Examensklausur: Ein vertanes Talent und die Verlockungen des elektronischen Zahlungsverkehrs

Von Wiss. Mitarbeiter **Sebastian Laudien**, Hannover*

Der Fall wurde im Wintersemester 2014/2015 als Examensklausur im Rahmen des Hannoverschen Examensstudiums (HannES) gestellt. Die Klausur ist als schwer einzustufen. Auch wenn eine Durchfallquote i.H.v. 39% grundsätzlich als gering einzuschätzen ist, so wurde durchschnittlich nur eine Punktzahl von 3,7 Punkten erreicht; die Note „vollbefriedigend" und besser erreichten nur zwei Bearbeiter.

Eine wesentliche Schwierigkeit der Klausur besteht darin, dass die Bearbeiter zunächst erkennen müssen, dass der ggf. exotisch anmutende Sachverhalt bekannte Rechtsgutsverletzungen zum Gegenstand hat. So gilt es Vermögens-, Urkunds-, Sachbeschädigungs- und Geheimnisschutzdelikte (§§ 202a f. StGB) zu prüfen. Auch wenn letztere typischerweise nicht zum Kernbereich der Ausbildung gehören, ist ihre Praxisrelevanz umso größer.[1]

Sachverhalt

Hacker H ist ein begnadetes Talent seiner Zunft. Da er weder Angebote der freien Wirtschaft noch des öffentlichen Dienstes anzunehmen gedenkt, ist er aktuell noch auf prekäre Arbeitsverhältnisse angewiesen. Zurzeit arbeitet er aushilfsweise an der Rezeption eines Hotels. Dort ist er für die Abwicklung der Zahlungsvorgänge zuständig. Aber auch hier schaut sich H nach weiteren Einkommensmöglichkeiten um. Er fasst den Entschluss in das Geschäft mit Kreditkartendaten und -betrügereien einzusteigen.

Um einen ersten Datensatz zu erhalten, präpariert er das handelsübliche Lesegerät an der Hotelrezeption so, dass bei einer Zahlung mittels Kreditkarte (Zahlungskarte mit Garantiefunktion) nicht nur – wie gewohnt – die Kreditkartendaten vom Magnetstreifen für den Zahlungsvorgang ausgelesen werden, sondern unmittelbar vor Beginn dieser Datenübertragung die fraglichen Daten auch auf einem gesondert angebrachten USB-Stick gespeichert werden. Im Zahlungsfall bedient stets der Kunde das Lesegerät. Dabei wird weder der Zahlungsvorgang beeinflusst, noch bedurfte es eines größeren Manipulationsaufwands bezüglich des Lesegeräts, da die Daten unverschlüsselt auf dem Magnetstreifen gespeichert sind. Im Anschluss an die Datenerhebung beabsichtigt H entsprechende Kartendubletten zu erstellen. Doch bevor er damit beginnen kann, fällt ihm auf, dass ihm – unbedacht wie er seinen ersten Coup nun mal angegangen ist – die persönlichen Identifikationsnummern (PINs) der jeweiligen Kreditkarten fehlen, sodass ein Geldabheben – anders als eigentlich beabsichtigt – ohne diese nicht möglich sein wird. Enttäuscht verwirft er daher das weitere Vorgehen und vernichtet den Datensatz.

Nun aber will H professioneller vorgehen. Zu diesem Zweck verschafft er sich Zugang zu gegen unbefugten Zugriff durch Dritte gesondert geschützte Server des Kreditinstituts Cash Unltd. (C), um dort direkt sowohl die Kreditkartendaten, die dazugehörigen Prüfnummern als auch die entsprechenden PINs einer Vielzahl Kunden auszulesen. Dank seiner außerordentlichen IT-Fähigkeiten gelingt es ihm sogar die Kreditkartenlimits der betroffenen Konten aufzuheben, sodass endlich „Geld ohne Ende" fließen könne, so der H. In Besitz der neu gewonnenen Daten fertigt er tags darauf Kreditkarten-Dubletten an, indem er die Magnetstreifen von Kreditkarten-Rohlingen (sog. White-Plastics) mit den entsprechenden Daten bespielt.

Für den „Eigenbedarf" hat sich H insbesondere die Nutzung der Kreditkartendaten seines wohlhabenden Nachbarn N vorbehalten, die zufällig auch Teil des Datensatzes sind. Mit der entsprechenden Dublette ausgestattet, sucht H mehrere Filialen der C auf. An den dortigen Bankautomaten gelingt es ihm unter Eingabe der PIN insgesamt einen Betrag von 25.000 € abzuheben. Am Folgetag fällt H auf, dass er auch einen neuen Fernseher gebrauchen könnte. Kurzerhand bestellt er einen Fernseher im Wert von 5.000 € online als Selbstabholer. Im Rahmen des Zahlungsvorgangs gibt er die Kreditkartendaten des N sowie die dazugehörige Prüfnummer ein. Diese Daten werden angenommen. Da sich N jedoch für Einkäufe in dieser Höhe gesondert für das sog. mTAN-Verfahren angemeldet hatte, stellt sich dem H eine neue Schwierigkeit. Denn nur wenn er zusätzlich die für jeden Einzelkauf mittels SMS an das Handy des N übermittelte mTAN eingibt, kann er den Bestellvorgang über den Fernseher abschließen. Umgehend passt er den N im Hausflur ab und entwendet diesem geschickt dessen Handy. Die transaktionsgebundene mTAN kann er daraufhin erfolgreich einge-

* Der *Verf.* ist Wiss. Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht (Prof. *Dr. Carsten Momsen*) und Mitglied der Forschungsstelle für Bank- und Kapitalmarktrecht sowie Kapitalmarktstrafrecht an der Juristischen Fakultät der Leibniz Universität Hannover.

[1] Vgl. Bundesministerium des Innern, Polizeiliche Kriminalstatistik 2013, S. 67 f. (im Internet abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Pressemitteilungen/2014/06/PKS2013.pdf?__blob=publicationFile [19.5.2015]); Bundeskriminalamt, Bundeslagebild Zahlungskartenkriminalität 2013 (abrufbar unter www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaet__node.html?__nnn=truewww.bka.de [19.5.2015]; Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), BaFinJournal Februar 2015, S. 13 ff. [abrufbar unter http://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2015/bj_1502.html [19.5.2015]; siehe auch exemplarisch für konkrete Vorfälle *Diehl*, Der Spiegel v. 18.8.2014, S. 36; Frankfurter Allgemeine Zeitung v. 17.8.2014 (abrufbar unter http://www.faz.net/-gus-7su7x [19.5.2015]). Den Problemschwerpunkten des Sachverhalts liegen die Entscheidungen BGH, Beschl. v. 14.1.2010 – 4 StR 93/09 = NStZ 2010, 275; BGH, Beschl. v. 6.7.2010 – 4 StR 555/09 = NStZ 2010, 154 (zum sog. Skimming) sowie BGH, Beschl. v. 14.2.2012 – 3 StR 392/11 = NStZ 2012, 627 (zur fehlenden Aneignungskomponente bei Wegnahme) zugrunde.

ben. An dem Handy als solches hat H allerdings keinerlei Interesse, zurückgeben will er es dem N aber auch nicht. Daher zerstört er das Handy schließlich.

Da die Kreditkarte des N innerhalb kürzester Zeit mit enormen Beträgen belastet wurde, schlägt das Überwachungssystem der C Alarm. Das Kreditinstitut setzt sich mit N in Verbindung und lässt nachfragen, ob sich N die fraglichen Zahlungen erklären könne. N, der soeben im Begriff ist eine von seiner Frau schon seit langem ersehnte Kette im Wert von 20.000 € zu kaufen, sieht eine günstige Gelegenheit gekommen. Noch bevor er auf die Nachfrage der C reagiert, flüstert er der Verkäuferin der Kette zu: „Mit Karte, bitte!". Verunsichert aufgrund des diebischen Lächelns nimmt sie die Kreditkarte des N entgegen und – noch bevor dieser das Telefongespräch fortsetzt und die Kreditkarte in der Folge gesperrt werden kann – ist die Kette bezahlt. Dem Angestellten der C gibt er dann noch zu verstehen, dass er im Ausland sei und sich daher die Zahlungsflüsse im Inland nicht erklären könne, er aber selbstverständlich davon ausgehe, dass diese und „etwaige" andere Belastungen – so wie er es aus zahlreichen Verbrauchermagazinen kenne – erstattet würden. Die durch den Angestellten veranlasste Sperrung der Karte kommt freilich zu spät, der Erstattungsbetrag zugunsten des N beläuft sich auf 50.000 €.

Bearbeitervermerk

Prüfen Sie die Strafbarkeit von H und N nach dem StGB. Strafanträge gelten als gestellt. Die §§ 145d, 152 ff., 164 StGB sind nicht zu prüfen.

Lösungsvorschlag

Tatkomplex 1: Auslesen der Daten (sog. Skimming)

I. § 202a Abs. 1 StGB, Ausspähen von Daten

H könnte sich des Ausspähens von Daten nach § 202a Abs. 1 StGB strafbar gemacht haben, indem er im Zuge der Bearbeitung der Zahlungsvorgänge die Kreditkartendaten der Hotelkunden so hat auslesen lassen, dass sie auch ihm persönlich schließlich zur Verfügung standen.[2]

Die auf den Magnetstreifen hinterlegten Kreditkartendaten sind Daten im Sinne des § 202a Abs. 2 StGB.[3] Da die den Kreis der Berechtigten determinierenden kartenausgebenden Kreditinstitute[4] wohl kaum ein Interesse daran haben dürften, dass die Kreditkartendaten ihrer Kunden auch dem H persönlich zur Kenntnis gelangen, ist mit dem Auslesen durch H von einem unbefugten Sich-Verschaffen der Daten auszugehen.[5]

Fraglich ist aber, ob die Kreditkartendaten mit einer besonderen Zugangssicherung versehen waren. Das Auslesen durch H hätte gerade unter Überwindung einer solchen Zugangssicherung erfolgen müssen. Nach dem BGH fehlt es bei Kreditkarten, deren Daten unverschlüsselt auf dem Magnetstreifen gespeichert sind, an einer besonderen Sicherung gegen unberechtigten Zugang im Sinne von § 202a Abs. 1 StGB.[6] H konnte hier die entsprechenden Kreditkartendaten mittels eines handelsüblichen Lesegeräts auslesen. Auch wenn die Sicherung hier auf einem Magnetstreifen erfolgt und die Daten damit nicht unmittelbar wahrnehmbar sind, so ist darin gerade (noch) keine besondere Sicherung zu sehen.[7] Darüber hinausgehende Schutzeinrichtungen, die einen unberechtigten Zugriff ausschließen oder zumindest erheblich erschweren,[8] sind – anders als z.T. bereits in der Praxis bestehend[9]– nicht ersichtlich. Mithin scheiden die betroffenen Kreditkarten als taugliche Tatobjekte im Sinne von § 202a Abs. 1 StGB aus.

II. § 202b StGB, Abfangen von Daten

Das Auslesen und anschließende Speichern der Daten erfolgt unmittelbar vor Beginn der Datenübertragung. Mithin fängt H keine Daten aus einer nichtöffentlichen Datenübermittlung ab, sondern bildet gerade den Empfänger des vorgeschalteten Auslesens der Daten.[10]

III. §§ 263a Abs. 1 Alt. 3, 25 Abs. 1 Alt. 2 StGB, Computerbetrug

Eine Strafbarkeit wegen Computerbetrugs ist nur nach § 263a Abs. 1 Alt. 3 StGB denkbar, denn bei der Kreditkartennutzung durch die Kunden am Lesegerät erfolgt grundsätzlich eine Verwendung richtiger Daten.[11] Tatbestandlich erfasst ist dabei nicht nur die eigenhändige, sondern auch eine mittelbare Eingabe in den Datenverarbeitungsvorgang, bei der sich der Täter einer anderen, vorsatzlos handelnden Person – der jeweiligen Kreditkartenkunden – bedient.[12] Der Streitstand, ob die Verwendung unbefugt vorgenommen wurde („unbefugte Verwendung von Daten") kann hier dahin stehen,[13] da es dem (bloßen) Auslesen der Daten bereits an einer Beeinflussung eines Datenverarbeitungsvorgangs fehlt; denn das Ergebnis des Zahlungsvorgangs wird gerade nicht beeinflusst. Damit besteht keine Strafbarkeit nach § 263a Abs. 1 Alt. 3 StGB.

---

[2] Instruktiv zum Prüfungsaufbau *Jahn*, JuS 2010, 1030 (1031).

[3] *Seidl/Fuchs*, HRRS 2011, 265 (267).

[4] *Lenckner/Eisele*, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 29. Aufl. 2014, § 202a Rn. 8.

[5] Vgl. *Seidl/Fuchs*, HRRS 2011, 265 (267).

[6] BGH, Beschl. v. 14.1.2010 – 4 StR 93/09 = NStZ 2010, 275 und BGH, Beschl. v. 6.7.2010 – 4 StR 555/09 = NStZ 2010, 154.

[7] BGH, Beschl. v. 6.7.2010 – 4 StR 555/09 = NStZ 2010, 154.

[8] *Joecks*, Strafgesetzbuch, Studienkommentar, 11. Aufl. 2014, § 202a Rn. 13.

[9] Hierzu auch *Seidl/Fuchs*, HRRS 2011, 265 f.

[10] *Seidl/Fuchs*, HRRS 2011, 265 (268)

[11] Vgl. *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 62. Aufl. 2015, § 263a Rn. 9.

[12] *Fischer* (Fn. 11), § 263a Rn. 8.

[13] Näher dazu *Wohlers/Mühlbauer*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 2. Aufl. 2014, § 263a Rn. 36 ff; *Fischer* (Fn. 11), § 263a Rn. 10 ff.

IV. § 303b Abs. 1 StGB, Computersabotage

Auch fehlt es einer Strafbarkeit wegen Computersabotage an einem tatbestandlichen Erfolg. Beim (bloßen) Auslesen der Daten fehlt es an einer Verursachung einer erheblichen Störung im Sinne des § 303b Abs. 1 StGB.[14]

V. § 303a Abs. 1 Alt. 4 StGB, Datenveränderung

Gleichsam kommt es auch nicht zu einer rechtswidrigen Veränderung von Daten, sodass auch eine Strafbarkeit wegen Datenveränderung ausgeschlossen ist.

VI. § 303 Abs. 1 StGB, Sachbeschädigung

Auch wenn das Auslesen keine Datenveränderung mit sich bringt, so könnte indes die Manipulation des Lesegeräts eine Sachbeschädigung begründen. Je nach Sachverhaltsinterpretation und entsprechender Darlegung im Rahmen der Prüfung ist hier sowohl die Annahme als auch Ablehnung der Sachbeschädigung betreffend das Tatbestandsmerkmal des Beschädigens als nicht ganz unerhebliches substantielles Einwirken nach § 303 Abs. 1 StGB vertretbar.[15] Regelmäßig wird es beim Skimming aber nicht zu Substanzeinwirkungen kommen.

VII. §§ 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB, Fälschung beweiserheblicher Daten

H beabsichtigt mit den ausgelesenen Daten Kartendubletten zu erstellen. Hierfür ist zunächst deren Speicherung auf einem USB-Stick erforderlich. Auch wenn die gespeicherten Daten für sich mangels Wahrnehmbarkeit, also fehlender Perpetuierung, (noch) keine unechte Urkunde im Sinne von § 267 StGB darstellen,[16] so könnte sich H gleichwohl mit der Speicherung wegen Fälschung beweiserheblicher Daten in mittelbarer Täterschaft nach §§ 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB strafbar gemacht haben, indem er die unwissenden Kreditkartenkunden dazu veranlasst an dem von ihm präparierten Lesegerät zu zahlen, um so die Daten vom Magnetstreifen auslesen und sie schließlich auf dem USB-Stick speichern zu können.

1. Objektiver Tatbestand

Als beweiserhebliche Daten gelten solche, die dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden,[17] d.h. für ein Rechtsverhältnis Beweis zu erbringen.[18] Die den Zahlungsvorgang ermöglichenden Kreditkartendaten bilden solche Daten, denn die auf dem Magnetstreifen hinterlegten Daten beinhalten eine Garantieerklärung des kartenausgebenden Kreditinstituts zugunsten des Karteninhabers.[19]

Mit der Sicherung auf dem USB-Stick speichert H die Daten auch in der Weise, dass bei Überführung in ein wahrnehmbares Falsifikat – bspw. durch Erstellung einer Kartendublette auf der Grundlage dieser Daten – eine unechte Urkunde vorliegen würde; denn allein die auf dem Magnetstreifen hinterlegten Daten genügen, um bei Erstellung einer Kartendublette den Anschein einer weiteren Gedankenerklärung zu erregen.[20] Die Kenntnis der PIN braucht es dafür nicht.

Die unwissenden Kreditkartenkunden handeln im Zeitpunkt des Zahlungsvorgangs als absichtslos-doloses Werkzeug bezüglich des Speicherns und mithin der Fälschung beweiserheblicher Daten im Sinne von § 269 Abs. 1 Alt. 1 StGB.

2. Subjektiver Tatbestand

H handelt demgegenüber gerade mit dem Willen, die Kreditkartenkunden kraft überlegenden Wissens zum Zwecke der Speicherung der beweiserheblichen Daten einzusetzen, indem er sie zur Zahlung am Lesegerät veranlasst. Somit handelt er vorsätzlich als mittelbarer Täter.

Zudem kam es H gerade darauf an, die beweiserheblichen Daten zu speichern; mithin handelte er vorsätzlich bezüglich des objektiven Tatbestands. Auch handelt H im Zeitpunkt der Tat mit dem Willen die beweiserheblichen Daten, wenn auch nicht zur Täuschung im Rechtsverkehr, so jedoch wohl zur nach § 270 StGB gleichgestellten fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr einzusetzen, weil er die Kartendubletten für Geldabhebungen an einem Automaten einzusetzen beabsichtigte. Dass H das weitere Vorgehen nach der Speicherung verwirft, ist unbeachtlich.

> *Hinweis*: Wird unter dem Begriff des Geldabhebens indes die Nutzung eines Bankschalters verstanden, so bliebe es in Bezug auf den zu täuschenden Schalterangestellten bei einer Täuschung im Rechtsverkehr.

3. Rechtswidrigkeit/Schuld

> *Hinweis*: An dieser Stelle ist allein mit dem Behauptungsstil (Urteilsstil) zu operieren, mithin verbietet sich eine gutachterliche Darstellung des Prüfungspunktes.[21]

4. Strafzumessung

H könnte Regelbeispiele nach § 269 Abs. 3 i.V.m. § 267 Abs. 3 StGB verwirklicht haben. H schaut sich nach weiteren Einkommensquellen um und beabsichtigt in das Geschäft mit Kreditkartendaten und -betrügereien einzusteigen, sodass davon auszugehen ist, dass er sich dergestalt durch wiederholte Tatbegehung eine nicht nur vorübergehende und nicht

[14] Näher *Stree/Hecker*, in: Schönke/Schröder (Fn. 4), § 303b Rn. 9.
[15] *Fischer* (Fn. 11), § 303 Rn. 6.
[16] Vgl. *Joecks* (Fn. 8), § 269 Rn. 1.
[17] *Fischer* (Fn. 11), § 269 Rn. 4.
[18] *Joecks* (Fn. 8), § 269 Rn. 6.
[19] *Seidl/Fuchs*, HRRS 2011, 265 (268 f.).
[20] *Seidl/Fuchs*, HRRS 2011, 265 (268).
[21] Instruktiv zur Wahl des (jeweils) sachangemessenen Stils in der (Klausur-)Bearbeitung *Lagodny/Mansdörfer/Putzke*, ZJS 2014, 157 (159).

ganz unerhebliche Einnahmenquelle verschaffen will; mithin handelt er gewerbsmäßig im Sinne von Abs. 3 Nr. 1.[22]

Hinweis: Bei entsprechender Darstellung ist freilich auch Gegenteiliges vertretbar.

Auch könnte H die Sicherheit des Rechtsverkehrs angesichts der großen Zahl der betroffenen beweiserheblichen Daten gem. Abs. 3 Nr. 3 erheblich gefährdet haben. Das Vorliegen einer solchen Gefährdung ist normativ zu bestimmen.[23] Selbst wenn also die z.T. in der Lit. vertretene Grenze von 20 Tatobjekten wohl überschritten worden sein dürfte,[24] so fehlt es gleichwohl an hinreichenden Hinweisen darauf, dass bereits damit eine erhebliche Beeinträchtigung der Sicherheit des Rechtsverkehrs gegeben ist. Nicht zuletzt verwirft H – noch bevor er erste Dubletten herstellen kann – das weitere Vorgehen.

5. Ergebnis

H hat sich nach § 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB strafbar gemacht.

Tatkomplex 2: Zugriff auf die Server der C/Aufheben der Kreditkartenlimits/Erstellung der Kreditkarten-Dubletten

I. § 202a StGB, Ausspähen von Daten

Indem sich H Zugang zu den mit besonderer Zugangssicherung versehenen Servern der C verschafft und dort Kreditkartendaten einschließlich Prüfnummern und PINs einer Vielzahl Kunden ausliest, hat er sich Zugriff auf Daten im Sinne von § 202a Abs. 2 StGB, die nicht für ihn bestimmt sind, unter Überwindung einer besonderen Zugangssicherung verschafft. H handelt vorsätzlich, rechtswidrig und schuldhaft. Von einer Strafantragsstellung nach § 205 Abs. 1 StGB ist auszugehen. Mithin besteht eine Strafbarkeit nach § 202a Abs. 1 StGB.

II. § 303a Abs. 1 Alt. 4 StGB, Datenveränderung

Mit der Aufhebung der Kreditkartenlimits hat H, ohne dazu befugt zu sein, den Informationsgehalt (Aussagewert) der jeweiligen Kreditkartendaten (Daten im Sinne von § 202a Abs. 2 StGB, s.o.), insoweit verändert, als sie ihren ursprünglichen Verwendungszweck – den Verfügungsrahmen für die einzelnen Kreditkarten zu begrenzen – nicht länger erfüllen.[25] Da ein Strafantrag nach § 303c StGB als gestellt gilt, besteht somit auch eine Strafbarkeit nach § 303a Abs. 1 Alt. 4 StGB.

III. § 269 Abs. 1 Alt. 1 StGB, Fälschung beweiserheblicher Daten

Um die ausgespähten Kreditkartendaten auf die Magnetstreifen der Karten-Rohlinge spielen zu können, ist es zwingend erforderlich auch diese zuvor auf einem Datenträger zu speichern, wobei H erneut beweiserhebliche Daten in der Weise speichert, dass bei anschließender Erstellung der Kartendubletten eine unechte Urkunde vorliegt (s.o.). H handelt abermals vorsätzlich bezüglich der Merkmale des objektiven Tatbestands sowie mit dem Willen einen Datenverarbeitungsvorgang im Rechtsverkehr fälschlich beeinflussen zu wollen (§ 270 StGB, vgl. oben). Rechtswidrigkeit und Schuld sind gegeben. Aus strafzumessungsrechtlicher Sicht ist auch hier von gewerbsmäßigem Handeln (§ 269 Abs. 3 i.V.m. § 267 Abs. 3 Nr. 1 StGB) auszugehen. Da H Dubletten auf der Grundlage aller erhaltenen Kreditkartendaten anfertigt, kann davon ausgegangen werden, dass auch ohne Kenntnis über deren weitere Verwendung eine erhebliche Gefährdung für die Sicherheit des Rechtsverkehrs besteht, denn die Vielzahl betroffener Kunden dürfte sich, wenn sie von dem Ausspähen ihrer Daten Kenntnis hätte, veranlasst sehen, rechtserheblich aktiv zu werden.[26] Somit hat sich H nach § 269 Abs. 1 Alt. 1 StGB strafbar gemacht.

IV. § 267 Abs. 1 Alt. 1 StGB, Urkundenfälschung

Mit der Überführung der Kreditkartendaten in wahrnehmbare Kartendubletten bilden diese nun auch verkörperte menschliche Gedankenerklärungen. Da sie die C als kartenausgebendes Kreditinstitut bei gewöhnlicher Nutzung im Bankautomatenverkehr als Aussteller der Kartendubletten erkennen lassen,[27] obwohl deren tatsächlicher Aussteller der H ist, besteht auch eine Strafbarkeit nach § 267 Abs. 1 Alt. 1 StGB wegen Herstellung unechter Urkunden. Bezüglich § 267 Abs. 3 StGB gilt das zu § 269 Abs. 3 StGB Gesagte entsprechend.

V. Konkurrenzen

§ 269 StGB tritt neben § 267 StGB, da die Dubletten die Garantieerklärung zugunsten der Karteninhaber sowohl optisch wahrnehmbar als auch in magnetisch codierter Form auf dem Magnetstreifen mit sich führen.[28] Auch im Übrigen stehen die Delikte in Idealkonkurrenz.

Tatkomplex 3: Einsatz der Dublette der Kreditkarte des N/Kauf des Fernsehers

I. § 263a Abs. 1 Alt. 3 StGB, Computerbetrug (durch das Geldabheben)

Indem H an den Bankautomaten der C mit Hilfe der Dublette der Kreditkarte des N Geld abhebt, könnte er sich des Computerbetrugs strafbar gemacht haben.

[22] Ausführlich *Fischer* (Fn. 11), Vor § 52 Rn. 61 f.
[23] Vgl. *Fischer* (Fn. 11), § 267 Rn. 54.
[24] *Wittig*, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 2. Aufl. 2014, § 267 Rn. 100 m.w.N; a.A. *Heine/Schuster*, in: Schönke/Schröder (Fn. 4), § 267 Rn. 108.
[25] Näher *Stree/Hecker* (Fn. 14), § 303a Rn. 2 ff., 8.
[26] Vgl. *Heine/Schuster* (Fn. 23), § 267 Rn. 108.
[27] Näher zum Begriff der Gedankenerklärung i.S.d. § 267 StGB *Fischer* (Fn. 11), § 267 Rn. 3; vgl. hierzu auch *Seidl/Fuchs*, HRRS 2011, 265 (268).
[28] *Erb*, in: Joecks/Miebach (Fn. 13), § 267 Rn. 221.

1. Objektiver Tatbestand

Da die auf dem Magnetstreifen der Dublette kopierten Kreditkartendaten denen auf der Originalkarte entsprechen, vermitteln beide den gleichen Informationsgehalt. Mithin ist auch im Einsatz der Dublette eine Verwendung richtiger Daten im Sinne von § 263a StGB zu sehen.[29] Die Verwendung müsste unbefugt erfolgt sein. Berechtigter Karteninhaber ist der N. Bedient sich indes H dieser Daten mittels der erstellten Dublette, so erfolgt dies ohne Berechtigung der kartenausgebenden C, die die Garantieerklärung nur zugunsten des N erteilt hat (s.o.). Erfolgt nun mit Hilfe der Dublette eine Eingabe dieser Daten in den Datenverarbeitungsvorgang der Bankautomaten, so ist zwar das Ergebnis inhaltlich richtig, da die eingegebenen Daten einschließlich PIN grundsätzlich zur Abhebung berechtigen; jedoch nur in Bezug auf N. Die Auszahlung an H stellt damit insofern ein kausal herbeigeführtes unzutreffendes und beeinflusstes Ergebnis eines Datenverarbeitungsvorgangs dar, als die Auszahlung unbefugtermaßen erfolgt.[30]

Die Auszahlungen wirken unmittelbar vermögensmindernd. Fraglich ist aber, ob und bei wem ein kausaler Vermögensschaden eintritt. Zwar wird mit den Abhebungen das Konto des N im Verhältnis zu C auf der Grundlage des mit ihr geschlossenen Zahlungsdienstevertrags (§ 675f BGB) belastet, diese Zahlungsvorgänge sind aber nach § 675j Abs. 1 S. 1 BGB nur dann gegenüber N wirksam, wenn dieser den Zahlungsvorgängen zugestimmt hat. An einer solchen Autorisierung fehlt es hier aber gerade, sodass N gegen die C gem. § 675u S. 2 BGB einen Anspruch auf Erstattung der Überweisungsbeträge hat. Einwendungen dagegen sind nicht ersichtlich. Mithin lässt sich in Bezug auf N bei einem Vergleich der Gesamt-Vermögenslage vor und nach den (Einzel-)Verfügungen kein Vermögensschaden feststellen.[31] Gleichwohl lässt sich ein solcher aufseiten der C feststellen, denn diese trägt den wirtschaftlichen Schaden der durch sie getätigten Auszahlungen.

2. Subjektiver Tatbestand

H handelt mit Vorsatz bezüglich der Merkmale des objektiven Tatbestands. Auch kommt es ihm gerade darauf an sich einen Vermögensvorteil zu verschaffen; mithin handelt H mit dem Willen eine rechtswidrige, stoffgleiche Bereicherung vorzunehmen.

3. Rechtswidrigkeit/Schuld

Hinweis: Siehe Fn. 21.

4. Strafzumessung

Insoweit man die Abhebungen auch im Zusammenhang mit dem Ausgangsmotiv des H sieht, weitere Einnahmequellen erschließen zu wollen, ist abermals das Regelbeispiel des gewerbsmäßigen Handelns (§ 263a Abs. 2 i.V.m. § 263 Abs. 3 Nr. 1) erfüllt. Von einem Vermögensverlust großen Ausmaßes (Abs. 3 Nr. 2) kann bei einem Gesamtbetrag von 25.000 € regelmäßig noch nicht ausgegangen werden.[32]

5. Ergebnis

H hat sich nach § 263a Abs. 1 Alt. 3 StGB strafbar gemacht.

II. § 263a Abs. 1 Alt. 3 StGB, Computerbetrug (durch die Internetbestellung)

Mit der Eingabe der Kreditkartendaten, der Prüfnummer sowie der transaktionsgebundenen mTAN nimmt H erneut eine Verwendung richtiger Daten im Sinne von § 263a Abs. 1 Alt. 3 StGB vor (s.o.). Gleichermaßen führt auch die Eingabe im Rahmen des Bestellvorgangs insofern zu einem kausal herbeigeführten unzutreffenden Ergebnis eines Datenverarbeitungsvorgangs, als die Überprüfung der Kreditkartendaten (einschließlich Prüfnummer) sowie der mTAN grundsätzlich eine Berechtigung zur Zahlung mit der Kreditkarte des N suggerieren, ihre Verwendung gleichwohl aber unbefugtermaßen erfolgt.

H handelt vorsätzlich, rechtswidrig und schuldhaft. Aus strafzumessungsrechtlicher Sicht gilt das unter I. 4. Gesagte entsprechend. Es besteht eine Strafbarkeit nach § 263a Abs. 1 Alt. 3 StGB.

III. § 242 Abs. 1 StGB, Diebstahl

Das Handy des N ist eine fremde bewegliche Sache für H. Mit dessen Entwendung bricht er fremden und begründet eigenen Gewahrsam; verwirklicht also das objektive Tatbestandsmerkmal der Wegnahme.

Bezüglich der Verwirklichung der objektiven Tatbestandsmerkmale ist ihm jedenfalls dolus eventualis vorzuwerfen. H müsste zudem mit Zueignungsabsicht gehandelt haben. H wollte zwar Zugriff auf das Handy des N nehmen, jedoch nur deshalb, um sich anschließend in Kenntnis der mTAN zu setzen. Mithin ist fraglich, ob H somit auch mit dem Willen handelt, das Handy wenigstens vorübergehend in seinen Vermögensbestand aufnehmen zu wollen (Aneignungsabsicht). Nach Auffassung des BGH fehlt es an einer Aneignungskomponente, wenn der Täter nur die (bloße) Verwertung der auf einem Datenträger gespeicherten Daten unter Zuhilfenahme des die Daten beinhaltenden Geräts beabsichtigt.[33] Hier besteht gerade kein darüber hinausgehendes vermögensrelevantes Interesse des H; im Zeitpunkt der Wegnahme beabsichtigte er sich weder den Substanz- oder Sachwert des Handy anzueignen noch dessen Wert durch den vorübergehenden Gebrauch zu mindern.[34] Die ausgeübte Eigen-

[29] *Wohlers/Mühlbauer* (Fn. 13), § 263a Rn. 28.

[30] *Seidl/Fuchs*, HRRS 2011, 265 (271); vgl. auch BGH, Urt. v. 22.11.1991 – 2 StR 376/91 = NStZ 1991, 180; *Joecks* (Fn. 8), § 263a Rn. 25.

[31] *Fischer* (Fn. 11), § 263 Rn. 88.

[32] Anstatt vieler *Fischer* (Fn. 11), § 263 Rn. 215a.

[33] BGH, Beschl. v. 14.2.2012 – 3 StR 392/11 = NStZ 2012, 627.

[34] Vgl. BGH, Beschl. v. 14.2.2012 – 3 StR 392/11 = NStZ 2012, 627; zust. *Wessels/Hillenkamp*, Strafrecht, Besonderer Teil, Bd. 2, 37. Aufl. 2014, Rn. 152; *Hecker*, JuS 2013, 468 (469); abl. *Jäger*, JA 2012, 709 f.; weitere Fälle, in denen es

macht beschränkte sich hier ausschließlich auf das Interesse der – hier aufgrund fehlender Überwindung besonderer handyeigener Zugangssicherungen – tatbestandslosen Ausspähung der mTAN.[35] Auch dürfte zweifelhaft sein, ob H im Zeitpunkt der Wegnahme bereits mit Enteignungsvorsatz handelt, da der Entschluss, das Handy schließlich zerstören zu wollen, im Zeitpunkt der Wegnahme noch nicht abschließend gefasst war. Mithin besteht keine Strafbarkeit nach § 242 Abs. 1 StGB.

IV. § 246 Abs. 1 StGB, Unterschlagung

Auch fehlt es in Bezug auf die Zerstörung des Handy an einer Manifestation des Zueignungswillens. Eine äußerlich in Erscheinung tretende Zueignungshandlung, die sich nach Maßgabe der auf eine vermögensrelevante Bestandsänderung abzielende Zueignungsabsicht gem. § 242 StGB bestimmt,[36] kann bereits gedankenlogisch nicht in der Zerstörung des Handy gesehen werden, da dies gerade kein Verhalten zum Ausdruck bringt, wonach sich H die Sache selbst oder den in ihr verkörperten Wert zumindest vorübergehend aneignet. Dies ist allein für den Fall des eigennützigen – also bestimmungsgemäßen – Verbrauchs einer Sache denkbar.[37]

Mit der Zerstörung des Handys hat sich H also auch nicht nach § 246 Abs. 1 StGB strafbar gemacht.

V. § 303 Abs. 1 StGB, Sachbeschädigung

Mit der Zerstörung des Handy verwirklicht H aber eine Strafbarkeit nach § 303 Abs. 1 StGB.

VI. § 269 Abs. 1 Alt. 3 StGB, Fälschung beweiserheblicher Daten

Sowohl durch das Geldabheben mittels Dublette als auch durch Eingabe der Kreditkarten im Rahmen des Bestellvorgangs gebraucht H die zuvor tatbestandlich gespeicherten beweiserheblichen Daten.

VII. § 267 Abs. 1 Alt. 3 StGB, Urkundenfälschung

Jedenfalls der Einsatz der Kartendublette begründet auch eine Strafbarkeit nach § 267 Abs. 1 Alt. 3 StGB wegen Gebrauchens einer unechten Urkunde.

VIII. Konkurrenzen

Idealkonkurrenz (§ 52 StGB) besteht jeweils für den Einsatz der Dublette der Kreditkarte des N bzw. den Kauf des Fernsehers zwischen §§ 263a, 267 Abs. 1 Alt. 3, 269 Abs. 1 Alt. 3 StGB. Zudem bildet §§ 267 Abs. 1 Alt. 3, 269 Abs. 1 Alt. 3 StGB nach ständiger Rechtsprechung mit den in Tatkomplex 2 verwirklichten Urkundsdelikten nur eine Tat.[38] Im Übrigen besteht zwischen den Strafbarkeiten in Tatkomplex 3 Realkonkurrenz (§ 53 StGB).

Tatkomplex 4: Die Zahlung des N

I. § 266 Abs. 1 StGB, Untreue

Für eine Untreue-Strafbarkeit fehlt es dem N bereits an einer (echten) Vermögensbetreuungspflicht im Sinne des § 266 Abs. 1 StGB gegenüber dem kartenausstellenden Kreditinstitut, der C.

II. § 266b Abs. 1 Alt. 2 StGB, Missbrauch von Scheck- und Kreditkarten

Gleichwohl könnte sich N nach § 266b Abs. 1 Alt. 2 StGB strafbar gemacht haben, indem er die ihm von der C als Aussteller überlassene Kreditkarte missbräuchlich einsetzt und C damit zu einer Zahlung veranlasst. In der Tat veranlasst N mit dem Kauf der Kette die C wirksam zur Zahlung i.H.v. 20.000 €. Fraglich ist aber, ob N damit missbräuchlich handelt. Missbräuchlich handelt, wer wirksam nach außen, im Rahmen seines rechtlichen Könnens, die ihm im Innenverhältnis gesetzten Grenzen (rechtliches Dürfen) überschreitet.[39] Die Missbrauchsmöglichkeiten durch den berechtigten Karteninhaber ergeben sich daher aus dessen vertraglichen Hauptpflichten gegenüber dem Aussteller; (bloße) Nebenpflichtverletzungen vermögen nicht die mit dem Merkmal des Missbrauchs im Sinne des § 266b Abs. 1 StGB geforderten gravierenden Vertragsverletzungen zu begründen.[40] Die vertraglichen Hauptpflichten des berechtigten Karteninhabers beschränken sich regelmäßig darauf, dass die Kreditkarte nur innerhalb des vereinbarten Verfügungsrahmens zu nutzen ist (vgl. § 675k BGB) und die Forderungen des Ausstellers jeweils zum Fälligkeitszeitpunkt zu befriedigen sind.[41] Ein Verfügungsrahmen besteht für die Kreditkarte des N ohnehin nicht mehr (s.o.). Auch ist von der Solvenz des N auszugehen. Ob auch darüber hinausgehende Rücksichtnahmepflichten bestehen, die ggf. dadurch verletzt worden sind, dass N die Kreditkarte nutzt, obwohl er von C kontaktiert und mit dem Verdacht des Missbrauchs seiner Kreditkartendaten konfrontiert wird und zudem daraufhin wahrheitswidrig angibt, dass er sich im Ausland aufhalte – mithin also weder für die fraglichen noch weitere inländische Belastungen verantwortlich ist –, ist nicht relevant, da diese allenfalls unbeachtliche Nebenpflichtverletzungen zu begründen vermögen. Mithin fehlt es an einer missbräuchlichen Nutzung der Kreditkarte.

III. § 263a Abs. 1 Alt. 3 StGB, Computerbetrug

Auch hat N mit der Zahlung unter Nutzung seiner Kreditkarte keine richtigen Daten zur Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs verwendet, da er die Daten – anders als in Tatkomplex 3 I. – gerade nicht unbefugterma-

an einer Aneignungskomponente fehlt BGH, Urt. v. 27.1.2011 – 4 StR 502/10 = NStZ 2011, 699 (Kutten-Fall); OLG Nürnberg, Beschl. v. 7.11.2012 – 1 StOLG Ss 258/12 = NStZ-RR 2012, 78 (Fanjacken-Fall).

[35] Vgl. *Hecker*, JuS 2013, 468 (469).

[36] Vgl. *Wessels/Hillenkamp* (Fn. 33), Rn. 309.

[37] *Wessels/Hillenkamp (Fn. 33)*, Rn. 153.

[38] Vgl. *Fischer* (Fn. 11), § 267 Rn. 58; § 269 Rn. 12.

[39] BGH, Beschl. v. 3.12.1991 – 4 StR 538/91 = NStZ 1991, 278; *Joecks* (Fn. 8), § 266b Rn. 12.

[40] BGH, Beschl. v. 3.12.1991– 4 StR 538/91 = NStZ 1991, 278 (279).

[41] *Rengier*, in: Hilgendorf (Hrsg.), Festschrift für Wolfgang Heinz zum 70. Geburtstag, 2012, S. 808 (813 f.).

ßen einsetzt. Dies wäre nur denkbar, wenn die Kreditkarte bereits im Zeitpunkt der Zahlung gesperrt gewesen und eine Zahlung gleichwohl erfolgt wäre.

IV. § 263 Abs. 1 StGB, Betrug (ggü. dem Angestellten der C, zulasten der C)

Mit der wahrheitswidrigen Aussage, dass er derzeit im Ausland sei und daher im Inland keine Zahlungen der C veranlassen könne, täuscht N den für die C handelnden Bankangestellten über die Tatsache, dass er soeben die Zahlung der Kette vorgenommen hat (Dreiecksbetrug). Aufgrund dessen besteht auf Seiten der C irrtümlich der Eindruck, dass auch die mit dem Kauf der Kette einhergehende Belastung auf eine missbräuchliche Nutzung der Kreditkartendaten des N durch Dritte zurückzuführen ist. Infolgedessen verfügt der Angestellte der C vermögenswirksam in Gestalt des Erstattungsbetrags i.H.v. 50.000 €. Da jedoch in der Zahlung der Kette ein autorisierter Zahlungsvorgang zu sehen ist, besteht nach § 675u S. 1 BGB tatsächlich nur ein Erstattungsanspruch i.H.v. 30.000 € des N gegen die C. Somit besteht ein Vermögensschaden in Höhe des Kaufpreises der Kette (20.000 €).

N handelt vorsätzlich bezüglich der Merkmale des objektiven Tatbestands. Auch wollte er sich gerade um den in der Kette liegenden rechtswidrigen, stoffgleichen Vermögensvorteil bereichern. N handelt rechtswidrig und schuldhaft. Demnach besteht eine Strafbarkeit nach § 263 Abs. 1 StGB.