

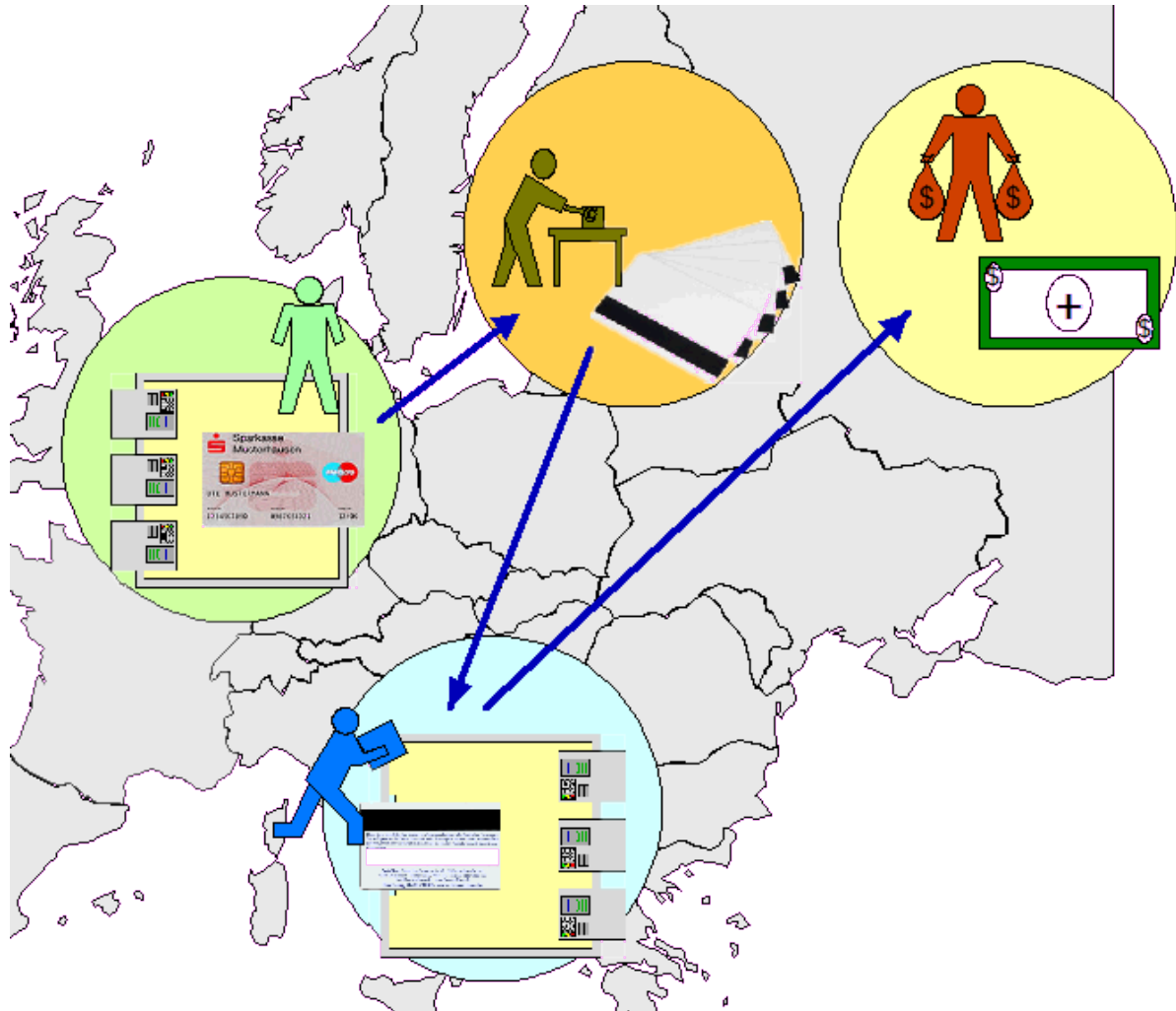


Dieter Kochheim

Skimming

Erscheinungsformen und strafrechtliche Verfolgung

Dezember 2009



Das **Skimming** leitet sich ab von dem Skimmer¹, also dem Lesegerät, mit dem die Magnetstreifen von „Identitätsdokumenten“² ausgelesen werden können. Den Kriminellen geht es aber nicht um das Ausspähen der Daten auf den Zahlungskarten und der Persönlichen Identifikationsnummern – PIN – von Bankkunden, sondern einzig um das Geld, das sich beim Missbrauch gefälschter Zahlungskarten erzielen lässt.

¹ CF, Sicherheitsvorkehrungen, Juli 2007; CF ist das Kürzel für „Cyberfahnder“.

² CF, Überwachungstechnik: Zahlungskarten, 18.05.2008

Das Skimming ist zu einem einträglichen Geschäft geworden, in dem sich wenige Einzelpersonen, im Übrigen aber 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.

Cyberfahnder

S. Inhalt

3	Vorwort	22	D. Strafverfahren
4	A. Phänomen Skimming	22	1. geheime Ermittlungen
7	B. bargeldloser, kartengestützter Zahlungsverkehr	22	2. Organisierte Kriminalität
7	1. Fälschungssicherung	23	E. kriminalistische Erfahrungen
7	2. bargeldloser Zahlungsverkehr	23	1. Programm
8	3. Autorisierung	23	2. Garantiefunktion
8	4. Clearing	23	3. Ausspähen
8	5. Schadensausgleich	23	3.1 Vorerkundung
9	6. Ergebnisse	24	3.2 Spezialisten
9	7. arbeitsteilige Handlungen beim Skimming	24	3.3 Einsatz
11	C. Strafbarkeit	24	4. Abstimmung und Bericht
11	1. arbeitsteiliges Vorgehen	24	5. Banden
11	2. einschlägige Normen und Konkurrenzen	26	Glossar
12	3. Garantiefunktion		
13	4. Cashing im Ausland		
14	5. Cashing im Inland		
14	6. Ausspähen im Inland		
14	6.1 Skimmer: Strafbarkeit im Vorbereitungsstadium		
15	6.2 Ausspähen mit Skimmern: Versuchsstadium		
15	6.3 Ausspähen der PIN im Inland		
16	6.3.1 PIN-Skimming und Computerbetrug		
17	6.3.2 Schadenseintritt		
17	6.3.3 PIN-Skimming und Computersabotage		
18	6.4 Anfang und Ende		
18	7. Ausspähen im Ausland		
19	8. Tatplan und Beteiligung		
20	8.1 materielle Taten beim Cashing		
20	8.2 materielle Taten beim Skimming		
20	9. Verabredung zu einem Verbrechen		
21	10. Ergebnisse		

Thema:	Skimming
Autor:	Dieter Kochheim
Version:	1.05
Stand:	31.01.2010

Vorwort

Seit April 2007 berichtet der Cyberfahnder über die Cybercrime, das IT-Strafrecht, die einschlägigen Probleme bei der Strafverfolgung und über die technischen Hintergründe, soweit sie zum Verständnis nötig sind. Die ersten Themen, denen er sich widmete, war das Phishing³ und die für Angriffe nutzbaren Schnittstellen der IT⁴. Seither werden Schwerpunktthemen der Webseite in Arbeitspapieren im PDF-Format zusammengefasst.

Mit dem Thema „Skimming“⁵ 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 gefasst⁶.

Das Skimming als Kriminalitätsform war zunächst ein Randthema und ich habe es nicht als einen Teil der Cybercrime⁷ 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.

Dieser Aufsatz fasst die Erörterungen im CF zusammen und aktualisiert sie. Seine Aufgabe ist es auch, eine schnelle Orientierung in Bezug auf die Rechtsfragen zu liefern, die bei der Strafverfolgung wegen des Skimmings auftreten.

Überblick

Dieses Arbeitspapier beschreibt zunächst die aktuellen Erscheinungsformen (S. 4) des Skimmings als kriminelle Mode.

Dazu wird zwischen dem Skimming im engeren Sinne, also dem Ausspähen von Kartendaten

und Persönlichen Identifikationsnummern – PIN, und dem Cashing unterschieden, also dem Missbrauch gefälschter Zahlungskarten an Geldautomaten, die den Beginn und den Abschluss des Tatplanes kennzeichnen.

Der zweite Hauptteil widmet sich den finanzwirtschaftlichen Prozessen des bargeldloser, kartengestützter Zahlungsverkehrs (S. 7), ohne deren Verständnis auch die Rechtsfragen nur ungenügend geklärt werden können. Ihre wesentlichen Ergebnisse sind, dass die Finanzwirtschaft mit dem Autorisierungs- und dem Clearingverfahren ein mächtiges technisches Instrument entwickelt hat, das es zulässt, den internationalen Zahlungsverkehr in Echtzeit so durchzuführen, dass jeder Zahlungsvorgang von der Bank geprüft werden kann, die eine Zahlungskarte ausgestellt hat. Im Zuge der Autorisierung wird die Kontodeckung auch von Debitkarten geprüft und 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 (S. 11) im Vorfeld (S. 15), beim Ausspähen (ab S. 13) und beim Cashing (S. 12). 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 (S. 18).

Das Arbeitspapier schließt mit knappen Anmerkungen zum Strafverfahrensrecht (S. 21), über kriminalistische Erfahrungen (S. 22) und einem Glossar (S. 25).

³ CF, Phishing, April 2007; PDF-Version.

⁴ CF, IT-Sicherheit, Schwachstellen, Angriffe, April 2007

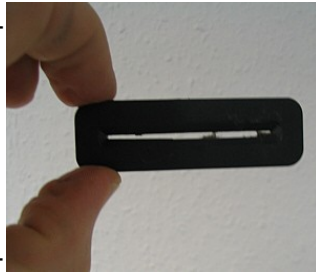
⁵ CF, Skimming, Juli 2007

⁶ CF, arbeitsteiliges Skimming, 18.05.2008

⁷ 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 Kamera⁸ 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 statt einer Kamera einen Tasta-



turaufsatz⁹ oder sogar eine vollständige Fassade (Front Covering) einsetzen¹⁰. Der wechselnde Einsatz verschiedener Karten für den Zugang zur Bank und für die Verfügung am Geldautomaten schützt dann nicht mehr, wenn der Skimmer direkt am Geldautomaten angebracht ist¹¹.



Seit zwei Jahren mehrer sich die Fälle des POS-Skimming¹². 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 aufnehmen¹³. Alle notwendigen Daten durchlaufen diese Geräte. Wenn die Täter es schaffen, sie entsprechend umzurüsten, dann speichern oder senden sie die Dumps¹⁴ an die Täter.



In Russland wurden unlängst die Geldautomaten selber gehackt, um die Dateneingabe vollständig aufzuzeichnen¹⁵. Vermutlich wurde dazu eine technische Schnittstelle an den Geräten genutzt, die zur Wartung, Funktionsprüfung oder Aktualisierung der Software bestimmt ist.

⁹ CF, Tastaturaufsatz, 13.04.2009; CF, Tastaturblende, 13.04.2009

¹⁰ CF, Skimming, Juli 2007

¹¹ CF, BKA: Lagebild OK. Zahlungskartenkriminalität, 01.11.2008

¹² CF, POS-Skimming, 18.05.2008; CF, Datenklau und -missbrauch, 19.08.2008

¹³ CF, BKA: Lagebild OK. Manipulation von POS Terminals, 01.11.2008

¹⁴ vollständige Kartendaten einschließlich PIN; CF, Fachworte, April 2007

¹⁵ CF, Skimming an der Quelle, 20.03.2009

⁸ CF, Kamera, 13.04.2009

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 eindringen und die Kartendaten einschließlich PIN von 100 Kunden ausspähen¹⁶. 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.

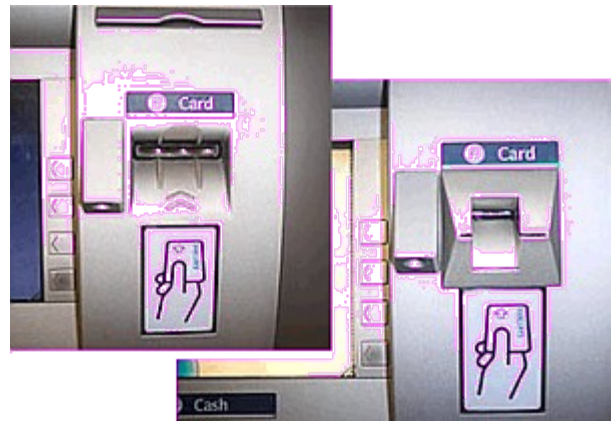
Dieses Beispiel zeigt, wie sich die Methoden der Cybercrime in den Formen des Hackings, des Ausspähens und des Verfälschens von Daten mit denen anderer Kriminalitätsformen vermengen.

Das Skimming ist von seiner Herkunft her eher beim Trickdiebstahl und -betrug angesiedelt¹⁷, 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 Täter¹⁸ und die grenzüber-

¹⁶ CF, Skimming-Coup, 06.02.2009

¹⁷ CF, Proll-Skimming, 18.05.2008; CF, Beobachtung. Trickdiebstahl, Juli 2007

¹⁸ CF, Grafik, Juni 2008. Wegen der Herstellung von Skimmern (Kartenlesegeräte) fehlt noch der Hinweis



schreitende Logistik des Gesamtplans sprechen für eine Arbeitsteilung mit einer zentralen planenden und steuernden Instanz.

Die bisher gemachten Erfahrungen zeigen, dass Skimmer¹⁹ und Casher²⁰ 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, und dass zur Funktionsprüfung der präparierten Kartenlesegeräte und zur Markierung der ausgespähten Zahlungskartendaten Testkarten eingesetzt werden²¹. Andere Bilder haben eindrucksvoll gezeigt, wie Casher beim Einsatz von White Cards²² mit ihren Handys telefonieren und sich dabei offenbar die PIN übermitteln lassen.

Die bevorzugten Zeiten für das Ausspähen liegen außerhalb der Banköffnungszeiten, also

auf § 149 StGB. Die Diskussion um die Strafbarkeit wegen des Umgangs mit diesen Geräten wurde erst ab Herbst 2008 öffentlich.

¹⁹ Skimmer: siehe Glossar.

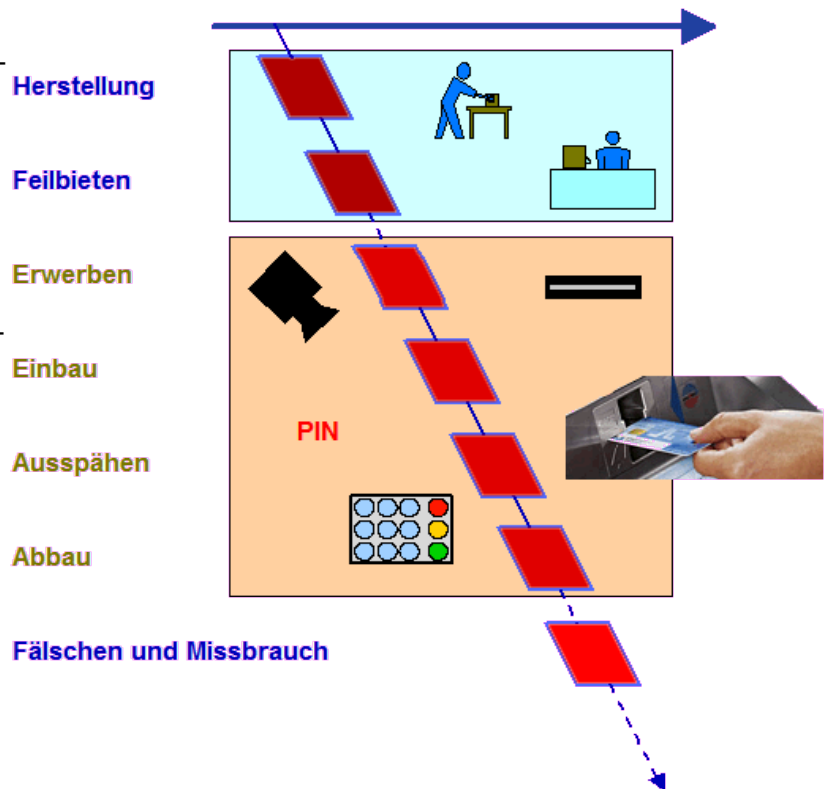
²⁰ Casher: siehe Glossar.

²¹ 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.

²² White Cards, auch White Plastics: siehe Glossar.

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 Phishing²³ 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 wird²⁴, so dass am Samstag Morgen das neue Wochenlimit angegriffen werden kann.



Grafik: frühe Phasen beim Skimming

²³ 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.

²⁴ 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 Zahlungskarten²⁵ verfügen über mehrere Vorrichtungen gegen das Fälschen der Karte selber²⁶. Neben dem Unterschriftsfeld, den Merkmalen des Aufdrucks und des für die Individualdaten verwendeten Schrifttyps (OCR-B²⁷) sind das besonders der EMV-Chip und das Maschinenlesbare Merkmal – MM. Das MM ist eine Besonderheit, die es nur in Deutschland gibt. Es handelt sich um eine Substanz, die in den Kartenkörper eingebracht ist und von jedem Geldautomaten in Deutschland geprüft werden muss. Das verhindert es, dass gefälschte Zahlungskarten mit deutscher Herkunft des Originals überhaupt in Deutschland eingesetzt werden können.

Der EMV-Chip wird von den großen Verbänden für grenzüberschreitend einsetzbare Zahlungskarten gefordert. Das Kürzel geht auf „Electronic Cash – **Master/Maestro** – **Visa**“ zurück²⁸. 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.

²⁵ Es handelt sich um standardisierte Identitätsdokumente nach ISO/IEC 7810 (Wikipedia).

²⁶ CF, Zahlungskarten, 18.05.2008

²⁷ CF, Zeichensatz OCR-B, Juli 2007

²⁸ CF, Zahlungskarten mit Garantiefunktion, 13.04.2009

2. bargeldloser Zahlungsverkehr

Beim klassischen Euroscheck verkörperte die Bank des Kunden ihre Zahlungsgarantie in Papierform, also durch den Euroscheck selber²⁹. 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 Abbuchungsauftrag³⁰.

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 gibt³¹. 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 Datenverkehr übermittelt werden und die einen Genehmigungscode zurückmeldet. Der Genehmigungscode ersetzt die im Euroscheck verkörperte Garantiefunktion und enthält eine Auszahlungsgarantie der kartenausge-

²⁹ 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.

³⁰ CF, Einzugsermächtigung und Lastschriftverfahren, 2007

³¹ Die Einzugsverfahren sind in das SEPA-Übereinkommen aufgenommen worden und gelten jetzt europaweit; siehe CF, Single Euro Payments Area, 26.01.2008.

benden Bank. Sie erklärt damit verbindlich, dass die Zahlungskarte akzeptiert wird und der geforderte Betrag zur Verfügung steht.

3. Autorisierung

Die wesentlichen Sicherungen für das Autorisierungsverfahren³² bestehen in den Sicherheitsmerkmalen der Zahlungskarte, in der PIN und schließlich in dem Genehmigungscode, den die kartenausgebende Bank an den Akzeptanten meldet³³.

Zum Zweck der Autorisierung von Debitkarten³⁴ liest der ausländische Geldautomat die Kartendaten aus, kombiniert sie mit der vom Kunden eingegebenen PIN, dem Auszahlungsbetrag, der Gebühr, den Individualmerkmalen des Geldautomaten und der Uhrzeit. Der daraus gebildete Datensatz wird über Kommunikationsnetze und durch verschiedene Zwischenstellen (zum Beispiel in Deutschland: First Data³⁵, Finanz IT³⁶) bis zur kartenausgebenden Bank geleitet³⁷. Diese prüft, ob die Karte von ihr ausgestellt ist, nicht gesperrt ist, die Auszahlung im Ausland erlaubt, das Tages- oder Wochenlimit nicht überschritten sind und schließlich ob Kontodeckung besteht. Danach sendet die Bank an den Geldautomaten einen Genehmigungscode zurück, der die Auszahlung autorisiert und eine Garantie enthält, dass die autorisierende Bank für den Auszahlungsbetrag bürgt³⁸.

³² Wegen der technischen Einzelheiten: [ISO 8583 \(Wikipedia\)](#).

³³ [CF, Autorisierung im POS-Verfahren, 13.04.2009](#)

³⁴ Gemeint sind Zahlungskarten auf Guthabenbasis, wobei als Guthaben auch der gewährte Überziehungskredit gilt.

³⁵ früher Gesellschaft für Zahlungssysteme

³⁶ Rechenzentrum der Sparkassen

³⁷ Siehe Glossar: Autorisierung, Clearing.

³⁸ 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 Ver-

4. Clearing

Nach der Autorisierung erfolgt keine unmittelbare Belastung des Kundenkontos, sondern eine Zwischenbuchung auf einem bankinternen Konto. 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 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

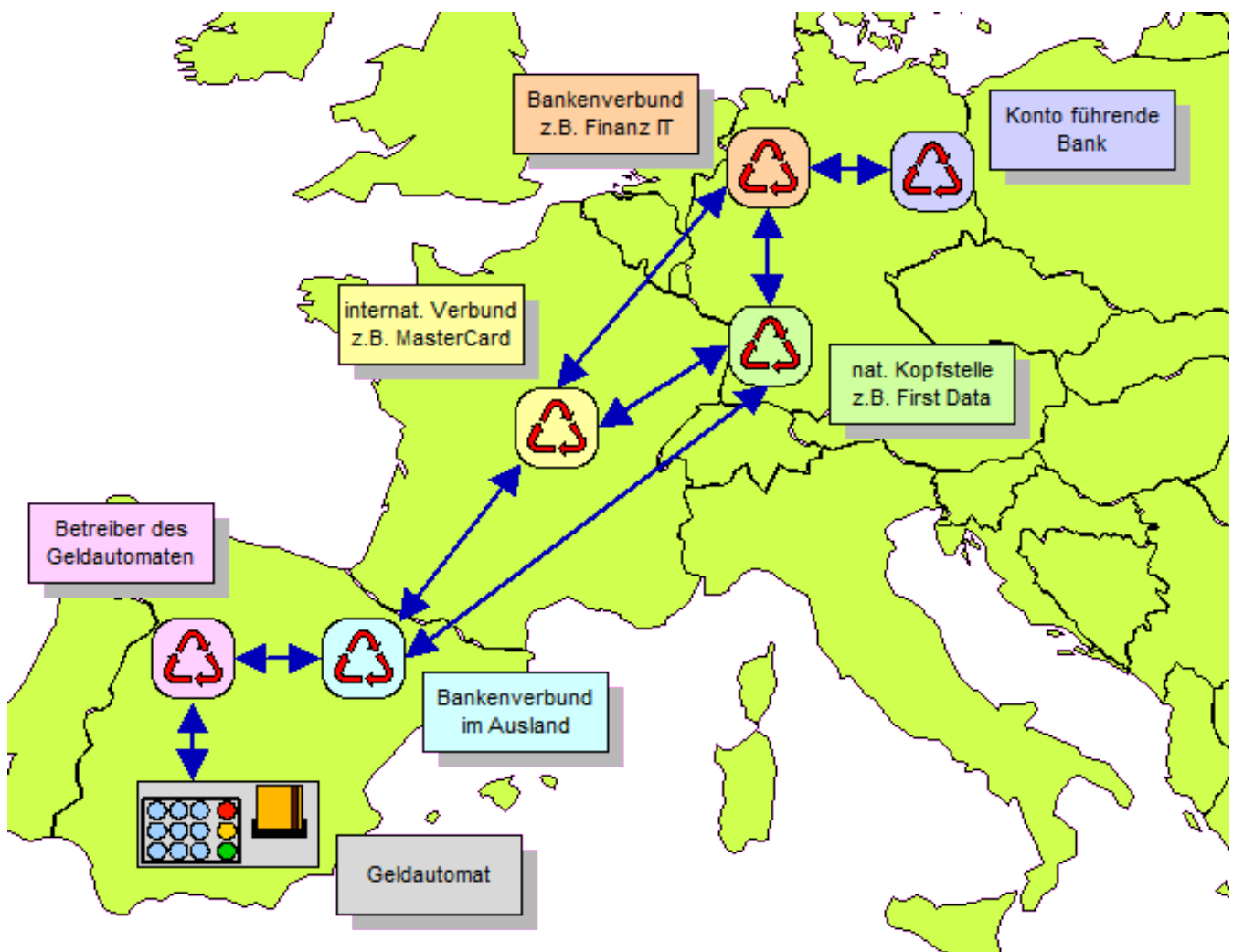
Beanstandet der Kunde eine Kontobelastung und ist diese auf den Einsatz einer gefälschten Zahlungskarte zurückzuführen, wird grundsätzlich ein Schadensausgleich durchgeführt, bei dem zunächst die Hausbank des Kunden die Belastung gegenbucht und diese Forderung bei der EURO Kartensysteme - EKS³⁹ - zum Ausgleich anmeldet. Stellt sich dann heraus, dass der ausländische Geldautomat⁴⁰ von einer Karte, deren Original mit einem EMV-Chip ausgestattet ist, nur den Magnetstreifen geprüft hat, dann haftet im 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 entferntere Ausland verlagern sollte. Die Finanzwirtschaft

fühlung autorisiert hat.

³⁹ Siehe auch [EKS – Analyse](#).

⁴⁰ Der Schadensausgleich wird nur in Europa praktiziert, nicht auch außerhalb des Kontinents.



wird dann neue Formen der Sicherung und des Schadensausgleiches entwickeln müssen.

ßiges Handeln in diesen Fällen grundsätzlich anzunehmen ist.

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).

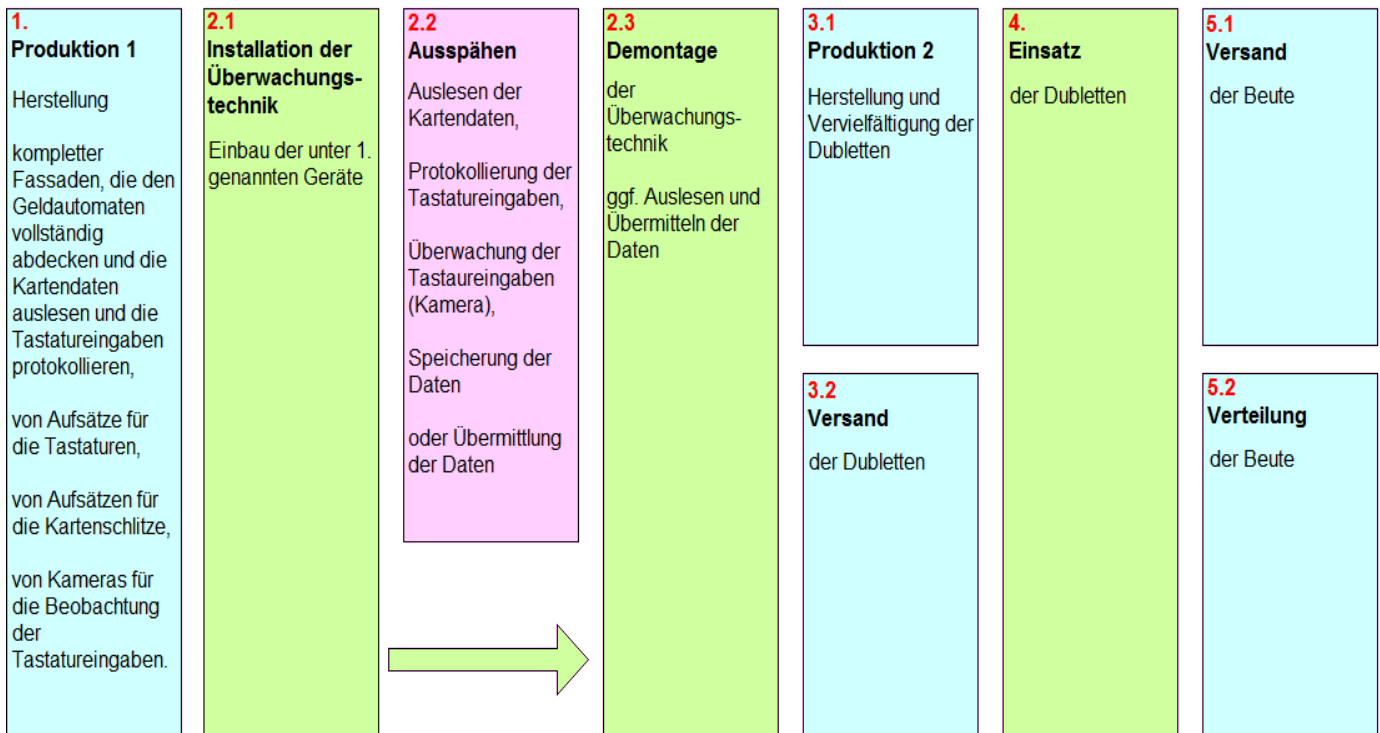
Daraus folgt ferner, dass im Ausland eine gefälschte Zahlungskarte, die gegen Fälschung besonders geschützt ist (Fälschungssicherung), mit Garantiefunktion verwendet wurde. Das qualifiziert die Tat zu einem Verbrechen gemäß § 152b Abs. 2 StGB mit einer Mindeststrafe von 2 Jahren Freiheitsstrafe, wobei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

7. arbeitsteilige Handlungen beim Skimming

Das Skimming ist geprägt von verschiedenen Tat handlungen, die in der Grafik auf Seite 10 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 im Einzelnen vorgenommen werden, die auf ein erhebliches Fachwissen 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 eingebürgert hat. Es umfasst die Installation der Ausspähtechnik, das Ausspähen selber und den Abbau der (wertvollen) Geräte. Entsprechend der eingesetzten Technik müssen die Geräte während des Ausspähens überprüft werden. Besonders dann, wenn der Abgriff der Kartendaten nicht direkt am Geldautomaten erfolgt, müssen die ausgespähten Kartendaten und PIN synchronisiert werden. Das erfolgt häufig in der Weise, dass die Täter Testkarten einsetzen, deren Merkmale ihnen geläufig sind.

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 Beuterealisation. Es wird uns wahrscheinlich noch lange erhalten bleiben.

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 ⁴¹.

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. Einzeltäter, die alle Arbeitsschritte persönlich ausüben, mögen im seltenen Einzelfall vorkommen. In aller Regel haben wir es jedoch mit Tätergruppen zu tun, die sich nur deshalb zusammentun, um eine dauerhafte Einnahmequelle zu haben. Das wird auch durch die Schäden belegt, die von Cashing-Aktionen hervorgerufen werden und bei denen binnen weniger Tage mehrere Zehntausend Euro erbeutet werden.

2. einschlägige Normen und Konkurrenzen

Das Fälschen von Zahlungskarten und ihren Gebrauch hat der Gesetzgeber neben die Vorschriften über das Fälschen von Geld gestellt. Von der Rechtsprechung des BGH ist anerkannt, dass sich die Fälschung auch alleine auf

die Daten auf dem Magnetstreifen beschränken kann ⁴².

Die Missbrauchshandlung beim Skimming ist im Grunddelikt der Gebrauch falscher ausländischer Zahlungskarten gemäß [§ 152a Abs. 1 Nr. 2 StGB](#) ⁴³. In Tateinheit ⁴⁴ damit steht der Computerbetrug gemäß [§ 263a StGB](#) ⁴⁵, dessen Vollendung mit der Auszahlung am Geldautomaten eintritt.

Dagegen tritt die Fälschung beweis erheblicher Daten gemäß [§ 269 StGB](#) hinter der spezielleren Vorschrift des [§ 152a Abs. 1 Nr. 1 StGB](#) zurück ⁴⁶. Das mit ihr verbundene „Speichern“ realisiert sich nur bei der Fälschung selber und nicht auch beim Missbrauch der gefälschten Zahlungskarten.

Der Tat als strafbare Vorbereitungshandlung vorgelagert ist [§ 149 StGB](#), der bereits den Umgang mit Computerprogrammen und ähnlichen Vorrichtungen unter Strafe stellt. Dies ist jedenfalls für die Kartenlesegeräte der Fall (Skimmer), die zum Zweck des Skimmings mit einem digitalen Speicher oder einer Funkeinrichtung ⁴⁷ ausgestattet, also umgebaut wurden. Die mit ihnen erspähten Kartendaten dienen unmittelbar zur Herstellung von gefälschten Zahlungskarten.

Daraus folgt, dass spätestens dann, wenn die Daten aus dem Magnetstreifen einer Zahlungskarte von Dritten ausgelesen und im Skimmer gespeichert oder per Funk weiter vermittelt wur-

⁴² Zur Verfälschung einer echten Zahlungskarte: [BGH, Urteil vom 21.09.2000 - 4 StR 284/00](#)

⁴³ Strafraumen: Geldstrafe bis 5 Jahre Freiheitsstrafe.

⁴⁴ Zur Tateinheit zwischen dem Gebrauch gefälschter Zahlungskarten (§ 152 StGB) und Betrug (§ 263 StGB): [BGH, Urteil vom 21.09.2000 - 4 StR 284/00](#)

⁴⁵ Fallgruppe: Unbefugte Verwendung von Daten.

⁴⁶ grundsätzlich zum Verhältnis zwischen Urkunden- und Zahlungsmittelfälschung: [BGH, Beschluss vom 26.01.2005 - 2 StR 516/04](#).

⁴⁷ Die Funktechnik ist deshalb noch nicht beobachtet worden, weil sie zu viel Strom verbraucht und deshalb die Ausspäzzeit verringert.

⁴¹ Siehe Glossar: POS

den, der Eintritt in den Versuch beginnt und zwar zu einer (gewerbsmäßigen) Straftat nach § 152b Abs. 2 StGB.

3. 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)⁴⁸. Diese Voraussetzungen liegen angesichts der beschriebenen Sicherheitsmerkmale bei den üblichen von Banken herausgegebenen Karten vor⁴⁹. Für den bargeldlosen Zahlungsverkehr im Zusammenhang mit dem Autorisierungsverfahren⁵⁰ kommen dem EMV-Chip und dem Maschinenlesbaren Merkmal eine besondere Bedeutung als Sicherheitsmerkmale zu, wobei das nur in Deutschland verwendete MM den Einsatz gefälschter Karten auf der Grundlage in Deutschland ausgegebener Karten konsequent verhindert⁵¹. Das ändert nichts daran, dass Fälschungen im Ausland eingesetzt werden können, wenn die dortigen Geldautomaten auf die Prüfung der maßgeblichen Sicherheitsmerkmale verzichten und sich auf die Informationen auf dem Magnetstreifen beschränken⁵².

Ausländische Kartendaten können hingegen auch in Deutschland missbraucht werden, weil ihren Originalen das MM fehlt und Kreditkarten in aller Regel über keinen EMV-Chip verfügen.

Dem Schutz des § 152a StGB unterliegen schließlich auch andere Zahlungskarten von Finanzdienstleistungsinstituten, zum Beispiel

Tank- und Telefonkarten, die hier nicht weiter betrachtet werden sollen.

§ 152b Abs. 4 StGB definiert die Zahlungskarten mit Garantiefunktion als Kredit-, Euroscheck- und sonstige Karten, die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu veranlassen⁵³, und die durch ihre Ausgestaltung oder Codierung besonders gegen Nachahmung gesichert sind.

Der Begriff „Ausgestaltung“ spricht die körperliche Form der Karte an, so dass die beschriebenen Sicherheitsmerkmale einschlägig sind⁵⁴. Nicht nur sie machen die üblichen Karten zu besonders geschützten, sondern auch ihre „Codierung“. Sie äußert sich (wiederum) im MM und in der PIN, ohne die keine erfolgreiche Autorisierung möglich ist.

Die im Übrigen geforderte Zahlungsgarantie besteht in dem im Autorisierungsverfahren übermittelten Genehmigungscode⁵⁵, der den Geldautomaten zur Auszahlung veranlasst. Mit ihm garantiert die autorisierende Bank, dass sie für die Auszahlung und die Gebühren einsteht⁵⁶.

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 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

⁵³ Für die EC-Karte hat der BGH anerkannt, dass sie auch eine Garantiefunktion hat, wenn sie im Lastschriftverfahren eingesetzt wird: BGH, Urteil vom 21.09.2000 - 4 StR 284/00

⁵⁴ Für die besondere Strafbarkeit kommt es nur darauf an, dass die Garantiefunktion besteht, und nicht auch darauf, dass der Täter sie missbrauchen will: BGH, Beschluss vom 17.06.2008 - 1 StR 229/08.

⁵⁵ Siehe oben **Autorisierung**

⁵⁶ CF, Autorisierung und Clearing, 02.08.2009

⁴⁸ CF, Skimming und Fälschungsrecht, 13.04.2009

⁴⁹ Siehe oben **Fälschungssicherung**.

⁵⁰ Siehe oben **Autorisierung**

⁵¹ Siehe oben **Fälschungssicherung**.

⁵² Siehe oben **Schadensausgleich**

das klassische Modell eine frühe Autorisierung bei der Ausgabe der Schecks durchgeführt hat, erfolgt sie jetzt in Echtzeit durch die Übermittlung des Genehmigungs-codes. Nicht anders als im alten Verfahren erfolgt die Buchung der Forderung gegen die Bank zunächst auf einem ihrer Zwischenkonten⁵⁷, was der Ausgabe der Euro-schecks gleich kommt. Das zeigt auch, dass die autorisierende Bank die buchhalterische Haftung für die betreffende Forderung übernimmt.

4. Cashing im Ausland

Der Missbrauch gefälschter Karten deutscher Herkunft im Ausland begründet unter mehreren Gesichtspunkten eine inländische Strafverfolgungszuständigkeit.

Dies gilt zunächst wegen des damit begangenen Computerbetruges (§ 263a StGB), weil der zum Tatbestand gehörende Erfolg (= Schaden) zu lasten der Bankkunden eintritt, deren Kartendaten und PIN missbraucht werden (§ 9 Abs. 1 StGB). Mit der Soll-Buchung zu lasten des Zwischenkontos bei der kartenausgebenden Bank tritt bereits eine schadensgleiche Vermögensgefährdung ein, die sich zu einem Schaden des Bankkunden verdichtet, sobald im Clearingverfahren die Buchung gegen sein Girokonto erfolgt⁵⁸. Der anschließende Schadensausgleich dient nur der Rückabwicklung unter Haftungs- und Risikogesichtspunkten. Würde dieses versicherungsähnliche Absicherungssystem fehlen, dann verbliebe der Schaden beim Bankkunden.

Für die Fälschungstat gilt darüber hinaus gemäß § 6 Nr. 7 StGB das Weltrechtsprinzip, wonach Taten der Geld- und Zahlungskartenfälschung auch dann im Inland verfolgt werden müssen, wenn sie im Ausland begangen wurden.

Diese Zuständigkeit für Auslandstaten folgt zudem aus § 9 Abs. 2 StGB, weil der im Ausland handelnde Casher nur tätig werden kann, weil ein im Inland tätig gewordener Mittäter oder Ge-

hilfe die Kartendaten ausgespäht hat. Das Ausspähen eröffnet den Versuch der Auslandstat⁵⁹, so dass auch der Tatort des Versuchs der Tatort der vollendeten Tat ist (§ 9 Abs. 2 StGB).

Das Cashing im Ausland auf der Grundlage von im Inland ausgespähten Kartendaten und PIN⁶⁰ ist somit immer im Inland verfolgbar. Darüber hinaus führt das Weltrechtsprinzip auch dazu, dass im Ausland missbrauchte Kartendaten ausländischer Herkunft im Inland verfolgbar sind.

Das Cashing im Ausland mit inländischen Kartendaten 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 dar⁶¹.

Streng genommen ist jeder einzelne Gebrauch einer Dublette eine einzelne und selbständige Straftat. Sowohl beim Ausspähen wie auch beim Cashing handeln die Täter mit dem weit gefassten Vorsatz, einerseits alle sich bietenden Kartendaten zu skimmen und andererseits alle vorhandenen Dubletten bis zu ihrem Limit zu missbrauchen. Ihr Handeln stellt sich somit als ein von einem Gesamtvorsatz umfasster, einheitlicher Lebenssachverhalt dar, der jedenfalls alle Missbrauchshandlungen, die ohne erkennbare Pause erfolgen, zu einer Tat zusammen fasst (§ 52 StGB)⁶².

⁵⁹ Siehe **Ausspähen im Inland**

⁶⁰ Siehe **Ausspähen der PIN im Inland**

⁶¹ Das Landgericht Hannover ist am 17.11.2009 meinen rechtlichen Auffassungen gefolgt: **CF, Skimming-Rechtsprechung, 18.11.2009**

⁶² Eine einheitliche Tat hat der BGH ausdrücklich dann angenommen, wenn das Sichverschaffen von gefälschten Zahlungskarten im engen zeitlichen Zusammenhang mit ihrem Missbrauch steht: **BGH, Beschluss vom 26.01.2005 - 2 StR 516/04, BGH, Beschluss vom 07.03.2008 - 2 StR 44/08**

⁵⁷ Siehe oben **Clearing**

⁵⁸ Siehe oben **Clearing**

5. Cashing im Inland

§ 152a Abs. 1 StGB stellt den Missbrauch ausländischer Karten denen aus dem Inland gleich. Somit werden Karten unabhängig von ihrer Herkunft unter dem Gesichtspunkt der Fälschung geschützt. Der mit dem Kartenmissbrauch verbundene Computerbetrug am Geldautomaten wird zudem im Inland betrieben, so dass der gewerbsmäßige Missbrauch ausländischer Zahlungskarten mit Garantiefunktion in Tateinheit mit Computerbetrug als Vorwurf einschlägig ist. Im Gegensatz zum Cashing im Ausland führt bei der Inlandstat der Handlungsort unmittelbar zur örtlichen Zuständigkeit (§ 9 Abs. 1 StGB).

6. Ausspähen im Inland

Eine Straftat versucht, wer nach seiner Vorstellung von der Tat zur Verwirklichung des Tatbestandes unmittelbar ansetzt (§ 22 StGB).

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.

Wegen der Strafbarkeit des Umgangs mit den Geräten zum Ausspähen muss zwischen den Kartenlesegeräten (Skimmer), für die ein Umgangsverbot besteht, und denen zum Beobach-

ten der PIN-Eingabe unterschieden werden, die keinem Verbot unterliegen.

6.1 Skimmer: Strafbarkeit im Vorbereitungsstadium

§ 149 StGB stellt bereits die Vorbereitung der Geld- und Wertzeichenfälschung unter Strafe. Der Gesetzgeber behandelt Zahlungskarten damit gleich und verweist von den §§ 152a Abs. 5 und 152b Abs. 5 StGB auf die Gefährdungstatbestände.

Noch 2003 hat der Bundesgerichtshof den „Umgang“⁶³ mit Skimmern als nicht strafbar angesehen⁶⁴, weil er sie nicht als „ähnliche Vorrichtungen“ wie Druckstöcke und Druckplatten angesehen hat, mit denen Geld gefälscht werden kann.

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“. Das hat den Generalbundesanwalt in seiner Stellungnahme zur Revision gegen ein Urteil des Landgerichts München dazu veranlasst, auch die Skimmer als verbotene Gegenstände im Sinne von § 149 StGB zu betrachten⁶⁵. Der BGH hat darauf die Revision ohne nähere Begründung verworfen⁶⁶. Dabei hat er jedoch die Urteilsformel des angegriffenen Urteils berichtigt, was zeigt, dass er sich den Argumenten des GBA angeschlossen haben muss.

Das sind zwei Gründe dafür, ihnen zu folgen. Sie sind schlüssig und der BGH hat keinen Anlass gesehen, ihnen zu widersprechen.

⁶³ „Umgang“ ist ein aus dem Waffenrecht stammender Begriff, der verschiedene Handlungsformen zusammen fasst. In Bezug auf den § 149 StGB sind das:

- a) Herstellen,
- b) sich oder einem anderen Verschaffen,
- c) Feilhalten,
- d) Verwahren und
- e) einem anderen Überlassen.

⁶⁴ BGH, Urteil vom 16.12.2003 - 1 StR 297/03

⁶⁵ CF, Vorverlagerung, 13.04.2009

⁶⁶ BGH, Beschluss vom 09.09.2008 - 1 StR 414/08

Im Zusammenhang mit dem Hackerstrafrecht⁶⁷ hat sich das Bundesverfassungsgericht auch mit der Dual Use-Software auseinander gesetzt⁶⁸. Es handelt sich dabei um Programme, die eine nützliche Funktion haben und im Alltag dazu genutzt werden, um die Funktionstüchtigkeit informationsverarbeitender Systeme⁶⁹ und ihrer Netzverbindungen zu prüfen. Sie können aber auch zum Hacking und zur Datenspionage missbraucht werden, so dass sich die Frage stellt, wo die Strafbarkeit des Umgangs mit ihnen beginnt.

Das BVerfG kommt zu dem Ergebnis, dass die Dual Use-Software deshalb nicht der Strafbarkeit nach § 202c StGB unterliege, weil weder ihr Zweck noch ihre Eignung auf die missbräuchliche Nutzung ausgerichtet sei. Zur verbotenen Software würde sie erst, wenn sie zum Missbrauch besonders angepasst oder ausdrücklich beworben würde.

Diese Grundsätze lassen sich problemlos auf Skimmer übertragen. Ihre Komponenten sind im Einzelhandel frei verfügbar. Zu „ähnlichen Vorrichtungen“ werden sie erst durch ihre Bearbeitung und Kombination. Hilfreich an dieser Stelle ist wieder die gesetzliche Definition des Versuchs. Er beginnt, sobald der Täter nach seiner eigenen Vorstellung zur Tatbestandsverwirklichung unmittelbar ansetzt. „Herstellen“ im Sinne von § 149 StGB ist ein Prozess, wonach der Skimmer fertig und einsatzfähig ist. Verboten ist deshalb bereits die noch nicht abgeschlossene Arbeit an dem Skimmer. Auf seine Funktionstüchtigkeit kommt es somit nicht an.

Auch der unfertige Skimmer ist deshalb ein verbotener Gegenstand gemäß § 149 StGB, wenn

⁶⁷ CF, vorverlagertes Hackerstrafrecht, 04.09.2008

⁶⁸ BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07, 1151/08, 1524/08

⁶⁹ Der Begriff „informationsverarbeitende Systeme“ wurde vom BVerfG im Zusammenhang mit der Onlinedurchsuchung eingeführt; BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07; CF, Bundesverfassungsgericht: Onlinedurchsuchung, 05.04.2008

er bereits zum Einsatz als Ausspähergerät bearbeitet wurde. Auch ihn darf man nicht erwerben, weiter geben oder erwerben, wenn damit die Vorstellung verbunden ist, ihn zum Ausspähen von Kartendaten zu benutzen.

6.2 Ausspähen mit Skimmern: Versuchsstadium

Das Vorbereitungsstadium ist dem Versuchsstadium **unmittelbar** vorgelagert. Die Konsequenz daraus ist, dass der Versuch der Fälschung von Zahlungskarten genau dann beginnt, wenn der Skimmer installiert wird.

Ich habe bislang eine andere Meinung vertreten und bin davon ausgegangen, dass der Versuch erst mit dem ersten erfolgreichen Ausspähen von Kartendaten einsetzt⁷⁰. Dabei habe ich mich von der Rücktrittsproblematik und der fehlenden Versuchsstrafbarkeit in § 202a StGB verleiten lassen. Das gilt es zu berichtigen.

Ausschlaggebend ist wiederum die Vorstellung des Täters (§ 22 StGB). Selbstverständlich will der Skimmer (Täter) die Kartendaten ausspähen, wenn er die dafür bestimmte Hardware installiert. Damit setzt er auch unmittelbar zur Tatbestandsverwirklichung an. Er bleibt straflos, wenn er vor der Tatvollendung vom Versuch zurücktritt (§ 24 StGB).

Mit dem ersten erfolgreichen Ausspähen von Kartendaten ist ein Ausspähen von Daten gemäß § 202a StGB vollendet, wofür dem Skimmer eine Freiheitsstrafe bis zu 3 Jahren droht. Das Versuchsstadium in Bezug auf die Fälschung von Zahlungskarten dauert aber weiter, bis die erste falsche Zahlungskarte erstellt ist. Daraus folgt zweierlei:

Vom Versuch der Fälschung von Zahlungskarten kann er erfolgreich (und damit straflos) zurücktreten, bis er die ausgespähten Kartendaten an die Hinterleute meldet, die damit falsche Zahlungskarten herstellen sollen. Damit endet seine Tatherrschaft und die Möglichkeit, den kriminell-

⁷⁰ CF, Einstiegshandlungen, 19.04.2009

len Erfolg direkt zu verhindern. Um einer Strafe wegen der Fälschung von Zahlungskarten zu entgehen, muss er fortan besondere Anstrengungen zur Verhinderung unternehmen (§ 24 Abs. 2 StGB). Er bleibt nur dann straffrei, wenn die Nachtäter auf die geplante Vollendung verzichten oder die Tat ohne seinen Tatbeitrag ausführen. Im Zusammenhang mit dem Skimming bedeutet das, dass sie zwar das Fälschen und das Cashing durchführen, aber nur mit anderen Kartendaten als die, die vom Skimmer (Täter) stammen (Akzessorietät bei der Beihilfe und dem Rücktritt vom Versuch).

Ist sein Rücktritt wirksam, so verbleiben zwei Vorwürfe gegen den Skimmer als Täter: Der Umgang mit der Ausspähhardware gemäß § 149 StGB und das erfolgreiche Ausspähen von Kartendaten gemäß § 202a Abs. 1 StGB. Insofern bleibt die Installation der Skimming-Hardware straffrei. Sie geht in die vorverlagerte Strafbarkeit wegen des Umgangs mit Skimmern (Geräte) auf.

6.3 Ausspähen der PIN im Inland

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 direkt abgeleitet werden kann.

Wegen des Ausspähens der PIN greift auch das Hackerstrafrecht nicht. 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. Sie 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.

6.3.1 PIN-Skimming und Computerbetrug

Mit § 263a Abs. 3 StGB wird die strafrechtliche Haftung in das Vorbereitungsstadium übertragen, soweit es um den Umgang mit **Programmen** geht, die besonders zum Computerbetrug bestimmt sind. Das betrifft nur die Software, nicht aber die Hardware.

Daraus folgt, dass „einfache“ technische Ausspähvorrichtungen für die PIN nicht verboten sind, wohl aber die in ihnen verbauten Programme, mit denen die PIN gespeichert, übermittelt oder mit den Kartendaten synchronisiert werden. Nicht die Kamera als Gerät und nicht ihr Einbau in einen vorgetäuschten Rauchmelder oder in einer Leiste, die über der Tastatur angebracht werden soll, sind strafbar, sondern nur die Verarbeitungslogik, die die Täter zu dem Zweck installieren, die PIN auszuspähen, zu speichern und zu übermitteln. Ob jedoch die Kombination fertiger technischer Bauteile und die sie verbindenden Routinen schon die Qualität eines Computerprogrammes haben, wird man nur im Einzelfall entscheiden können.

Selbst wenn solche Programme eingesetzt werden stellt sich die Frage, ob der Begriff des Computerprogramms im Sinne von § 263a Abs. 3 StGB auch solche Programme umfasst, die zur Vorbereitung der Tat eingesetzt werden. Die üblichen Vorrichtungen zum Ausspähen der PIN werden nicht zum Computerbetrug selber verwendet, sondern ausschließlich zur Vorbereitung der abschließenden Tat.

Sobald der Täter die Hardware zum Ausspähen installiert, soll sie ihm den künftigen Missbrauch von gefälschten Zahlungskarten ermöglichen. Nach seiner Vorstellung beginnt er damit, den Tatbestand des Gebrauchs gefälschter Zahlungskarten und den damit verbundenen Computerbetrug zu erfüllen. Das Versuchsstadium

beginnt damit und setzt sich bis zum Cashing fort.

Ob der Täter im Vorfeld eines polizeilichen Zugriffs erfolgreich vom Versuch zurücktritt, weil er flieht und die Skimming-Hardware mitnimmt, ist eine andere Frage. Behält er die ausgespähten PIN bei sich, tritt er nicht vom Versuch zurück.

6.3.2 Schadenseintritt

Die hier vertretene Auffassung, die auf dem Begriff der schadensgleichen Vermögensgefährdung⁷¹ zurück greift, wird nicht von der jüngeren Rechtsprechung des BGH in Frage gestellt. Diese juristische Konstruktion nähert die konkreten Gefährdungsdelikte des Vermögensstrafrechts abstrakten Gefährdungsdelikten an⁷² und wird vom 1.⁷³ und vom 3. Strafsenat des BGH⁷⁴ zunehmend in Frage gestellt. An seine Stelle setzen sie einen feineren Begriff des Schadens, der an der Tatvollendung nichts ändert⁷⁵ und den Bankkunden frühzeitig zum Geschädigten macht.

Wegen des mit dem Cashing verbundenen Computerbetruges vertrete ich die Ansicht, dass in dem Moment, in dem das Rechenzentrum der kartenausgebenden Bank nach dem Einsatz einer gefälschten Zahlungskarte mit Garantiefunktion den Genehmigungscode "0" sendet und den vom Geldautomaten geforderten Betrag - Auszahlungsbetrag und Gebühr - gegen das bankeigene cpd-Konto bucht, sei eine schadensgleiche Vermögensgefährdung zulasten der Bank eingetreten.

Zur Deckung für die zunächst bankinterne Buchung dient das laufende Konto des Kunden. Mit

⁷¹ Bestätigt vom BVerfG: [Beschluss vom 10.03.2009 - 2 BvR 1980/07](#)

⁷² CF, [Schaden und schadensgleiche Vermögensgefährdung](#), 31.01.2010

⁷³ BGH, [Beschluss vom 18.02.2009 - 1 StR 731/08](#)

⁷⁴ BGH, [Urteil vom 13.08.2009 - 3 StR 576/08](#); BGH, [Urteil vom 14.08.2009 - 3 StR 552/08](#)

⁷⁵ Siehe unten: [Anfang und Ende](#).

der Forderung der Bank droht dem Kunden eine Verringerung seines Vermögens in gleicher Höhe. Allein das reicht nach der neuen Rechtsprechung dazu aus, einen Schaden als solchen zulasten des Bankkunden anzunehmen.

Die heute praktizierte Schadensabwicklung, die die Bankkunden faktisch von den Schäden freistellt und sie zwischen den beteiligten Banken und ihren Verbänden verteilt, ist davon unabhängig, weil es sich dabei um eine Art Versicherungssystem handelt, das den Risikoausgleich vornimmt. Mit den ausgespähten Daten werden jedoch die betroffenen Kunden unmittelbar angegriffen. Würde das System der Schadensabwicklung fehlen, dann blieben ihre Vermögen vom Cashing belastet und die Finanzwirtschaft hätte ein existenzielles Vertrauensproblem.

Die Schadensabwicklung führt auch nicht dazu, dass im Saldo der Bankkunde nicht geschädigt wäre. Abzustellen ist mit dem 3. Strafsenat des BGH auf den Zeitpunkt des Ereignisses und das ist die Genehmigung der Auszahlung, von der an die Belastung des Kundenkontos droht, und spätestens die Realisierung des Schadens, die im Zuge des Clearingverfahrens mit der Buchung gegen das Konto des Kunden erfolgt. Spätestens damit ist der handfeste Schaden beim Kunden eingetreten. Alles Nachfolgende ist vertrauensbildende Kompensation.

6.3.3 PIN-Skimming und Computersabotage

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

[§ 303b Abs. 5 StGB](#) erweitert jedoch die Strafbarkeit auch auf das Vorbereitungsstadium, indem er auf [§ 202c StGB](#) verweist. Diese Vorschrift schützt nicht nur Computerprogramme, sondern ausdrücklich auch Passwörter und

sonstigen Sicherungscode (§ 202c Abs. 1 Nr. 1 StGB). Der Umgang mit ihnen mit dem Ziel, sie zum Cashing zu verwenden, steht unter Strafe⁷⁶.

Die Schutzrichtung dieser Normen beschränkt sich jedoch auf Computerprogramme einerseits und PIN (als Passwörter) andererseits, nicht aber auf die zum Ausspähen genutzten Geräten. Im Ergebnis stellt sich deshalb die Lage wie beim Computerbetrug dar.

6.4 Anfang und Ende

Der BGH hat für den Beginn des Versuchs den schönen Satz verwendet: **Jetzt geht es los!**⁷⁷:

„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.“

Daraus folgt auch, dass der Beginn des Versuchs im Zusammenhang mit dem Skimming dort einsetzt, wo die Täter mit der Installation der Ausspähhardware beginnen, sie befestigen montieren und dann einrichten.

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

Etwas anderes gilt für den gleichzeitig begangenen Computerbetrug. Sein Erfolg tritt erst ein,

⁷⁶ CF, Ausspähen der PIN, 06.12.2008

⁷⁷ BGH, Beschluss vom 07.11.2007 - 5 StR 371/07

sobald sich der Täter einen Vermögensvorteil verschafft hat. Das ist der Fall, sobald der Geldautomat das angeforderte Geld zur Entnahme präsentiert und der Täter es nimmt. Zu diesem Zeitpunkt ist bereits eine schadensgleiche Vermögensgefährdung bei der kartenausgebenden Bank eingetreten, weil der Geldautomat von ihr den Genehmigungscode empfangen hat und sie gleichzeitig damit eine Buchung des Auszahlungsbetrages und der Gebühr zulasten eines bankinternen Kontos (conto pro diverse - cpd) erfolgt ist.

Im anschließenden Clearingverfahren wird der tatbestandliche Erfolg nur verschoben. Bankintern wird dabei die Verbindlichkeit aus dem cpd an die Verrechnungsstelle überwiesen und gleichzeitig gegen das Girokonto des Kunden gebucht. Dort tritt der Schaden, also der Erfolg ein.

Aufgrund der Garantiefunktion, die mit der Mitteilung des Genehmigungscode 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.

7. Ausspähen im Ausland

Nach § 6 Nr. 7 StGB ist nicht nur das Fälschen und Gebrauchen von Zahlungskarten mit Garantiefunktion dem Weltrechtsprinzip unterworfen, sondern auch die der Vorbereitung dienenden Handlungen gemäß § 149 StGB. Das führt dazu, dass auch der Umgang mit Skimmern und das Ausspähen der Kartendaten nach den hier entwickelten Grundsätzen dann strafbar sind, wenn der Täter im Ausland gehandelt hat⁷⁸.

⁷⁸ Die Geltung des deutschen Strafrechts begründet nicht auch die örtliche Zuständigkeit einer Strafverfolgungsbehörde. Sie richtet sich nach der StPO, so dass vor Allem der Ergreifungsort (§ 9 StPO) und der Zusammenhang bedeutsam sind (§ 13 Abs. 1 StPO). Im Zweifel muss der BGH die örtliche Zuständigkeit bestimmen (§ 13a StPO).

Der gewerbsmäßige Computerbetrug unterliegt nicht dem Weltrechtsprinzip. Das bedeutet, dass das PIN-Skimming solange nicht verfolgt werden kann, bis der Täter oder ein anderer, mit dem er zusammenarbeitet, auch im Inland handelt. Dann greift § 9 Abs. 2 S. 1 StGB, so dass der Tatort im Inland auch zum Tatort für die im Ausland begangenen Handlungen im Versuchsstadium wird.

8. Tatplan und Beteiligung

*"Sind an einer Deliktserie mehrere Personen als Mittäter, mittelbare Täter, Anstifter oder Gehilfen beteiligt, ist die Frage, ob die Straftaten tateinheitlich oder tadmehrheitlich zusammenfallen, nach ständiger Rechtsprechung des Bundesgerichtshofs für jeden der Beteiligten gesondert zu prüfen und zu entscheiden."*⁷⁹

Wegen der Tatbeiträge arbeitsteilig handelnder Täter und ihrer rechtlichen Bewertung verlangt der BGH deshalb eine Betrachtung des einzelnen Täters, eine genaue Bezeichnung seiner Handlungen und Feststellungen dazu, wie sie sich in den Gesamtplan einfügen⁸⁰.

2001 hat sich der BGH vom vorher geltenden Bandenbegriff abgewandt und eine erweiterte Zurechnung der Tatvollendung auch auf die Tatbeteiligten bestimmt, die der Vorbereitung dienen oder nur Teilakte der Tat ausführen⁸¹. Ihre Beteiligung an der Tatvollendung ist nicht erforderlich, wie es der BGH am Beispiel des Diebstahls entwickelt hat.

Danach reicht es aus,

"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 besonde-

*ren 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"*⁸².

In der Konsequenz daraus betrachtet der BGH auch den Täter, der die allgemeinen Voraussetzungen für eine Tatserie schafft, indem er zum Beispiel einen Firmenmantel finanziert und zur Verfügung stellt, als **eine** Tat dieses Täters, auch wenn sich die folgenden Handlungen seiner Mittäter für sie als mehrere materielle Taten darstellen⁸³. Beteiligt er sich zudem an den Folgehandlungen der Mittäter, so ist ihm eine weitere materielle Tat vorzuwerfen.

Im Zusammenhang mit mehraktigen Bandenstrafataten müssen sich die Täter aus den verschiedenen Tatstadien nicht persönlich untereinander kennen, wenn nur jeder den Willen hat, sich zur künftigen Begehung von Straftaten mit (mindestens) zwei anderen zu verbinden⁸⁴. Der BGH hat im Oktober 2009 nochmals deutlich gemacht, dass auch der Mittäter für die Handlungen der anderen als Täter haftet, wenn ihr Tun seinen groben Vorstellungen vom Tatplan und -ablauf entspricht⁸⁵. Die Grenzen für die mittäterschaftliche Haftung bestimmen sich nach der Tatvollendung, wie sie die Strafgesetze vorgeben. Die neue Rechtsprechung schafft kein neues Organisationsstrafrecht⁸⁶.

Für das Skimming und das Cashing hat diese Rechtsprechung eine besondere Bedeutung.

⁸² Ebenda.

⁸³ BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

⁸⁴ BGH, Urteil 16.06.2005 - 3 StR 492/04

⁸⁵ BGH, Urteil vom 28.10.2009 - 1 StR 205/09; siehe auch CF, Mittäterschaft und strafrechtliche Haftung, 23.12.2009.

⁸⁶ BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

⁷⁹ BGH, Beschluss vom 29.04.2008 - 4 StR 125/08

⁸⁰ BGH, Beschluss vom 13.08.2002 - 4 StR 208/02

⁸¹ BGH, Beschluss vom 22.03.2001 - GSSt 1/00

8.1 materielle Taten beim Cashing

Beim Cashing wird der gewerbsmäßigen 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. Im Sinne der natürlichen Handlungseinheit werden sich dabei mehrere Handlungen des Gebrauchs als eine materielle Tat darstellen, wenn sie unmittelbar aufeinander folgen und dem Willen des Cashers folgen, alle ihm zur Verfügung stehenden Dubletten bis zum Limit zu missbrauchen.

Ob die Vollendung in mehreren materiellen Taten erfolgt, orientiert sich am Handeln des Cashers. Anhand der Abbuchungsdaten können 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 stammen⁸⁷.

Die Zeitstempel der Geldautomaten sagen aus, dass die bekannten Kartendaten missbraucht wurden. Damit ist nicht ausgeschlossen, dass die Casher weitere Dubletten eingesetzt haben, die wegen ihrer Herkunft unbekannt sind.

Das kann dazu führen, dass sich alle Gebrauchsfälle für den Casher als eine einheitliche materielle Tat darstellen⁸⁸.

⁸⁷ Allein Europa verfügt über mindestens 4 Zeitzonen, von der die Mitteleuropäische Zeit – MEZ – die verbreitetste ist.

⁸⁸ Der BGH erkennt in ständiger Rechtsprechung die Zusammenfassung vieler Missbrauchsfälle zu einer von einem einheitlichen Vorsatz getragenen Tat an: BGH, Beschluss vom 14.12.2006 - 5 StR 464/06

8.2 materielle Taten beim Skimming

Das Skimming ist in Bezug auf die ausgespähten Kartendaten ein notwendiger Handlungsakt für die geplante Fälschung von Zahlungskarten und die ausgespähten PIN für das geplante Gebrauchen der Dubletten.

In arbeitsteiligen Strukturen gibt der Skimmer jedoch seine Tatherrschaft auf, sobald er die ausgespähten Daten an seine Mittäter übermittelt. Sie bestimmen darüber, wann die weiteren Taten vollendet werden. Wie bei dem vom BGH entschiedenen Fall wegen des Firmenmantels beteiligt sich der Skimmer im Zweifel an nur einer materiellen Tat, auch wenn dem Casher am Ende mehrere Taten vorzuwerfen sind⁸⁹.

Daran ändert sich auch nichts, wenn der Casher mehrere Skimming-Angriffe nacheinander an verschiedenen Orten durchgeführt hat, wenn er dabei die Vorstellung hatte, dass alle Daten im Zusammenhang mit **einem** Cashingangriff missbraucht werden sollen.

Bei der Strafzumessung gemäß § 46 Abs. 2 StGB sind dem Skimmer jedoch „die verschuldeten Auswirkungen der Tat“ zuzurechnen. Das ist der beim Cashing angerichtete Gesamtschaden, auch wenn der Skimmer nicht alle Daten ausgespäht hat, die dabei missbraucht wurden.

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 Verbrechen⁹⁰. Das führt dazu, dass bereits die Verabredung,

⁸⁹ Es reicht der Einsatz einer gefälschten oder verfälschten Karte. Wird sie nur wenige Male missbraucht – hier 10 Fälle des betrügerischen Einsatzes einer Karte – ist ein minder schwerer Fall zu prüfen, nicht aber zwingend anzuwenden: BGH, Urteil vom 21.09.2000 - 4 StR 284/00

⁹⁰ Das BVerfG hat den § 152b StGB geprüft und auch die besonders schwere Strafdrohung in § 152b Abs. 2 StGB nicht beanstandet: BVerfG, Beschluss vom 18.03.2009 - 2 BvR 1350/08

Skimming zu begehen, oder die Anstiftung dazu gemäß § 30 StGB strafbar ist.

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, der als selbständiger Verbrechenstatbestand ausgelegt ist. Darin unterscheidet er sich vom „nur“ gewerbsmäßigen Betrug, der einen besonders schweren Fall des Grundtatbestandes definiert (§ 263 Abs. 3 StGB).

Für den Rücktritt vom Versuch der Beteiligung, so die inoffizielle Überschrift im Gesetzestext, gelten vereinfachte Regeln über den Rücktritt (§ 31 StGB), so dass in aller Regel ein Tatnachweis nicht mehr zu führen ist, sobald mehr Zeit seit der Verabredung verstrichen ist und die Täter nicht zur Tatausführung angesetzt haben.

10. Ergebnisse

Der erfolgreiche Missbrauch einer gefälschten Zahlungskarte dokumentiert, dass ihr eine Zahlungskarte mit Garantiefunktion und dem Zahlungsvorgang eine erfolgreiche Autorisierung zugrunde gelegen haben, wobei die Garantiefunktion bei der Übermittlung des Genehmigungscoodes zum Tragen kam. Der Schaden im Sinne des mit der Tat verbundenen Computerbetruges trat zunächst bei der kartenausgebenden Bank und nach Abschluss des Clearingverfahrens zu Lasten des Bankkunden ein, dessen Daten ausgespäht worden sind.

Das erleichtert die Ermittlungen und die Beweisführung, weil wegen des Cashings die Daten über die Missbrauchsfälle, die die Rechenzentren der Banken oder die EURO Kartensysteme zur Verfügung stellen, alle bedeutsamen Auskünfte geben, ohne dass die Vertragsverhältnisse wegen aller geschädigten Kunden im Einzelnen erhoben und bewertet werden müssen.

Mit der Installation der Skimmer treten die Skimming-Täter in das Versuchsstadium zur Fälschung und zum Gebrauch gefälschter Zah-

lungskarten mit Garantiefunktion ein, so dass sie sich von diesem Moment an strafbar machen. Ihre Tatherrschaft geben sie in dem Moment auf, in dem sie die ausgespähten Daten an ihre Mittäter übermitteln. Von diesem Moment an muss der Täter besondere Anstrengungen unternehmen, wenn er strafbefreiend vom Versuch zurücktreten will (§ 24 StGB).

Schon im Vorfeld des Skimmings ist jedenfalls der Umgang mit den manipulierten Kartenlesegeräten gemäß § 149 StGB unter Strafe gestellt. Das gilt nicht für die Geräte, die zum Ausspähen der PIN eingesetzt werden. Sie dienen nicht zum „Fälschen“, sondern zum „Gebrauchen“ gefälschter Zahlungskarten, das zugleich auch einen Tateinheitlich begangenen Computerbetrug enthält (§ 263a StGB).

Das führt jedenfalls dazu, dass der Täter mit der Installation des Ausspähgerätes für PIN in den Versuch des Computerbetruges eintritt. Entgegen meiner früher geäußerten Ansicht kommt es nicht darauf an, ob tatsächlich eine Zahlungskarte oder eine PIN erfolgreich ausgelesen wurden.

Aufgrund der verschiedenen, auch inländischen Tatorte und dem nach § 6 Nr. 7 StGB geltenden Weltrechtsprinzips sind alle Tatphasen des Skimmings dem deutschen Strafrecht unterworfen. Das gilt auch wegen des Umgangs mit Skimmern im Ausland.

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 ist⁹¹, dass die angedrohte Höchststrafe mehr als 5 Jahre Freiheitsstrafe beträgt. Zuletzt im Zusammenhang mit den Verkehrsdaten hat das BVerfG ausgeführt⁹²:

„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 werden⁹³. Die bisher bekannten Erscheinungsformen im Zusammenhang mit Tätergruppen ausländischer Herkunft lassen zudem geschäftsähnliche Strukturen erkennen⁹⁴.

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 machen⁹⁵.

⁹¹ BVerfG, Urteil vom 03.03.2004 - 1 BvR 2378/97, 1 BvR 1084/99

⁹² BVerfG, Beschluss vom 11.03.2008 - 1 BvR 256/08

⁹³ Nr. 2.3 der Anlage E zu den RiStBV.

⁹⁴ Nr. 2.1 der Anlage E zu den RiStBV.

⁹⁵ 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 ⁹⁶, lassen sich bereits einige Erfahrungswerte formulieren, die für die Bewertung in anderen und neuen Verfahren herangezogen werden können ⁹⁷.

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.

⁹⁶ 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

⁹⁷ Siehe CF, Erfahrungswerte wegen des Skimmings, 29.11.2009

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

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

Es wurde eine gefälschte Zahlungskarte mit Garantiefunktion genutzt.

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

3. Ausspähen

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

3.1 Vorerkundung

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

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

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

3.2 Spezialisten

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

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

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

Daraus folgt:

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

Und:

Skimmer arbeiten arbeitsteilig.

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

3.3 Einsatz

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

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

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

Daraus folgt auch:

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

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

Dieses Vorgehen ist durch Kameraaufnahmen belegt.

4 Abstimmung und Bericht

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

Überraschend viele Belege gibt es dafür, dass die Skimming-Täter, Skimmer wie auch 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.

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.

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

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

EMV-Chip: Im Kartenkörper integrierter Speicherchip, der die Autorisierungsdaten und weitere Informationen enthält (zum Beispiel über Guthaben auf der Karte). Das Kürzel leitet sich von EuroCard, Master und Visa ab.

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

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

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

Garantiefunktion: Auszahlungsgarantie des Kartenausstellers für 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: Ausspähhardware 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. Finanz-Data) 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).

MM: Maschinenlesbares Merkmal; besondere Fälschungssicherung. Im Kartenkörper eingebettete Substanz, die Geldautomaten in Deutschland prüfen müssen.

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

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

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

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

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

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

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

Skimming: a) 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.