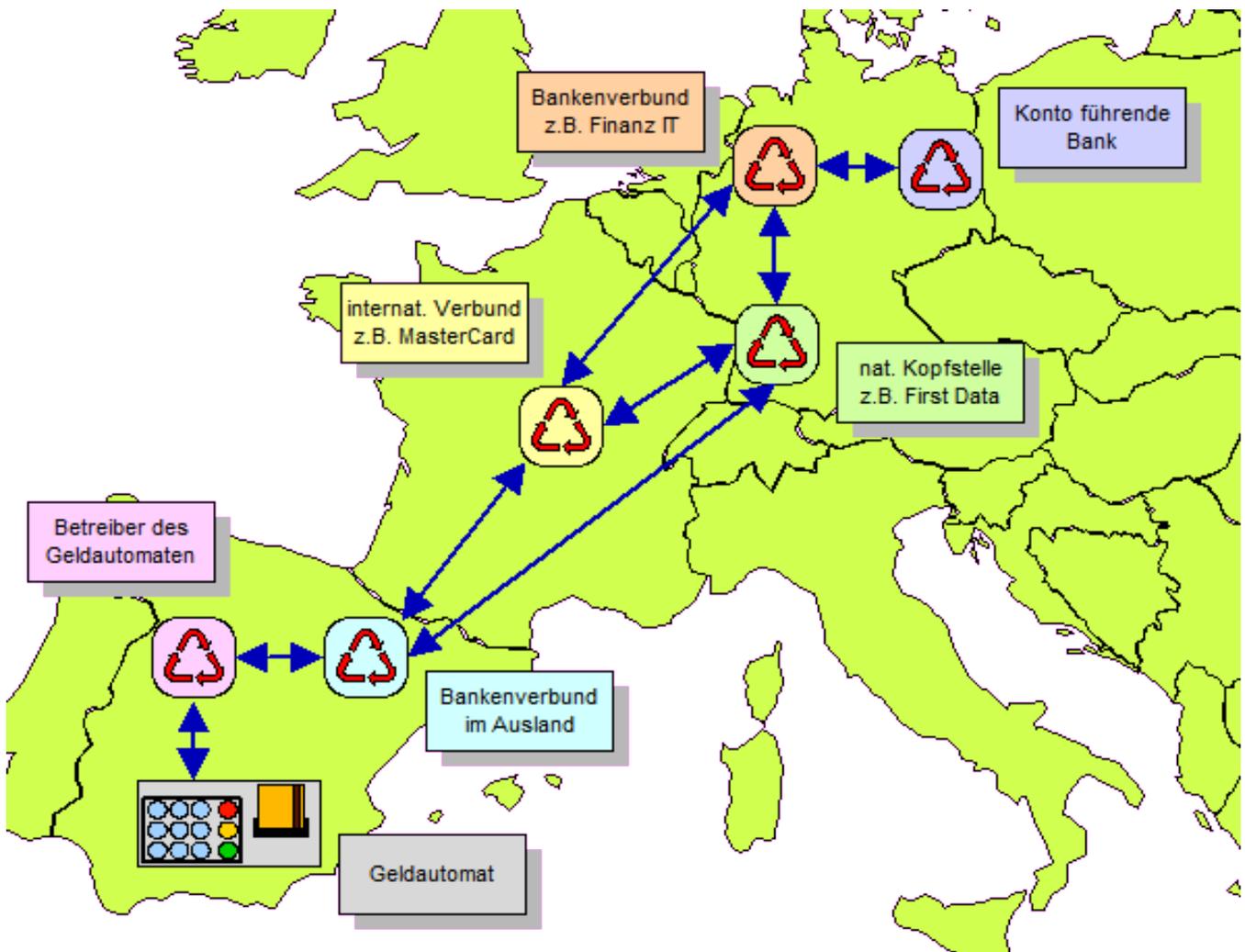
PIN-Prüfung im EMV-Verfahren bei EC- und Kreditkarten ausgehebelt, Heise online 12.02.2010; Bericht: PIN-Prüfung bei EC- und Kreditkarten unsicherer als angenommen, Heise online 19.01.2010;

Daniel Bachfeld, Phish & Chips, Angriff auf das EMV-Verfahren bei Bezahlkarten, c't 6/2010

<sup>52</sup> EC-Karten-Update soll Fehler beheben, c't 3/2010, S. 53; Update für EC-Karten, c't 4/2010, S. 54.

<sup>53</sup> Die Garantie war auf 400 DM beschränkt. Auch höhere Beträge konnten mit dem EC angewiesen werden, der überschüssige Betrag war dann aber nicht von der Garantie der Bank umfasst.

<sup>54</sup> CF, Einzugsermächtigung und Lastschriftverfahren, 2007



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.

Die heute übliche Autorisierung fußt auf dem Abbuchungsauftrag, der dem Akzeptanten eine höhere Auszahlungssicherheit gibt <sup>55</sup>. 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

<sup>55</sup> Die Einzugsverfahren sind in das SEPA-Übereinkommen aufgenommen worden und gelten jetzt europaweit; siehe CF, Single Euro Payments Area, 26.01.2008.

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 <sup>56</sup>. 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.

<sup>56</sup> CF, eierlegende Wollmilchsau, 20.03.2011

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.

### 3. Autorisierung

Die wesentlichen Sicherungen für das Autorisierungsverfahren<sup>57</sup> bestehen in den Sicherheitsmerkmalen der Zahlungskarte, in der PIN und schließlich in dem Genehmigungscode, den die kartenausgebende Bank an den Akzeptanten meldet<sup>58</sup>.

Zum Zweck der Autorisierung von Debitkarten<sup>59</sup> liest der ausländische Geldautomat die Kartendaten aus, kombiniert sie mit der vom Kunden eingegebenen 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<sup>60</sup>, Finanz IT<sup>61</sup>) bis zur kartenausgebenden Bank geleitet<sup>62</sup>. 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<sup>63</sup>, der

<sup>57</sup> Wegen der technischen Einzelheiten: [ISO 8583 \(Wikipedia\)](#).

<sup>58</sup> CF, [Autorisierung im POS-Verfahren, 13.04.2009](#)

<sup>59</sup> Gemeint sind Zahlungskarten auf Guthabenbasis, wobei als Guthaben auch der gewährte Überziehungskredit gilt.

<sup>60</sup> früher Gesellschaft für Zahlungssysteme - GZS

<sup>61</sup> Rechenzentrum der Sparkassen

<sup>62</sup> Siehe Glossar: [Autorisierung, Clearing](#).

<sup>63</sup> Der Genehmigungscode lautet „0“. Andere Codeziffern belegen Zeitüberschreitungen, Kartensperren, Verwendungsbeschränkungen und andere Ereignisse. Sie führen immer dazu, dass die Transaktion verweigert wird.

#### **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

die Auszahlung autorisiert und eine Garantie enthält, dass die autorisierende Bank für den Auszahlungsbetrag bürgt<sup>64 65</sup>.

### 4. Clearing

Nach der Autorisierung erfolgt bei Debitkarten in aller Regel keine unmittelbare Belastung des Kundenkontos, sondern eine Zwischenbuchung auf einem bankinternen Konto<sup>66</sup>. Nach der Auszahlung erfolgt im Bankenverbund über die Verbindungsstellen das Clearingverfahren, wobei die gegenseitig bestehenden Forderungen der Verbünde und schließlich der Institute untereinander ausgeglichen werden. Am Ende wird die Zwischenbuchung der Hausbank gegen das Konto des Kunden aufgelöst.

Diese Buchung zulasten des Kundenkontos markiert den Eintritt des Erfüllungsschadens im Sinne von [§ 263a StGB](#)<sup>67</sup>. Er tritt erst nach der Autorisierung, der Auszahlung und schließlich dem

<sup>64</sup> Siehe auch das [Glossar bei kartensicherheit.de](#) und das Zitat im Kasten oben.

<sup>65</sup> 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.

<sup>66</sup> Conto pro Diverse – CPD

<sup>67</sup> Wegen der Einzelheiten: [CF, Der Eingehungsschaden löst den Gefährdungsschaden ab, 16.02.2011](#).

Clearing ein, wenn eine gefälschte Zahlungskarte eingesetzt wurde.

## 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<sup>68</sup> - 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<sup>69</sup>.

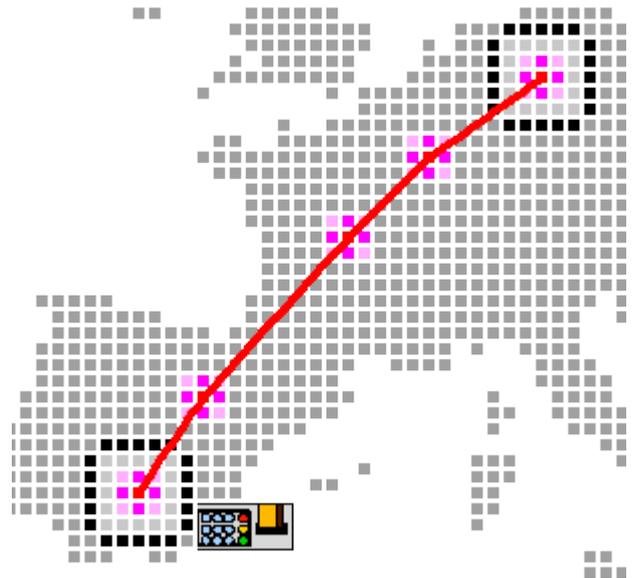
Dieser Anpassungsdruck funktioniert dann nicht mehr, wenn sich das Cashing in das entfernte Ausland verlagert, was zunehmend geschieht. Die Finanzwirtschaft wird dafür neue Formen der Sicherung und des Schadensausgleiches entwickeln müssen.

## 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).

<sup>68</sup> Siehe auch [EKS – Analyse](#).

<sup>69</sup> [CF, das Schweigen der L@mmers](#), 12.09.2010



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.

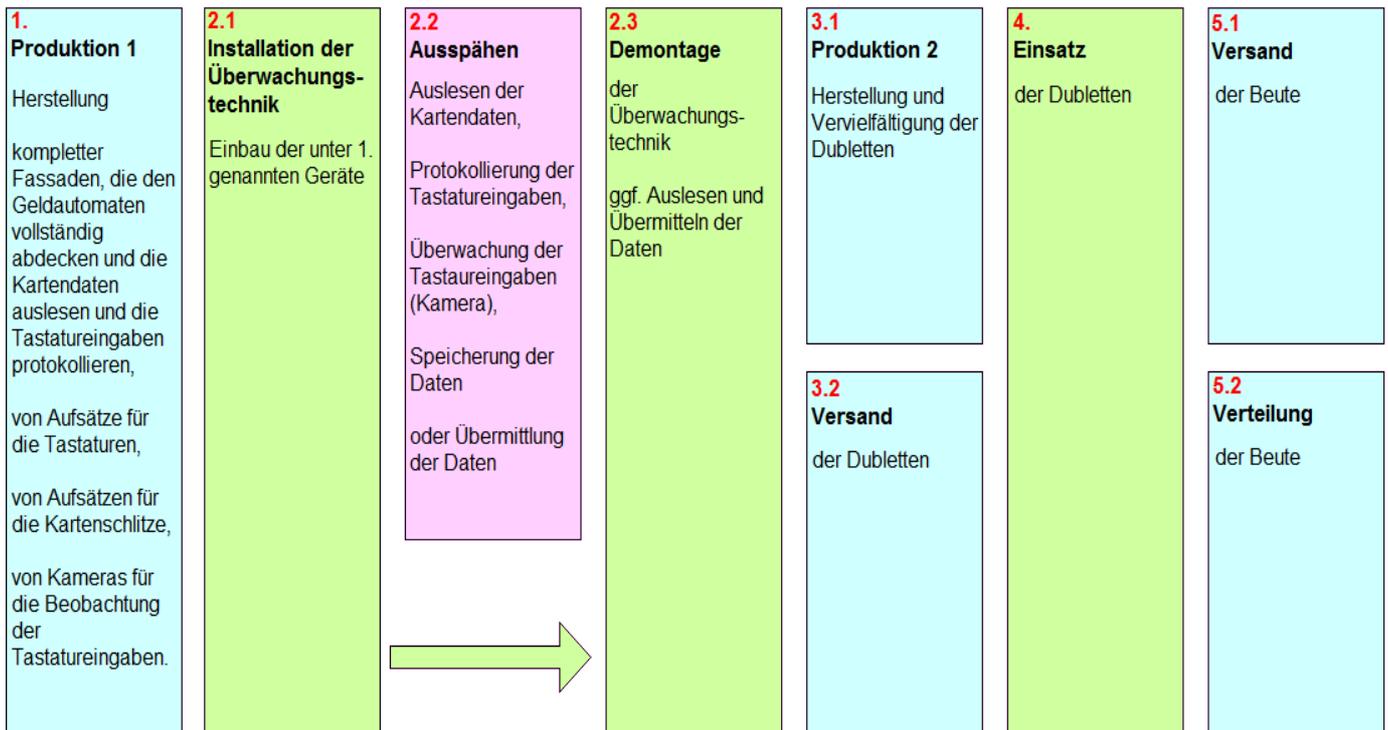
Der finanzwirtschaftliche Schadensausgleich hat dazu geführt, dass die durch das Skimming bei den Bankkunden eingetretenen Schäden im Bankenverbund ausgeglichen wurden. Dieses System wird jetzt einer besonderen Belastungsprobe ausgesetzt, weil sich das Cashing in das außereuropäische Ausland verlagert.

## 7. arbeitsteilige Handlungen beim Skimming

Das Skimming ist geprägt von verschiedenen Tathandlungen, die in der Grafik auf der nächsten Seite 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 oder Tastaturaufsätze 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 Bankverbänden 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.

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<sup>70</sup>.

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

<sup>70</sup> Siehe jetzt: BGH, Urteil vom 17.02.2011 – 3 StR 419/10

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 Beuterealisation. Es ist zu erwarten, dass es uns noch lange erhalten bleibt.

## 8. 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 <sup>71</sup>. 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 <sup>72</sup>. 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.

<sup>71</sup> CF, Sicherheitsmerkmale und Merkmalstoffe, 06.02.2010

<sup>72</sup> CF, Quellenkritik an Heise, 09.04.2011

Mindestens eine deutsche Bank ist dazu übergegangen, ihren Kunden nur noch Zahlungskarten mit EMV-Chip und ohne Magnetstreifen anzuliefern. 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, 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 nur den Magnetstreifen auslesen konnten.

Die Skimming-Täter haben ihre Probleme mit den Umstellungen und das Cashing ist nach meinem Eindruck zurück gegangen oder 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 <sup>73</sup>. 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

<sup>73</sup> CF, eierlegende Wollmilchsau, 20.03.2011

**Zahlen für 2009**

▶ Geldautomaten	59.394		
▶ Angriffe gegen GAA	809		
▶ ... Türzugangskontrollen	155	= 1,62 %	
▶ POS-Terminals	3		
▶ Zahlungskarten	125.801.300		
▶ Cashing-Fälle	17.072	= 0,014 %	
▶ Bargeld Inland	156.785.000.000		
▶ Bargeld Ausland	8.377.000.000		
▶ Gebühren (1 %)	84.000.000	~ 1,00 %	
▶ Cashing-Schaden	40.000.000	= 0,48 %	
▶ Phishing-Schaden	10.000.000		
		▶ Dumps pro Angriff	18
		▶ Schaden pro Dump (€)	2.350

Quellen:  
 Deutsche Bundesbank 8/2010  
 EKS 3/2010 (Spiegel online)  
 BKA 5/2010 (PKS)

eigene Berechnungen

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.

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.

## C. Strafbarkeit

An die Stelle der früher üblichen Euroschecks ist das Autorisierungsverfahren und die mit ihm verbundene Genehmigung der kartenausstellenden Bank gegenüber der Zahlstelle im POS-Verfahren getreten <sup>74</sup>.

### 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 der Mittäterschaft und das gewerbsmäßige Handeln <sup>75</sup>. 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.

Auf die Rechtsfragen im Zusammenhang mit der Mittäterschaft und Bandeneigenschaft wird unten im einzelnen eingegangen.

*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

### 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 <sup>76</sup>. Die hohen Mindestfreiheitsstrafen, mit denen die §§ 152b Abs. 1, Abs. 2 StGB drohen, sind von Verfassungs wegen nicht zu beanstanden <sup>77</sup>.

Die Missbrauchshandlung beim Skimming (Cashing) ist im Grunddelikt der Gebrauch falscher inländischer oder ausländischer Zahlungskarten gemäß § 152a Abs. 1 Nr. 2 StGB <sup>78</sup>. In Tateinheit

<sup>74</sup> Siehe Glossar: POS

<sup>75</sup> Siehe Zitat im Kasten oben rechts: BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5.

<sup>76</sup> BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 11.

<sup>77</sup> BVerfG, Beschluss vom 18.03.2009 - 2 BvR 1350/08; siehe auch CF, Fälschung von Zahlungskarten, 01.05.2009.

<sup>78</sup> Strafrahmen: Geldstrafe bis 5 Jahre Freiheitsstrafe.

*Ins Gewicht fällt vielmehr, dass <die Täter> vor Ort bezüglich des gesamten Ausspärens 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

<sup>79</sup> damit steht der Computerbetrug gemäß § 263a StGB <sup>80</sup>, dessen Vollendung mit der Auszahlung am Geldautomaten eintritt <sup>81</sup>.

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

<sup>79</sup> 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.

<sup>80</sup> 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.

<sup>81</sup> 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 entgegen zu sein, die das Urteil mit seiner sowieso schon *milde(n) Gesamtfreiheitsstrafe von drei Jahren* (BGH, Rn 7) nicht angegriffen hat.

*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

vom Grundtatbestand des § 263a Abs. 1 StGB 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 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 beweis erheblicher Daten gemäß § 269 StGB hinter der spezielleren Vorschrift des § 152a Abs. 1 Nr. 1 StGB zurück <sup>82</sup>. Das mit ihr verbundene „Speichern“ realisiert

<sup>82</sup> Grundsätzlich zum Verhältnis zwischen Urkunden- und Zahlungsmittelfälschung: BGH, Beschluss vom 26.01.2005 - 2 StR 516/04.

sich nur bei der Fälschung selber und nicht auch beim Missbrauch der gefälschten Zahlungskarten.

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

## 2.1 Ausspähen von Daten

§ 202a Abs. 1 StGB kommt wegen des Ausspäehens der Daten auf den Magnetstreifen der Zahlungskarten der betroffenen Bankkunden nicht in Betracht, weil ihm eine besondere Sicherungsfunktion fehlt<sup>83</sup>. 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*<sup>84</sup>.

## 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 Ausspäehens 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. Verantwortlich dafür ist 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. 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 sonstiger Sicherheitscode (§ 202c Abs. 1 Nr. 1 StGB). Der Umgang mit ihnen mit dem Ziel, sie zum Cashing zu verwenden, steht unter Strafe<sup>85</sup> 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.

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.

<sup>83</sup> 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

<sup>84</sup> BGH, Beschluss vom 19.05.2010 - 1 ARs 6/10; CF, Ausspähen von Magnetstreifen, 02.07.2010

<sup>85</sup> CF, Ausspähen der PIN, 06.12.2008

## 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*<sup>86</sup>. 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<sup>87</sup>, nicht zuletzt deshalb, weil sie erhebliche Nachteile für die Angeklagten barg<sup>88</sup>.

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<sup>89</sup>.

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 ei-

<sup>86</sup> [lexexakt.de](http://lexexakt.de), natürliche Handlungseinheit

<sup>87</sup> BGH, Großer Senat, Beschluss vom 03.05.1994 - GSSt 2/93, 3/93; zum Steuerstrafrecht:

<sup>88</sup> Siehe BGH, Urteil vom 20.06.1994 - 5 StR 595/93; wenn verschiedene Handlungen (Steuererklärungen) durch den Fortsetzungszusammenhang zusammengefasst 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 denselben Akt oder Modus betrafen.

<sup>89</sup> BGH, Beschluss vom 19.12.2000 - 4 StR 503/00, mwN.

*Ob die Vollendung in mehreren materiellen Taten erfolgt, orientiert sich am Handeln des Cashers. Anhand der Abbuchungsdaten können erfahrungsgemäß deutliche Pausen festgestellt werden, die aber nicht zwingend auf eine Unterbrechung und die Beendigung einer Tat schließen lassen. Zwei Fehlerquellen sind insoweit zu betrachten:*

*Die Zeitstempel, die die Geldautomaten übermitteln, richten sich nach den Einstellungen im Geldautomaten selber und werden nicht synchronisiert. Sie können von der genauen Zeit abweichen und aus einer anderen Zeitzone stammen .*

*Allein Europa verfügt über mindestens 4 Zeitzonen, von der die Mitteleuropäische Zeit – MEZ – die verbreitetste ist. Die EKS stellt aber die Zeitstempel der Rechenzentren bei der Autorisierung zur Verfügung, so dass die Fehlerquelle abweichender Zeitangaben nahezu ausgeschlossen ist.*

nem einheitlichen Vorsatz umschlossen sind<sup>90</sup>. Solche deliktischen Einheiten können auch die gleichzeitig Fälschung mehrerer Karten<sup>91</sup> und ihren Gebrauch beim Cashing bilden<sup>92</sup>.

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<sup>93</sup>. Das ist zum Beispiel der Fall, wenn Skimmer ihre technischen Geräte installieren, ihre Funktionsfähigkeit gelegentlich überprüfen und die Geräte schließlich wieder abbauen. Das Ausspähen bildet dabei einen einheitlichen Handlungsrahmen, wobei der Vorsatz der Täter darauf gerich-

<sup>90</sup> 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

<sup>91</sup> BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 13; BGH, Beschluss vom 23.06.2010 - 2 StR 243/10, Rn 3.

<sup>92</sup> BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 8.

<sup>93</sup> Weitere Einzelheiten: CF, Angleichung des Rechts beim Falschgeld und Rauschgift, 13.03.2011; BGH, Beschluss vom 02.02.2011 - 2 StR 511/10.

tet 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<sup>94</sup>, kann eine deliktische Einheit bestehen<sup>95</sup>.

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 Du-bletten zu versorgen<sup>96</sup>.

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<sup>97</sup>.

### 3. Fälschungssicherheit

Von der Rechtsprechung des BGH ist anerkannt, dass sich die Fälschung auch alleine auf die Daten auf dem Magnetstreifen beschränken kann<sup>98</sup>. In Bezug auf Zahlungskarten hat der BGH 2010 ausgeführt<sup>99</sup>:

*„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 erhobenen Kartenummer und der Prüfnummer (bei Kreditkarten) sowie dem Unterschriftsfeld 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 Kartenummern, 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 al-

<sup>94</sup> BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 9.

<sup>95</sup> 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.

<sup>96</sup> Siehe: BGH, Urteil vom 10.05.2005 - 3 StR 425/04, S. 9.

<sup>97</sup> BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn. 12.

<sup>98</sup> Zur Verfälschung einer echten Zahlungskarte: BGH, Urteil vom 21.09.2000 - 4 StR 284/00.

<sup>99</sup> BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn. 11

lem 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<sup>100</sup>.

#### 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)<sup>101</sup>. Diese Voraussetzungen liegen angesichts der beschriebenen Sicherheitsmerkmale bei den üblichen von Banken herausgegebenen Karten vor<sup>102</sup>.

Die Garantiefunktion wird darin gesehen, dass *das die Karte ausgebende Unternehmen ... sich gegenüber Vertragsunternehmen <verpflichtet>, deren Forderungen gegen den Kartenbenutzer zu bezahlen*<sup>103</sup>. Diese Definition nimmt § 152b Abs. 4 StGB auf und definiert die Zahlungskarten mit Garantiefunktion als Kredit-, Euroscheck- und

<sup>100</sup> 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.

<sup>101</sup> CF, Skimming und Fälschungsrecht, 13.04.2009

<sup>102</sup> Siehe oben **Fälschungssicherung**.

<sup>103</sup> 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).

sonstige Karten, die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu veranlassen<sup>104</sup>. 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 Kreditkartenverbände sind die von American Express, Master und Visa<sup>105</sup>. Die Autorisierung im Onlineverfahren und die damit verbundene Genehmigung, ohne die keine Verfügung akzeptiert wird, ist bei Kredit- und Debitkarten jedoch identisch<sup>106</sup>, so dass auch die Debitkarten, die an dem Autorisierungsverfahren teilnehmen können, Karten mit Garantiefunktion sind<sup>107</sup>. 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<sup>108</sup>.

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<sup>109</sup>.

<sup>104</sup> 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

<sup>105</sup> Siehe die Übersicht und Erklärungen bei [kartensicherheit.de](http://kartensicherheit.de) – Zahlungsverfahren.

<sup>106</sup> 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.

<sup>107</sup> Siehe oben **Autorisierung**.

<sup>108</sup> BGH, Beschluss vom 17.06.2008 - 1 StR 229/08.

<sup>109</sup> Wenn die Karte ausschließlich zur Forderungsberechnung zwischen Aussteller und Inhaber verwendet werden soll, handelt es sich um eine schlichte Zahlungskarte. Karten für Akzeptanz-Verbände (zum Bei-

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<sup>110</sup> 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 Genehmigungscode. Nicht anders als im alten Verfahren erfolgt die Buchung der Forderung gegen die Bank zunächst auf einem ihrer Zwischenkonten<sup>111</sup>, was der Ausgabe der Euroschecks gleich kommt. Das zeigt auch, dass die 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 Auspähen 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 (Buchung gegen das interne CPD-Konto) und damit gleichzeitig zulasten des

spiel DKV) garantieren dem Akzeptanten die Abrechnung und Vergütung im Dreiecksverhältnis und verbürgen deshalb eine Zahlungsgarantie

<sup>110</sup> Das Markenzeichen „EC“ wurde als „electronic cash“ fortgeführt und wird auf neu ausgegebenen Karten nicht mehr verwendet.

<sup>111</sup> Siehe oben **Clearing**

einzelnen Bankkunden ein<sup>112</sup>, 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<sup>113</sup>.

Eine Ausnahme bilden die vollständigen Auslandsstaten, 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<sup>114</sup>.

### 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<sup>115</sup>. Anlass geben ihm dazu die Fälle, *wenn der Täter unter Vorlage eines gefälschten*

<sup>112</sup> Das BVerfG verlangt seit 2010 nach einem bezifferten Schaden. Auch wenn die Verfügung zunächst gegen ein CPD-Konto gebucht wird, verringert sich dadurch der Verfügungsrahmen des Kunden. Er ist dadurch unmittelbar und bezifferbar geschädigt. Siehe: 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.

<sup>113</sup> Das Landgericht Hannover ist bereits am 17.11.2009 meinen rechtlichen Auffassungen gefolgt (rechtskräftig seit Ende April 2010): CF, Skimming-Rechtsprechung, 18.11.2009

<sup>114</sup> Wegen der Strafverfolgung Deutscher und solcher Ausländer, die nicht abgeschoben werden können, siehe § 7 Abs. 2 StGB.

*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 <sup>116</sup>.

Der BGH spricht damit das POZ-Verfahren an <sup>117</sup>, das Ende 2006 eingestellt wurde <sup>118</sup>, 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 Skimming 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 <sup>119</sup>. Damit stellt sie den Betreiber als Dritten wegen der zivilrechtlichen Störungen im Innenverhältnis frei. Sie kann zwar in aller Regel auf den Karteninhaber und dessen Vermögen befreiend zurückgreifen, haftet jedoch im Außenverhältnis in eigener Person.

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

<sup>115</sup> BGH, Beschluss vom 18.11.2009 - 4 StR 485/08; siehe auch CF, Betrug mit Zahlungskarten auf falschem Namen, 28.01.2009.

<sup>116</sup> Siehe jetzt auch: BGH, Beschluss vom 14.10.2010 - 2 StR 447/10; CF, vom Kontoeröffnungsbetrug zum Identitätsglibber, 03.12.2010.

<sup>117</sup> Point of Sale ohne Zahlungsgarantie – POZ.

<sup>118</sup> Zentraler Kreditausschuss, Kreditwirtschaft stellt POZ-Verfahren Ende 2006 ein, 15.10.2004

<sup>119</sup> Bei Geldautomaten ist das der Auszahlungsbetrag einschließlich der Gebühr.

## 5.2 schadensgleiche Vermögensgefährdung

Die unbezifferte schadensgleiche Vermögensgefährdung <sup>120</sup> wurde jüngst von der Rechtsprechung des BGH in Frage gestellt, weil sie die konkreten Gefährdungsdelikte des Vermögensstrafrechts den abstrakten Gefährdungsdelikten annähert <sup>121</sup> und deshalb vom 1. <sup>122</sup> und vom 3. Strafsenat des BGH <sup>123</sup> tendenziell abgelehnt wird. Auch das BVerfG verlangt seit 2010 immer nach einer Berechnung und Bezifferung des eingetretenen Schadens <sup>124</sup>.

Eine erfreuliche Klärung lieferte der 3. Strafsenat im Januar 2011, weil er an die Stelle der schadensgleichen Vermögensgefährdung den Eingehungsschaden setzt <sup>125</sup>. 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.

Das Cashing bleibt davon unberührt. Mit jeder missbräuchlichen Verfügung des Cashers wird 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

<sup>120</sup> Bestätigt vom BVerfG: Beschluss vom 10.03.2009 - 2 BvR 1980/07

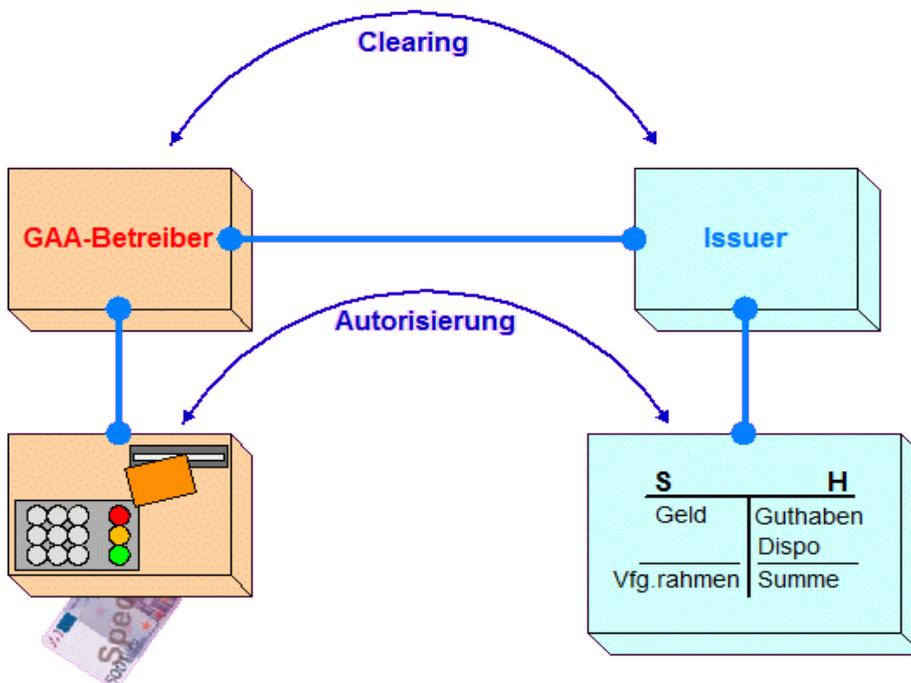
<sup>121</sup> CF, Schaden und schadensgleiche Vermögensgefährdung, 31.01.2010

<sup>122</sup> BGH, Beschluss vom 18.02.2009 - 1 StR 731/08

<sup>123</sup> BGH, Urteil vom 13.08.2009 - 3 StR 576/08

<sup>124</sup> BVerfG, Beschluss vom 23.06.2010 - 2 BvR 2559/08, 105/09, 491/09; CF, BVerfG: Bezifferter Gefährdungsschaden, 15.08.2010.

<sup>125</sup> 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.



Die Autorisierung mit anschließender Geldauszahlung verringert unmittelbar den Verfügungsrahmen des Kunden um den Auszahlungsbetrag zuzüglich den Gebühren. Dadurch sind gleichzeitig die kartenausgebende Bank (Issuer) wegen ihrer Einstandspflicht gegenüber dem Betreiber des Geldautomaten und ihr Kunde wegen der drohenden Belastung seines Kontos mit gleichzeitiger Verringerung seines Verfügungsrahmens geschädigt. Wie die die Verrechnung organisiert, ist ohne Bedeutung (Buchung auf CPD, gegen das Konto des Kunden mit Wertstellung, gegen Unterkonto).

des Kunden gebucht wird. Dadurch tritt unmittelbar ein rechnerischer Eingehungschaden ein.

Die dem Clearing anschließende Schadensverrechnung über die EURO-Kartensicherheit – EKS - ist ein versicherungsähnlicher Prozess, der der Vertrauensbildung dient. Dadurch werden die Bankkunden faktisch von den Schäden freigestellt und zwischen den beteiligten Banken und ihren Verbänden verteilt. Durch das Cashing werden die betroffenen Kunden jedoch unmittelbar geschädigt, weil entweder ihr Kontoguthaben oder ihr Verfügungsrahmen verringert wird (Dispokredit). Würde das System der Schadensabwicklung fehlen, dann blieben die Kundenvermögen vom Cashing belastet und die Finanzwirtschaft hätte ein existenzielles Vertrauensproblem.

### 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 Gebrauchs 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<sup>126</sup>. 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 sind bezifferbare Schäden sowohl beim Bankkunden als auch 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.

<sup>126</sup>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!**“<sup>127</sup>

Das Ausspähen der Daten auf den Magnetstreifen von Zahlungskarten ist im Vorbereitungsstadium des Fälschens von Zahlungskarten gemäß § 152b StGB angesiedelt. Der Versuch in einer arbeitsteiligen Organisation beginnt erst, wenn der Skimmer (Ausspäher) die Daten an den Fälscher weiter gibt<sup>128</sup>. Nach dieser Klarstellung 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 (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 so gleich mit der Fälschung beginnen.

Diese Entscheidung folgt konsequent der zunächst einschränkenden Spruchpraxis<sup>129</sup>:

<sup>127</sup> BGH, Beschluss vom 07.11.2007 - 5 StR 371/07, Rn 17.

<sup>128</sup> 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.

<sup>129</sup> 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.

*„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).

## 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<sup>130</sup>.

<sup>130</sup> BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07, 1151/08, 1524/08; siehe auch CF, Klarstellungen zum Hackerstrafrecht, 20.06.2009.

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<sup>131</sup>. 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 Täterverbänden 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<sup>132</sup>, 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<sup>133</sup>. Im Zusammenhang mit dem Skimming hat das Gericht bei mehrtägigem Ausspähen je nach den

<sup>131</sup> BGH, Urteil vom 27.01.2011 - 4 StR 338/10, Rn 8, 11.

<sup>132</sup> Siehe oben, Kasten vor **2.1 Ausspähen von Daten**.

<sup>133</sup> BGH, Urteil vom 20.05.2009 - 2 StR 576/08, Rn 6; siehe auch CF, Grenzen des Rücktritts, 12.07.2009.

Umständen Tatmehrheit (§ 53 StGB) und Tateinheit (§ 52 StGB) angenommen<sup>134</sup>.

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 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 be-

<sup>134</sup> BGH, Urteil vom 10.05.2005 – 3 StR 425/04, S. 9.

ginnen <sup>135</sup>. 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 folgenden Handlungen, das Fälschen sowie das Gebrauchen gefälschter Zahlungskarten und Computerbetrug (Cashing <sup>136</sup>) bilden ungeachtet der Anzahl der Fälschungen und ihrer Einsätze in aller Regel eine deliktische Einheit <sup>137</sup>, so dass sie zu einer materiellen Tat verschmelzen <sup>138</sup>.

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 Strafraum gesetzt werden muss, hat der BGH ausgeführt <sup>139</sup>:

*... Dies genügt den Anforderungen an die Strafraumwahl 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 <sup>140</sup> 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 <sup>141</sup>. 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 <sup>142</sup>. 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) <sup>143</sup>. Diese drei unterschiedlichen Gefährdungstatbestände führen dazu, dass bereits der Umgang – hier in den Formen des

<sup>135</sup> CF, Versuch der Fälschung, 21.02.2011

<sup>136</sup> CF, Cashing, 26.07.2010

<sup>137</sup> Siehe oben: **6.4 natürliche Handlungseinheiten**

<sup>138</sup> Siehe auch: CF, keine deliktische Einheit, 24.10.2010

<sup>139</sup> BGH, Beschluss vom 28.09.2010 - 3 StR 261/10, Rn 3

<sup>140</sup> CF, Gehilfe in einer Bande, 11.11.2010

<sup>141</sup> Siehe auch oben **6.1 Versuch der Kartenfälschung**.

<sup>142</sup> Siehe auch oben **6.2 Versuch des Computerbetruges**.

<sup>143</sup> Siehe auch oben **2.3 PIN-Skimming und Computersabotage**.

Sich-Verschaffens und Verwahrens – für die meisten zum Skimming eingesetzten Ausspähergeräte 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. Die ältere Rechtsprechung zu den Fälschungswerkzeugen<sup>144</sup> hat jedenfalls den [§ 149 StGB](#) restriktiv ausgelegt und 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 nur 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<sup>145</sup>. 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<sup>146</sup>. 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<sup>147</sup>.

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<sup>148</sup> 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 Computer-routinen.

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.

<sup>146</sup> 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](#).

<sup>147</sup> [BGH, Urteil vom 17.02.2011 - 3 StR 419/10](#), Rn 12

<sup>148</sup> Die Funktechnik wird selten beobachtet, weil sie zu viel Strom verbraucht und deshalb die Ausspäzzeit verringert.

<sup>144</sup> Siehe unten [7.1 Kartenlesegeräte](#).

<sup>145</sup> [BGH, Urteil vom 16.12.2003 - 1 StR 297/03](#).

## 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 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 einer 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<sup>149</sup> oder die elektronischen Bauteile mit Kamerafunktion, die hinter dem Chassis 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 Rechtspre-

<sup>149</sup> CF, Sichtblende mit Kamera, 26.06.2010

chung des BVerfG als straflos anzusehen sind<sup>150</sup>. 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 dahin, 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 das Gesetz ebenfalls die Mehrzahl. Dem entgegen hat der BGH bereits die Fälschung *einer* EC-Karte genügen lassen<sup>151</sup>, 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

<sup>150</sup> BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07, 1151/08, 1524/08; siehe auch oben **6.2 Versuch des Computerbetruges**.

<sup>151</sup> BGH, Urteil vom 21.09.2000 - 4 StR 284/00, Rn 11.

*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

Programm verfügen, das für die Speicherung der Eingaben sorgt.

## 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<sup>152</sup>. Er hat keine Tatherrschaft und übt in aller Regel eine "ganz untergeordnete Tätigkeit" aus<sup>153</sup>.

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 Be-

<sup>152</sup> 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.

<sup>153</sup> BGH, Beschluss vom 02.02.2010 - 3 StR 4/10 (Bunkerhalter und Kurier beim BtM-Handel).

*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 Teilnahmemehandlung 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

*teiliger 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“<sup>154</sup>.*

Die bisher gemachten Erfahrungen und die Rechtsprechung<sup>155</sup> lassen für arbeitsteilig handelnde Skimming-Täter grundsätzlich den Schluss zu, dass sie in allen Tatphasen als Mittäter in fest gefügten Strukturen dauerhaft zusammenarbeiten.

<sup>154</sup> BGH, Beschluss vom 13.01.2010 - 5 StR 506/09, Rn 5

<sup>155</sup> BGH, Urteil vom 17.02.2011 - 3 StR 419/10

*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.

### 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<sup>156</sup>. Er trägt damit der besonderen Gefährlichkeit der arbeitsteiligen und gleichzeitig spezialisierten Tätergruppen Rechnung, ohne damit ein neues Organisationsstrafrecht zu schaffen<sup>157</sup>. 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"*.

<sup>156</sup> BGH, Beschluss vom 22.03.2001 - GSSt 1/00.

<sup>157</sup> BGH, Beschluss vom 29.04.2008 - 4 StR 125/08.

*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 strafscharfendes Merkmal.*

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

Diese Grundsätze sind auch auf die reine Mittäterschaft übertragbar<sup>158</sup>. 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<sup>159</sup>, ihr krimineller Erfolg vorhersehbar ist und sich die Beteiligten im Tatplan halten<sup>160</sup>. Der BGH begründet das damit, dass die arbeitsteilige 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<sup>161</sup>.

Diese Betrachtung hat der BGH auf die Beschaffung eines Firmenmantels, unter dessen Struktur die Komplizen selbständig betrügerische Geschäfte begehen<sup>162</sup>, und sogar auf spontan wir-

<sup>158</sup> CF, Tatanteile des Mittäters, 16.02.2011; BGH, Beschluss vom 07.12.2010 - 3 StR 433/10.

<sup>159</sup> BGH, Beschluss vom 13.08.2002 - 4 StR 208/02.

<sup>160</sup> BGH, Beschluss vom 16.09.2009 - 2 StR 259/09, Rn 4 (Mittätersexzess).

<sup>161</sup> BGH, Urteil vom 16.06.2005 - 3 StR 492/04, S. 8.

<sup>162</sup> 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 Firmen-

*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

kende Zusammenschlüsse übertragen, wenn sie gleichartige Straftaten einer umgrenzbaren Tätergruppe betreffen <sup>163</sup>.

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 <sup>164</sup>. 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 <sup>165</sup>. Er haftet zunächst nur für die konkreten Handlungen, die er

\_\_\_\_\_ mantel) beschaffende Täter aber nur eine, die alle Taten seiner Mittäter umfasst.

<sup>163</sup> BGH, Urteil vom 21.12.2007 - 2 StR 372/07.

<sup>164</sup> BGH, Beschluss vom 29.04.2008 - 4 StR 125/08.

<sup>165</sup> Der BGH wendet sich gegen eine ausufernden Anwendung seiner Rechtsprechung: BGH, Beschluss vom 29.07.2009 - 2 StR 160/09, Rn 5.

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 <sup>166</sup>. 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.“* <sup>167</sup>

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 <sup>168</sup>, ein Qualifizierungsmerkmal ist <sup>169</sup>, das zu einer schärferen Strafdrohung führt <sup>170</sup>.

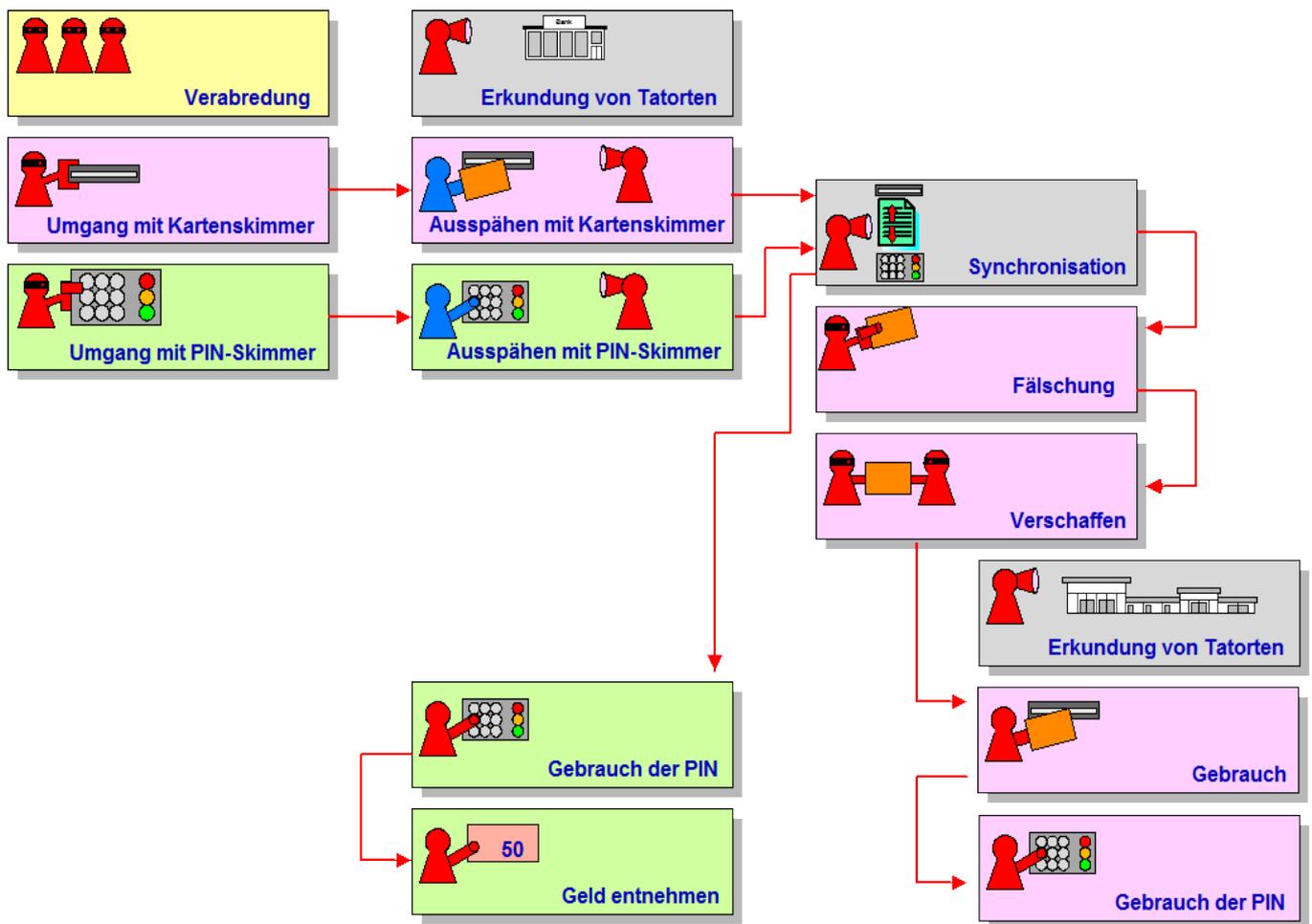
<sup>166</sup> BGH, Beschluss vom 13.08.2002 - 4 StR 208/02

<sup>167</sup> BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

<sup>168</sup> Siehe CF, *Bandenstraftaten*, 17.01.2010 (mit einer Aufstellung der vom Gesetzgeber qualifizierten Tatbestände – *Bandenliste*).

<sup>169</sup> Der besonders schwere Fall bereichert den Grundtatbestand um weitere Tatbestandsmerkmale mit der Folge, dass sich nur der Strafraumen 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.

<sup>170</sup> 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.



Die Hinterleute in arbeitsteiligen Täterstrukturen sind in aller Regel keine Mittäter, weil ihnen die Tatherrschaft fehlt. Sie können als Anstifter zu einer konkreten Straftat (§ 26 StGB), als „Bestimmer“ im Zusammenhang mit einer Verbrechenabrede (§ 30 Abs. 1 StGB) oder als mittelbare Täter (§ 25 Abs. 1 StGB) „in Fällen mafia-ähnlich 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 Mit-täterschaft spricht“<sup>171</sup>.

## 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<sup>172</sup>. 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<sup>173</sup>. Dazu müssen andere persönliche Merkmale herangezogen werden, die sich aus

<sup>171</sup> BGH, Urteil vom 26.07.1994 - 5 StR 98/94, Rn. 84; weitere Einzelheiten: CF, Der Hintermann als Täter, 03.01.2010.

<sup>172</sup> Siehe oben **2.4 natürliche Handlungseinheiten**.

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 Strafraum 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<sup>174</sup>. 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<sup>175</sup> und die Casher (auch) die von ihm ausgespähten Daten erfolgreich missbrauchen.

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<sup>176</sup>), er „*sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen*“<sup>177</sup> (Gewerbsmäßigkeit) und sich einem Bandenwillen anschlie-

ßen will (Bande). Diese Fragen werden immer nur im Rahmen einer individuellen Gesamtwürdigung beantwortet werden können, bei der das 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<sup>178</sup> – das Vorliegen von tatsächlichen Anhaltspunkten, um zum Beispiel dem Täter einen strafbefreienden Rücktritt vom Versuch zuzubilligen<sup>179</sup>, und wendet sich damit gegen eine unkritische Auseinandersetzung mit den von Verteidigungsstrategien gefärbten Einlassungen<sup>180</sup>.

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<sup>181</sup>. Sie lässt in der Parallelwertung der Skimmer erwarten, dass sie jedenfalls mit bedingtem Vorsatz die Tatvollendung billigen<sup>182</sup>.

In den Fällen, in denen es nicht zur Vollendung durch Mittäter kommt, stellt sich die Frage nach

<sup>173</sup> CF, Angleichung des Rechts beim Falschgeld und Rauschgift, 13.03.2011; BGH, Beschluss vom 02.02.2011 - 2 StR 511/10.

<sup>174</sup> Siehe oben 5. Tatorte und deutsche Gerichtsbarkeit.

<sup>175</sup> Arbeitsteilige Skimming-Täter handeln grundsätzlich als Mittäter: BGH, Urteil vom 27.01.2011 - 4 StR 338/10, Rn. 8.

<sup>176</sup> BGH, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09

<sup>177</sup> BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5.

<sup>178</sup> „Im Zweifel für den Angeklagten“

<sup>179</sup> BGH, Urteil vom 20.05.2009 - 2 StR 576/08, Rn 6

<sup>180</sup> Zur (unbeachtlichen) Verteidigererklärung: BGH, Urteil vom 20.06.2007 - 2 StR 84/07; siehe auch CF, Prozessklärung unbeachtlich, 05.09.2007.

<sup>181</sup> 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

<sup>182</sup> Siehe Kasten bei 8.1.

dem Beginn des Versuchsstadiums, die jetzt in Bezug auf arbeitsteilige Skimmingbanden geklärt ist. Im übrigen verbleibt es nur bei einer Strafbarkeit wegen der aufgeführten Vorbereitungshandlungen<sup>183</sup>, die in Tateinheit mit einer Verbrechensabrede stehen können<sup>184</sup>.

### 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<sup>185</sup>, 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<sup>186</sup>. 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,

<sup>183</sup> Siehe oben **7. Vorbereitungshandlungen**.

<sup>184</sup> 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.

<sup>185</sup> BGH, Urteil vom 04.02.2009 - 2 StR 165/08; siehe auch CF, Verbrecher muss Mittäter sein, 25.04.2009.

<sup>186</sup> BGH, Urteil vom 13.01.2010 – 2 StR 439/09.

*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

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<sup>187</sup>.

### 10. Beteiligungsmodell beim arbeitsteiligen Skimming

Der typische Tatplan beim arbeitsteiligen Skimming<sup>188</sup> 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,

<sup>187</sup> Siehe oben **6.3 Rücktritt vom Versuch**.

<sup>188</sup> Siehe oben **1. arbeitsteiliges Vorgehen**.

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 Ausspäehens in Bezug auf den Gesamtplan zu ziehen sind. Bei der Beurteilung sind zwei Gesichtspunkte besonders wichtig:

- ▶ 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 unbekanntem 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 Strafraum 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 betreiben.“*

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 sich dann als Beihilfe zum Fälschen und Gebrauch von Zahlungskarten mit Zahlungsgarantie sowie in Bezug auf das Gebrauchen in Tateinheit mit Beihilfe zum Computerbetrug dar.

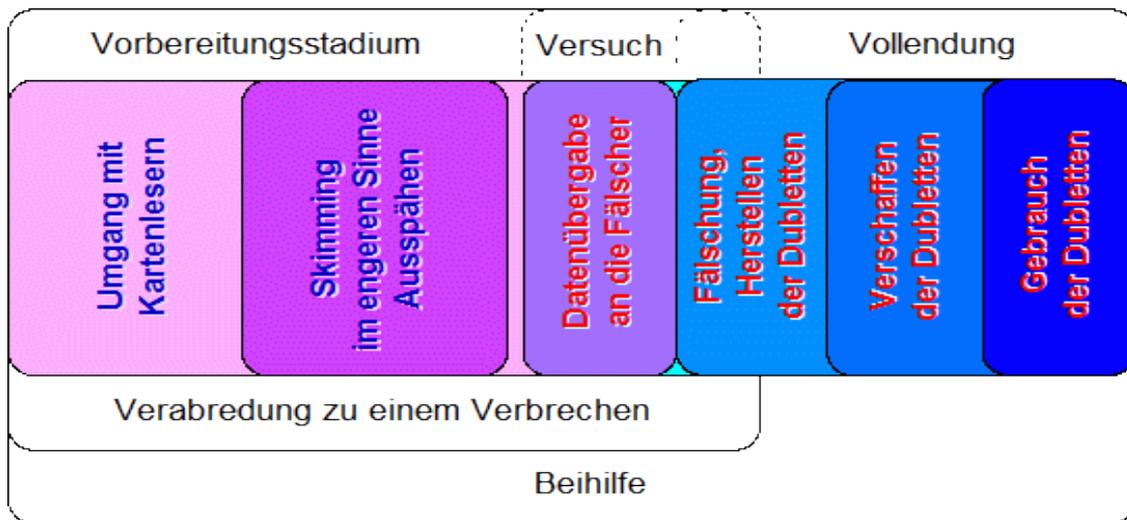
### 10.4 Umgang mit Skimming-Geräten

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.

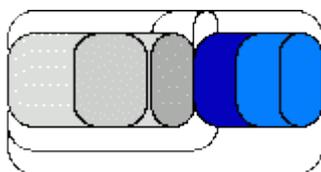
**10.4.3** Attrappen mit handelsüblichen Kameras zum Ausspähen der PIN: Insoweit kommen vor allem Mobiltelefone mit Kamerafunktion und handelsübliche Digitalkameras zum Einsatz, die mit ihrer eigenen, nicht umgebauten Elektronik zur Steuerung betrieben werden. Es handelt sich um Dual-Use-Komponenten, 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.



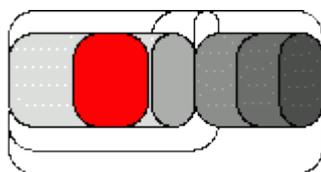
**Anhang: Grafiken zum Beteiligungsmodell**

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 <sup>189</sup>.

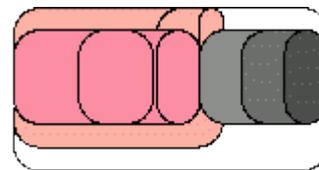
Dem liegt das oben gezeigte Phasenmodell zugrunde <sup>190</sup>:



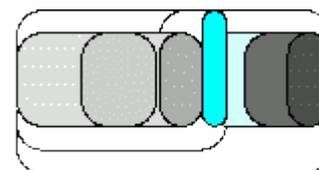
Das Grunddelikt ist das Fälschen von Zahlungskarten im Sinne der §§ 152a, 152b StGB (dunkelblau). Gleichrangige (aber nachfolgende) Tathandlungen sind das Sich-Verschaffen und das Gebrauchen von falschen Zahlungskarten (marineblau).



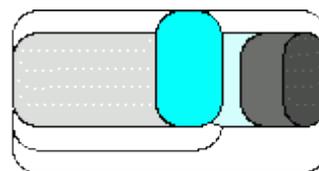
Das Skimming im engeren Sinne, also das Ausspähen der Kartendaten und PIN (rot), ist im Vorbereitungsstadium des Fälschungsdelikts angesiedelt. Es ist kein Erfolgsdelikt, also vor allem kein Ausspähen von Daten im Sinne von § 202a StGB <sup>191</sup>.



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.



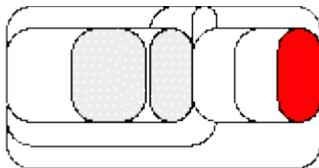
In arbeitsteiligen Täterstrukturen lässt der BGH jetzt den Versuch bereits zu, sobald die Skimmer das Ausspähen abgeschlossen haben und die ausgespähten Daten an ihre arbeitsteilig eingebundenen Mittäter übermitteln, wenn sie die Vorstellung haben,

<sup>189</sup> CF, Bilderbuch Skimming-Strafrecht, 26.07.2010

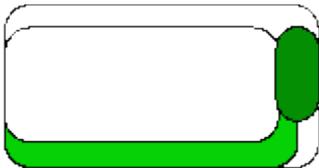
<sup>190</sup> CF, Skimming: aktuelles Beteiligungsmodell, 13.03.2011

<sup>191</sup> CF, Ausspähen von Daten und das Skimming, 14.05.2010

dass die Mittäter mit der Fälschung unverzüglich beginnen<sup>192</sup>.



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

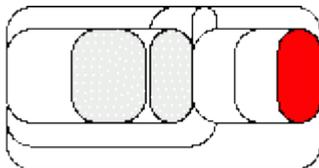
auch für den Umgang mit PIN-Skimmern, wenn sie besondere Schaltungen ("Programme") enthalten, die auf den Computerbetrug spezialisiert sind.

<sup>192</sup> CF, Versuch der Fälschung, 21.02.2011; BGH, Urteil vom 27.01.2011 - 4 StR 338/10.

## Cashing



Grafik 1: Cashing



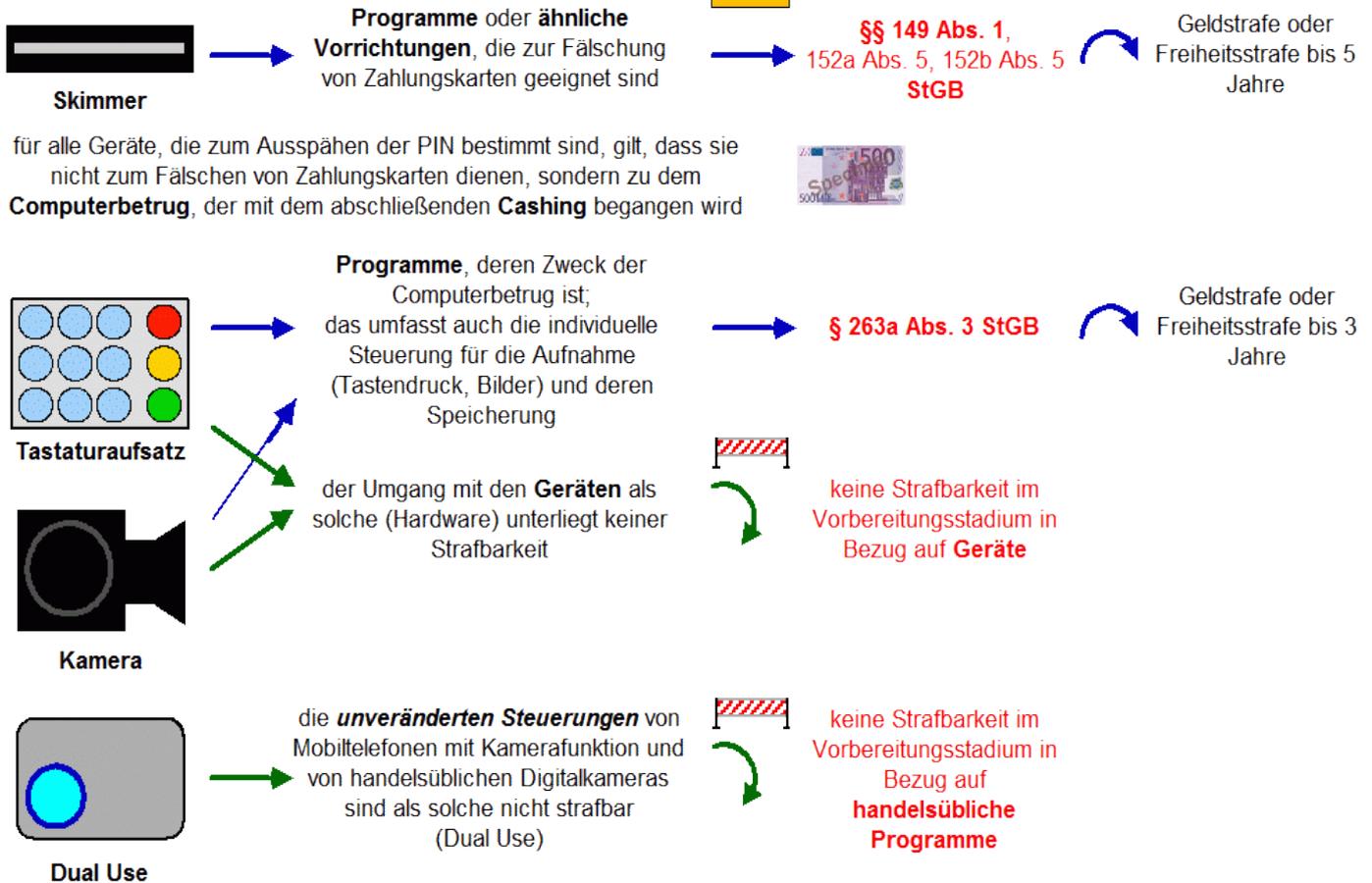
Das finale Ziel des Skimmings, das Cashing, ist am einfachsten darzustellen.

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 voraussetzen sein, so dass sich der Strafraum auf Freiheitsstrafe von 2 bis 15 Jahre erhöht (§ 152b Abs. 2 StGB).

### Umgang im Vorbereitungsstadium



### Grafik 2:

#### Umgang mit Skimminggeräten im Vorbereitungsstadium



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

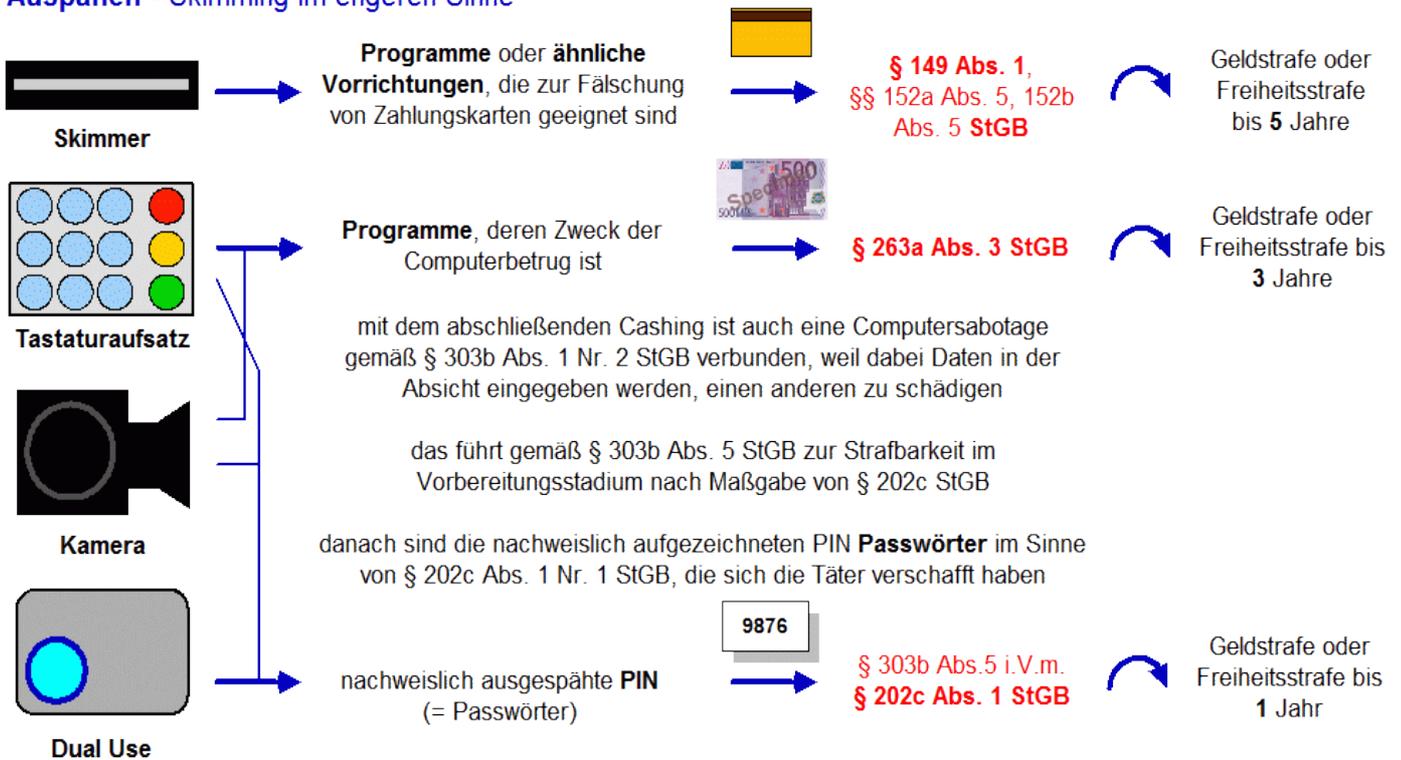
Die Geräte, die zum Ausspähen der PIN bestimmt sind, werden von dieser Vorschrift nicht erfasst, weil sie nicht zur Fälschung von Zahlungskarten dienen, sondern zu dem abschließenden Computerbetrug beim Cashing. Insoweit richtet sich die Strafbarkeit nach § 263a Abs. 3

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.

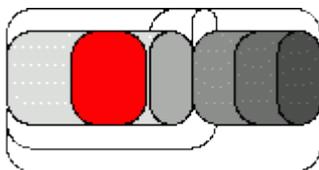
Eine weitere Einschränkung ergibt sich beim Einsatz handelsüblicher Mobiltelefone mit Kamerafunktion und digitaler Kameras, die ohne Änderung der werksseitigen Steuerung verbaut werden. Sie sind Dual Use-Produkte und sind deshalb strafneutral.

### Auspähen - Skimming im engeren Sinne



### Grafik3:

#### Einsatz von Skimminggeräten



Mit dem Einsatz der Skimminggeräte ändert sich wegen der Kartenlesegeräte und der in den Attrappen verbau-

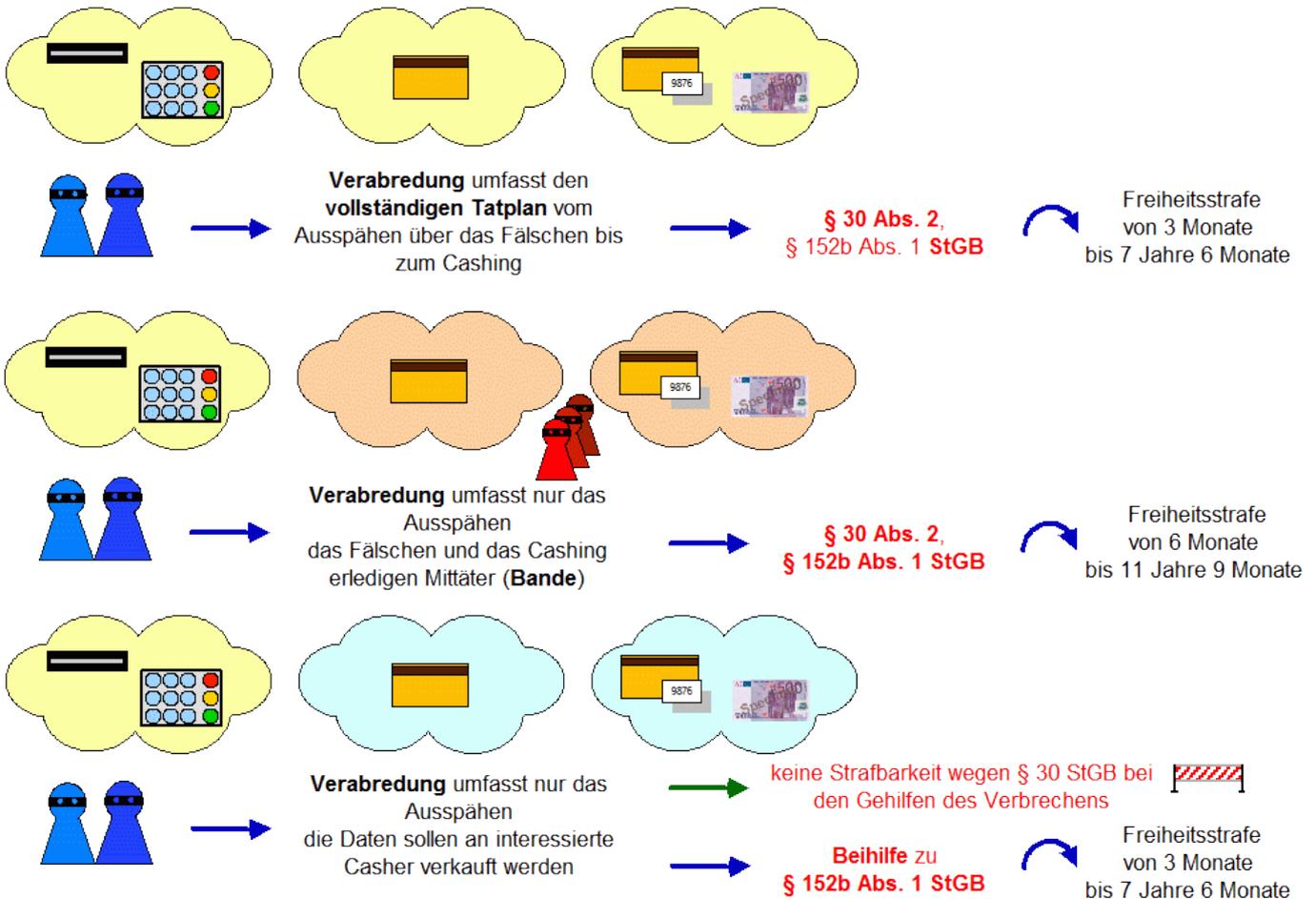
ten Programmen nichts (Grafik 2).

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 „Hackerparagrafen“ § 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.

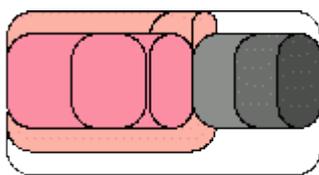
Bei strenger Auslegung müssen mindestens zwei PIN ausgespäht werden, bis die Strafbarkeit eintritt (Gesetzeswortlaut in Mehrzahl).

### 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 be-

handeln 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 Gebrauchs 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 (§ 2). Die Qualifizierungen durch § 1 oder § 3 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 § 1 und § 3 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 § 2 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 (§ 1, § 3) 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

### ① *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:

### ② *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 § 1 oder § 3 ausgerichtet, so ergibt sich die Strafbarkeit der Skimmer in Bezug auf eine Tat nach § 152b Abs. 2 StGB, wobei der Strafraum 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<sup>193</sup>.

### ③ *selbständiges Skimming*

Fehlt es sowohl an dem Cashing, am strafbaren Versuch wie auch an der Verbrechensabrede, so greifen ausschließlich die strafbaren Vorbereitungshandlungen<sup>194</sup>.

Der Umgang mit Skimmern, also den präparierten Kartenlesegeräten<sup>195</sup>, 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-

<sup>193</sup> Siehe oben [7.2 Kameras](#) und [7.3 Tastaturaufsätze](#).

<sup>194</sup> Siehe oben [7. Vorbereitungshandlungen](#).

<sup>195</sup> Siehe oben [7.1 Kartenlesegeräte](#).

nem Strafraumen 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 <sup>196</sup>.

### 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 Teila-

spekte 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 <sup>197</sup> 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

<sup>196</sup> Siehe oben **2.3 PIN-Skimming und Computersabotage**.

<sup>197</sup> 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 <sup>198</sup>, dass die angedrohte Höchststrafe mehr als 5 Jahre Freiheitsstrafe beträgt. Zuletzt im Zusammenhang mit den Verkehrsdaten hat das BVerfG ausgeführt <sup>199</sup>:

*„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 <sup>200</sup>. Die bisher bekannten Erscheinungsformen im Zusammenhang mit Tätergruppen ausländischer Herkunft lassen zudem geschäftsähnliche Strukturen erkennen <sup>201</sup>.

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 <sup>202</sup>.

<sup>198</sup> BVerfG, Urteil vom 03.03.2004 - 1 BvR 2378/97, 1 BvR 1084/99

<sup>199</sup> BVerfG, Beschluss vom 11.03.2008 - 1 BvR 256/08

<sup>200</sup> Nr. 2.3 der Anlage E zu den RiStBV.

<sup>201</sup> Nr. 2.1 der Anlage E zu den RiStBV.

<sup>202</sup> 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 <sup>203</sup>, lassen sich bereits einige Erfahrungswerte formulieren, die für die Bewertung in anderen und neuen Verfahren herangezogen werden können <sup>204</sup>.

### 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.**

<sup>203</sup> 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

<sup>204</sup> Siehe CF, Erfahrungswerte wegen des Skimmings, 29.11.2009

**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 ausbaldovert 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.

### 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 angeleiteten Dilettanten besteht, gibt es jedoch nicht.

Daraus folgt:

**Die Installation der Ausspähergeräte 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 (Funktionsfähigkeit, 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 stress-resistent, so dass nicht zu erwarten ist, dass sie liebevolle 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.

## 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

## 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 EuroCard, Master und Visa 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 Tastaufsatz.

**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.