Dieter Kochheim

Skimming

Hintergründe und Strafrecht

Zweite überarbeitete Fassung,
aktualisiert im Juli 2010

Erscheinungsformen und Strafbarkeit des Skimmings

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

Cybercrime im Cyberfahnder

Die Webseite ▸ cyberfahnder.de widmet sich seit 2007 der Cybercrime, ihren Erscheinungsformen und ihrer Strafverfolgung. Dazu gehört die Darstellung der technischen Grundlagen, soweit sie zum Verständnis nötig sind, und die Auseinandersetzung mit den einschlägigen Gesetzen und der Rechtsprechung.

Die Arbeitspapiere im Cyberfahnder fassen die wesentlichen Aufsätze, Beiträge und Meldungen zusammen.

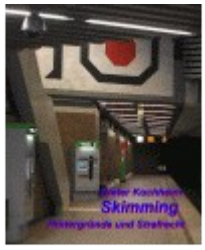
Zuletzt ist das ▸ Arbeitspapier Netzkommunikation erschienen, das sich mit den Grundlagen der Telekommunikation und des Internets befasst. Von der Adressierung in den Netzen führt das Arbeitspapier über das Routing und die Verschlüsselung zu den Manipulationen im Internet von Schurkenprovidern und anderen Netzbetreibern. Den Abschluss bildet eine Auseinandersetzung mit den miteinander verflochtenen Formen der Cybercrime und des Cyberwar.

Alle Beiträge in diesem Arbeitspapier sind Neuveröffentlichungen.

Mit den wichtigsten Erscheinungsformen der Cybercrime befasst sich das ▸ Arbeitspapier Cybercrime. Es beschreibt zunächst die Angriffspunkte gegen die Informations- und Kommunikationstechnik, die Nummerntricks, 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.

Alle Beiträge wurden für diese Zusammenstellung überarbeitet. Das Kapitel über den Identitätsdiebstahl und das Phishing ist neu und der Teil über die Underground Economy wurde weitgehend neu gefasst.

Als erstes Arbeitspapier in dieser Reihe erschien im Dezember 2009 das zum Thema Skimming (▸ Arbeitspapier Skimming, Fassung aus 2009). Bedingt durch neue Erkenntnisse aus der Praxis und klärenden Entscheidungen des Bundesgerichtshofes von Anfang 2010 wurde eine gründliche Überarbeitung nötig.



Die zweite Fassung des ▸ Arbeitspapiers Skimming ist Ende Februar 2010 erschienen und wird seither fortgeschrieben und aktualisiert. Neu ist jetzt vor allem das Beteiligungsmodell und die dazu erstellten Grafiken.

Hannover, Juli 2010

Thema:	**Skimming**
Autor:	Dieter Kochheim
Version:	2.11
Stand:	25.07.2010
Cover:	U-Bahn-Station Werderstraße, Hannover
Impressum:	cyberfahnder.de

S. **Inhalt**

Vorwort

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

Das Skimming ist zu einem einträglichen Geschäft geworden, in dem sich gut aufgestellte einheimische und internationale Banden tummeln.

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

Zweite Auflage, Version 2.11

Mit mehreren Anfang 2010 veröffentlichten Entscheidungen hat der Bundesgerichtshof – BGH – die Rechtsprechung über das Fälschen von Zahlungskarten mit Garantiefunktion präzisiert. Das erforderte eine umfassende Überarbeitung dieses Arbeitspapiers im Hinblick auf die Strafbarkeit des Skimmings in den verschiedenen Tatphasen und zu Änderungen in den von mir vertretenen Positionen. Alle Zweifelsfragen sind jedoch noch nicht geklärt.

Wegen des Auslesen der Magnetstreifen von Zahlungskarten tendiert der BGH entgegen einer früheren Auffassung [4] jetzt dazu, dass das Ausspähen der Magnetstreifen von Zahlungskarten kein Ausspähen von Daten gemäß § 202a Abs. 1 StGB ist, weil es den Karten an einer besonderen Zugangssicherung fehlt [5]. In anderer Sache hat das Gericht den Eintritt des Versuchsstadiums beim Nachmachen (Fälschen) von Zahlungskarten mit Garantiefunktion präzisiert [6]. Das reine Ausspähen von Kartendaten ist deshalb grundsätzlich noch als Vorbereitungshandlung zum abschließenden Verbrechen beim Cashing anzusehen. An der von mir entwickelten Lösung, das Ausspähen von Kartendaten als den Eintritt in den Versuch der Fälschung von Zahlungskarten zu betrachten (§§ 152a, 152b StGB) halte ich als Möglichkeit der juristischen Auslegung fest. Den Ausführungen im Arbeitspapier lege ich jetzt (Juli 2010) aber die strenge Auslegung zugrunde, dass der Versuch erst beim unmittelbaren Ansetzen zum Fälschen beginnt.

Zu allen Einzelheiten einer strafbaren Verbrechensabrede (§ 30 StGB) hat sich der BGH noch nicht geäußert, aber in mehreren Fällen die betreffenden Revisionen verworfen. In den Fällen der gewerbs- oder bandenmäßigen Begehung dürfte das einzeln betrachtete Ausspähen als Verabredung zu einem Verbrechen gemäß § 152b StGB gewertet werden, wobei nach einer Äußerung des Generalbundesanwalts Tateinheit (§ 52 StGB) mit Tathandlungen aus § 149 StGB besteht [7]. Insoweit verdichtet sich auch die Meinung, dass die Herstellung und der „Umgang“ mit präparierten Kartenlesegeräten nach § 149 StGB strafbar ist [8]. Das gilt aber nicht in Bezug auf Tastaturaufsätze und Kameras zum Ausspähen der Persönlichen Identifikationsnummern – PIN.

Auch die zweite Auflage dieses Arbeitspapiers ist eine Zwischenbilanz in Bezug auf die Rechtsprechung, die sich wegen der Einzelheiten erst entwickelt. Das gilt nicht nur für das Skimming, son-

---

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

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

[3] CF, Überwachungstechnik: Zahlungskarten, 18.05.2008

[4] BGH, Urteil vom 10.05.2005 – 3 StR 425/04

[5] BGH, Beschluss vom 14.01.2010 – 4 StR 93/09, S. 4

[6] BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn 9, 10

[7] Stellungnahme vom 09.12.2009 zu 3 StR 539/09

[8] 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 (noch nicht veröffentlicht). Siehe auch Fischer, § 149 StGB Rn 3.

dern auch für andere Erscheinungsformen der Cybercrime und in neuen Kriminalitätsfeldern. Sie erfordern meistens eine tiefe Auseinandersetzung mit grundsätzlichen Rechtsfragen und stellen hohe Ansprüche an die Strafverfolger, die mit ihnen befasst sind.

Das Thema Skimming im Cyberfahnder

Mit dem Thema „Skimming“ [9] 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 [10] und im November 2009 erschien die erste Fassung dieses Arbeitspapiers [11].

Das Skimming als Kriminalitätsform war zunächst ein Randthema und ich habe es nicht als einen Teil der Cybercrime [12] im engeren Sinne angesehen. Das sehe ich heute anders, weil sich die Formen, in denen sich die Kriminellen der Informationstechnik – IT – und des Internets bedienen, immer mehr annähern und Mischformen bilden.

Dieses Arbeitspapier fast die Beiträge im Cyberfahnder zusammen und aktualisiert sie. Seine Aufgabe ist es auch, eine schnelle Orientierung in Bezug auf die durchaus schwierigen Rechtsfragen zu geben, die bei der Strafverfolgung wegen des Skimmings auftreten.

Überblick

Zunächst werden die aktuellen Erscheinungsformen des Skimmings beschrieben.

Dazu wird zwischen dem Skimming im engeren Sinne, also dem Ausspähen von Kartendaten und Persönlichen Identifiktionsnummern – PIN, und dem Cashing unterschieden, also dem Missbrauch gefälschter Zahlungskarten an Geldautomaten, die den Beginn und den Abschluss des Tatplanes kennzeichnen.

Der zweite Teil widmet sich den finanzwirtschaftlichen Prozessen des bargeldloser, kartengestützter 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 Genehmigungscodes 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. Den Abschluss bildet eine Auseinandersetzung mit der Rechtsprechung zu arbeitsteiligen Tätergruppen, die auch bei der Beteiligung an vorbereitenden Handlungen und an Teilakten des Gesamtplans zur Strafbarkeit am finalen Verbrechen führt. Neu sind das Beteiligungsmodell, das bei der Systematisierung der Tathandlungen in Bezug auf die einschlägigen Strafvorschriften helfen soll, und die dazu entwickelten Grafiken.

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

Hannover, 25.07.2010

[9] CF, Skimming, Juli 2007

[10] CF, arbeitsteiliges Skimming, 18.05.2008

[11] CF, Zwischenbilanz: Skimming, 14.11.2009

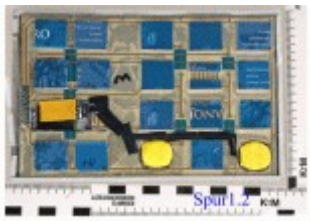
[12] CF, Cybercrime und IT-Strafrecht, 08.08.2008

A. Phänomen Skimming

„Skimming“ als kriminelle Erscheinungsform hat seinen Ausgang beim Ausspähen der auf den Magnetstreifen von Kredit- und Zahlungskarten gespeicherten Kartendaten und den Persönlichen Identifikationsnummern – PIN, die von den Bankkunden bei ihren Verfügungen am Geldautomaten eingegeben werden. 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.

Die klassischen Skimming-Täter treten in zwei Tatphasen öffentlich auf, beim Ausspähen von Daten und abschließend beim Missbrauch von Zahlungskarten. Anlässlich dieser öffentlichen Auftritte erfolgen auch erfahrungsgemäß die polizeilichen Zugriffe. Der Fälschungsvorgang selber wird nach den bisherigen Erkenntnissen vorwiegend im osteuropäischen Ausland unternommen.

Wie jede kriminelle Mode wandelt sich auch das Skimming, wobei verfeinerte Methoden zum Einsatz kommen. Gegen das Ausspähen der PIN mit einer Kamera [13] 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 flach oberhalb der Tastatur anbringen [14] oder statt einer Kamera einen Tastaturaufsatz [15] oder sogar eine vollständige Fassade (Front Covering) einsetzen [16] (Bild unten: Rückseite eines Tastaturaufsatzes).



Der wechselnde Einsatz verschiedener Karten für den Zugang zur Bank und für die Verfügung am Geldautomaten schützt den Kunden dann nicht mehr, wenn der Skimmer direkt am Geldautomaten angebracht ist [17].

Seit zwei Jahren treten Fälle des POS-Skimmings auf [18]. POS bedeutet 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 [19]. Alle notwendigen Daten durchlaufen diese Geräte. Wenn die Täter es schaffen, sie entsprechend umzurüsten, dann

[13] CF, Kamera, 13.04.2009

[14] CF, Sichtblende mit Kamera, 26.06.2010

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

[16] CF, Skimming, Juli 2007

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

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

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

speichern oder senden sie die Dumps [20] an die Täter.

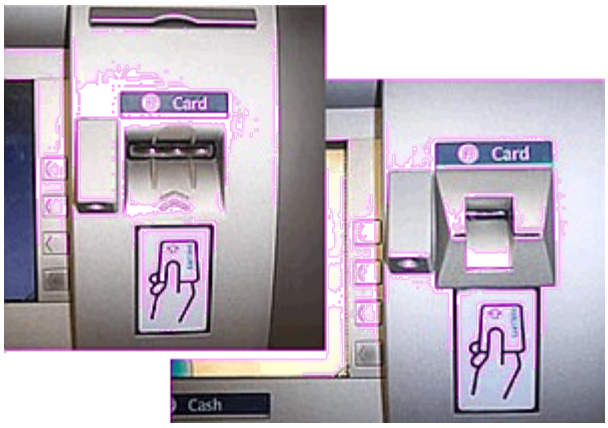
In Russland wurden unlängst die Geldautomaten selber gehackt, um die Dateneingabe vollständig aufzuzeichnen [21]. Vermutlich wurde dazu eine technische Schnittstelle an den Geräten genutzt, die zur Wartung, Funktionsprüfung oder Aktualisierung der Software bestimmt ist.

Beide Beispiele zeigen, dass die Beschaffung der Kartendaten und PIN auf mehreren Wegen erfolgen kann. Sie ist 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 eindrangen und die Kartendaten einschließlich PIN von 100 Kunden ausspähten [22]. Gleichzeitig erhöhten sie deren Auszahlungslimit. Am 08.11.2008 wurden weltweit und gleichzeitig an 130 Geldautomaten in 49 Städten die gefälschten Zahlungskarten eingesetzt und damit 9 Millionen US-$ erbeutet.

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

Das Skimming ist von seiner Herkunft her eher beim Trickdiebstahl und -betrug angesiedelt [23], weil es ihm ursprünglich nur um das Stehlen von Zahlungskarten und ihre Fälschung ging. Es verlangt handwerkliche Fertigkeiten bei der Herstellung der eingesetzten Geräte, besonderes Wissen wegen der Auswahl der Geldautomaten und Standorte, die sich einerseits zum Ausspähen der erforderlichen Daten und andererseits zum Missbrauch der gefälschten Zahlungskarten eignen, sowie logistisches Geschick bei der Installation der Überwachungshardware. Die verschiedenen Arbeitsschritte im Tatplan, ihre wechselnden Anforderungen an die Fähig- und Fertigkeiten der Täter [24] und die grenzüberschreitende Logistik des Gesamtplans sprechen für eine Arbeitsteilung mit einer zentralen planenden und steuernden Instanz.



Die bisher gemachten Erfahrungen zeigen, dass Skimmer [25] und Casher [26] regelmäßig 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. Aus den Journalen von angegriffenen Geldautomaten ergeben sich Stromunterbrechungen, wenn Lesegeräte ausgewechselt werden, dass zur Funktionsprüfung der präparierten Kartenlesegeräte und zur Markierung der ausgespähten Zahlungskartendaten Testkarten eingesetzt werden [27]. Andere Bilder haben eindrucksvoll gezeigt, wie

[20] vollständige Kartendaten einschließlich PIN; CF, Fachworte, April 2007

[21] CF, Skimming an der Quelle, 20.03.2009

[22] CF, Skimming-Coup, 06.02.2009

[23] CF, Proll-Skimming, 18.05.2008; CF, Beobachtung. Trickdiebstahl, Juli 2007

[24] 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.

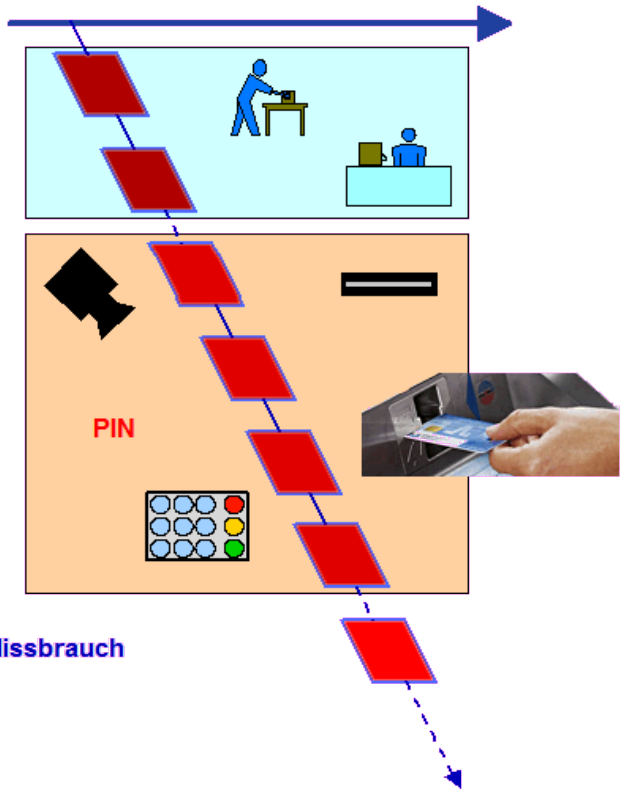
[25] Skimmer: siehe Glossar.

[26] Casher: siehe Glossar.

Casher beim Einsatz von White Cards [28] mit ihren Handys telefonieren und sich dabei offenbar die PIN übermitteln lassen.

Die bevorzugten Zeiten für das Ausspähen liegen außerhalb der Banköffnungszeiten, also ganz besonders ab Freitag Mittag bis über das Wochenende hinweg. Das verbindet die Skimming-Täter mit denen beim klassischen Phishing. Beiden geht es darum, den störenden Eingriff der Bankmitarbeiter zu unterlaufen. Beim Phishing [29] 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 [30], so dass am Samstag Morgen das neue Wochenlimit angegriffen werden kann.



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

[27] 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.

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

[29] 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.

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

B. bargeldloser, kartengestützter Zahlungsverkehr

Unter dem Gesichtspunkt des klassischen Skimmings, bei dem das Ausspähen und der Missbrauch gefälschter Zahlungskarten in der Öffentlichkeit stattfindet, bedarf das Verfahren des bargeldlosen Zahlungsverkehrs einer besonderen Betrachtung.

1. Fälschungssicherung

Die in Deutschland herausgegebenen Zahlungskarten [31] verfügen über mehrere Vorrichtungen gegen das Fälschen der Karte selber [32]. Neben dem Unterschriftsfeld, den Merkmalen des Aufdrucks und des für die Individualdaten verwendeten Schrifttyps (OCR-B [33]) sind das besonders der EMV-Chip und das Maschinenlesbare Merkmal – MM.

Das MM ist eine Besonderheit, die es nur in Deutschland gibt. Dabei handelt es sich um einen im Kartenkörper eingebetteten Merkmalstoff, der eine individuelle Codierung der Karte zulässt [34]. Diese Codierung wird im Geldautomaten mit einer Prüfsumme abgeglichen, die auf dem Magnetstreifen der Zahlungskarte gespeichert ist. Es wird jedoch nicht von den 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.

Der EMV-Chip wird von den großen Verbünden für grenzüberschreitend einsetzbare Zahlungskarten gefordert und ist bereits weit verbreitet [35]. Das Kürzel geht auf „**E**lectronic Cash – **M**aster/Maestro – **V**isa“ zurück [36]. Der Chip ist zwar programmierbar [37], soll aber nicht manipulierbar sein [38] und eine verschlüsselte Datenkommunikation ermöglichen [39].

In den meisten west- und nordeuropäischen Staaten erfolgt die Autorisierung anhand der Chip- und nicht mehr anhand der Daten auf dem Magnetstreifen. Die Geldautomaten in Teilen Süd- und Osteuropas beschränken sich jedoch häufig 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 [40]. 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 [41].

---

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

[32] CF, Zahlungskarten, 18.05.2008

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

[34] CF, Sicherheitsmerkmale und Merkmalstoffe, 06.02.2010

[35] Kartensicherheit.de, EMV-Chip

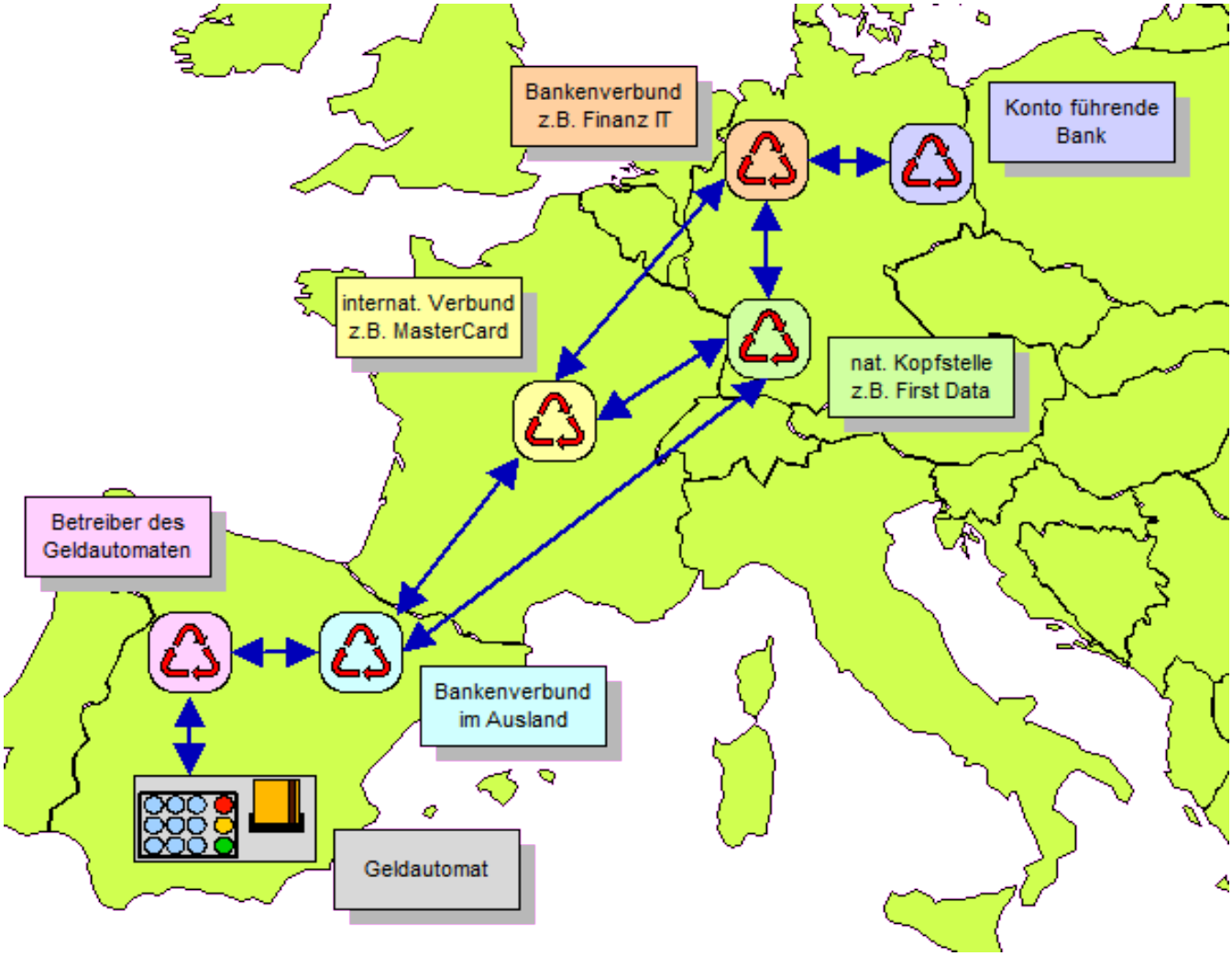
[36] CF, Zahlungskarten mit Garantiefunktion, 13.04.2009

[37] CF, Turbulenzen beim bargeldlosen Zahlungsverkehr, 06.02.2010

[38] 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

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

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



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 [42]. Im Alltag zeigt sich die Autorisierung darin, dass nicht nur die Zahlungskarte geprüft wird, sondern auch die PIN eingegeben werden muss. Die damit ausgelöste Prüfung erfolgt bei der kartenausgebenden Bank, der die Transaktionsdaten im elektronischen Onlineverfahren übermittelt werden und die einen Genehmigungscode zurückmeldet. 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.

[41] CF, Einzugsermächtigung und Lastschriftverfahren, 2007

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

Genehmigungsnummer | Authorisation Code

Die Genehmigungsnummer wird infolge einer Autorisierungsanfrage von der Karten ausgebenden Bank (Issuer) vergeben und wiederum von dem Acquirer an den Händler bestätigt. Ohne diese Genehmigungsnummer hat der Händler für die Transaktion keine Zahlungsgarantie.

kartensicherheit.de

3. Autorisierung

Die wesentlichen Sicherungen für das Autorisierungsverfahren [43] bestehen in den Sicherheitsmerkmalen der Zahlungskarte, in der PIN und schließlich in dem Genehmigungscode, den die kartenausgebende Bank an den Akzeptanten meldet [44].

Zum Zweck der Autorisierung von Debitkarten [45] liest der ausländische Geldautomaten die Kartendaten aus, kombiniert sie mit der vom Kunden eingegeben PIN, dem Auszahlungsbetrag, der Gebühr, den Individualmerkmalen des Geldautomaten und der Uhrzeit. Der daraus gebildete Datensatz wird über Kommunikationsnetze und durch verschiedene Zwischenstellen (zum Beispiel in Deutschland: First Data Corporation [46], Finanz IT [47]) bis zur kartenausgebenden Bank geleitet [48]. 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 [49], der die Auszahlung autorisiert und eine Garantie enthält, dass die autorisierende Bank für den Auszahlungsbetrag bürgt [50] [51].

4. Clearing

Nach der Autorisierung erfolgt bei Debitkarten in aller Regel keine unmittelbare Belastung des Kundenkontos, sondern eine Zwischenbuchung auf einem bankinternen Konto [52]. 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 abschließenden Schadenseintritt im Sinne von § 263a StGB. Er erfolgt erst nach der Autorisierung, der Auszahlung und schließlich dem Clearing, 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 Be-

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

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

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

[46] früher Gesellschaft für Zahlungssysteme - GZS

[47] Rechenzentrum der Sparkassen

[48] Siehe Glossar: Autorisierung, Clearing.

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

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

[51] 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.

[52] Conto pro Diverse – CPD

lastung gegenbucht und diese Forderung bei der EURO Kartensysteme - EKS [53] - 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.

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

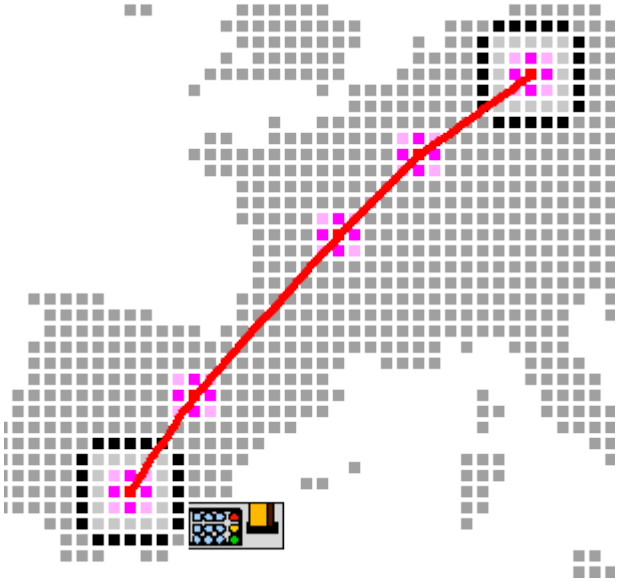
6. Ergebnisse

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

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

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

[53] Siehe auch EKS – Analyse.



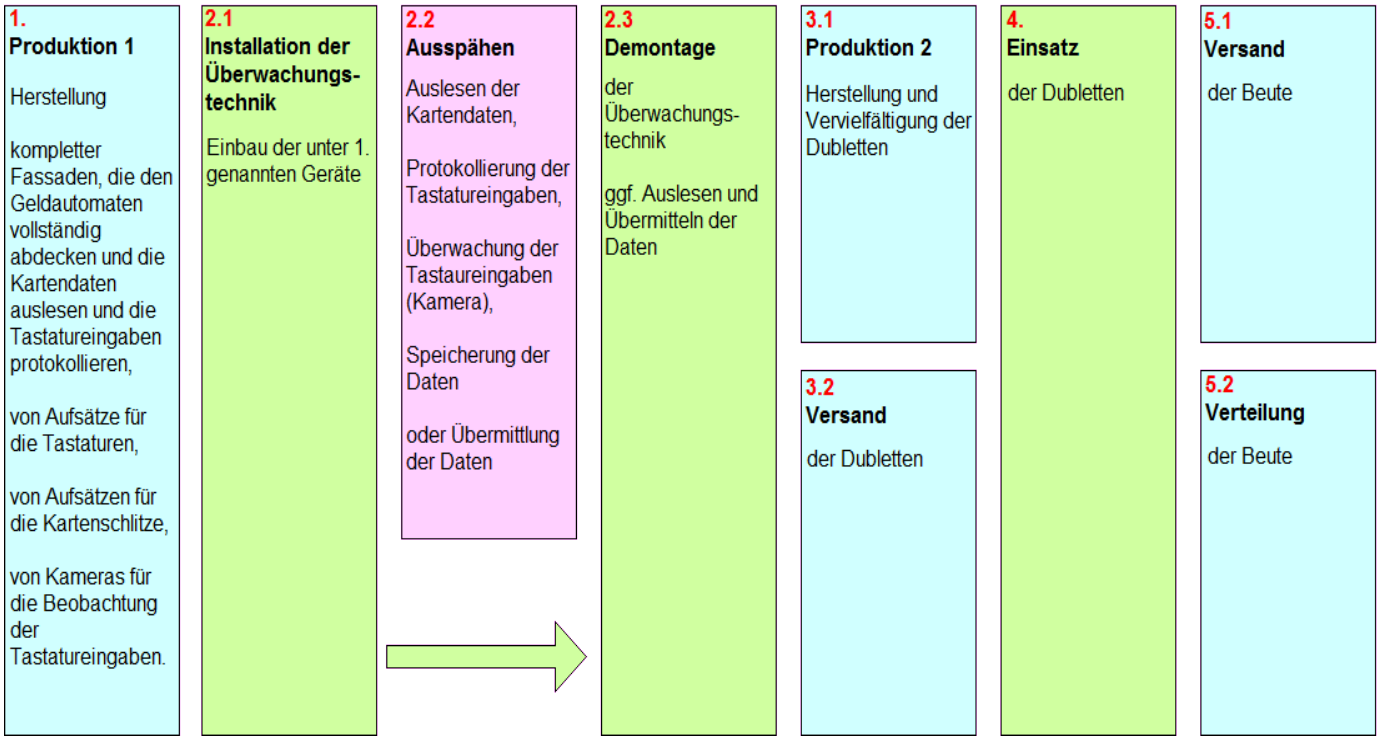
7. arbeitsteilige Handlungen beim Skimming

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. Zur Vorbereitung und während der Installation müssen gelegentlich Anpassungen am Geldautomaten 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 Kar-



tendaten 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.

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

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

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

Die gewandelten Erscheinungsformen beim Ausspähen, allen voran das POS-Skimming, zeigen, dass die hier beschriebene 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 andere Länder und Kontinente verlagern wird.

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

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 [54].

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 eines gewerbsmäßigen Handelns [55]. Einzeltäter, die alle Arbeitsschritte persönlich ausüben, treten allenfalls in Einzelfällen 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 [56]. Die hohen Mindestfreiheitsstrafen, mit denen § 152b Abs. 1, Abs. 2 StGB drohen, sind von Verfassungs wegen nicht zu beanstanden [57].

Die Missbrauchshandlung beim Skimming ist im Grunddelikt der Gebrauch falscher inländischer oder ausländischer Zahlungskarten gemäß §

[54] Siehe Glossar: POS

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

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

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

152a Abs. 1 Nr. 2 StGB [58]. In Tateinheit [59] damit steht der Computerbetrug gemäß § 263a StGB [60], dessen Vollendung mit der Auszahlung am Geldautomaten eintritt [61].

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

Der Computerbetrug im Zusammenhang mit dem Cashing ist ein besonders schwerer Fall, der sich vom Grundtatbestand des § 263a Abs. 1 StGB 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 geschieht in § 263 Abs. 2 StGB, auf den der § 263a Abs. 2 StGB ausdrücklich verweist.

Dagegen tritt die Fälschung beweiserheblicher Daten gemäß § 269 StGB hinter der spezielleren Vorschrift des § 152a Abs. 1 Nr. 1 StGB zurück [62]. Das mit ihr verbundene „Speichern“ realisiert sich nur bei der Fälschung selber und nicht auch beim Missbrauch der gefälschten Zahlungskarten.

> *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

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

---

[58] Strafrahmen: Geldstrafe bis 5 Jahre Freiheitsstrafe.

[59] 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.

[60] 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.

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

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

2.1 Ausspähen von Daten

§ 202a Abs. 1 StGB kommt wegen des Ausspähens der Daten auf den Magnetstreifen der Zahlungskarten der betroffenen Bankkunden nicht in Betracht, weil ihm eine besondere Sicherungsfunktion fehlt. Das führt dazu, dass die gespeicherten Daten in aller Regel mit handelsüblichen Lesegeräten und Komponenten ausgelesen werden können.

In einer früheren Entscheidung ist der BGH noch von einer Tateinheit zwischen dem Nachmachen von Zahlungskarten und dem Ausspähen von Daten ausgegangen [63]. Die Revision führte zur Aufhebung des angefochtenen Urteils, weil das Tatsachengericht keine Strafanträge festgestellt hat [64] (§ 205 StGB [65]). Davon wendet sich der 2. Strafsenat des BGH jetzt in zwei Beschlüssen ab [66], ohne jedoch zunächst die übrigen Senate beteiligt zu haben (§ 132 GVG) [67]. 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* [68].

2.2 Abfangen von Daten

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

Wegen des Ausspähens der PIN greift auch das Hackerstrafrecht nicht, wenn es unmittelbar angewendet wird. Es handelt sich dabei weder um ein Ausspähen von Daten gemäß § 202a Abs. 1 StGB noch um ein Abfangen von Daten gemäß § 202b StGB. 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. Sie ist der Speicherung und Übermittlung vorgelagert.

2.3 PIN-Skimming und Computersabotage

Das Cashing ist mit 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 Sicherungscode (§ 202c Abs. 1 Nr. 1 StGB). Der Umgang mit ihnen mit dem Ziel, sie zum Cashing zu verwenden, steht unter Strafe [69]

---

[63] BGH, Urteil vom 10.05.2005 – 3 StR 425/04, S. 7

[64] Dateninhaber ist danach die kartenausgebende Bank, die somit auch strafantragsberechtigt ist; ebenda.

[65] Wegen des Ausspähens (§ 202a StGB) und Abfangens von Daten (§ 202b StGB) kann die Staatsanwaltschaft jetzt auch das besondere öffentliche Interesse an der Strafverfolgung bejahen (§ 205 Abs. 1 S. 2 StGB).

[66] CF, Ausspähen von Daten und das Skimming, 14.05.2010;
BGH, Beschluss vom 14.01.2010 – 4 StR 93/09, S. 4;
BGH, Beschluss vom 18.03.2010 - 4 StR 555/09.

[67] Kritisch auch: Goya Gräfin **Tyszkiewicz**, Skimming als Ausspähen von Daten gemäß § 202a StGB? HRR 4/2010, 207 (mit Zitat zum Cyberfahnder).

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

[69] CF, Ausspähen der PIN, 06.12.2008

und wird mit einer Höchststrafe von einem Jahr Freiheitsstrafe bedroht.

Die Schutzrichtung dieser Normen beschränkt sich jedoch auf Computerprogramme einerseits und PIN (als Passwörter) andererseits, nicht aber 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.

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* [70]. 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 [71], nicht zuletzt deshalb, weil sie erhebliche Nachteile für die Angeklagten barg [72].

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 [73].

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.

Im Zusammenhang mit dem Skimming spricht der BGH von ***deliktischen Einheiten***, die einerseits zwischen dem Gebrauchen nachgemachter Zahlungskarten und dem damit verbundenen Betrug und andererseits zwischen den Tathandlungen des Nachmachens und des Gebrauchens im Sinne von § 152a Abs. 1 StGB bestehen, soweit sie räumlich-zeitlich eng verbunden und von einem einheitlichen Vorsatz umschlossen sind [74]. Solche deliktischen Einheiten können auch die gleichzeitig Fälschung mehrerer Karten [75] und ihren Gebrauch beim Cashing bilden [76].

Die praktische Konsequenz daraus ist, dass als eine materielle Tat alle Fälschungen, alle Missbräuche von Zahlungskarten und alle unmittelbar

[70] lexexakt.de, natürliche Handlungseinheit

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

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

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

[74] 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

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

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

aufeinander folgenden Ausspähungen von Kontozugangsdaten zusammengefasst werden müssen, soweit sie einen engen Zusammenhang miteinander haben. Das ist zum Beispiel der Fall, wenn Skimmer ihre technischen Geräte installieren, ihre Funktionstüchtigkeit gelegentlich überprüfen und die Geräte schließlich wieder abbauen. Das Ausspähen bildet dabei einen einheitlichen Handlungsrahmen, wobei der Vorsatz der Täter darauf gerichtet ist, möglichst viele Kundendaten bei ihrem Angriff zu erlangen. Auch wenn die Täter über mehrere Tage hinweg dieselbe Bankfiliale ausspähen und die Technik nur während der Bankgeschäftszeiten abbauen und anschließend wieder einrichten [77], kann eine deliktische Einheit bestehen [78].

Dasselbe gilt wegen des Cashings, wenn die Täter mit engem zeitlichen Zusammenhang handeln. Eine Zäsur kann jedoch dann angenommen werden, wenn die Täter ihr Handeln unterbrechen, um sich zum Beispiel mit weiteren Dubletten zu versorgen [79].

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 [80].

3. Fälschungssicherheit

Von der Rechtsprechung des BGH ist anerkannt, dass sich die Fälschung auch alleine auf die Daten auf dem Magnetstreifen beschränken kann [81]. In Bezug auf Zahlungskarten hat der BGH jetzt ausgeführt [82]:

„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 unklar bleibt, ob sie unterschiedliche Sicherheitsmerkmale meinen. Dafür könnte sprechen, dass bei gleichem Wortlaut § 152a StGB das Verfälschen und Nachmachen und § 152b StGB die Garantiefunktion in den Vordergrund stellen.

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

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

[78] 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.

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

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

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

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

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, der zudem einen verschlüsselten Datenverkehr zulassen soll.

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 besondere Sicherheitsmerkmale in Bezug auf die Garantiefunktion sind dieselben, die auch zur allgemeinen Kartensicherheit dienen. Das sind vor allem die Prüfwerte auf dem Magnetstreifen und die Sicherungsmechanismen im EMV-Chip. Von besonderer Bedeutung ist insoweit die PIN, die im Autorisierungsverfahren geprüft wird. Im Zusammenhang mit § 152b Abs. 4 Nr. 2 StGB kommt auch den Verschlüsselungsmechanismen im EMV-Chip eine besondere Bedeutung zu; er ist jedoch noch nicht allgemein verbreitet [83].

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) [84]. Diese Voraussetzungen liegen angesichts der beschriebenen Sicherheitsmerkmale bei den üblichen von Banken herausgegebenen Karten vor [85].

Die Garantiefunktion wird darin gesehen, *dass das die Karte ausgebende Unternehmen ... sich gegenüber Vertragsunternehmen* <verpflichtet>, *deren Forderungen gegen den Kartenbenutzer zu bezahlen* [86]. Diese Definition nimmt § 152b Abs. 4 StGB auf und definiert die Zahlungskarten mit Garantiefunktion als Kredit-, Euroscheck- und sonstige Karten, die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu veranlassen [87]. Die Modalitäten des Forderungsausgleiches zwischen der Bank und ihrem Kunden wirken sich darauf nicht aus.

In Literatur und Rechtsprechung bestehen an der Garantiefunktion keine Zweifel, wenn es sich um Kreditkarten handelt, bei denen der Auszahlungsbetrag gegen ein eigenes Konto des Kartenausstellers erfolgt. Die bekanntesten Kreditkartenverbünde sind die von American Express, Master und Visa [88]. Die Autorisierung im Onlineverfahren und die damit verbundene Genehmigung, ohne die keine Verfügung akzeptiert wird, ist bei Kredit- und Debitkarten jedoch identisch [89], so dass auch die Debitkarten, die an dem Autorisierungsverfahren teilnehmen können, Karten

[83] 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 lässt sich der Chip jedoch abdecken, so dass das Terminal ihn als defekt betrachtet. Darauf beschränkt es sich auf die Prüfung des Magnetstreifens.

[84] CF, Skimming und Fälschungsrecht, 13.04.2009

[85] Siehe oben **Fälschungssicherung**.

[86] 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).

[87] 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

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

[89] 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.

mit Garantiefunktion sind [90]. 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 [91].

Dem Schutz des § 152a StGB unterliegen schließlich auch andere Zahlungskarten von Finanzdienstleistungsinstituten, zum Beispiel Tank- und Telefonkarten, die hier nicht weiter betrachtet werden.

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 [92] 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 Buchung genehmigt. Das EC-Verfahren hat dadurch eine neue Ausprägung erfahren. Während das klassische Modell eine frühe Autorisierung bei der Ausgabe der Schecks durchgeführt hat, erfolgt sie jetzt in Echtzeit durch die Übermittlung des Genehmigungscodes. Nicht anders als im alten Verfahren erfolgt die Buchung der Forderung gegen die Bank zunächst auf einem ihrer Zwischenkonten [93], 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 Ausspähen im Inland bildet für den Mittäter einen eigenen Tatort (§ 9 Abs. 1 StGB) und für den Teilnehmer greifen § 9 Abs. 2 S. 1, S. 2 StGB. Wegen des im Ausland vollendeten Computerbetruges tritt der Taterfolg zunächst bei der kartenausgebenden Bank (Buchung gegen das interne CPD-Konto) und im Zuge des Clearingverfahrens zulasten des einzelnen Bankkunden ein, 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 [94].

Eine Ausnahme bilden die vollständigen Auslandstaten, in denen das Cashing im Ausland mit 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 wegen des Gebrauchs gefälschter Zahlungskarten verfolgt werden, nicht aber wegen Computerbetruges, für den das Weltrechtsprinzip nicht gilt [95].

---

[90] Siehe oben **Autorisierung**.

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

[92] Das Markenzeichen „EC“ wird jetzt als „electronic cash“ fortgeführt.

[93] Siehe oben **Clearing**

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

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

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 [96]. Anlass geben ihm dazu die Fälle, *wenn der Täter unter Vorlage eines gefälschten Personalausweises und Täuschung über seine Zahlungswilligkeit bei einer Bank ein Konto eröffnet und ihm - antragsgemäß - eine EC-Karte (Eurocheque-Karte) und Schecks ausgehändigt werden*. Bereits darin kann ein vollendeter Betrug bestehen, wenn die Bank eine Auszahlung garantiert oder eine Rückbelastung nicht möglich ist.

Der BGH spricht damit das POZ-Verfahren an [97], das Ende 2006 eingestellt wurde [98], 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 [99]. 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 ändert sich die Person des Geschädigten, weil spätestens jetzt die Drittforderung gegen das Konto des Kunden gebucht wird. Cashingangriffe werden jedoch regelmäßig erst danach bekannt, so dass der Geschädigte des Cashings im Endeffekt immer der Kontoinhaber ist.

5.2 schadensgleiche Vermögensgefährdung

In der Zwischenzeit ist die kartenausgebende Bank die Geschädigte nach Maßgabe der schadensgleichen Vermögensgefährdung [100]. Diese Schadenskonstruktion wird von der jüngeren Rechtsprechung des BGH in Frage gestellt, weil sie die konkreten Gefährdungsdelikte des Vermögensstrafrechts den abstrakten Gefährdungsdelikten annähert [101] und deshalb vom 1. [102] und vom 3. Strafsenat des BGH [103] tendenziell abgelehnt wird. An seine Stelle setzen sie einen erweiterten Begriff des Schadens, der an der Tatvollendung nichts ändert und den Bankkunden frühzeitig zum Geschädigten macht.

Abzustellen ist dabei mit dem 3. Strafsenat des BGH auf den Zeitpunkt des Ereignisses, das ist die Genehmigung der Auszahlung, durch die die Belastung des Kundenkontos droht, und spätestens auf die Realisierung des Schadens, die im Zuge des Clearingverfahrens mit der Buchung gegen das Konto des Kunden erfolgt. Spätestens damit ist der wirtschaftlich bewertbare Schaden beim Kunden eingetreten.

Das nachfolgende Verrechnungsverfahren ist eine vertrauensbildende Kompensation, wobei die Schadensabwicklung die Bankkunden faktisch von den Schäden freistellt und den Schaden zwischen den beteiligten Banken und ihren Verbünden verteilt. Mit den ausgespähten Daten und ihrer missbräuchlichen Nutzung werden die betroffenen Kunden in Anwendung des erweiterten Schadensbegriffes unmittelbar angegriffen. Würde das System der Schadensabwicklung

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

[97] Point of Sale ohne Zahlungsgarantie – POZ.

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

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

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

[101] CF, Schaden und schadensgleiche Vermögensgefährdung, 31.01.2010

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

[103] BGH, Urteil vom 13.08.2009 - 3 StR 576/08; BGH, Urteil vom 14.08.2009 - 3 StR 552/08

fehlen, dann blieben ihre Vermögen 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 Gebrauchens zurücktreten (§ 24 Abs. 1 S. 1 StGB). Sobald er jedoch die Taste „Bestätigung“ drückt, ist ihm der Abbruch und der Rücktritt verwehrt. Der Gebrauch einer Zahlungskarte mit Garantiefunktion ist damit vollendet.

Etwas anderes gilt für den gleichzeitig begangenen Computerbetrug [104]. Sein Erfolg tritt erst ein, sobald sich der Täter einen Vermögensvorteil verschafft hat. Das ist der Fall, wenn der Geldautomat das angeforderte Geld zur Entnahme präsentiert und der Täter es nimmt. Zu diesem Zeitpunkt ist eine schadensgleiche Vermögensgefährdung bei der kartenausgebenden Bank sowie – nach dem erweiterten Schadensbegriff – ein Schaden beim Bankkunden eingetreten, weil der Geldautomat den Genehmigungscode empfangen, die Bank eine Buchung des Auszahlungsbetrages und der Gebühr zulasten eines bankinternen Kontos (Conto pro Diverse - CPD) vorgenommen und der Bankkunde eine Buchung in gleicher Höhe gegen sein Kredit- oder laufendes Konto zu erwarten hat.

Im anschließenden Clearingverfahren wird der tatbestandliche Erfolg verschoben. Bankintern wird dabei die Verbindlichkeit aus dem CPD mit der Clearingstelle verrechnet und gleichzeitig gegen das Girokonto des Kunden gebucht. Dort tritt abschließend der Schaden, also der betrügerische Erfolg ein.

Aufgrund der Garantiefunktion, die mit der Mitteilung des Genehmigungscodes verbunden ist, ist der Schadenserfolg jedoch bereits eingetreten, sobald der Genehmigungscode übermittelt wurde. Die Vollendung des Computerbetruges tritt somit ein, sobald der Täter das Geld aus dem Geldautomaten nimmt.

6. Beginn des Versuchsstadiums

In einer wegen ihres Sachverhalts nicht einschlägigen Entscheidung hat der BGH im Januar 2010 den Beginn des Versuchs beim Fälschens von Zahlungskarten streng ausgelegt [105]. Der Versuch beginnt somit erst unmittelbar beim Fälschungsvorgang selber:

„Danach ist ein Versuch des (gewerbs- und bandenmäßigen) Nachmachens von Zahlungskarten mit Garantiefunktion (§§ 152b Abs. 1 und 2, 152a Abs. 1 Nr. 1, 22, 23 Abs. 1 StGB) erst dann gegeben, wenn der Täter vorsätzlich und in der tatbestandsmäßigen Absicht mit der Fälschungshandlung selbst – also dem Herstellen der falschen Karte … - beginnt. 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“.

Der BGH betrachtet dabei einen nicht als Mittäter oder Bandenmitglied handelnden Täter. Hinzu kommt, dass die in Frage stehenden Karten noch keine Individualmerkmale zeigten. Sie verfügten über Aufdrucke und Logos der ausstellenden Bank, aber über keine Kundennamen, keine Konto- oder Kartennummern und keine Daten auf den Magnetstreifen [106]. In dieser Form sind die Rohlinge tatsächlich den Tatgegenständen vergleichbar, die klassisch von § 149 StGB angesprochen werden (Druckstöcke, Papiere).

Eine klare Aussage zum Skimming gibt es jedoch noch nicht.

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

[105] BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn 9.

[106] Der BGH verweist u.a. auf OLG Thüringen (Jena), wistra 2009, 204; der Lebenssachverhalt ist in beiden Fällen derselbe.

6.1 Versuch der Kartenfälschung

§ 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!“*** [107]

„Dies ist insbesondere der Fall, wenn der Täter subjektiv die Schwelle zum "jetzt geht es los" überschreitet, es eines weiteren Willensimpulses nicht mehr bedarf und er objektiv zur tatbestandsmäßigen Angriffshandlung ansetzt, so dass sein Tun ohne Zwischenakte in die Erfüllung des Tatbestandes übergeht.“

Muss der Täter erst noch mehrere Willensentscheidungen treffen oder wird der Tatbestand erst nach mehreren zeitlich und räumlich getrennten Handlungsschritten erfüllt, dann bewegt sich der Täter noch im Vorbereitungs- und noch nicht im Versuchsstadium.

Das arbeitsteilige Skimming könnte nach einer besonderen Auslegung verlangen. Seine Täter wollen keine Grundstoffe für beliebige Taten beschaffen, sondern tragen unmittelbar zur Individualisierung der geplanten Fälschungen bei, wobei die ausgespähten Kartendaten zum Nachmachen von Zahlungskarten verwendet werden sollen. Mit dem BGH könnte deshalb eine weniger strenge Auslegung zum Tragen kommen [108]:

„Auch eine frühere, vorgelagerte Handlung kann bereits die Strafbarkeit wegen Versuchs begründen. Dies gilt aber nur dann, wenn sie nach der Vorstellung des Täters bei ungestörtem Fortgang ohne Zwischenakte in die Tatbestandsverwirklichung unmittelbar einmündet oder mit ihr in unmittelbarem räumlichen und zeitlichen Zusammenhang steht. Diese abstrakten Maßstäbe bedürfen jedoch stets der wertenden Konkretisierung unter Beachtung der Umstände des Einzelfalles. Hierbei können etwa die Dichte des Tatplans oder der Grad der Rechtsgutsgefährdung, der aus Sicht des Täters durch die zu beurteilende Handlung bewirkt wird, für die Abgrenzung zwischen Vorbereitungs- und Versuchsstadium Bedeutung gewinnen.“

Für die weniger strenge Auslegung spricht, dass der Gesetzgeber das Herstellen, Feilbieten und Sich-Verschaffen von Skimmern zur Straftat im Vorbereitungsstadium erklärt hat [109]. In logischer Konsequenz könnte ihr Einsatz mit dem Ziel der Tatvollendung den Beginn des Versuchsstadiums einleiten.

Angesichts der schweren Strafdrohung von § 152b StGB ist von der Rechtsprechung zu erwarten, dass sie auch auf das Skimming die strenge Auslegung anwenden wird. Das legen bereits die Arbeitsschritte nahe, die dem Ausspähen der Kartendaten folgen: Synchronisation der aus zwei Quellen stammenden Kartendaten und PIN sowie die Übermittlung der Dumps an die Hinterleute oder Mittäter im Ausland.

Soweit ich bisher vertreten habe, dass der Versuch im Hinblick auf den Einsatz des arbeitsteilig handelnden Skimmers in dem Moment beginnt, wenn er das präparierte Kartenlesegerät nimmt (noch Vorbereitungsstadium) und beginnt, es zu installieren (schon Versuchsstadium), ist das eine mögliche, aber weniger wahrscheinliche Auslegung. Die weiteren Ausführungen setzen deshalb die strenge Auslegung des Versuchsbeginns zugrunde.

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

[108] BGH, Urteil vom 09.03.2006 – 3 StR 28/06, Rn 4.

[109] § 152a Abs. 5 und § 152b Abs. 5 StGB verweisen beide auf den Gefährdungstatbestand des .§ 149 StGB. Wegen der weiteren Einzelheiten siehe unten. Die Tathandlungen fasse ich nach dem Vorbild des Waffenrechts mit dem Begriff des „Umgangs“ zusammen.

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 verbaut werden, ohne deren Elektronik zu verändern, greift die Rechtsprechung des BVerfG zum Hackerstrafrecht. Es handelt sich bei ihnen um strafneutrale Dual Use-Produkte [110].

Zwischen dem Ausspähen der PIN und ihren missbräuchlichen Einsätzen liegen mehrere Arbeitsschritte. Zunächst müssen die ausgespähten Daten synchronisiert und Zahlungskarten gefälscht werden. Das führt dazu, dass der Versuch des Computerbetruges mit dem Gebrauch gefälschter Zahlungskarten mit Garantiefunktion zusammen fällt. Das Ausspähen der PIN, ihre Synchronisation mit den ausgespähten Kartendaten und ihr Transport zwischen den beteiligten Mittätern ist noch im Vorbereitungsstadium angesiedelt.

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

6.3 Rücktritt vom Versuch

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

Sobald das Versuchsstadium erreicht ist, kann der vollendend handelnde Tatgenosse nur dann strafbefreiend vom Versuch zurücktreten (§ 24 StGB), wenn er Anstrengungen unternimmt, die Tatvollendung wirklich zu verhindern. Deshalb neigt der Generalbundesanwalt zu einer zurückhaltenden Anwendung der Rücktrittsregeln und lässt vorübergehende technische Störungen, die behoben werden können [111], und Abbauten 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 [112]. Im Zusammenhang mit dem Skimming hat das Gericht bei mehrtägigem Ausspähen je nach den Umständen Tatmehrheit (§ 53 StGB) und Tateinheit (§ 52 StGB) angenommen [113].

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.

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

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

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

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 [114]. 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 [115]. 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) [116]. Diese drei unterschiedlichen Gefährdungstatbestände führen dazu, dass bereits der Umgang – hier in den Formen des Sich-Verschaffens und Verwahrens – für die meisten zum Skimming eingesetzten Ausspähgeräte mit geringen Strafen bedroht ist.

Eine noch offene Frage ist die, ob die von § 263a Abs. 3 StGB angesprochenen Programme nur beim Computerbetrug selber eingesetzt werden dürfen oder auch solche umfassen, die zum Ausspähen von PIN dienen. Die ältere Rechtsprechung zu den Fälschungswerkzeugen [117] 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. Ich schließe daraus, dass auch die Computerprogramme umfasst sind, die für das Ausspähen erstellt werden.

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

Obwohl die Verabredung zu einem Verbrechen auch im Vorbereitungsstadium angesiedelt ist, gehe ich auf sie erst im Anschluss an die Ausführungen zur Mittäterschaft und zur Bande ein, weil auch sie meistens mehrere Beteiligte erfordert.

7.1 Kartenlesegeräte

Noch 2003 hat der BGH den Umgang mit Skimmern, also mit Kartenlesegeräten, als nicht strafbar im Sinne von § 149 StGB angesehen [118]. 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. Es ist vergleichbar 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 in zwei mir bekannten Fällen gefolgert, dass jetzt jedenfalls auch der Umgang mit Skimmern im Vorbereitungsstadium strafbewehrt ist [119]. In beiden Fällen hat der BGH

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

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

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

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

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

[119] 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. Siehe auch Fischer, § 149

die Revisionen der verurteilten Skimmer ohne Begründung verworfen.

Dies ist jedenfalls für die Skimmer der Fall, die zum Zweck des Skimmings mit einem digitalen Speicher oder einer Funkeinrichtung [120] ausgestattet, also umgebaut wurden.

Als Vorrichtungen im Sinne von § 149 StGB betrachte ich die Stromversorgung, das Lesemodul, den Speicher und die kleine Hardware für die kleine Computerlogik, die die Komponenten verbindet. Das „Programm“ sind die verbindenden Computerroutinen.

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

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

7.2 Kameras

Eine übliche Methode zum Ausspähen der PIN ist die Installation einer Kamera, die auf das Tastaturfeld ausgerichtet wird. Die PIN wird jedoch nicht für das Nachmachen der eingesetzten Zahlungskarten benötigt, sondern nur zu ihrem Gebrauch und vor allem zum geplanten Computerbetrug. Deshalb kann ein strafbarer Umgang mit 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. Das zielt nur auf die Software, nicht aber auch auf die Hardware, und verlangt nach einer differenzierten Betrachtung der bekannten Kamerainstallationen zum Skimming.

Eine ältere Form besteht in dem Einbau von elektronischen Bauteilen in einen Halter für Werbematerial, der an die Innenwand des Geldautomaten geklebt wird. Hierbei werden Kamera, Stromversorgung und Speicher verwendet, die mit Hilfe eines Schaltung zusammengeführt werden. Diese Schaltung kann als Programm im Sinne von § 263a Abs. 3 StGB angesehen werden. Dasselbe gilt für den jüngst bekannt gewordenen Einbau in einen vorgetäuschten Sichtschutz für die Tastatur [121].

In Rauchmeldern und Kameraleisten werden in aller Regel handelsübliche Digitalkameras oder Mobiltelefone mit Kamerafunktion eingebaut. Zum Betrieb werden ihre internen Speicher und Steuerungen verwendet, so dass sie als Dual Use-Komponenten zu betrachten und der Umgang mit ihnen im Anschluss an die Rechtsprechung des BVerfG als straflos anzusehen sind [122]. Besondere Computerprogramme kommen dabei nicht zum Einsatz.

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 des Gesetz ebenfalls die Mehrzahl. Dem entgegen hat

StGB Rn 3.

[120] Die Funktechnik wird selten beobachtet, weil sie zu viel Strom verbraucht und deshalb die Ausspähzeit verringert.

[121] CF, Sichtblende mit Kamera, 26.06.2010

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

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

der BGH bereits die Fälschung ***einer*** EC-Karte genügen lassen [123], weil er die Gefährlichkeit bereits einer einzelnen Tathandlung als ausreichend angesehen hat. Das lässt sich angesichts der geringen Strafdrohung von einem Jahr Freiheitsstrafe im Höchstmaß nicht auf das Ausspähen von PIN übertragen.

7.3 Tastaturaufsätze

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

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

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

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

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

8. Mittäter und Bande

Arbeitsteilig handelnde Täter sind Mittäter (§ 25 Abs. 2 StGB), wenn sie in 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 [124]. Er hat keine Tatherrschaft und übt in aller Regel eine *"ganz untergeordnete Tätigkeit"* aus [125].

Der Beurteilungsmaßstab ist stark subjektiv geprägt: *„Mittäterschaft liegt ... dann vor, wenn ein Tatbeteiligter nicht bloß fremdes Tun fördern will, sondern seinen Beitrag als Teil der Tätigkeit des anderen und umgekehrt dessen Tun als Ergänzung seines eigenen Tatanteils will. Ob ein Beteiligter dieses enge Verhältnis zur Tat hat, ist nach den gesamten von seiner Vorstellung umfassten Umständen in wertender Betrachtung zu*

[124] 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.

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

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“ [126].

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

8.1 arbeitsteilige Tätergruppen

2001 hat der große Senat des BGH kein neues Organisationsstrafrecht geschaffen [127], wohl aber am Beispiel des Bandendiebstahls (§ 244 Abs. 1 Nr. 2 StGB) die vom gemeinsamen Tatplan geprägte Zusammenarbeit von Mittätern auf das mittelbare Zusammenwirken erweitert [128]. Dabei ist nicht mehr ausschlaggebend die Zusammenarbeit am Tatort und im Zusammenhang mit der Vollendung oder Beendigung der Tat, sondern das arbeitsteilige Zusammenwirken im 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".*

> *Eine Bande ist danach gekennzeichnet durch den Zusammenschluss von mindestens drei Personen, die sich mit dem Willen verbunden haben, künftig für eine gewisse Dauer mehrere selbstständige, im Einzelnen noch ungewisse Straftaten zu begehen; ein gefestigter Bandenwille und ein Tätigwerden in einem übergeordneten Bandeninteresse sind demgegenüber nicht mehr erforderlich (...). Nach deutschem Recht ist indes allein die Mitgliedschaft in einer Bande nicht strafbar; vielmehr führt das Handeln als Bandenmitglied (lediglich) dazu, dass der Täter nicht nur einen strafrechtlichen Grundtatbestand erfüllt, sondern ein Qualifikationsmerkmal. … Die Mitgliedschaft in einer Bande ist deshalb kein strafbegründendes, sondern ein strafschärfendes Merkmal.*
>
> BGH, Urteil vom 03.12.2009 - 3 StR 277/09, S.18

Der Mittäter 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 [129], ihr krimineller Erfolg vorhersehbar ist und sich die Beteiligten im Tatplan halten [130]. Der BGH begründet das damit, dass die akzessorische 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 [131].

Diese Betrachtung hat der BGH auf die Beschaffung eines Firmenmantels, unter dessen Struktur die Komplizen selbständig betrügerische Geschäfte begehen [132], und sogar auf spontan wirkende Zusammenschlüsse übertragen, wenn sie

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

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

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

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

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

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

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

gleichartige Straftaten einer umgrenzbaren Tätergruppe betreffen [133].

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 [134]. 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 [135]. Er haftet zunächst nur für die konkreten Handlungen, die er ausgeübt hat, wenn sie selbständig strafbar sind. Deshalb verlangt der BGH wegen der Tatbeiträge arbeitsteilig handelnder Täter und ihrer rechtlichen Bewertung eine genaue Betrachtung des einzelnen Täters, eine genaue Bezeichnung seiner Handlungen und Feststellungen dazu, wie sie sich in den Gesamtplan einfügen [136]. 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.“* [137]

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 [138], ein Qualifizierungsmerkmal ist, das zu einer schärferen Strafdrohung führt [139].

> *Bedingt vorsätzliches Handeln setzt voraus, dass der Täter den Eintritt des tatbestandlichen Erfolges als möglich und nicht ganz fern liegend erkennt, ferner, dass er ihn billigt oder sich um des erstrebten Zieles willen mit der Tatbestandsverwirklichung zumindest abfindet. Da die Schuldformen des bedingten Vorsatzes und der bewussten Fahrlässigkeit im Grenzbereich eng beieinander liegen, müssen bei der Annahme bedingten Vorsatzes beide Elemente der inneren Tatseite, also sowohl das Wissens- als auch das Willenselement, umfassend geprüft und gegebenenfalls durch tatsächliche Feststellungen belegt werden.*
>
> BGH, Urteil vom 28.01.2010 - 3 StR 533/09, Rn 5.

Die 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 Verbrechensabrede (§ 30 Abs. 1 StGB) oder als mittelbare Täter (§ 25 Abs. 1 StGB) *„in Fällen mafiaähnlich organisierten Verbrechens in Betracht kommen, bei denen der räumliche, zeitliche und hierarchische Abstand zwischen der die Befehle verantwortenden Organisationsspitze und den unmittelbar Handelnden gegen arbeitsteilige Mittäterschaft spricht“* [140].

---

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

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

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

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

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

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

[139] 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.

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

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 [141]. Allein die Tatsache, dass dabei Karten verwendet werden, deren Originale eine Garantiefunktion haben, führt zu einer Strafdrohung von 1 bis 10 Jahre Freiheitsstrafe.

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

Das Cashing unterliegt der deutschen Gerichtsbarkeit unabhängig davon, wo es begangen wird und woher die Kartendaten stammen, die dabei missbraucht werden [142]. 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 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 [143]), er *„sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen“* [144] (Gewerbsmäßigkeit) und sich einem Bandenwillen anschließen 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 [145] – das Vorliegen von tatsächlichen Anhaltspunkten, um zum Beispiel dem Täter einen strafbefreienden Rücktritt vom Versuch zuzubilligen [146], und wendet sich damit gegen eine unkritische Auseinandersetzung mit den von Verteidigungsstrategien gefärbten Einlassungen [147].

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 gänzlich 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 [148]. Sie lässt in der

---

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

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

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

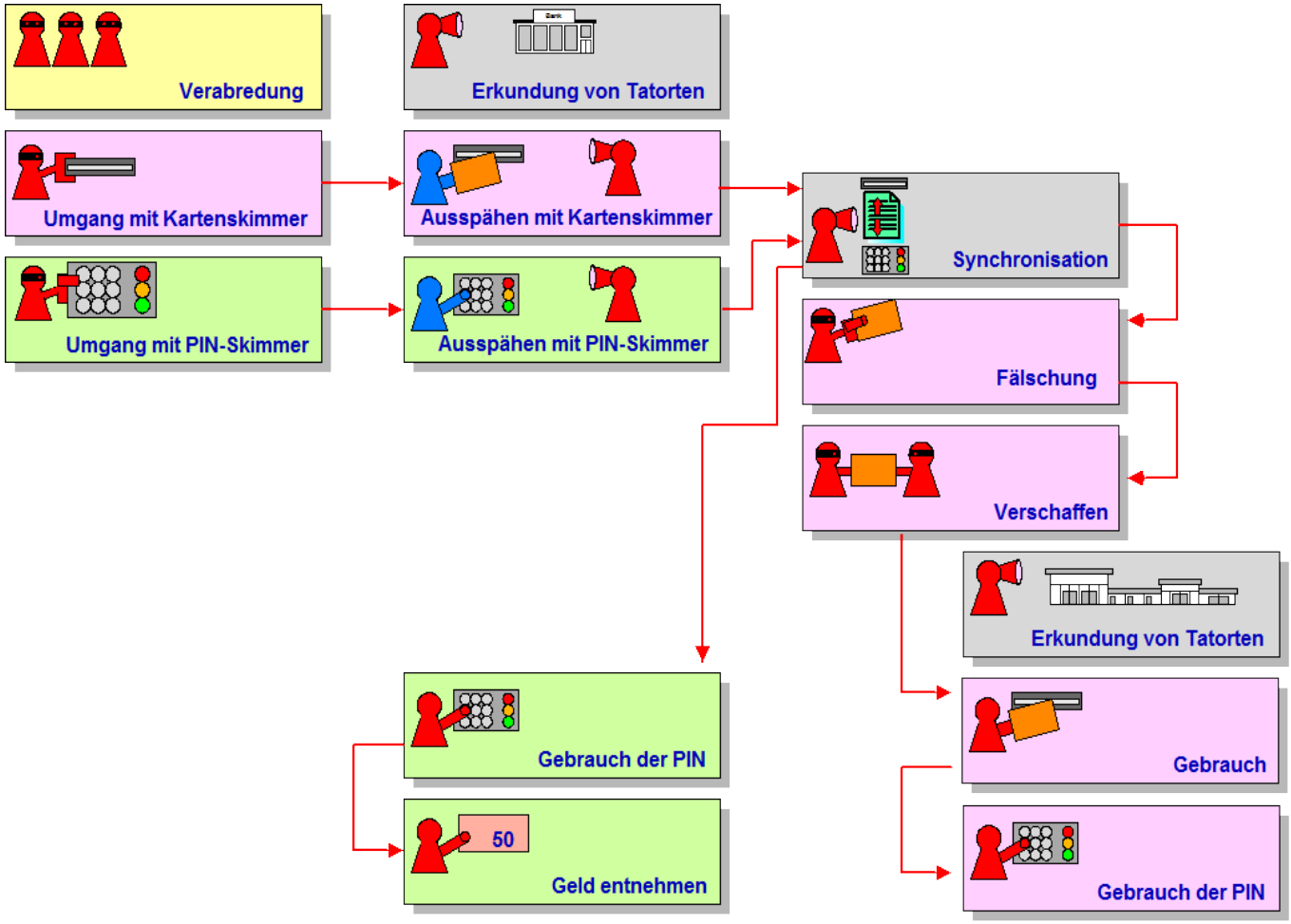
[144] BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5.

[145] *„Im Zweifel für den Angeklagten“*

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

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

[148] 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



Parallelwertung der Skimmer erwarten, dass sie jedenfalls mit bedingtem Vorsatz billigen [149].

In den Fällen, in denen es nicht zur Vollendung durch Mittäter kommt, stellt sich mit Nachdruck die Frage nach dem Beginn des Versuchsstadiums [150] im Zusammenhang mit dem Fälschen von Zahlungskarten. Bei strenger Betrachtung beginnt es erst beim unmittelbaren Ansetzen zum Fälschen selber [151], wobei der BGH noch keine Stellung zum arbeitsteiligen Skimming genommen hat und in anderen Fällen auch eine *„frühere, vorgelagerte Handlung“* <genügen ließ,> *„wenn sie nach der Vorstellung des Täters bei ungestörtem Fortgang ohne Zwischenakte in die Tatbestandsverwirklichung unmittelbar einmündet oder mit ihr in unmittelbarem räumlichen und zeitlichen Zusammenhang steht“* [152]. Auch insoweit ist eine Gesamtwürdigung der Tatumstände geboten und eine versuchsweise Haftung des Skimmers am Cashing nicht ausgeschlossen.

Anderenfalls verbleibt es nur bei einer Strafbarkeit wegen der aufgeführten Vorbereitungshandlungen [153], die in Tateinheit mit einer Verbrechensabrede stehen können [154].

[149] Siehe Kasten auf der Vorseite.

[150] Siehe oben **6. Beginn des Versuchsstadiums**.

[151] BGH, Urteil vom 13.01.2010 – 2 StR 439/09, Rn 9.

[152] BGH, Urteil vom 09.03.2006 – 3 StR 28/06, Rn 4.

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

[154] GBA, Stellungnahme vom 09.12.2009 zu 3 StR 539/09.

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.

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 [155], 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 [156]. Zu betrachten ist deshalb der Tatbeitrag, den der einzelne an der Abrede Beteiligte leisten soll und will (siehe unten). Nicht der besonders gefährliche Täter als solcher soll der Strafdrohung aus dem § 30 StGB unterliegen, sondern besonders gefährliche Straftaten sollen durch ihre ins Vorbereitungsstadium vorverlagerte Strafbarkeit verhindert werden.

Für den Rücktritt vom Versuch der Beteiligung gelten vereinfachte Regeln (§ 31 StGB), die jedoch nicht bei jedem Scheitern zur Straffreiheit führen [157].

10. Beteiligungsmodell beim arbeitsteiligen Skimming

Der typische Tatplan beim arbeitsteiligen Skimming [158] 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 Zahlungsgarantie dar, also ebenfalls als Verbrechen, und in Tateinheit damit als Computerbetrug gemäß § 263a StGB. Der Computerbetrug ist dann ein Verbrechen, wenn er gewerbs- und bandenmäßig betrieben wird (§§ 263a Abs. 2 i.V.m. 263 Abs. 5 StGB).

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

---

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

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

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

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

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

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

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

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

10.1 Abrede einschließlich eigenhändiges Cashing

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

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

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

10.2 Abrede einschließlich Cashing durch Mittäter

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

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

10.3 Abrede mit Absatzabsicht

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

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

Cashing

Anhang: Grafiken zum Beteiligungsmodell

Grafiken erklären häufig mehr als viele Worte. Ich habe deshalb mit den vier Darstellungen in diesem Anhang habe ich die wesentlichen Aussagen zur strafrechtlichen Beurteilung des Skimmings und aus dem Beteiligungsmodell zusammengefasst.

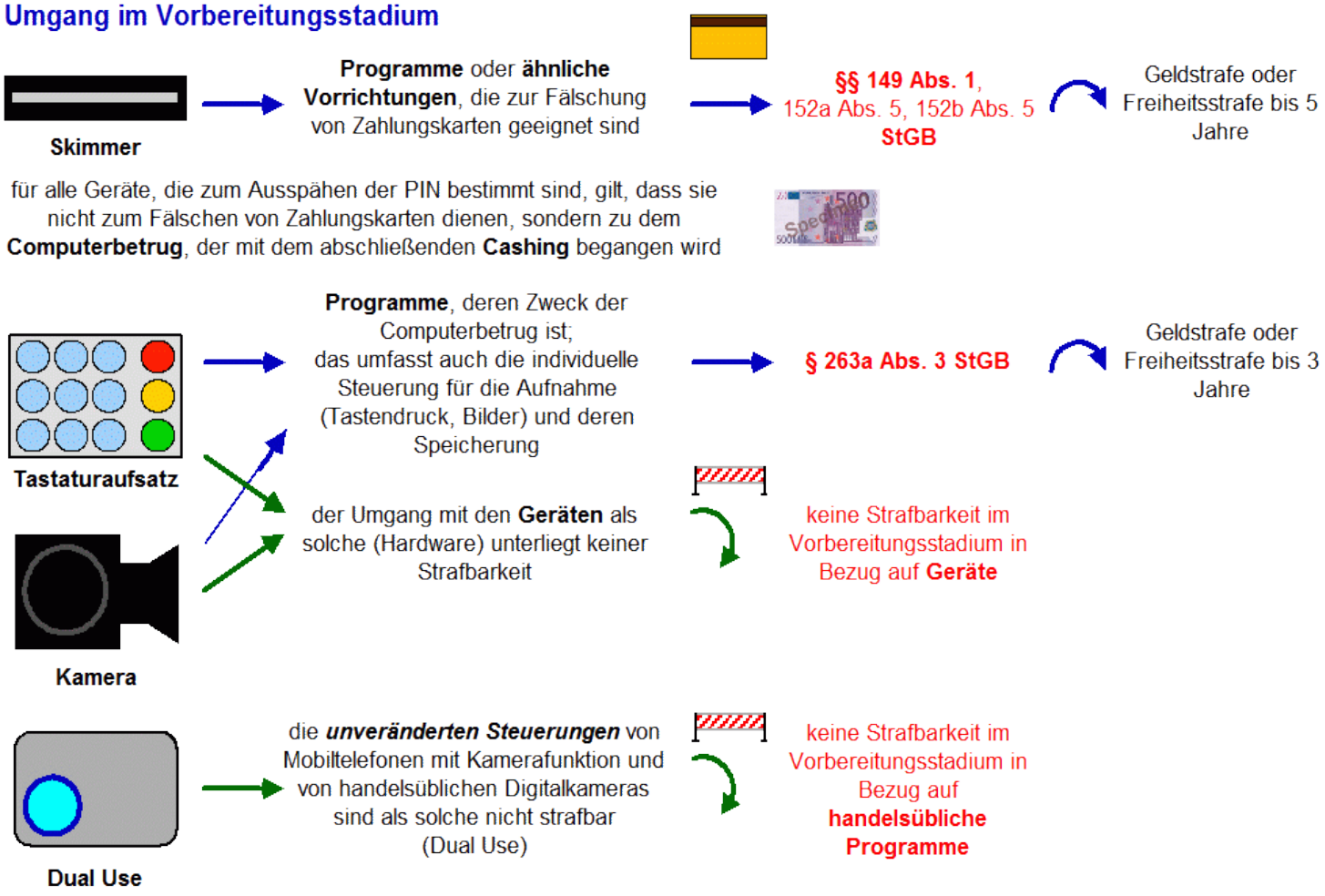
Grafik 1: Cashing

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

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

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

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



Grafik 2:

Umgang mit Skimminggeräten im Vorbereitungsstadium

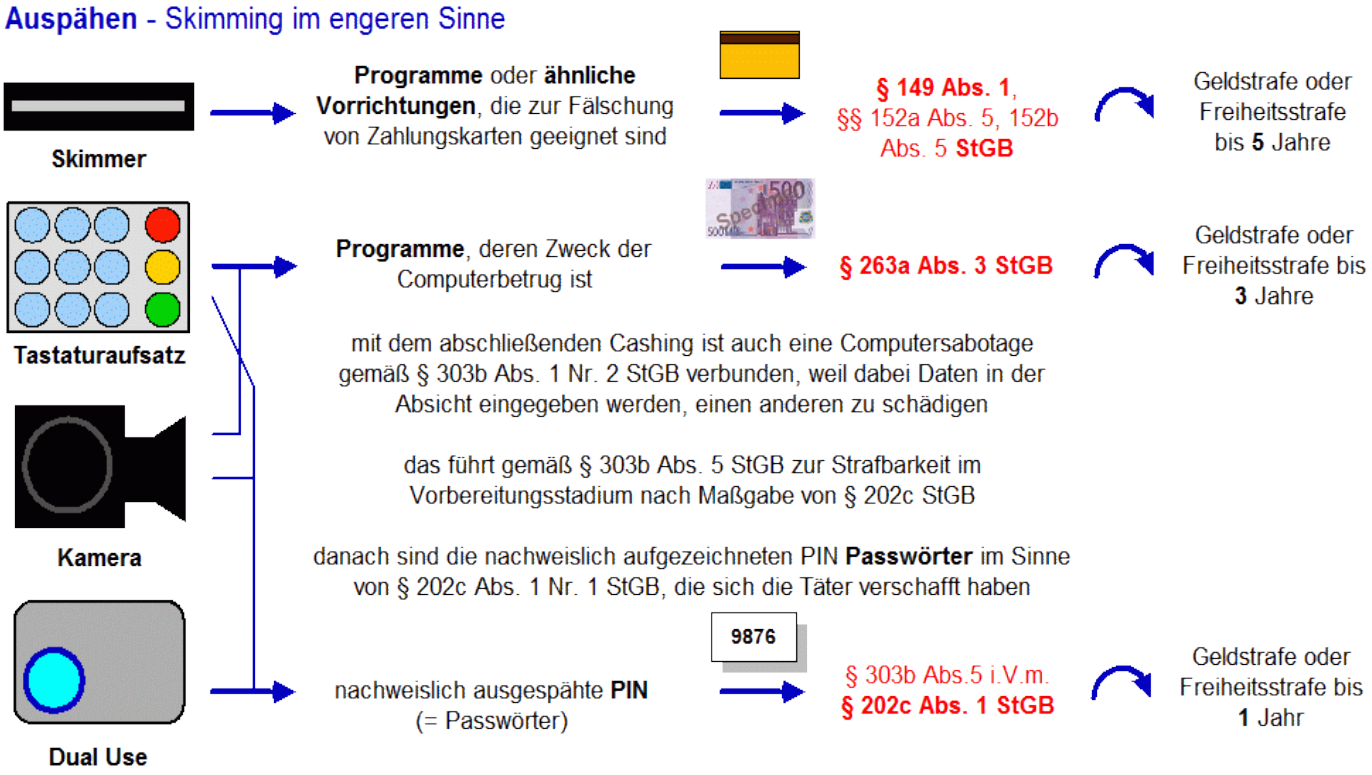
Im Zusammenhang mit dem Skimming sind bereits im Vorbereitungsstadium verschiedene Handlungen strafbar (Gefährdungsdelikte)

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

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

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

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



Grafik3:

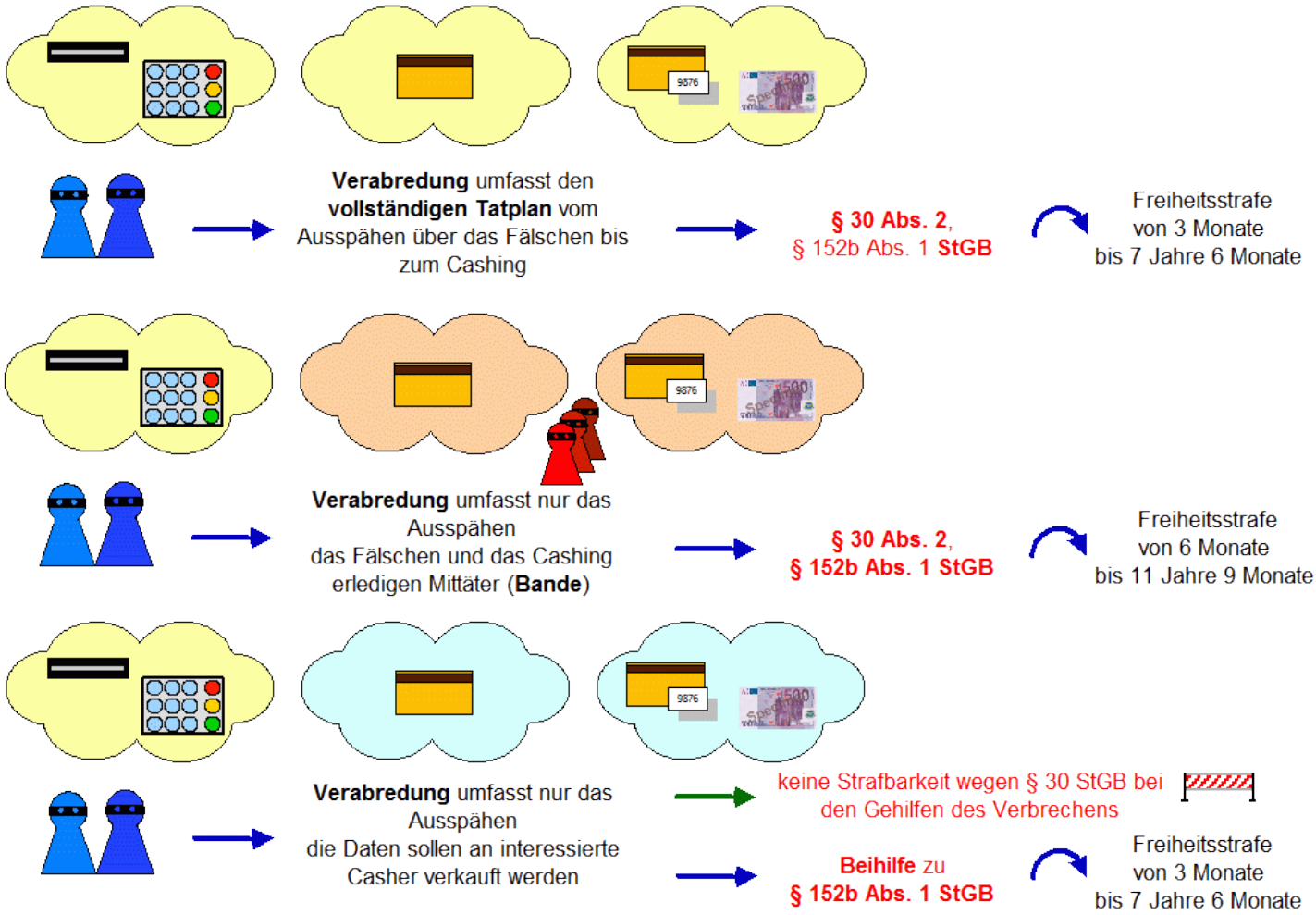
Einsatz von Skimminggeräten

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

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

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

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



Grafik 4:

Verabredung zu einem Verbrechen

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

Die vorgestellten Varianten orientieren sich an dem oben ausgeführten Beteiligungsmodell.

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

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

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

11. Nichtanzeige des geplanten Skimmings

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

Noch schärfer kann das Strafrecht nicht reagieren.

12. Prüfungsschema

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

12.1 vollendetes Cashing

① ***Kartenqualität***

①① *Zahlungskarte*

①② *Kredit- oder Finanzdienstleistungsinstitut*

①③ *Sicherheitsmerkmale*

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

①④ *Garantiefunktion*

①⑤ *Sicherheitsmerkmale*

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

② ***Fälschung***

②① *Verfälschen*
Manipulation des Magnetstreifens

②② *Nachmachen*
Herstellung von WhiteCards

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

③ ***Gewahrsam***

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

④ ***Gebrauch***

④① *Einstecken der Karte* in das Lesegerät.

④② *Eingabe der PIN*

④③ *„Bestätigung“*

④④ *Entnahme des Geldes*

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

⑤ ***Qualifizierung***

⑤① *gewerbsmäßiges Handeln*

⑤② *arbeitsteiliges Handeln*

⑤②① *Zusammenarbeit beim Cashing*

⑤②② *Zusammenarbeit mit Hinterleuten*

⑤②③ *Zusammenarbeit mit Skimmern*

⑤③ *bandenmäßiges Handeln*

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

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

12.2 Ausspähen von Karten und PIN bei vollendetem Cashing

⑥ *Tatplan der Skimmer*

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

12.3 Ausspähen von Karten und PIN ohne Cashing

❶ *Mittäterschaft*

Im mittäterschaftlichem Verbund stellt sich besonders die Frage nach dem Beginn des Versuchs. Wenn das Ausspähen der Kartendaten bereits dem Versuchsstadium zuzurechnen ist, führt das Ausspähen zur Strafbarkeit der Skimmer wegen versuchten Herstellens und Gebrauchens von Zahlungskarten mit Garantiefunktion, sobald sie ihre Tatherrschaft im Hinblick auf die ausgespähten Daten aufgeben. Scheitert die weitere Tatausführung aus technischen Gründen oder weil Dritte die Tat vereiteln, bleiben sie strafbar wegen eines fehlgeschlagenen Versuchs.

Bei strenger Betrachtung des Versuchsbeginns ergeben sich noch andere Folgen:

❷ *Verbrechensabrede*

Die Strafbarkeit der Verbrechensabrede zwischen Skimmer und Casher beginnt bereits im Vorbereitungsstadium unmittelbar mit der Verabredung und dauert bis zur geplanten Vollendung durch die Casher an. War die Abrede auf Handlungen nach ⑤① oder ⑤③ ausgerichtet, so ergibt sich die Strafbarkeit der Skimmer in Bezug auf eine Tat nach § 152b Abs. 2 StGB, wobei der Strafrahmen gemäß §§ 30 Abs. 1 S. 2, 49 StGB gemildert werden muss. Er umfasst dann 6 Monate bis 11 Jahre 9 Monate Freiheitsstrafe. Der Umgang mit Skimmern (Kartenlesegeräte) führt dabei zu einer tateinheitlichen Handlung, wobei alle einzelnen Täterhandlungen in 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 [159].

❸ *selbständiges Skimming*

Fehlt es sowohl an dem Cashing, am strafbaren Versuch wie auch an der Verbrechensabrede, so greifen ausschließlich die strafbaren Vorbereitungshandlungen [160].

Der Umgang mit Skimmern, also den präparierten Kartenlesegeräten [161], 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-

---

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

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

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

nem Strafrahmen von Geldstrafe bis 3 Jahre Freiheitsstrafe aus.

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

Werden zum Beispiel Kameraleisten oder präparierte Rauchmelder eingesetzt, in denen handelsübliche Dual Use-Komponenten ohne verbindendes Programm verbaut werden, dann entfällt eine Strafbarkeit gemäß § 263a Abs. 3 StGB. Sobald jedoch mindestens zwei PIN ausgespäht wurden, greift der Gefährdungstatbestand im Vorfeld der Computersabotage (§§ 303b Abs. 5, 202c StGB) und droht mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr [162].

13. Fazit

Gegen Fälscher hat der Gesetzgeber mit § 152b Abs. 1 StGB und gegen Fälscherbanden mit § 152b Abs. 2 StGB schweres Geschütz 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 § 149 StGB gefunden. Ihre Herstellung und der Umgang mit ihnen ist mit Strafe bedroht.

In das Leitbild vom Fälscher hat der Gesetzgeber die modernen Zahlungsmittel und namentlich die Zahlungskarten nur mühsam eingefügt und dabei die Erscheinungsform des Skimmings nur unvollständig erfasst. Präparierte Kartenlesegeräte können gerade noch als Programme und ähnliche Vorrichtungen angesehen werden und die gleichermaßen gefährlichen PIN-Skimmer überhaupt nicht. Die Verweise auf strafbare Vorbereitungshandlungen aus dem Computerbetrug und der -sabotage beschränken sich auf Teilaspekte wie Programme und Zugangscodes und leiden unter gesetzessprachlichen Mängeln, was die Verwendung der Mehrzahl in § 202c StGB und der unerwartete Verweis aus § 303b StGB auf diese Vorschrift belegen. Die Klarheit, mit der das Gesetz die Tathandlungen beim Computerbetrug benennt (§ 263a StGB), fehlt im übrigen vollständig. Das führt zum Beispiel dazu, dass die Fälschung beweiserheblicher Daten (§ 269 StGB) als Anwendungsfall des Identitätsdiebstahls [163] 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

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

[163] 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 [164], dass die angedrohte Höchststrafe mehr als 5 Jahre Freiheitsstrafe beträgt. Zuletzt im Zusammenhang mit den Verkehrsdaten hat das BVerfG ausgeführt [165]:

„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 [166]. Die bisher bekannten Erscheinungsformen im Zusammenhang mit Tätergruppen ausländischer Herkunft lassen zudem geschäftsähnliche Strukturen erkennen [167].

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 [168].

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

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

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

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

[168] 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 [169], lassen sich bereits einige Erfahrungswerte formulieren, die für die Bewertung in anderen und neuen Verfahren herangezogen werden können [170].

1. Programm

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

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

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

2. Garantiefunktion

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

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

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

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

Es wurde eine gefälschte Zahlungskarte mit Garantiefunktion genutzt.

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

3. Ausspähen

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

3.1 Vorerkundung

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

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

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

---

[169] 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

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

3.2 Spezialisten

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

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

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

Daraus folgt:

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

Und:

Skimmer arbeiten arbeitsteilig.

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

3.3 Einsatz

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

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

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

Daraus folgt auch:

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

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

Dieses Vorgehen ist durch Kameraaufnahmen belegt.

4. Abstimmung und Bericht

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

Überraschend viele Belege gibt es dafür, dass die Skimming-Täter, Skimmer wie auch Cacher, 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 liebreizende Gespräche mit ihren Freundinnen führen. Sie dürften sich eher mit ihren Mittätern und Hinterleuten abstimmen.

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

Rechtsprechungsübersicht

Die in diesem Arbeitspapier angesprochene Rechtsprechung im Überblick:

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

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, 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

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

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

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, 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
BGH, Urteil vom 14.08.2009 - 3 StR 552/08

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

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

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

Autorisierung: Automatisches Genehmigungsverfahren im bargeldlosen, kartengestützten Zahlungsverkehr.

Carder: Auf den Missbrauch von Karten spezialisierter Täter.

Casher: Am Cashing beteiligter Täter.

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

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

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

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

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

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

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

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

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

Garantiefunktion: Auszahlungsgarantie des Kartenausstellers für Debitkarten 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.

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 präparier-

tes Kartenlesegerät, das die Magnetstreifen von Karten ausliest.

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

Skimming: a) 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.