

I. Einleitung

Wenngleich Bargeld in Deutschland nach wie vor das beliebteste Zahlungsmittel darstellt, nimmt die Bedeutung des unbaren Zahlungsverkehrs stetig zu. Nach einer Studie der Bundesbank wurden im Jahr 2021 im stationären Handel zwar noch 58 % der Transaktionen in bar gezahlt; an zweiter und dritter Stelle stehen Zahlungen mit Debitkarte (32 %) und Kreditkarte (6 %); betrachtet man den Anteil am Umsatz, so liegt allerdings bereits die Debitkarte an erster Stelle (48 %), gefolgt von Bargeld (36 %) und Kreditkarte (10 %).¹ Der Rückgang von Barzahlungen ist dabei nicht nur auf die Pandemie zurückzuführen, sondern auch darauf, dass bargeldloses Zahlen einfacher geworden ist.² So kann der Inhaber einer Debitkarte kleinere Beträge allein dadurch bezahlen, dass er die Karte an ein Lesegerät hält und die für die elektronische Zahlung erforderlichen Daten kontaktlos übertragen werden (Near-Field-Communication, NFC); eine Eingabe der PIN oder eine Unterschrift sind nicht mehr erforderlich. Im Jahr 2021 wurden bereits zwei von drei Zahlungen mit einer Debitkarte auf diese Weise abgewickelt.³ Die Kartenzahlung wird auf diese Weise nicht nur für den Kunden einfacher und damit attraktiver, sondern ist auch für die Händler vorteilhaft, die nicht nur von der Erleichterung und Beschleunigung des Bezahlvorgangs, sondern auch davon profitieren, dass die für die Abwicklung von Barzahlungen erforderlichen Logistikkosten und -risiken sinken.⁴

* Prof. Dr. Martin Böse ist Inhaber des Lehrstuhls für Strafrecht und Strafprozessrecht sowie Internationales und Europäisches Strafrecht und Geschäftsführender Direktor des Instituts für Strafrecht an der Rheinischen Friedrich-Willhelms-Universität Bonn. Lucas Tomiak ist Wissenschaftlicher Mitarbeiter an diesem Lehrstuhl.

¹ Deutsche Bundesbank, Zahlungsverhalten in Deutschland, Juli 2022, S. 31, abrufbar unter

<https://www.bundesbank.de/de/presse/pressemitteilungen/zahlungsverhalten-in-deutschland-2021-894082> (19.7.2023).

² Deutsche Bundesbank (Fn. 1), S. 40.

³ Deutsche Bundesbank (Fn. 1), S. 26: Danach entfielen 22,6 % der Transaktionen auf Debitkarten; davon wurden 7 % mit PIN oder Unterschrift und 15,1 % kontaktlos abgewickelt.

⁴ Kanning, FAZ v. 13.1.2016, S. 23, abrufbar unter

<https://www.faz.net/aktuell/finanzen/meine-finanzen/geld-ausgeben/neue-technik-einkaufen-mit-karte-aber-ohne-pin-14010827.html> (19.7.2023);

Cabinakova/Knümann/Horst, Kosten der Bargeldzahlung im Einzelhandel, Studie zur Ermittlung und Bewertung der Kosten, die durch die Bargeldzahlung im Einzelhandel verursacht werden, 2019, insb. die Simulationen auf S. 69 ff., abrufbar unter

<https://www.bundesbank.de/resource/blob/776464/d0ff995f570846f130e425a4bf003bd9/mL/kosten-der-bargeldzahlung-im-einzelhandel-data.pdf> (19.7.2023).

Ungeachtet dieser Vorteile geht mit dem kontaktlosen Bezahlen allerdings auch ein erhöhtes Missbrauchsrisiko einher, wenn die Debitkarte dem Karten- bzw. Kontoinhaber abhandenkommt und von einem Dritten zur bargeldlosen Zahlung eingesetzt wird. In derartigen Fällen stellt sich nicht nur die Frage, wer das Missbrauchsrisiko und damit den Schaden trägt, sondern auch, ob und inwieweit ein solcher Missbrauch nach geltendem Recht mit Strafe bedroht ist. Der folgende Beitrag geht dieser Frage nach, konzentriert sich dabei allerdings auf die Vermögensdelikte, d.h. den Betrug (§ 263 StGB) und den Computerbetrug (§ 263a StGB). Das OLG Hamm hat eine Strafbarkeit nach diesen Vorschriften verneint⁵ und ist damit im Schrifttum überwiegend auf Zustimmung gestoßen⁶. Die für die Auslegung des Gerichts maßgeblichen Gründe sollen referiert und anschließend kritisch hinterfragt werden (III.). Zuvor sollen allerdings die zivilrechtlichen Grundlagen des kontaktlosen Zahlens dargelegt werden, da diese auch für die strafrechtliche Bewertung maßgebliche Bedeutung entfalten (II.).

II. Zivilrechtliche Grundlagen

1. Zahlung mit Debit- und Kreditkarten

a) Debitkarte

Betrachtet man die Zahlung mit einer Debitkarte (Bankkundenkarte, Girokarte), so sind am Bezahlvorgang der Konto- bzw. Karteninhaber, die Bank und der Händler beteiligt. Dementsprechend sind die rechtlichen Beziehungen zwischen Karteninhaber (Zahler) und seiner Bank als Zahlungsdienstleister (Deckungsverhältnis), zwischen Karteninhaber als Zahler bzw. Kunden und Händler als Zahlungsempfänger (Valutaverhältnis) und zwischen Händler und Bank (Zuwendungs- oder Vollzugsverhältnis) zu unterscheiden.

Ausgangspunkt ist zunächst das Verhältnis zwischen Karteninhaber und Händler (Valutaverhältnis): Indem der Kunde die Ware an der Kasse vorlegt, unterbreitet er ein Angebot zum Abschluss eines Kaufvertrages (§ 433 BGB), das der

⁵ OLG Hamm, Beschl. v. 7.4.2020 – 4 RVs 12/20 = NStZ 2020, 673 = BeckRS 2020, 9059.

⁶ Christoph/Dorn-Haag, NStZ 2020, 676; dies., NStZ 2020, 697 (701 f.); Duttge, in: Dölling/Duttge/König/Rössner (Hrsg.), *Gesamtes Strafrecht, Handkommentar*, 5. Aufl. 2022, § 263a Rn. 19; Eisele, *Strafrecht, Besonderer Teil II*, 6. Aufl. 2021, Rn. 681; Göhler, JR 2021, 6 (17 f.); Heger, in: Lackner/Kühl/Heger (Hrsg.), *Strafgesetzbuch, Kommentar*, 30. Aufl. 2023, § 263a Rn. 13a; Heghmanns, ZJS 2020, 494 (496); Hefendehl/Noll, in: Erb/Schäfer (Hrsg.), *Münchener Kommentar zum Strafgesetzbuch*, Bd. 5, 4. Aufl. 2022, § 263a Rn. 109; Rengier, *Strafrecht, Besonderer Teil I*, 25. Aufl. 2023 § 14 Rn. 46; Schramm, *Strafrecht, Besonderer Teil II*, 2. Aufl. 2020, § 8 Rn. 38 f.; ablehnend Puschke/Haas, RdZ 2022, 4 (8 f.); Schmidt, in: v. Heintschel-Heinegg (Hrsg.), *Beck'scher Online-Kommentar, Strafgesetzbuch*, Stand: 1.5.2023, § 263a Rn. 29.

Händler (bzw. eine von diesem bevollmächtigte Person) annimmt. Die vertragliche Verpflichtung zur Zahlung des Kaufpreises (§ 433 Abs. 2 BGB) kann der Kunde mit Bargeld erfüllen; in diesem Fall erlischt der Anspruch sofort (§ 362 Abs. 1 BGB). Sofern der Händler auch die Kartenzahlung akzeptiert, ist diese nach h.M. als Leistung erfüllungshalber anzusehen (§ 364 Abs. 2 BGB analog), d.h. der Zahlungsanspruch wird nur gestundet, der Händler ist aber verpflichtet, Erfüllung aus der Kartenzahlung zu suchen.⁷

Für die Erfüllung der Forderung per Kartenzahlung ist der Kunde auf die Mitwirkung seiner Bank angewiesen. Im Deckungsverhältnis ist die Bank aufgrund des mit dem Konto- und Karteninhaber geschlossenen Zahlungsdienstvertrags zur Ausführung der von dem Kunden erteilten Zahlungsaufträge verpflichtet (§ 675f Abs. 2 S. 1, Abs. 4 BGB). Die Debitkarte ist ein von der Bank zur Erteilung von Zahlungsaufträgen ausgegebenes Zahlungsinstrument (vgl. § 675c Abs. 3 BGB i.V.m. § 1 Abs. 20 ZAG), das insbesondere im sogenannten Point-of-Sale-Verfahren (POS-Verfahren) zur Bezahlung von Waren oder Dienstleistungen eingesetzt werden kann. In diesem Verfahren erteilt der Karteninhaber mit der Vorlage der Karte und der Eingabe der PIN seiner Bank nicht nur einen Zahlungsauftrag (Deckungsverhältnis)⁸, sondern durch den Einsatz der Debitkarte wird über das girocard-System der deutschen Kreditwirtschaft zugleich ein Zahlungsanspruch des Händlers gegenüber der kartenausgebenden Bank begründet (Zuwendungs- bzw. Vollzugsverhältnis):⁹ Die kartenausgebende Bank prüft, ob die ausgelesenen Daten und die PIN korrekt sind, ob die Karte gesperrt ist und der Umsatz innerhalb des Verfügungsrahmens liegt, und autorisiert auf dieser Grundlage den Umsatz.¹⁰ Mit der Autorisierung des Umsatzes erklärt die Bank, dass sie die Forderung in Höhe des autorisierten Betrags begleicht.¹¹ Nach h.M. entsteht damit eine Zahlungsverpflichtung der Bank aus einem abstrakten Schuldversprechen (§ 780 BGB). Dabei besteht keine Einigkeit, auf welche Weise der Vertrag zustande kommt: Überwiegend wird die Autorisierung als Angebot der kartenausgebenden Bank angesehen, das der Händler mit der weiteren Abwicklung des Zahlungsvorgangs annimmt.¹² Nach

anderer Ansicht tritt der Kunde als Stellvertreter seiner Bank auf, so dass bereits in der Vorlage der Karte ein Angebot auf Abschluss eines abstrakten Schuldversprechens liegt, das der Händler sodann annimmt, indem er die Zahlung mit der Karte akzeptiert.¹³ Die Wirksamkeit des Vertrages wäre dann aufschiebend durch die Autorisierung bedingt (§ 158 Abs. 1 BGB). Die aus dem Zahlungsverprechen resultierende Verpflichtung wird erfüllt, indem die Buchungsdaten an einen Zahlungsdienstleister des Händlers (z.B. dessen Hausbank) übermittelt werden, der dem Händler den Betrag gutschreibt und diesen per Lastschrift von der kartenausgebenden Bank einzieht¹⁴ („Clearing“).¹⁵ Mit der Gutschrift erlischt der Kaufpreisanspruch des Händlers im Valutaverhältnis.¹⁶ Da der Kunde mit dem Einsatz von Karte und PIN seiner Bank einen entsprechenden Zahlungsauftrag erteilt (§ 675f Abs. 2 S. 1, Abs. 4 S. 2 BGB) und dem betreffenden Zahlungsvorgang damit zugestimmt hat (§ 675j Abs. 1 S. 1, S. 3, S. 4 BGB)¹⁷, hat die Bank gegenüber dem Karten- und Kontoinhaber im Deckungsverhältnis einen Anspruch auf Ersatz ihrer Aufwendungen (§ 675c Abs. 1 BGB i.V.m. § 670 BGB), den die Bank mit einer entsprechenden Belastung des Kontos realisiert.¹⁸

b) Kreditkarte

Bei der Zahlung mit einer Kreditkarte¹⁹ besteht im Ausgangspunkt ebenfalls ein Dreiecksverhältnis, an dem die kartenausgebende Bank (Zahlungsdienstleister), der Karteninhaber (Zahler) und der Vertragshändler (Zahlungsempfänger) beteiligt sind; in der jüngeren Praxis dominiert allerdings ein Fünf-Parteien-System, in dem die Bank des Karteninhabers aufgrund eines Lizenzvertrages mit einem Kreditkartenunternehmen die Kreditkarte ausgibt, während die Akquisition von Vertragshändlern und die Abwicklung der Zahlung von einem davon getrennten Unternehmen (Acquirer) über-

1256 (1257). Zum Teil wird in der Autorisierung auch bereits die Annahme eines entsprechenden Angebots von Seiten des Händlers gesehen, siehe *Grüneberg*, in: ders., *Bürgerliches Gesetzbuch*, Kommentar, 82. Aufl. 2023, § 675f Rn. 60.

¹³ *Gößmann*, in: Horn (Hrsg.), *Bankrecht*, Schwerpunkte und Perspektiven, Festschrift für Herbert Schimansky, 1999, S. 145 (160 ff.).

¹⁴ Bedingungen (Fn. 9), Nr. 10.

¹⁵ *Casper* (Fn. 12), *ZahlungsverkehrsR* Rn. 715; *Toussaint*, *Das Recht des Zahlungsverkehrs im Überblick*, 2. Aufl. 2020, Rn. 419.

¹⁶ *Toussaint* (Fn. 15), Rn. 414.

¹⁷ *Casper* (Fn. 7), § 675f Rn. 133; *Haertlein* (Fn. 7), Teil 1 E. Rn. 246.

¹⁸ *Haertlein* (Fn. 7), Teil 1 E. Rn. 247; *Toussaint* (Fn. 15), Rn. 410, 423.

¹⁹ Mit diesem Begriff wird die Universalkreditkarte bezeichnet, die im Unterschied zur Kundenkreditkarte nicht nur bei dem Händler, der die Karte ausgegeben hat, sondern bei jedem Händler eingesetzt werden kann, der die Zahlung mit Kreditkarte akzeptiert, vgl. insoweit *Casper* (Fn. 7), § 675f Rn. 115; *Toussaint* (Fn. 15), Rn. 440.

⁷ *Casper*, in: Säcker/Rixecker/Oetker/Limberg (Hrsg.), *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, Bd. 6, 9. Aufl. 2023, § 675f Rn. 127, 136; *Haertlein*, in: Drescher/Fleischer/Schmidt (Hrsg.), *Münchener Kommentar zum Handelsgesetzbuch*, Bd. 6, 4. Aufl. 2019, Teil 1 E. Rn. 241.

⁸ *Haertlein* (Fn. 7), Teil 1 E. Rn. 246.

⁹ Siehe insoweit die Bedingungen für die Teilnahme am girocard-System der deutschen Kreditwirtschaft (Händlerbedingungen), Stand: 3.7.2020, abrufbar unter <https://www.girocard.eu/media/haendlerbedingungen.pdf> (20.7.2023).

¹⁰ *Haertlein* (Fn. 7), Teil 1 E. Rn. 238.

¹¹ Bedingungen (Fn. 9), Nr. 5.

¹² *Haertlein* (Fn. 7), Teil 1 E. Rn. 253; *Casper*, in: *Baumbach/Hefermehl/Casper*, *Wechselgesetz, Scheckgesetz, Recht des Zahlungsverkehrs*, 24. Aufl. 2020, *ZahlungsverkehrsR* Rn. 758; *Omlor*, in: *Staudinger, Bürgerliches Gesetzbuch*, Stand: 6.4.2021, § 675f Rn. 125; siehe auch BGH NJW 2003,

nommen werden.²⁰ Der Zahlungsvorgang wird im Präsenze Geschäft traditionell durch Vorlage der Kreditkarte und Unterzeichnung des vom Händler erstellten Belegs initiiert; zunehmend setzt sich aber auch bei der Kreditkarte die elektronische Zahlung durch, bei der die Kreditkarte in ein Lesegerät eingeführt und anschließend die PIN eingegeben wird (s.o. zum POS-Verfahren).²¹ Im Deckungsverhältnis liegt darin die Erteilung eines über den Händler (und ggf. den Acquirer) als Boten des Karteninhabers übermittelten Zahlungsauftrags an die kartenausgebende Bank sowie die Autorisierung des Zahlungsvorgangs.²² Der entsprechende Aufwendungsersatzanspruch der Bank gegen den Karteninhaber (§ 675c Abs. 1 BGB i.V.m. § 670 BGB) wird allerdings im Unterschied zum POS-Verfahren nicht sofort fällig, sondern aufgrund der Kreditabrede bis zum nächsten Abrechnungszeitpunkt gestundet.²³ Im Vollzugsverhältnis gibt die kartenausgebende Bank (bzw. der Acquirer²⁴) über den Karteninhaber als Boten ein Angebot auf Abschluss eines abstrakten Schuldversprechens (§ 780 BGB) ab, das der Händler konkludent annimmt.²⁵ Bei der elektronischen Zahlung wird in der Autorisierung der Zahlung durch die kartenausgebende Bank ein entsprechendes Angebot gesehen (s.o. zum POS-Verfahren).²⁶ Mit der Gutschrift wird nicht nur der Anspruch aus § 780 BGB, sondern zugleich die Kaufpreisforderung (§ 433 Abs. 2 BGB) im Valutaverhältnis erfüllt.²⁷

c) Missbrauch der Karte durch Dritte

Wird die Karte nicht durch den berechtigten Inhaber, sondern nach deren Verlust durch einen Dritten missbräuchlich zur Zahlung eingesetzt und wird der Umsatz von der kartenaus-

gebenden Bank autorisiert, weil der Dritte sich auch Kenntnis von der PIN verschafft hat, so ändert sich im Zuwendungs- bzw. Vollzugsverhältnis grundsätzlich nichts: Mit der Autorisierung verpflichtet sich die kartenausgebende Bank zur Zahlung des betreffenden Umsatzes; der Anspruch des Händlers nach § 780 BGB besteht damit auch dann, wenn die Karte durch einen Nichtberechtigten eingesetzt wird.²⁸ Geht man davon aus, dass das abstrakte Schuldversprechen über den Kartenverwender als Stellvertreter der kartenausgebenden Bank zustande kommt, so wird das Vertrauen des Händlers in das Bestehen einer entsprechenden Vollmacht nach § 172 BGB geschützt, da sich der Kunde mit der Vorlage der Karte legitimiert.²⁹ Dieser Schutz greift jedoch nicht mehr, wenn der Händler bösgläubig ist, weil er von der fehlenden Vollmacht wusste oder hätte wissen müssen (§ 173 BGB).³⁰ Diese Regelungen dürften analog gelten, wenn man den Kunden als Boten ansieht, der das Angebot der kartenausgebenden Bank übermittelt.³¹ Einer solchen Mitwirkung des Kunden bedarf es hingegen nicht, wenn man der vorherrschenden Auffassung folgt, wonach das abstrakte Schuldversprechen unmittelbar über die Autorisierung durch die kartenausgebende Bank zustande kommt. Nach der Rechtsprechung kann das von dem Kreditkartenunternehmen zu tragende Missbrauchsrisiko grundsätzlich nicht vertraglich auf den Händler abgewälzt werden.³² Davon unberührt bleibt allerdings eine verschuldensabhängige Haftung des Händlers; so hat das Kreditkartenunternehmen gegen den Händler einen Schadensersatzanspruch nach § 280 BGB, wenn dieser die Kreditkarte akzeptiert, ohne dem naheliegenden Verdacht eines Missbrauchs nachzugehen.³³

Im Valutaverhältnis bleibt es dabei, dass der Anspruch des Händlers gegen den Kunden, der die Karte missbräuchlich verwendet hat, mit der Gutschrift des autorisierten Betra-

²⁰ Casper (Fn. 7), § 675f Rn. 115; Herresthal, ZBB 2019, 353 (355 f.); Toussaint (Fn. 15), Rn. 442 f.; vgl. insoweit die AGB der BS Payone für Verträge zur Akzeptanz von Debit- und Kreditkarten, Stand: Juli 2016, abrufbar unter <https://www.ekom21.de/kunden/bspayone-agb-0716-v2.0.pdf?cid=13m> (20.7.2023).

²¹ Casper (Fn. 12), ZahlungsverkehrsR Rn. 786; Herresthal, ZBB 2019, 353 (359 f.).

²² Casper (Fn. 12), ZahlungsverkehrsR Rn. 786; Herresthal, ZBB 2019, 353 (356).

²³ Casper (Fn. 12), ZahlungsverkehrsR Rn. 791; Herresthal, ZBB 2019, 353 (357); Toussaint (Fn. 15), Rn. 441, 445.

²⁴ Linardatos, in: Drescher/Fleischer/Schmidt (Fn. 7), Teil 1 G. Rn. 19; Toussaint (Fn. 15), Rn. 451.

²⁵ Casper (Fn. 7), § 675f Rn. 121. Das Angebot steht allerdings unter der aufschiebenden Bedingung, dass der Händler innerhalb der vertraglich vereinbarten Frist einen vollständig ausgefüllten Leistungsbeleg übermittelt; vgl. dagegen zur Deutung als geschäftsbesorgungsrechtliche Pflicht des Acquirers zur Herausgabe des Erlangten: Herresthal, ZBB 2019, 353 (362 ff.). Überwiegend wird indes davon ausgegangen, dass sich durch den Übergang vom Drei-Parteien-System zum Fünf-Parteien-System im Kreditkartengeschäft an der Rechtsnatur der Ansprüche nichts geändert hat, siehe Casper (Fn. 12), ZahlungsverkehrsR Rn. 783, 824.

²⁶ Casper (Fn. 12), ZahlungsverkehrsR Rn. 825.

²⁷ Toussaint (Fn. 15), Rn. 458.

²⁸ BGH NJW-RR 2004, 481 (482 – zur Kreditkarte); Haertlein (Fn. 7), Teil 1 E. Rn. 254 (zur Debitkarte).

²⁹ Gößmann (Fn. 13), S. 164.

³⁰ Zur Anwendbarkeit des § 173 BGB auf eine von Anfang an nicht bestehende Vollmacht: Schubert, in: Säcker/Rixecker/Oetker/Limberg (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1, 9. Aufl. 2021, § 173 Rn. 2.

³¹ Zur analogen Anwendung des § 172 Abs. 2 BGB bei einer urkundlich verkörperten Willenserklärung, die sich im Besitz des Boten befindet: Singer, in: Staudinger, Bürgerliches Gesetzbuch, Stand: 2021, § 120 Rn. 3 m.w.N.

³² BGH NJW 2002, 2234 (2237); vgl. dagegen Herresthal, ZBB 2019, 353 (362 ff.), wonach die Zahlungszusage des Acquiring-Unternehmens als Aufwendungsersatzanspruch einzuordnen und dementsprechend eine weitergehende Verlagerung des Missbrauchsrisikos auf die Händler zulässig ist.

³³ BGH NJW-RR 2004, 481 (483); BGH NJW-RR 2005, 1570 (1572); Griineberg (Fn. 12), § 675f Rn. 57; Linardatos (Fn. 24), Rn. 223; Toussaint (Fn. 15), Rn. 457; siehe auch zur Prüfung der Unterschrift Hofmann, in: Schwintowski (Hrsg.), Bankrecht, 2. Teil Kap. 13 Rn. 19, 62; vgl. ferner AGB der BS Payone (Fn. 20), Nr. 3.1, 3.5, 3.6. sowie zum Ausschluss der Rückbelastung Nr. 11.3.

ges erlischt.³⁴ Gegen den berechtigten Karteninhaber hat der Händler ohnehin keinen Zahlungsanspruch, da ein Kaufvertrag zwischen diesen beiden nicht zustande gekommen ist. In Bezug auf das Deckungsverhältnis stellt § 675u S. 1 BGB klar, dass ein Aufwendungsersatzanspruch der kartenausgebenden Bank gegen den berechtigten Karteninhaber nicht besteht, da dieser dem Zahlungsvorgang nicht zugestimmt hat (Autorisierung des Zahlers, § 675j Abs. 1 S. 1 BGB).³⁵ Ist das Konto des Karteninhabers bereits mit dem betreffenden Betrag belastet worden, so ist die Buchung rückgängig zu machen (§ 675u Abs. 1 S. 2 BGB).³⁶ Der Kunde haftet allerdings für einen durch Missbrauch der Debitkarte entstandenen Schaden bis zu einem Betrag von 50 Euro, wenn es ihm möglich war, den Verlust oder Missbrauch der Karte vor dem nicht autorisierten Zahlungsvorgang zu bemerken (§ 675v Abs. 1, Abs. 2 Nr. 1 BGB). Der Karteninhaber haftet unbeschränkt, wenn er in betrügerischer Absicht gehandelt oder den Schaden durch eine vorsätzliche oder grob fahrlässige Pflichtverletzung (z.B. Verletzung der Anzeigepflicht bei Verlust der Karte) herbeigeführt hat (§ 675v Abs. 3 BGB). Schließlich steht der Bank, abgesehen von möglichen deliktischen Ansprüchen, ein Bereicherungsanspruch gegen den – regelmäßig unbekannt – Unberechtigten nach § 812 Abs. 1 S. 1 2. Fall BGB zu.³⁷

2. Authentifizierung und Haftung des Karteninhabers

a) Das Erfordernis starker Authentifizierung

Sowohl das POS-Verfahren als auch die elektronische Zahlung mit der Kreditkarte setzen grundsätzlich voraus, dass die Zahlung mit der Eingabe der zugehörigen PIN vom Karteninhaber autorisiert wird. Dies beruht auf unionsrechtlich harmonisierten³⁸ aufsichtsrechtlichen Vorgaben, wonach die Bank verpflichtet ist, eine sog. „starke Kundenauthentifizierung“ zu verlangen, wenn der Kunde einen elektronischen Zahlungsvorgang auslöst (§ 55 Abs. 1 S. 1 Nr. 2 ZAG³⁹). Während die (einfache) Authentifizierung „ein Verfahren [ist], mit dessen Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments [...] überprüfen kann“ (§ 1 Abs. 23 ZAG), erfordert eine starke Kundenauthentifizierung die Heranziehung von mindestens zwei der drei Elemente Wissen, Besitz oder Inhärenz (§ 1 Abs. 24

ZAG).⁴⁰ Diese Anforderungen werden durch das oben beschriebene POS-Verfahren gewahrt, da im Regelfall nur der Kunde über die Debitkarte verfügt (Besitz) und nur er die PIN kennt (Wissen). Mit dem dritten Merkmal (Inhärenz) werden ständige Merkmale des Berechtigten bezeichnet (z.B. Fingerabdrücke, Stimme, biometrische Gesichtsdaten).⁴¹ Diese Vorgaben beziehen sich indes nur auf elektronische Zahlungen, so dass die Zahlung mit einer Kreditkarte, bei der vom Karteninhaber ein nach Vorlage der Karte erstellter Leistungsbeleg unterschrieben wird, weiterhin ohne starke Authentifizierung zulässig ist.⁴²

Das Erfordernis einer starken Authentifizierung gilt jedoch auch für elektronische Zahlungsvorgänge nicht ausnahmslos. § 55 Abs. 5 ZAG verweist insoweit auf die von der Europäischen Kommission erlassene delegierte Verordnung zur Festlegung technischer Regulierungsstandards (RTS).⁴³ Dort ist eine Ausnahme für kontaktlose Zahlungen an der Verkaufsstelle vorgesehen, wonach der Zahlungsdienstleister auf eine starke Authentifizierung verzichten darf, wenn der Einzelbetrag des Zahlungsvorgangs nicht mehr als 50 Euro beträgt, die früheren kontaktlosen Vorgänge seit der letzten Durchführung einer starken Authentifizierung 150 Euro nicht überschreiten oder nicht mehr als fünf Zahlungsvorgänge ohne Authentifizierung seit dem letzten Vorgang mit starker Authentifizierung vergangen sind (Art. 11 RTS).⁴⁴ Dementsprechend lässt auch die aktuelle Fassung der Händlerbedingungen zum POS-Verfahren bei Zahlungen von bis zu 50 Euro einen Verzicht auf eine starke Authentifizierung zu.⁴⁵

Diese Ausnahmen betreffen vor allem kontaktlose Zahlungen, bei denen ein in die Karte integrierter Chip die für die Zahlungsabwicklung benötigten Daten über eine Entfernung von bis zu 10 cm auf das Lesegerät des Händlers überträgt (Near-Field-Communication – NFC).⁴⁶ Die technische Möglichkeit zur kontaktlosen Datenübertragung (d.h., ohne dass die Karte in ein Lesegerät gesteckt werden muss) lässt sich dabei sowohl für Zahlungsvorgänge mit starker Authentifizierung (Eingabe der PIN o.ä.) als auch für Zahlungen nutzen, bei denen auf dieses Erfordernis verzichtet wird.⁴⁷ Im

³⁴ *Nobbe*, in: Häuser/Hammen/Hennrichs/Steinbeck/Siebel/Welter (Hrsg.), Festschrift für Walther Hadding zum 70. Geburtstag am 8. Mai 2004, 2004, S. 1007 (1023).

³⁵ *Herresthal*, ZBB 2019, 353 (357); *Hofmann* (Fn. 33), Kap. 14 Rn. 42.

³⁶ *Toussaint* (Fn. 15), Rn. 423.

³⁷ *Nobbe* (Fn. 34), S. 1023, 1025; vgl. BGH NJW 2015, 3093 (3094); vgl. *Göhler*, JR 2021, 6 (19).

³⁸ Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates v. 25.11.2015 über Zahlungsdienste im Binnenmarkt (2. Zahlungsdiensterichtlinie), ABl. EU 2015 Nr. L 337/35.

³⁹ Vgl. insoweit auch 2. Zahlungsdiensterichtlinie (Fn. 38), Art. 97 Abs. 1 lit. b.

⁴⁰ Siehe zu den Definitionen auch Art. 4 Nr. 29, 30 der 2. Zahlungsdiensterichtlinie (Fn. 38).

⁴¹ *Jungmann*, in: Säcker/Rixecker/Oetker/Limpert (Fn. 7), § 675m Rn. 18.

⁴² *Casper* (Fn. 12), *ZahlungsverkehrsR* Rn. 786; *Linardatos* (Fn. 24), Rn. 29.

⁴³ Delegierte Verordnung (EU) 2018/389 der Kommission v. 27.11.2017 zur Ergänzung der Richtlinie (EU) 2015/2366 durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, ABl. EU 2017 Nr. L 69/23.

⁴⁴ Vgl. auch Art. 16 RTS für Kleinstbetragszahlungen im Ferngeschäft, bei denen die Höchstbeträge leicht abgesenkt sind.

⁴⁵ Bedingungen (Fn. 9), Nr. 8.

⁴⁶ *Hofmann/Rastegar*, WM 2021, 957.

⁴⁷ *Jungmann*, WM 2021, 557 (562); siehe dort auch zur Erstellung eines vom Karteninhaber zu unterschreibenden Leistungsbelegs.

Folgenden soll es allerdings allein um kontaktlose Zahlungen im letztgenannten Sinne gehen, bei denen das Wissenselement (Eingabe der PIN) entfällt und nicht durch ein anderes ersetzt wird, so dass die Voraussetzungen der starken Kundenauthentifizierung nicht mehr erfüllt sind.

b) Konsequenzen für die Verteilung des Missbrauchsrisikos

Die zivilrechtlichen Grundlagen des Zahlungsvorgangs bleiben von dem Verzicht auf die Eingabe der PIN im Ausgangspunkt unberührt, insbesondere erwirbt der Händler einen Zahlungsanspruch gegen die kartenausgebende Bank nach § 780 BGB. Im Unterschied zum POS-Verfahren sind allerdings im Deckungsverhältnis bei einem Missbrauch der Karte Schadensersatzansprüche der Bank gegen den Kunden weitgehend⁴⁸ ausgeschlossen, wenn die Bank keine starke Kundenauthentifizierung (d.h. Eingabe der PIN, s.o.) verlangt (§ 675v Abs. 4 S. 1 BGB). Allerdings soll dieser Haftungsausschluss nach überwiegender Auffassung nicht eingreifen, wenn der Verzicht auf eine starke Authentifizierung – wie beim kontaktlosen Bezahlen – aufsichtsrechtlich zulässig ist.⁴⁹ Dementsprechend wird der Haftungsausschluss auch in den AGB der Banken und Sparkassen auf den aufsichtsrechtswidrigen Verzicht beschränkt und damit das kontaktlose Zahlen ohne PIN-Abfrage ausgenommen; es bleibt damit grundsätzlich bei dem allgemeinen Haftungsregime (§ 675v Abs. 1–3 BGB; s.o. 1. c).⁵⁰

Eine noch weitergehende Übertragung des Missbrauchsrisikos auf den Bankkunden könnte sich aus den Sonderregelungen für Kleinbetragsinstrumente ergeben (§ 675i BGB). Bei einem Kleinbetragsinstrument handelt es sich nach § 675i Abs. 1 S. 2 BGB um ein Mittel, mit dem entweder einzelne

Zahlungsvorgänge von bis zu 30 Euro ausgelöst werden können, für das eine Ausgabenobergrenze von 150 Euro vorgesehen ist (Nr. 2) oder das nur Geldbeträge speichert, die nicht über 150 Euro hinausgehen (Nr. 3). Wird also etwa der Höchstbetrag von Zahlungsvorgängen, die kontaktlos (d.h. allein durch das Vorhalten der Karte) ausgelöst werden können, auf 25 € begrenzt⁵¹, so wäre die betreffende Karte als Kleinbetragsinstrument nach § 675i Abs. 1 S. 2 Nr. 1 BGB anzusehen. Dass mit derselben Karte bei Verwendung einer starken Authentifizierung auch darüber hinausgehende Zahlungen getätigt werden können, steht dem nicht entgegen, da die Karte insoweit mehrere Funktionen miteinander verbindet, also „multifunktional“ ist.⁵² In Bezug auf die Funktion als Kleinbetragsinstrument kann das Missbrauchsrisiko auf den Karteninhaber durch von den §§ 675u, 675v BGB abweichende Regelungen abgewälzt werden, wenn die Nutzung keinem Zahlungsdienstnutzer zugeordnet werden kann oder die kartenausgebende Bank eine Autorisierung aus anderen, dem Kleinbetragsinstrument immanenten Gründen nicht nachweisen kann (§ 675i Abs. 2 Nr. 3 BGB). Der EuGH hat diese Voraussetzung kürzlich bejaht, weil es dem Zahlungsdienstleister objektiv unmöglich sei, eine Autorisierung des Zahlungsvorgangs nachzuweisen, da eine solche allein aus physischem Besitz der Karte nicht abgeleitet werden könne und die Nutzung damit „anonym“ sei.⁵³ Im Schrifttum wird daraus gefolgert, dass für § 675 Abs. 2 Nr. 3 BGB nicht die – weiterhin mögliche – formale Zuordnung der Karte zu einem Konto, sondern deren Nutzung zum berechtigten Karteninhaber (Autorisierung) ausgeschlossen sein muss.⁵⁴ Dies ist jedoch insofern missverständlich, als auch die kontaktlose Zahlung nach der allgemeinen – und nicht nach § 675i Abs. 2 Nr. 3 BGB dispositiven Regelungen – Regelung weiterhin einer (einfachen) Autorisierung durch den Karteninhaber bedarf (§ 675j Abs. 1 S. 1 BGB).⁵⁵ Lässt sich die Zahlung – weil sie „anonym“ ausgelöst wird – nicht auf eine Autorisierung des Karteninhabers zurückführen, entfällt damit auch der Aufwendungsersatzanspruch der Bank (§ 675u S. 1 BGB). Dies müsste dann nicht nur bei missbräuchlicher Verwendung der Karte, sondern generell gelten, weil auch in der Verwendung der Karte durch den Inhaber keine Autorisierung gesehen werden könnte.⁵⁶ Der Sache nach geht es

⁴⁸ Eine Rückausnahme gilt, wenn der Karteninhaber selbst in betrügerischer Absicht handelt (§ 675v Abs. 4 S. 2 BGB).

⁴⁹ Casper (Fn. 12), ZahlungsverkehrsR Rn. 389; Linardatos (Fn. 24), Rn. 147; Omlor, in: Staudinger, Neubearbeitung 2020, Stand: 30.3.2021, § 675v Rn. 36 f.; siehe dagegen für einen Haftungsausschluss: Schmalenbach, in: Hau/Poseck (Hrsg.), Beck'scher Online-Kommentar, Bürgerliches Gesetzbuch, Stand: 1.5.2023, § 675v Rn. 17d.

⁵⁰ Siehe etwa Nr. 13 lit. a Abs. 4 der Bedingungen für die Commerzbank Girocard, Stand: 1.10.2020, abrufbar unter

https://www.commerzbank.de/portal/media/efw-dokumente/bed_girocard.pdf (20.7.2023);

Nr. 14.1. Abs. 6 der Bedingungen der Deutsche Bank AG für die Debitkarten, Stand 02/2022, abrufbar unter

https://www.deutsche-bank.de/content/dam/deutschebank/de/shared/pdf/ser-agb-bedingungen-debitkarten_ag.pdf (20.7.2023);

Nr. 13.1. Abs. 7 der DKB Bedingungen für die Visa Debitkarte, Stand: 14.9.2022, abrufbar unter

https://dok.dkb.de/pdf/b_debitkarte.pdf (20.7.2023);

Nr. 14.1. Abs. 7 der Bedingungen für die Sparkassen Card, Stand: September 2021, abrufbar unter

<https://www.sparkasse-holstein.de/content/dam/myif/spk-holstein/work/dokumente/pdf/vertragsbedingungen/bedingungen-fuer-die-verwendung-von-sparkassencards.pdf?n=true> (20.7.2023).

⁵¹ Vgl. die AGB für den Einsatz von Zahlungskarten der österreichischen DenizBank nach EuGH, Urt. v. 11.11.2020 – C-287/19 (DenizBank) = BKR 2021, 234 (235).

⁵² EuGH BKR 2021, 234 (238 Rn. 77, 79).

⁵³ EuGH BKR 2021, 234 (239 Rn. 88 f.), zu Art. 63 Abs. 1 lit. b der 2. Zahlungsdiensterichtlinie (Fn. 38).

⁵⁴ Omlor, RdZ 2021, 180 (184).

⁵⁵ Casper (Fn. 7), § 675f Rn. 131; Jungmann (Fn. 41), § 675j Rn. 86.

⁵⁶ Im Schrifttum wird deshalb der Anwendungsbereich des § 675i Abs. 2 Nr. 3 BGB auf Prepaid-Instrumente (z.B. Geldkarten) beschränkt, bei denen eine Autorisierung vorab durch das Aufladen der Karte mit einem bestimmten Geldbetrag erfolgt, der sodann zur Zahlung eingesetzt werden kann, ohne dass eine Verbindung zu dem Konto des Karteninhabers hergestellt werden muss, siehe Habersack, EuZW 2020, 767

dem EuGH jedoch um die Fälle, in denen eine Autorisierung nicht „belegt“ (also vom Zahlungsdienstleister nachgewiesen) werden kann (vgl. § 675w S. 1 BGB), weil es an einer Authentifizierung durch Unterschriftsleistung oder Eingabe einer PIN fehlt.⁵⁷ Wie bereits gesehen, handelt es sich bei der Authentifizierung um ein Verfahren, mit dem der Zahlungsdienstleister die Identität des Zahlungsdienstnutzers oder die berechnete Verwendung eines Zahlungsinstruments überprüfen kann (§ 1 Abs. 23 ZAG;⁵⁸ siehe auch § 675w S. 2 BGB). Da es sich bei diesem Verfahren nicht unbedingt um eine „starke“ Authentifizierung handeln muss (§ 1 Abs. 24 ZAG, s.o.), wird im Schrifttum die Auffassung vertreten, dass für eine (einfache) Authentifizierung der Besitz der Karte (ein Faktor anstelle von zwei Faktoren in Form von Besitz und Wissen) bei Auslösung des Zahlungsvorgangs ausreicht.⁵⁹ Dagegen spricht allerdings, dass der Besitz an der Karte kaum geeignet sein dürfte, die berechnete Verwendung durch deren Vorlage nachzuweisen; insbesondere werden persönliche Sicherheitsmerkmale nicht überprüft (vgl. § 675w S. 2 BGB; siehe insoweit § 1 Abs. 25 ZAG).⁶⁰ Dementsprechend wird beim kontaktlosen Bezahlen zum Teil nur eine „einfache“ Autorisierung angenommen, die nicht im Wege einer Authentifizierung überprüft wird.⁶¹ Steht jedoch der Einsatz der Originalkarte aufgrund der ordnungsgemäßen Aufzeichnung des Bezahlvorgangs fest, so trifft den Karteninhaber, der eine Autorisierung bestreitet, die sekundäre Darlegungslast in Bezug auf die Umstände, die zum Zugriff eines Dritten auf die Karte geführt haben.⁶² Vor dem Hintergrund der EuGH-Rechtsprechung wäre § 675i Abs. 2 Nr. 3 BGB daher so auszulegen, dass das Haftungsregime nach §§ 675u, 675v BGB abdingbar ist (z.B. durch einen Aufwendungsersatzanspruch für nicht autorisierte Zahlungen), soweit der Zahlungsdienstleister auf eine (starke) Authentifizierung, nicht aber generell auf eine Autorisierung verzichtet.⁶³ Soweit ersichtlich, ist ein Aufwendungsersatzanspruch für nicht autorisierte Zahlungen in den AGB der Banken und Sparkassen nicht vorgesehen; überwiegend wird die Haftung des Karteninhabers sogar auf vorsätzliche oder grob fahrlässige Pflichtverletzungen bzw. betrügerisches Handeln beschränkt.⁶⁴ Der Ausschluss von Schadensersatzansprüchen

beim Verzicht auf eine starke Authentifizierung (§ 675v Abs. 4 S. 1 Nr. 1 BGB) bleibt davon unberührt, sofern man diese Regelung entgegen der überwiegenden Ansicht beim aufsichtsrechtlich zulässigen Verzicht für anwendbar hält (s.o.).⁶⁵

c) Kontaktlose Zahlung mit Smartphones

Eine kontaktlose Zahlung kann schließlich auch mit Smartphones oder anderen Endgeräten (Smartwatches o.ä.) über eine entsprechende Applikation (Wallet, z.B. für Google Pay oder Apple Pay) ausgelöst werden, sofern diese für den Einsatz der NFC-Technologie geeignet sind. Der Karteninhaber hinterlegt zu diesem Zweck eine virtuelle Kopie der Zahlungskarte auf dem Endgerät oder auf einem Server; an die Stelle der Karte tritt beim Bezahlvorgang das Smartphone bzw. Endgerät (das ggf. eine Verbindung mit dem Server herstellt, auf dem die Kartendaten gespeichert sind).⁶⁶ Ein wichtiger Unterschied zur Zahlung mit der Karte selbst liegt jedoch darin, dass eine Authentifizierung nicht über die PIN-Eingabe, sondern über Sicherungsmechanismen des Smartphones erfolgt (Entsperrung, Fingerabdruckscanner).⁶⁷ In der Sache kann auf diese Weise auch bei einer Zahlung mit einem Smartphone eine starke Authentifizierung gewährleistet werden; dies wird allerdings teilweise verneint, weil die Überprüfung nicht (wie beim PIN-Abwurf) durch den Zahlungsdienstleister (die kartenausgebende Bank) selbst vorgenommen wird (vgl. § 1 Abs. 23 ZAG).⁶⁸ Soweit hingegen auf eine starke Authentifizierung verzichtet wird, gelten die obigen Ausführungen zur herkömmlichen Kartenzahlung entsprechend.

III. Strafrechtliche Bewertung der kontaktlosen Zahlung durch einen Nichtberechtigten

Mit der zivilrechtlichen Rekonstruktion des Zahlungsvorgangs ist die Grundlage für die strafrechtliche Bewertung von Sachverhalten gelegt, in denen ein Dritter eine dem berechtigten Inhaber abhandengekommene Karte missbraucht, um damit einen kontaktlosen Zahlungsvorgang auszulösen. Da der Händler in diesen Konstellationen einen Zahlungsanspruch gegen die kartenausgebende Bank aus § 780 BGB erlangt, die Bank aber wiederum aufgrund der fehlenden Autorisierung keinen Aufwendungsersatzanspruch gegen den Karteninhaber hat (§ 675u S. 1 BGB), erleidet sie einen Vermögensschaden in Höhe des Zahlungsbetrages. Damit stellt sich die Frage, ob der Missbrauch als Computerbetrug

(769); *Jungmann*, WM 2021, 557 (567 f.); *Linardatos*, BKR 2021, 665 (673).

⁵⁷ EuGH BKR 2021, 234 (239 Rn. 87 f.); siehe insoweit *Jungmann*, WM 2021, 557 (567).

⁵⁸ Siehe insoweit 2. Zahlungsdiensterichtlinie (Fn. 38), Art. 4 Nr. 29.

⁵⁹ *Habersack*, EuZW 2020, 767 (768 f.).

⁶⁰ *Hoffmann/Rastegar*, WM 2021, 957 (963).

⁶¹ *Jungmann* (Fn. 41), § 675j Rn. 86; *ders.*, WM 2021, 557 (562).

⁶² *Hoffmann/Rastegar*, WM 2021, 957 (963).

⁶³ *Hoffmann/Rastegar*, WM 2021, 957 (962 f.); siehe auch *Mimberg*, in: Schäfer/Omlor/Mimberg (Hrsg.), ZAG § 1 Rn. 446.

⁶⁴ Siehe etwa Bedingungen für die Commerzbank Girocard (Fn. 50), Nr. 13 lit. a; Bedingungen der Deutsche Bank AG für die Debitkarten (Fn. 50), Nr. 14.1. Abs. 1; Bedingungen

für die Sparkassen Card (Fn. 50), Nr. 14.1. Abs. 4; siehe dagegen zu einer den § 675v Abs. 1, Abs. 2 BGB entsprechenden Haftung: DKB Bedingungen für die Visa Debitkarte (Fn. 50), Nr. 13.1. Abs. 1.

⁶⁵ *Hoffmann/Rastegar*, WM 2021, 957 (962).

⁶⁶ Näher *Hoffmann/Rastegar*, WM 2021, 957 f.; *Linardatos*, BKR 2021, 665 f.

⁶⁷ *Hoffmann/Rastegar*, WM 2021, 957 f.

⁶⁸ *Hoffmann/Rastegar*, WM 2021, 957 (964); a.A. *Linardatos*, BKR 2021, 665 (671 f.).

(§ 263a StGB) oder Betrug (§ 263 StGB) zum Nachteil der kartenausgebenden Bank strafbar ist.

1. Computerbetrug (§ 263a Abs. 1 Var. 3 StGB)

Der Tatbestand des § 263a StGB setzt zunächst eine der darin beschriebenen Tathandlungen voraus. Durch den Missbrauch der Karte könnte der Täter die auf der Karte gespeicherten Daten unbefugt verwendet haben (§ 263a Abs. 1 Var. 3 StGB).

a) „unbefugte“ Verwendung (OLG Hamm)

Nach vorherrschender Auffassung ist eine Datenverwendung unbefugt, wenn sie gegenüber einer natürlichen Person Täuschungscharakter hätte.⁶⁹ Nach dieser betrugspezifischen Auslegung ist also maßgeblich, ob die Datenverwendung gegenüber einem fiktiven Bankangestellten, der anstelle des Computers agiert, als Täuschung anzusehen wäre; dabei soll sich dieser Bankangestellte nach der Rechtsprechung allerdings nur mit Fragen befassen, die auch der Computer prüft.⁷⁰ Danach ist eine Täuschungsäquivalenz bei dem Missbrauch einer Karte mit Eingabe der PIN durch einen Dritten zu bejahen, weil der Täter seine Berechtigung vorspiegeln, hingegen zu verneinen, wenn der berechtigte Karteninhaber die Karte einsetzt, ohne zum Ausgleich willens oder in der Lage zu sein, da der Computer nicht die Bonität der Karten- und Kontoinhabers überprüft.⁷¹ An diese Differenzierung anknüpfend hat das OLG Hamm eine Täuschungsäquivalenz auch beim kontaktlosen Zahlen ohne Eingabe der PIN mit folgender Begründung verneint:

„[...] anders als in den Fällen, in denen der Bankcomputer die PIN vom Kartenverwender abfragt, wird hierbei die Berechtigung desjenigen, der den elektronischen Zahlungsvorgang durch Vorhalten der Karte vor das Lesegerät auslöst, gerade nicht durch Anwendung einer starken Kundenauthentifizierung im Sinne von § 55 Abs. 1 Nr. 2 ZAG überprüft. Stattdessen überprüft der Computer [...] lediglich, ob die Karte in keine Sperrdatei eingetragen ist, der Verfügungsrahmen nicht überschritten wird und ob die Voraussetzungen für das Absehen von der PIN-

Abfrage nach Art. 11 der Technischen Regulierungsstandards und ggf. weiteren internen Bankregularien gegeben sind. Bereits bei Vorliegen dieser Voraussetzungen erteilt der Bankcomputer eine elektronische Autorisierung der Zahlung, die dem Händler übermittelt wird. Gegenüber einem an die Stelle des Bankcomputers in der Autorisierungszentrale tretenden Bankangestellten würden also auch nur die Einhaltung des Verfügungsrahmens, die Nicht-Eintragung in eine Sperrdatei und das Vorliegen der Voraussetzungen für das Absehen von der starken Kundenauthentifizierung erklärt. Nicht erklärt würde hingegen, dass die Voraussetzungen zur vollen Überprüfung der materiellen Berechtigung zur Kartennutzung vorliegen. Damit aber würde ein fiktiver menschlicher Bankangestellter anstelle des Bankcomputers auch keinem dahingehenden Irrtum bezüglich der Berechtigung unterliegen, womit es an der für die Unbefugtheit erforderlichen Betrugsähnlichkeit fehlt.“⁷²

Diese Unterscheidung des Kartenmissbrauchs mit und ohne Eingabe der PIN ist im Schrifttum überwiegend auf Zustimmung gestoßen.⁷³

b) Prüfung der Berechtigung durch den Computer nur bei PIN-Abfrage?

Die Orientierung an der vom Computer vorzunehmenden Prüfung wirft bei näherer Betrachtung eine Reihe von Fragen auf, die Zweifel an dieser Differenzierung aufkommen lassen: So wird auch bei der Abfrage der PIN nur geprüft, ob derjenige, der den Zahlungsvorgang auslöst, Kenntnis von dieser hat; über eine solche Kenntnis können auch Dritte verfügen, die sich die PIN – zusammen mit der Karte – durch Ausspähen o.ä. verschafft haben. Das Erklärungsverhalten des Täters, der die Karte zusammen mit der PIN einsetzt, ließe daher bei einer strikten Orientierung am Prüfumfang des Computers nur Rückschlüsse auf die Kenntnis des Täters von der PIN, nicht aber auf dessen Identität als Karteninhaber zu. Um die Identität des Kartennutzers festzustellen, wären hingegen weitergehende Kontrollmaßnahmen (z.B. Fingerabdruck- oder Netzhautscanner) erforderlich.⁷⁴ Dass eine solche Deutung auf der Grundlage der Rechtsprechung nicht völlig fernliegend ist, lässt sich daran ablesen, dass im Schrifttum eine Strafbarkeit nach § 263a Abs. 1 Var. 3 StGB auch bei einem Kartenmissbrauch im POS-Verfahren mit PIN-Abfrage verneint wird.⁷⁵ Auch der BGH hat eine unbefugte Verwendung bei einer durch Täuschung erlangten Debitkarte verneint, weil die Identität und Berechtigung des Verwenders

⁶⁹ BGHSt 47, 160 (162 f.); BGH NJW 2013, 2608 (2610); BGH NSTZ-RR 2023, 14; OLG Rostock JR 2020, 439 (441); *Altenhain*, in: *Matt/Renzikowski* (Hrsg.), *Strafgesetzbuch, Kommentar*, 2. Aufl. 2020, § 263a Rn. 12; *Fischer*, *Strafgesetzbuch mit Nebengesetzen, Kommentar*, 70. Aufl. 2023, § 263a Rn. 11; *Hefendehl/Noll* (Fn. 6), § 263a Rn. 85; *Hoyer*, in: *Wolter* (Hrsg.), *Systematischer Kommentar*, Bd. 5, 9. Aufl. 2019, § 263a Rn. 19; *Tiedemann/Valerius* in: *Laufhütte/Rissing-van Saan/Tiedemann* (Hrsg.), *Leipziger Kommentar zum Strafgesetzbuch*, Bd. 9/1, 12. Aufl. 2012, § 263a Rn. 44.

⁷⁰ BGHSt 47, 160 (163); OLG Rostock JR 2020, 439 (442); *Altenhain* (Fn. 69), § 263a Rn. 12; *Kluszczewski*, *Strafrecht, Besonderer Teil*, 2016, § 9 Rn. 146; *Momsen*, in: *Maurach/Schroeder/Maiwald/Hoyer/Momsen* (Hrsg.), *Strafrecht, Besonderer Teil, Teilbd. 1*, 11. Aufl. 2019, § 41 Rn. 240.

⁷¹ BGHSt 47, 160 (162, 163).

⁷² OLG Hamm BeckRS 2020, 9059 Rn. 21 f.

⁷³ *Christoph/Dorn-Haag*, NSTZ 2020, 676; *dies.*, NSTZ 2020, 697 (701 f.); *Duttge* (Fn. 6), § 263a Rn. 19; *Eisele* (Fn. 6), Rn. 681; *Göhler*, JR 2021, 6 (17 f.); *Heger* (Fn. 6), § 263a Rn. 13a; *Heghmanns*, ZJS 2020, 494 (496); *Hefendehl/Noll* (Fn. 6), § 263a Rn. 109; *Rengier* (Fn. 6), § 14 Rn. 46; *Schramm* (Fn. 6), § 8 Rn. 38 f.

⁷⁴ Vgl. *Wachter*, NSTZ 2018, 241 (243), der dies aber mit Blick auf die unverhältnismäßigen Kosten verwirft.

⁷⁵ *Eisele* (Fn. 6), Rn. 681; *Rengier* (Fn. 6), § 14 Rn. 45.

mit der Eingabe der Karte und zugehörigen PIN „hinreichend festgestellt“ seien.⁷⁶

Umgekehrt ließe sich einer Unterscheidung von Kartenzahlung mit und ohne PIN-Abfrage entgegenhalten, dass nicht nur die Kenntnis der PIN, sondern bereits der Besitz einer Debitkarte Rückschlüsse darauf zulässt, dass sie von dem Karteninhaber verwendet wird, da es sich um ein höchstpersönliches Zahlungsinstrument handelt, das nur den Inhaber zur Auslösung von Zahlungsvorgängen berechtigt.⁷⁷ Der Besitz der Karte ist einer der zwei Faktoren, die für eine starke Authentifizierung notwendig sind (s.o. II. 2. zu § 1 Abs. 24 und § 55 Abs. 1 Nr. 2 ZAG), und grundsätzlich geeignet, als Verkörperung einer von der Bank erteilten Vollmacht, sie im POS-Verfahren gegenüber dem Händler zu vertreten, eine Rechtsscheinhaftung zu begründen (s.o. II. 1. zu § 172 BGB). Wenngleich der Besitz der Karte allein für eine Authentifizierung nicht ausreicht, löst die Verwendung der Karte zum kontaktlosen Bezahlen beim Bestreiten einer Autorisierung Darlegungslasten des Karteninhabers aus; unterbleibt ein Vortrag zum Verlust der Karte, der deren Missbrauch ermöglicht hat, gilt die Autorisierung als zugestanden (s.o. II. 2. b). Die Annahme, dass die Karte in der Regel vom berechtigten Karteninhaber eingesetzt wird, ist damit alles andere als fernliegend und spiegelt sich auch in zivilrechtlichen Wertungen wider.

c) „Prüfung“ durch den Computer – die Nähe zur computerspezifischen Auslegung

Der Haupteinwand gegen die h.M. liegt indes nicht in diesen begrifflichen Unschärfen, sondern darin, dass die Täuschungsrelevanz von Tatsachen von der Reichweite der Überprüfung durch den Computer abhängig gemacht wird. Im Ergebnis läuft dies auf die computerspezifische Auslegung hinaus⁷⁸, die für das Merkmal „unbefugt“ im Ausgangspunkt auf den Willen des Berechtigten abstellt, aber darüber hinaus verlangt, dass sich dieser Wille im Computerprogramm niedergeschlagen haben muss.⁷⁹ Demgegenüber sei der Tatbestand des § 263a Abs. 1 Var. 3 StGB nicht erfüllt, wenn das Programm ordnungsgemäß bedient werde.⁸⁰ Die damit vorgenommene Reduzierung des Anwendungsbereichs auf den Missbrauch von Zugangscodes ist jedoch auf nahezu einhellige Ablehnung gestoßen, da sie dem § 263a Abs. 1 Var. 3 StGB kaum einen sinnvollen Anwendungsbereich

reich mehr belässt⁸¹, und wird in jüngerer Zeit nicht mehr vertreten⁸². Die enge Orientierung am Prüfprogramm des Computers ist grundsätzlich den gleichen Bedenken ausgesetzt. Ihre Kernaussage, dass ein Äquivalent zu einer konkludenten Täuschung bei einem Computer nur in Bezug auf Tatsachen vorliegen könne, die auch für die automatisierte Datenverarbeitung durch den Computer relevant sind⁸³, ist insofern richtig, als der Informationsgehalt der eingegebenen Daten Rückschlüsse auf weitere Tatsachen erlauben muss, deren Feststellung zu den Aufgaben des Computers bzw. der Vergleichsperson gehören muss.⁸⁴ Damit ist jedoch nicht gesagt, dass jede dieser Tatsachen auch von dem Computer „überprüft“ werden muss, indem ein entsprechender Nachweis gefordert wird. Ein solches Erfordernis könnte allenfalls darauf gestützt werden, dass ein strafrechtlicher Schutz als ultima ratio nur gerechtfertigt ist, soweit das Opfer selbst zumutbare Sicherungsmaßnahmen ergriffen hat.⁸⁵ Ganz in diesem Sinne wird die Entscheidung der kartenausgebenden Bank, beim kontaktlosen Bezahlen auf eine starke Authentifizierung zu verzichten, als eigenverantwortliche Selbstgefährdung eingeordnet, mit der die Vorteile dieser neuen Zahlungsmethode (Beschleunigung, Vereinfachung, s.o. I.) erkaufte werden.⁸⁶ Derartige Erwägungen lassen sich indes mit dem Ausgangspunkt der betrugsspezifischen Auslegung kaum vereinbaren, wonach die Reichweite des strafrechtlichen Schutzes bei § 263a StGB am Betrugstatbestand auszurichten ist, der auch das sorglose bzw. leichtfertige Opfer schützt⁸⁷. Dementsprechend sind auf der Grundlage der h.M. viktimodogmatisch begründete Einschränkungen auch bei § 263a StGB abzulehnen.⁸⁸ Auch das Argument, die Banken handelten mit dem Verzicht auf eine starke Authentifizierung auf eigenes Risiko, greift nicht durch, soweit dieser Verzicht aufsichtsrechtlichen Standards entspricht (§ 55 Abs. 5 ZAG i.V.m. Art. 11 RTS, s.o. II. 2. a). Die damit eröffnete Möglichkeit kann also nicht so verstanden werden, dass deren Gebrauch eine Verletzung von Obliegenheit zur Prävention

⁷⁶ BGH NStZ 2016, 149 (151); zur Kritik: Böse, ZJS 2016, 663 (665 f.).

⁷⁷ Haertlein (Fn. 7), Teil 1 E. Rn. 26, 48; Burghardt/Bardowicks, ZJS 2023, 593 (599, 602); siehe auch zur „unbefugter“ Verwendung fremder Kreditkartendaten: BGH NStZ-RR 2021, 214; BGH BeckRS 2022, 31922 Rn. 13; vgl. dagegen Christoph/Dorn-Haag, NStZ 2020, 697 (702).

⁷⁸ Siehe bereits Altenhain, JZ 1997, 752 (758); zum vorliegenden Kontext: Christoph/Dorn-Haag, NStZ 2020, 697 (701).

⁷⁹ LG Freiburg NJW 1990, 2635 (2636 f.); Achenbach, JR 1994, 293 (295).

⁸⁰ OLG Celle NStZ 1989, 367; Neumann, StV 1996, 375.

⁸¹ Vgl. nur Hefendehl/Noll (Fn. 6), § 263a Rn. 88; Kindhäuser/Hoven, in: Kindhäuser/Neumann/Paeffgen/Saliger (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 4, 6. Aufl. 2023, § 263a Rn. 24, jeweils m.w.N.

⁸² Soweit ersichtlich wurde diese Auffassung zuletzt von Achenbach, in: Dölling/Erb (Hrsg.), Festschrift für Karl Heinz Gössel zum 70. Geburtstag am 16. Oktober 2002, 2002, S. 481 (494 f.), vertreten.

⁸³ Altenhain (Fn. 69), § 263a Rn. 12.

⁸⁴ Hoyer (Fn. 69), § 263a Rn. 20.

⁸⁵ BGHSt 47, 160 (166); vgl. auch zur computerspezifischen Auslegung: Tiedemann/Valerius (Fn. 69), § 263a Rn. 45.

⁸⁶ Heghmanns, ZJS 2020, 494 (496); siehe auch Ceffinato, JuS 2021, 311 (313); Göhler, JR 2021, 6 (18); Kudlich, JA 2020, 710 (712).

⁸⁷ Siehe insoweit BGHSt 34, 199 (201); BGH NStZ 2003, 313 (314) m.w.N.

⁸⁸ Burghardt/Bardowicks, ZJS 2023, 593 (603); Hefendehl/Noll (Fn. 6), § 263a Rn. 17; Tiedemann/Valerius (Fn. 69), § 263a Rn. 5; vgl. dagegen Christoph/Dorn-Haag, NStZ 2020, 697 (702).

des Kartenmissbrauchs darstellt; dies zeigt sich insbesondere darin, dass der Haftungsausschluss für den Bankkunden (§ 675v Abs. 4 BGB) zugunsten der Banken auf den aufsichtsrechtswidrigen Verzicht beschränkt wird (s.o. II. 2. b). Für die Täuschungsäquivalenz ist damit – wie i.R.d. § 263 StGB – auf den Inhalt der Erklärung, nicht auf deren Überprüfung durch das Opfer abzustellen, die der Dritte mit dem Einsatz der Karte abgibt und die sodann vom Computer automatisiert verarbeitet wird.

d) Die Erklärung des Kartennutzers als Datenurkunde

Wie der Blick auf die zivilrechtlichen Grundlagen gezeigt hat, erteilt der Karteninhaber beim kontaktlosen Bezahlen seiner Bank einen Zahlungsauftrag und autorisiert zugleich die entsprechende Zahlung der Bank an den Händler (s.o. II. 1., 2.). Da nur der Karteninhaber aufgrund des mit der Bank abgeschlossenen Zahlungsdiensterahmenvertrages berechtigt ist, der Bank solche Aufträge zu erteilen und die entsprechenden Zahlungen zu autorisieren (§§ 675f Abs. 2, 675j Abs. 1 BGB), ist in dem Einsatz der Karte durch einen Dritten implizit die Erklärung enthalten, dass der berechtigte Karteninhaber die Zahlung anweist und autorisiert. Der elektronische Beleg, mit dem der Einsatz der Karte zum kontaktlosen Bezahlen zu Beweis Zwecken aufgezeichnet wird (vgl. § 675w S. 1 BGB), stellt daher eine Datenurkunde i.S.d. § 269 StGB dar.⁸⁹ Das OLG Hamm hat demgegenüber eine Strafbarkeit nach § 269 StGB mit folgender Erwägung verneint:

„Zwar werden bei dem Einsatz einer ec-Karte im POS-Verfahren am Kartenlesegerät die Transaktionsdaten (z.B. Kontonummer und Gültigkeitsdatum der ec-Karte) als Gedankenerklärung in das Autorisierungssystem eingelesen. Allerdings ist in Bezug auf die Transaktionsdaten bei den hier vorliegenden kontaktlosen Zahlungen [...] die Garantiefunktion des Urkundenbegriffs nicht erfüllt. Diese erfordert, dass der vermeintliche Aussteller der Gedankenerklärung erkennbar ist. An einer solchen eindeutigen Identifikationsmöglichkeit fehlt es aber mangels PIN-Abfrage. [...] der für die Anweisung hier allein erforderliche unmittelbare Besitz an der ec-Karte garantiert gerade nicht genauso wie die gleichzeitige Abfrage der herkömmlicherweise nur dem Berechtigten bekannten PIN, dass derjenige, der die Karte einsetzt, auch der berechtigte Karteninhaber ist. Die Eingabe der Transaktionsdaten ist damit nicht in einer von dem Urkundenbegriff vorausgesetzten Weise einer Person eindeutig zuzuordnen. Weil der Aussteller der Erklärung nicht hinreichend erkennbar

⁸⁹ A.A. *Heghmanns*, ZJS 2020, 494 (496 f.), der von einer Erklärung des Betreibers der Datenverarbeitungsanlage ausgeht; zust. *Burghardt/Bardowicks*, ZJS 2023, 593 (608). Diese Deutung wird indes dem zivilrechtlichen Hintergrund der Aufzeichnung nicht gerecht, die es der kartenausgebenden Bank ermöglichen soll, die Autorisierung der Zahlung (d.h. die Abgabe einer entsprechenden Erklärung) gegenüber dem Karteninhaber nachzuweisen.

ist, fehlt es an der für § 269 Abs. 1 StGB notwendigen Datenurkunde.“⁹⁰

In diesen Ausführungen sind Parallelen zu der bereits erwähnten Auffassung des EuGH erkennbar, der kontaktlose Zahlungen als „anonym“ qualifiziert hat. Wie oben dargelegt, lässt diese Rechtsprechung das Erfordernis einer Autorisierung auch beim kontaktlosen Zahlen nicht entfallen, sondern verzichtet allein auf die (starke) Authentifizierung (s.o. II. 2. b). Die Autorisierung der Zahlung (§ 675j Abs. 1 BGB) und deren Überprüfung im Wege der Authentifizierung (§ 675w BGB) sind vielmehr auch bei der strafrechtlichen Bewertung strikt zu trennen.⁹¹ Dementsprechend wird der Auslegung des § 269 StGB durch das OLG Hamm zu Recht entgegengehalten, dass die Erkennbarkeit des Ausstellers einer Urkunde keine Bekräftigung (z.B. durch eine Unterschrift) voraussetzt und es daher auch für die Annahme einer Datenurkunde keiner Authentifizierung des Ausstellers bedarf.⁹² Da in dem elektronischen Beleg nicht der den Zahlungsvorgang tatsächlich auslösende Dritte, sondern der Karteninhaber als Aussteller gespeichert wird, werden beweiserhebliche Daten mithin so gespeichert, dass bei ihrer Wahrnehmung eine unechte Urkunde vorläge (§ 269 Abs. 1 Var. 1 StGB). Der Täter handelt insoweit auch zur fälschlichen Beeinflussung einer Datenverarbeitung (§ 270 StGB), da es ihm darauf ankommt, mit der (vermeintlichen) Anweisung und Autorisierung eine Zahlung an den Händler zu veranlassen und damit die Voraussetzung dafür zu schaffen, dass ihm die Kaufsache übergeben wird. Im Schrifttum wird daher entgegen dem OLG Hamm eine Strafbarkeit nach § 269 Abs. 1 Var. 1 StGB bejaht.⁹³

Dessen ungeachtet verneinen einige Autoren weiterhin eine unbefugte Datenverwendung i.S.d. § 263a Abs. 1 Var. 3 StGB, weil dort anders als bei § 269 StGB nicht auf die Zuordnung der Transaktion oder die Identifizierbarkeit des Nutzers, sondern auf den konkreten Inhalt der Erklärung abzustellen sei.⁹⁴ Die Bedeutung dieser Differenzierung erschließt sich nicht ohne Weiteres: Denkbar wäre es, zwischen dem Aussteller der Erklärung und deren Inhalt zu unterscheiden. Da es sich bei dem Zahlungsauftrag und der Autorisierung um Willenserklärungen handelt,⁹⁵ schließt der Inhalt der Erklärung die Person bzw. Berechtigung des Erklärenden ein, wie es sich im vorliegenden Kontext aus der Einbettung in einen Zahlungsdiensterahmenvertrag und das auf dieser

⁹⁰ OLG Hamm BeckRS 2020, 9059 Rn. 27–29; ebenso *Göhler*, JR 2021, 6 (20).

⁹¹ Siehe auch *Puschke/Haas*, RdZ 2022, 4 (9 Fn. 51).

⁹² *Ceffinato*, JuS 2021, 311 (314); *Christoph/Dorn-Haag*, NSTZ 2020, 697 (699); *Erb*, in: Erb/Schäfer (Fn. 6), § 269 Rn. 35; *Kulhanek*, wistra 2021, 220 (224); *Puschke/Haas*, RdZ 2022, 4 (9 f.).

⁹³ *Ceffinato*, JuS 2021, 311 (314); *Christoph/Dorn-Haag*, NSTZ 2020, 697 (699); *Erb* (Fn. 92), § 269 Rn. 35; *Kulhanek*, wistra 2021, 220 (224); *Puschke/Haas*, RdZ 2022, 4 (10).

⁹⁴ *Christoph/Dorn-Haag*, NSTZ 2020, 697 (699); *Kulhanek*, wistra 2021, 220 (224).

⁹⁵ *Grüneberg* (Fn. 12), § 675f Rn. 19, § 675j Rn. 3.

Grundlage geführte Konto und die ebenfalls ausgegebene (persönliche) Karte ergibt.⁹⁶ Nach den oben zu § 269 StGB angestellten Erwägungen kommt man daher nicht umhin, auch i.R.d. § 263a Abs. 1 Var. 3 StGB von einer Täuschungsäquivalenz auszugehen. Insbesondere wäre es widersprüchlich, i.R.d. §§ 269, 270 StGB ein Handeln zur fälschlichen Beeinflussung einer Datenverarbeitung (dem Pendant zur Täuschung im Rechtsverkehr) zu bejahen, i.R.d. § 263a Abs. 1 Var. 3 StGB in Bezug auf die Verwendung der auf der Karte gespeicherten Daten den Täuschungscharakter hingegen zu verneinen. Die über den Einsatz der Karte abgegebenen Erklärungen (Zahlungsauftrag und Autorisierung) sind im Deckungsverhältnis notwendige Grundlage für die Ausführung der Zahlung durch die kartenausgebende Bank.

Für eine einheitliche Einordnung der Kartenzahlung mit und ohne Eingabe der PIN spricht zudem, dass der Täter vor dem Einsatz der Karte nicht überblicken kann, ob die Voraussetzungen für eine kontaktlose Zahlung (maximal fünf Verfügungen ohne PIN-Eingabe, Höchstbetrag von 150 Euro) vollständig gegeben sind oder nicht, und es daher wenig plausibel erscheint, den Inhalt der mit der Kartennutzung zum Ausdruck gebrachten Erklärung davon abhängig zu machen, ob bei der Zahlung eine PIN eingegeben wird oder nicht.⁹⁷ Folgt man der Auslegung des OLG Hamm, ist eine solche Unterscheidung zwar folgerichtig und eine Täuschung über die Berechtigung erst dann zu bejahen, wenn die PIN tatsächlich eingegeben wird.⁹⁸ Wird auf die Abfrage der PIN hingegen verzichtet, so wird der Inhalt der abgegebenen Erklärung durch eben diesen Verzicht erst zu einem Zeitpunkt festgelegt, zu dem das Erklärungsverhalten (Vorhalten der Karte) bereits abgeschlossen ist. Dieses Ergebnis ist aus der Sicht desjenigen, der die Erklärung abgibt, wenig plausibel.⁹⁹

Schließlich lässt sich auch auf die Nähe zu (kleineren) Bargeldzahlungen keine andere Bewertung stützen.¹⁰⁰ Der Verzicht auf eine starke Authentifizierung (und das damit einhergehende Missbrauchsrisiko) wird zwar nur bei kleineren Geldbeträgen zugelassen, allerdings erfolgt die Zahlung – anders als bei der Barzahlung – nicht anonym, vielmehr ist ein Bezug zu dem Konto des Karteninhabers für die Zah-

lungsabwicklung weiterhin zwingende Voraussetzung (II. 2. b) zur Autorisierung).¹⁰¹

e) Weite betrugsspezifische Auslegung und subjektive Auslegung

Schließlich lässt sich die Annahme einer unbefugten Datenverwendung auch auf die Variante der betrugsspezifischen Auslegung stützen, welche die Täuschungsäquivalenz nicht davon abhängig macht, dass die betreffenden Tatsachen auch vom Computer geprüft werden, sondern auch die konkludente Täuschung der fiktiven Vergleichsperson erfassen.¹⁰² Auch der BGH hat in seiner jüngeren Rechtsprechung Zweifel an der engen Auslegung erkennen lassen und es beim Computersportwettbetrug für eine unbefugte Verwendung von Daten ausreichen lassen, dass die von den Wettanbietern eingesetzten Programme durch Festlegung von Höchstgrenzen für Wetteinsätze den Willen dokumentieren, Wetten auf manipulierte Spiele nicht oder jedenfalls nicht zu den gegebenen Wettquoten zuzulassen.¹⁰³ Eine unbefugte Datenverwendung ist damit auf der Grundlage der betrugsspezifischen Auslegung zu bejahen, wenn – entsprechend den Grundsätzen der konkludenten Täuschung beim Betrug – die Befugnis des Täters typischerweise zur Grundlage des betreffenden Geschäfts gehört und nach der Verkehrsanschauung als selbstverständlich vorhanden vorausgesetzt wird.¹⁰⁴

So sieht der BGH inzwischen auch Bestellungen über das Internet, die mit fremden Kreditkarten getätigt und automatisiert abgewickelt werden, als Computerbetrug an, ohne insofern zu fordern, dass die Berechtigung zur Nutzung der Karte bei der Bearbeitung der Bestellung kontrolliert wird.¹⁰⁵ Gleich-

⁹⁶ Puschke/Haas, RdZ 2022, 4 (8).

⁹⁷ Puschke/Haas, RdZ 2022, 4 (8 f.).

⁹⁸ Christoph, ZJS 2022, 761 (767), mit der rhetorischen Frage, warum eine Berechtigung trotz des Verzichts auf die Abfrage der PIN stets miterklärt werden sollte.

⁹⁹ Siehe dagegen Christoph, ZJS 2022, 761 (767), wonach die Abfrage der PIN die Ausnahme und daher nicht der Auslegung der Erklärung zugrunde zu legen sei. Mit dem Verweis auf das Regel-Ausnahme-Verhältnis wird indes die oben genannte Differenzierung aufgegeben bzw. es müsste davon ausgegangen werden, dass der Nutzer beim Vorhalten der Karte noch keine Erklärung über seine Berechtigung abgibt (also kontaktlos bezahlen will), den Inhalt der Erklärung aber bei Abfrage der PIN ändert bzw. um seine Berechtigung erweitert.

¹⁰⁰ So aber Ceffinato, JuS 2021, 311 (313); siehe auch Kudlich, JA 2020, 710 (712).

¹⁰¹ Darüber hinaus erscheint zweifelhaft, ob aus § 935 Abs. 2 BGB abgeleitet werden kann, dass bei einer Zahlung mit gestohlenem Geld nicht über die Berechtigung getäuscht wird (so Ceffinato JuS 2021, 311 [313]), denn der Eigentumserwerb setzt auch insoweit die Gutgläubigkeit des Erwerbers und damit einen Irrtum voraus, siehe dazu unten 2. c), d).

¹⁰² Heger (Fn. 6), § 263 Rn. 13a; Hefendehl/Noll (Fn. 6), § 263a Rn. 82; Hoyer (Fn. 69), § 263a Rn. 19; Perron, in: Schönke/Schröder, Strafgesetzbuch Kommentar, 30. Aufl. 2019, § 263a Rn. 9; Rengier (Fn. 6), § 14 Rn. 22; Wessels/Hillenkamp/Schuh, Strafrecht, Besonderer Teil 2, 45. Aufl. 2022, Rn. 649; Waßmer, in: Leitner/Rosenau (Hrsg.), Nomos Kommentar, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2022, § 263a Rn. 40.

¹⁰³ BGH NJW 2013, 1017 (1018); BGH NJW 2016, 1336 (1337); krit. insoweit Altenhain (Fn. 69), § 263a Rn. 12; vgl. ferner bereits zu BGH NStZ 2016, 149 oben unter b).

¹⁰⁴ BGH NJW 2013, 1017 (1018); BGH NJW 2016, 1336 (1337); OLG Zweibrücken NStZ 2022, 550 (551).

¹⁰⁵ BGH BeckRS 2020, 16555 Rn. 13; siehe auch BGH BeckRS 2020, 28985 Rn. 12 f.; BGH BeckRS 2022, 31922 Rn. 11 f.; siehe ferner zur Prüfung der Bonität des berechtigten Karteninhabers bei der Bestellung: Hefendehl/Noll (Fn. 6), § 263a Rn. 119; Rengier, in: Saliger/Isfen/Kim/Liu/Mylonopoulos/Tavares/Yamanaka/Zheng (Hrsg.), Rechtsstaatliches Strafrecht, Festschrift für Ulfrid Neumann zum

ches müsste für die Verwendung einer Kredit- oder Debitkarte zum kontaktlosen Bezahlen gelten, da es auch insoweit nicht darauf ankäme, ob die Berechtigung des Kartennutzers bei der Zahlung überprüft wird.

Zu dem gleichen Ergebnis käme die subjektive Auslegung des Merkmals „unbefugt“, die auf den Willen des zur Verwendung dieser Daten Berechtigten abstellt.¹⁰⁶ Auch für diese Auslegung finden sich Ansätze in der neueren Rechtsprechung.¹⁰⁷ Der Missbrauch einer Karte, die dem Inhaber abhandengekommen ist, erfolgt gegen den Willen des Berechtigten und damit unbefugt, da sie sowohl dem Willen der kartenausgebenden Bank als auch dem Willen des Karteninhabers widerspricht. Nach beiden Auffassungen liegt das Handlungsunrecht darin, dass der Täter mit dem Missbrauch der Karte eine Befugnis vorspiegelt, über die er tatsächlich nicht verfügt.

f) Weitere Tatbestandsmerkmale des § 263a Abs. 1 Var. 3 StGB

Sieht man in dem Missbrauch der Karte zum kontaktlosen Zahlen eine unbefugte Verwendung von Daten, so ist der objektive Tatbestand des § 263a Abs. 1 Var. 3 StGB erfüllt: Mit der Nutzung der Karte wird das Ergebnis eines Datenverarbeitungsvorgangs beeinflusst, denn der (vermeintliche) Zahlungsauftrag des Karteninhabers führt zu einer Autorisierung der Zahlung durch die kartenausgebende Bank, mit der sich diese gem. § 780 BGB gegenüber dem Händler zur Zahlung des autorisierten Betrages verpflichtet. Da der Karteninhaber diese Zahlung nicht autorisiert hat, wird diese Vermögensminderung nicht durch einen Aufwendungsersatzanspruch der Bank kompensiert, so dass die Bank einen Vermögensschaden erleidet (s.o. III. vor 1.).¹⁰⁸ Der objektive Tatbestand ist damit erfüllt.

Geht man davon aus, dass der Täter in Bezug auf die auf diese Weise bewirkte Schädigung der Bank zumindest mit bedingtem Vorsatz handelt, so wäre für die Verwirklichung des subjektiven Tatbestands weiterhin erforderlich, dass der Täter in der Absicht handelt, sich oder einen Dritten rechtswidrig und „stoffgleich“ zu bereichern.

Die vom Täter selbst angestrebte Bereicherung um die gekaufte Ware beruht nicht auf dem Schaden der Bank, son-

dern auf der vertraglichen Leistung des Händlers und ist damit nicht „stoffgleich“.¹⁰⁹ Allerdings wird der Käufer mit der Zahlung der Bank von seiner Verpflichtung zur Kaufpreiszahlung frei (s.o. II. 1.); dieser Vorteil beruht auf dem vom Täter veranlassten Datenverarbeitungsvorgang, so dass die Anforderungen der Bereicherungsabsicht insoweit gegeben wären.¹¹⁰ Dagegen wird allerdings eingewandt, dass der Anspruch des Händlers mit dem Zustandekommen des abstrakten Schuldversprechens noch nicht erlischt, da die Kartenzahlung nur als Leistung erfüllungshalber angenommen wird (s.o. II. 1.).¹¹¹ Diesem Einwand ist indes entgegenzuhalten, dass bereits die Aussicht auf das Erlöschen der Forderung einen wirtschaftlichen Wert hat und überdies auch der Eintritt der Erfüllungswirkung mit der Gutschrift des Zahlungsbetrages auf dem Konto des Händlers auf dem vom Täter angestoßenen Datenverarbeitungsvorgang beruht.

Selbst wenn man die Stoffgleichheit in Bezug auf die vom Täter angestrebte (eigene) Bereicherung verneint, liegt eine solche jedenfalls in Bezug auf eine ebenfalls vom Täter beabsichtigte Drittbereicherung vor, denn die Bereicherung des Händlers um den Zahlungsanspruch gegen die kartenausgebende Bank (§ 780 BGB) ist notwendige Voraussetzung dafür, dass der Händler die Ware an den Täter übergibt, ohne die ihm zustehende Einrede nach § 320 BGB geltend zu machen.¹¹² Der subjektive Tatbestand des § 263a Abs. 1 Var. 3 StGB ist daher ebenfalls erfüllt.

g) Die Pflicht zur richtlinienkonformen Auslegung

Für eine Auslegung des § 263a Abs. 1 Var. 3 StGB, die auch den Missbrauch von Kredit- und Debitkarten zur kontaktlosen Zahlung erfasst, spricht schließlich das Gebot zur unionsrechts- bzw. richtlinienkonformen Auslegung.¹¹³ Art. 6 lit. b der Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug

70. Geburtstag, 2017, S. 1149 (1154 ff.); a.A. OLG Karlsruhe NJW 2009, 1287 (1288).

¹⁰⁶ Hilgendorf, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafgesetzbuch, Kommentar, 5. Aufl. 2021, § 263a Rn. 10, 14; Kindhäuser/Hoven (Fn. 81), § 263a Rn. 27; Mitsch, Strafrecht, Besonderer Teil 2, 3. Aufl. 2015, S. 398; Kindhäuser/Böse, Strafrecht, Besonderer Teil II, 12. Aufl. 2022, § 28 Rn. 23.

¹⁰⁷ Vgl. BGH NZWiSt 2017, 79 f., mit dem Hinweis, dass eine Weitergabe der Debitkarte zur Verwendung nach den AGB ausgeschlossen ist, daher nicht als Erteilung einer entsprechenden Vollmacht gedeutet werden kann; zur entsprechenden Deutung dieser Entscheidung: Christoph/Dorn-Haag, NSTZ 2020, 697 (703); Kindhäuser/Böse (Fn. 106), § 28 Rn. 49; Stam, NZWiSt 2017, 238 (240).

¹⁰⁸ So auch Göhler, JR 2021, 8 (19).

¹⁰⁹ Göhler, JR 2021, 8 (19); Hefendehl/Noll (Fn. 6), § 263a Rn. 185; a.A. Burghardt/Bardowicks, ZJS 2023, 593 (605).

¹¹⁰ Hoyer (Fn. 69), § 263a Rn. 56.

¹¹¹ Göhler, JR 2021, 8 (19).

¹¹² Hefendehl/Noll (Fn. 6), § 263a Rn. 185; Kindhäuser/Böse (Fn. 106), § 28 Rn. 53. Der Umstand, dass der Händler seine Leistung erbringt und damit sein eigenes Vermögen mindert, steht dem nicht entgegen (so aber Göhler, JR 2021, 8 [19]), denn bei der Stoffgleichheit von Bereicherung und Vermögensschaden geht es um das Verhältnis von Verfügendem (Bank) und Bereichertem (Händler). Nach Burghardt/Bardowicks, ZJS 2023, 593 (606), soll die Rechtswidrigkeit der Drittbereicherung aufgrund des bestehenden Anspruchs des Händlers gegen die Bank ausgeschlossen sein. Indes bleiben Ansprüche, die Produkt der Täuschung sind, bei der Rechtswidrigkeit der Bereicherung außer Betracht, Mitsch (Fn. 106), S. 342.

¹¹³ Siehe zu diesem Gebot und seinen Grenzen: EuGH, Urt. v. 8.10.1987 – C-80/86 (Kolpinghuis Nijmegen) = Slg. 1987, 3969 Rn. 12 f.; EuGH, Urt. v. 28.6.2012 – C-7/11 (Caronna) = BeckRS 2012, 81321 Rn. 51 f.; BGHSt 37, 330 (336); 50, 347 (355); BGH NSTZ 2004, 285; Hecker, Europäisches Strafrecht, 6. Aufl. 2021, S. 366 ff.; Satzger, Internationales und Europäisches Strafrecht, 10. Aufl. 2022, § 9 Rn. 106 ff.

und Fälschung bei unbaren Zahlungsmitteln¹¹⁴ verpflichtet die Mitgliedstaaten sicherzustellen, dass „das vorsätzliche [...] Veranlassen einer Übertragung von Geld, monetären Werten oder virtueller Währung, durch das einer anderen Person ein unrechtmäßiger Vermögensverlust entsteht, mit der Absicht, dem Zuwiderhandelnden oder einem Dritten einen unrechtmäßigen Vermögensvorteil zu verschaffen, als Straftat geahndet wird, wenn [...] Computerdaten unrechtmäßig eingegeben, verändert, gelöscht, übertragen oder unterdrückt werden.“

Nutzt ein anderer als der berechtigte Karteninhaber eine Kredit- oder Debitkarte zum kontaktlosen Bezahlen, so werden damit Computerdaten unrechtmäßig eingegeben und übertragen. Die dadurch veranlasste Übertragung von Geldwerten führt bei der kartenausgebenden Bank zu einem Vermögensschaden (Verlust), zugleich will sich der Täter selbst bzw. dem Händler als Dritten einen unrechtmäßigen Vermögensvorteil verschaffen (s.o. f). Dass die damit bestehende unionsrechtliche Kriminalisierungspflicht auch und gerade das Bezahlen ohne PIN-Abfrage umfasst, lässt sich den Erwägungsgründen entnehmen, wonach die Richtlinie auch neue Zahlungstechnologien und neue Arten von Zahlungsinstrumenten einbeziehen soll, die Verbrauchern und Unternehmen – wie das kontaktlose Bezahlen – neue Möglichkeiten bieten, gleichzeitig aber auch mehr Gelegenheit zum Betrug schaffen (Erwägungsgrund 6).

Der deutsche Gesetzgeber hat insoweit keinen Umsetzungsbedarf gesehen, da § 263a StGB das unter Strafe zu stellende Verhalten vollständig erfasse.¹¹⁵ Dementsprechend ist mit dem Gesetzgeber davon auszugehen, dass § 263a Abs. 1 Var. 3 StGB auch die unrechtmäßige Eingabe und Übertragung der auf der jeweiligen Karte gespeicherten Computerdaten beim kontaktlosen Bezahlen umfasst. Ob die unionsrechtlichen Vorgaben mit der Formulierung „unrechtmäßig“ darüber hinaus eine subjektive Auslegung favorisieren, die sich vom Erfordernis eines Täuschungsäquivalents löst (s.o. e), kann dabei letztlich dahingestellt bleiben.

2. Dreiecksbetrug (§ 263 StGB) gegenüber dem Händler und zum Nachteil der Bank

Beim Missbrauch der Karte interagiert der Täter nicht nur mit dem Computer der kartenausgebenden Bank, sondern auch mit dem Händler, der das Angebot der Bank auf Abschluss eines abstrakten Schuldversprechens (§ 780 BGB) annimmt; mit der Entstehung einer Verbindlichkeit in Höhe des autorisierten Betrages wird das Vermögen der Bank gemindert. Als

¹¹⁴ Richtlinie (EU) 2019/713 v. 17.4.2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. 2019 EU Nr. L 123/18. Eine im Wesentlichen gleichlautende Verpflichtung ist bereits in Art. 3 Rahmenbeschluss 2001/413/JI v. 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (ABl. 2001 EU Nr. L 149/1) und Art. 8 des Europarats-Übereinkommens über Computerkriminalität v. 23.11.2001 (BGBl. II 2008, S. 1243) enthalten.

¹¹⁵ BT-Drs. 19/25631, S. 9; siehe bereits zu Art. 3 Rahmenbeschluss 2001/413/JI: BT-Drs. 15/1720, S. 7.

Vermögensverfügung wäre in diesem Fall also nicht die Autorisierung der Zahlung durch die Bank selbst, sondern eine Willenserklärung des Händlers anzusehen. Diese Erklärung wird entweder durch den Händler selbst oder eine von diesem bevollmächtigte Person abgegeben, so dass insoweit eine Strafbarkeit nach § 263 Abs. 1 StGB in Betracht kommt.

a) Keine Täuschung des Händlers (OLG Hamm)

Der Betrugstatbestand setzt insoweit eine Täuschung und einen entsprechenden Irrtum des Händlers voraus. Beides verneint das OLG Hamm mit folgender Begründung:

„Die Einlösungsgarantie der Bank gegenüber dem Händler entfällt nur im Ausnahmefall, insbesondere unter dem Gesichtspunkt des Rechtsmissbrauchs, wenn der Händler vorsätzlich kollusiv mit einem Nichtberechtigten zusammenwirkt [...]. Für das Entstehen des Zahlungsanspruchs gegen die Bank muss der Händler die Berechtigung des kartenvorlegenden Kunden deshalb weder positiv überprüfen noch muss er sich diese auch nur vorgestellt haben. [...] Vor dem Hintergrund dieser Zahlungsmodalitäten hatten die Kassenkräfte des H-Marktes vorliegend keinerlei Anlass, sich Vorstellungen über die Berechtigung des Angeklagten zur Kartenverwendung zu machen. Im Gegenteil liefen sie vielmehr Gefahr, bei positiver Kenntnis von der Nichtberechtigung wegen kollusiven Zusammenwirkens mit dem Kartenverwender ihren Zahlungsanspruch [...] zu verlieren, weshalb aus Händlersicht gerade kein Anreiz bestand, über die Berechtigung des Angeklagten nachzudenken und so womöglich bösgläubig zu werden. [...] Auch traf den [Händler ...] keine Pflicht, die Berechtigung des Angeklagten anderweitig zu überprüfen, etwa durch Ausweiskontrolle. Damit aber fehlt es an einer Grundlage für die Annahme, dass der Angeklagte als Kunde seine Berechtigung zur Kartennutzung nach der Verkehrsanschauung fälschlich konkludent erklärt hätte und dass die Kassenmitarbeiter wenigstens im Sinne eines sachgedanklichen Mitbewusstseins einer entsprechenden irrigen Vorstellung unterlegen wären. Eine Betrugsstrafbarkeit scheidet damit in den vorliegenden Fällen einer kontaktlosen ec-Kartenzahlung ohne PIN-Abfrage schon mangels Täuschung des Angeklagten über seine Berechtigung zur Verwendung der ec-Karte und mangels damit korrespondierenden Irrtums der im Lager des Händlers stehenden Kassenmitarbeiter aus.“¹¹⁶

b) Einheitliche Bedeutung der vom Kartennutzer abgegebenen Erklärung

Ob die Kartenzahlung durch einen nichtberechtigten Dritten als Täuschung des Händlers anzusehen ist, bestimmt sich wiederum danach, welcher Erklärungsgehalt diesem Verhalten zukommt. Wie bereits dargelegt, enthält der Einsatz der Karte (mit oder ohne Eingabe der PIN) im Deckungsverhältnis einen Zahlungsauftrag an die Bank und eine Autorisierung dieser Zahlung. Da diese Erklärung nicht vom berechtigten Karteninhaber, sondern von einem dazu nichtberechtigten

¹¹⁶ OLG Hamm BeckRS 2020, 9059 Rn. 13–15.

ten Dritten abgegeben wird, liegt insoweit eine Täuschung vor (s.o. I. d), e). Eine Täuschung gegenüber dem Händler lässt sich daher nur unter der Voraussetzung verneinen, dass dem Verhalten des Kartennutzers im Verhältnis zum Händler eine andere Bedeutung zukommt, dieser also gegenüber dem Händler keine Erklärung über die Autorisierung der Zahlung abgibt und dieser damit auch nicht Täuschungsadressat der vom Täter erstellten unechten Datenurkunde ist (s.o. I. d) zu § 269 StGB).

Dagegen spricht indes, dass die Auslösung der Zahlung nicht nur im Deckungsverhältnis, sondern auch im Vollzugs- und Valutaverhältnis relevant ist: Sofern man der Auffassung folgt, wonach das abstrakte Schuldversprechen (§ 780 BGB) im Zuwendungsverhältnis zwischen kartenausgebender Bank und Händler über den Kunden als Boten bzw. Vertreter der Bank zustande kommt (s.o. I. 1.), setzt dies – wie im Deckungsverhältnis – voraus, dass der Kunde als berechtigter Karteninhaber (d.h. nicht als falsus procurator bzw. Pseudobote) für die kartenausgebende Bank gegenüber dem Händler ein entsprechendes Angebot abgibt.¹¹⁷ Selbst wenn man davon ausgeht, dass das abstrakte Schuldversprechen unmittelbar durch die von der Bank erteilte Autorisierung der Zahlung zustande kommt, spricht gegen die Deutung des OLG Hamm, dass es sich um ein und dasselbe Verhalten (Einsatz der Karte zur Zahlung) handelt, das nicht nur im Deckungsverhältnis, sondern auch im Valutaverhältnis Rechtswirkungen (Kartenzahlung als Leistung erfüllungshalber) entfaltet. Für eine einheitliche Deutung spricht auch ein zentrales Kriterium für die Annahme konkludenter Täuschungen, wonach jedenfalls solche Tatsachen schlüssig miterklärt werden, deren Gegenteil in einem normativen, empirischen oder logischen Widerspruch zum Erklärungsinhalt stünde.¹¹⁸ Eine unterschiedliche, vom Erklärungsempfänger abhängige Deutung des Erklärungsverhaltens, mit dem eine Berechtigung zum Teil miterklärt (Deckungsverhältnis), zum Teil nicht miterklärt wird, liefe auf eine in sich widersprüchliche Erklärung des Kartennutzers hinaus.

c) Irrelevanz der Berechtigung des Kartennutzers für den Händler?

Nun ließe sich ein solcher Widerspruch möglicherweise ausräumen, indem man im Verhältnis zum Händler von einer inhaltlich verkürzten Erklärung ausgeht, die keine Aussage zur Identität des Nutzers bzw. seiner Berechtigung enthält. Für eine solche „empfängerrelative“ Auslegung des Erklärungsverhaltens ließe sich mit dem OLG Hamm anführen, dass eine bestimmte Tatsache (die Berechtigung zur Nutzung der Karte) nicht für jeden Erklärungsempfänger mit Blick auf die von ihm zu treffenden Vermögensdispositionen gleicher-

maßen relevant sind: Da der Händler auch bei einer Kartenzahlung durch einen Nichtberechtigten einen Zahlungsanspruch gegen die kartenausgebende Bank erwirbt, bleiben seine Vermögensinteressen von diesem Umstand unberührt. Dieses Argument beruht auf dem zutreffenden Ausgangspunkt, dass eine Täuschung i.S.d. § 263 StGB sich auf Umstände beziehen muss, die nach der Verkehrsanschauung für das Opfer Voraussetzung der von ihm vorzunehmenden Verfügung sind.¹¹⁹ Daraus wird die allgemeine Regel abgeleitet, dass eine Täuschung zu verneinen sei, wenn sie sich auf Umstände beziehe, von deren Prüfung der Adressat der Erklärung im Interesse des Verkehrsschutzes befreit sei.¹²⁰ Weil vom Adressaten nicht erwartet werde, sich über diese Umstände Gedanken zu machen, wird zum Teil auch ein entsprechender Irrtum verneint.¹²¹

Aus diesem Grund wird eine Strafbarkeit nach § 263 StGB bei der Abhebung des Guthabens von einem Sparbuch durch einen Nichtberechtigten¹²², aber auch beim Missbrauch einer Kreditkarte durch einen Nichtberechtigten¹²³ oder deren Einsatz einer Debitkarte im POS-Verfahren durch einen anderen als den Karteninhaber¹²⁴ abgelehnt.

Beim Sparbuch soll dies allerdings nicht gelten, wenn besondere Umstände auf die fehlende Berechtigung hindeuten, weil die befreiende Wirkung der Leistung an den Nichtberechtigten nicht eintritt, wenn der Schuldner diese kennt oder grob fahrlässig nicht erkennt.¹²⁵ Es erscheint jedoch wenig plausibel, den Inhalt der mit der Vorlage des Sparbuchs einhergehenden Erklärung über die Berechtigung an derartige Verdachtsmomente zu knüpfen, im Übrigen aber davon auszugehen, dass der Täter lediglich erklärt, im Besitz des Sparbuchs zu sein.¹²⁶ Aufgrund der Einschränkungen der befreienden Wirkung bei Vorsatz und grober Fahrlässigkeit und den damit einhergehenden Prüfungspflichten wird vielmehr überwiegend davon ausgegangen, dass der Täter über die eigene Berechtigung täuscht und der Schuldner einem entsprechenden Irrtum unterliegt.¹²⁷ Nach dieser Prämisse müss-

¹¹⁹ Frisch, in: Pawlik/Zaczyk (Hrsg.), Festschrift für Günther Jakobs zum 70. Geburtstag am 26. Juli 2007, 2007, S. 97 (128 f.); Wachter, NSTZ 2018, 241 (244).

¹²⁰ Hefendehl, in: Erb/Schäfer (Fn. 6), § 263 Rn. 199.

¹²¹ Hoyer (Fn. 69), § 263 Rn. 77 ff.

¹²² OLG Düsseldorf NJW 1989, 2003 (2004); Duttge (Fn. 6), § 263 Rn. 24; Hoyer (Fn. 69), § 263 Rn. 77; Saliger (Fn. 118), § 263 Rn. 62; Tiedemann (Fn. 117), § 263 Rn. 44.

¹²³ Eisele (Fn. 6), Rn. 544; Hoyer (Fn. 69), § 263 Rn. 78; Rengier (Fn. 6), § 13 Rn. 49.

¹²⁴ Eisele/Fad, JURA 2002, 305 (308); Fischer (Fn. 69), § 263 Rn. 59; Hefendehl (Fn. 120), § 263 Rn. 201; Hoyer (Fn. 69), § 263 Rn. 79; Rengier (Fn. 6), § 13 Rn. 49; Saliger (Fn. 118), § 263 Rn. 61; Satzger (Fn. 118), § 263 Rn. 129.

¹²⁵ Siehe die Nachweise in Fn. 122.

¹²⁶ So Hefendehl (Fn. 120), § 263 Rn. 206; Saliger (Fn. 118), § 263 Rn. 61; Tiedemann (Fn. 117), § 263 Rn. 44.

¹²⁷ Dannecker, in: Graf/Jäger/Wittig (Hrsg.), Wirtschafts- und Steuerstrafrecht, Kommentar, 2. Aufl. 2017, § 263 Rn. 61; Eisele (Fn. 6), Rn. 544; Heger (Fn. 6), § 263 Rn. 14; Heinrich, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht, Beson-

¹¹⁷ Zur Täuschung über eine tatsächlich nicht bestehende Vollmacht: BGH NJW 1968, 1147 (1148); Tiedemann, in: Laufhütte/Rissing-van Saan/Tiedemann (Fn. 69), § 263 Rn. 39.

¹¹⁸ Kindhäuser/Hoven (Fn. 81), § 263 Rn. 110; zustimmend Saliger, in: Matt/Renzikowski (Fn. 69), § 263 Rn. 37; Satzger, in: Satzger/Schluckebier/Widmaier (Fn. 106), § 263 Rn. 44.

te dies auch für Kreditkartenzahlungen gelten, da der Händler vertraglichen Schadensersatzansprüchen ausgesetzt ist, wenn er einen naheliegenden Missbrauchsverdacht ignoriert (s.o. I. 1.; vgl. dort auch zur Bösgläubigkeit nach § 173 BGB).¹²⁸

Die Bedeutung derartiger Prüfungspflichten sollte indes nicht überschätzt werden, denn sie benennen nur einen Aspekt, der Rückschlüsse darauf zulässt, dass der zu prüfende Umstand für das Opfer als Voraussetzung der vorzunehmenden Vermögensverfügung relevant ist.¹²⁹ Der Gegenstand einer (konkludenten) Täuschung ist jedoch nicht auf die Umstände zu beschränken, auf die sich eine dem Erklärungsadressaten obliegende Prüfungspflicht bezieht. Es ist vielmehr zwischen den aus der Sicht des Opfers relevanten Verfügungsvoraussetzungen als Gegenstand von Täuschung und Irrtum und den dafür erforderlichen Feststellungen („Prüfung“) zu unterscheiden. In der Sache entspricht dies der in der Auseinandersetzung mit der computerspezifischen Auslegung des § 263a StGB herausgearbeiteten Unterscheidung zwischen Autorisierung durch den berechtigten Karteninhaber und deren Überprüfung durch eine (starke) Authentifizierung. (s.o. I. d): Verfügungsrelevant ist die Berechtigung des Kartennutzers. Diese Berechtigung wird anhand der Vorlage der Karte und ggf. weiterer Faktoren (Eingabe der PIN) überprüft. Der Besitz und ggf. die Kenntnis der PIN sind für den Händler ausreichend, um von der Berechtigung des Kartennutzers ausgehen zu können; aus der Sicht des Händlers setzt die Verfügung aber weiterhin voraus, dass es sich bei dem Kunden um den berechtigten Karteninhaber handelt. Der Inhalt der Erklärung lautet daher nicht „Ich bin im Besitz dieser Karte und habe Kenntnis von der zugehörigen PIN.“, sondern: „Ich bin berechtigt, mit dieser Karte einen Zahlungsvorgang auszulösen.“

Diese Deutung des Erklärungsverhaltens entspricht der allgemeinen Regel, dass mit dem Abschluss eines Rechtsgeschäfts schlüssig miterklärt wird, zur Vornahme des beabsichtigten Geschäfts befugt zu sein.¹³⁰ Die Kartenzahlung als Leistung erfüllungshalber setzt die Berechtigung voraus, die kartenausgebende Bank zu einer Zahlung an den Händler zu veranlassen. Der nichtberechtigte Besitz der Karte begründet für sich allein kein Recht des Besitzers, einen Zahlungsvorgang auszulösen, sondern nur eine im Interesse des Verkehrsschutzes bestehende Rechtsmacht gegenüber gutgläubigen Erklärungsempfängern. Dass der Besitz der Karte für sich genommen keine Zahlungsbefugnis vermittelt, wird daran deutlich, dass der Händler bei einer Offenlegung der fehlenden Berechtigung gehalten wäre, die Zahlung mit der vorge-

legten Karte zurückzuweisen.¹³¹ Es wäre daher widersprüchlich, dem Händler gegenüber anzugeben, mit Karte zu zahlen, aber zugleich zu erklären, nicht der berechtigte Karteninhaber zu sein.¹³² Die Rechtsmacht, die über die Zuweisung des Missbrauchsrisikos an die kartenausgebende Bank begründet wird, steht und fällt daher mit der Gutgläubigkeit, d.h. einem entsprechenden Irrtum des Erklärungsempfängers.¹³³ In diesem Punkt unterscheidet sich der Kartenmissbrauch durch einen nichtberechtigten Dritten von Konstellationen, in denen der berechtigte Karteninhaber seine Karte zur Zahlung einsetzt, obwohl sein Konto keine genügende Deckung aufweist (vgl. § 266b StGB); da die Bonität des Karteninhabers aus der Sicht des Händlers keine Verfügungsvoraussetzung ist, liegt keine Täuschung über die Berechtigung vor und eine Betrugsstrafbarkeit scheidet insoweit aus.¹³⁴

Dementsprechend geht auch die Rechtsprechung davon aus, dass der Missbrauch einer Kreditkarte durch einen Nichtberechtigten den Tatbestand des Betrugs erfüllt.¹³⁵ In dem Unterschreiben des Kreditkartenbelegs mit dem Namen des Karteninhabers wird dabei sogar eine ausdrückliche Täuschung gesehen.¹³⁶ Da der Kreditkartenbeleg die Anweisung zur bzw. Autorisierung der Zahlung verkörpert, wirkt die Täuschung also nach h.M. über das Deckungsverhältnis hinaus auch im Verhältnis zum Händler. Dies muss entsprechend für den Missbrauch der Debitkarte im POS-Verfahren gelten, denn die Abfrage der PIN hat dort die gleiche Funktion, da sie der Überprüfung (Authentifizierung) desjenigen dient, der den Zahlungsvorgang auslöst. Selbst wenn auf eine PIN-Abfrage verzichtet wird, liegt in der Verwendung einer Kredit- oder Debitkarte im POS-Verfahren, in dem der nichtberechtigte Dritte ebenfalls als (vermeintlicher) Karteninhaber eine Zahlung autorisiert und damit gegenüber der Bank seine Berechtigung vortäuscht, wie bei der Nutzung der Kreditkarte im Belegverfahren zugleich eine Täuschung des Händlers. Auch in dieser Hinsicht gebietet es die Parallele zu den Urkundendelikten, eine Täuschung im Rechtsverkehr (und

derer Teil, 4. Aufl. 2021, § 20 Rn. 57; *Momsen* (Fn. 70), § 41 Rn. 64; *Perron* (Fn. 102), § 263 Rn. 16b, 48; *Rengier* (Fn. 6), § 13 Rn. 48; *Wessels/Hillenkamp/Schuhr* (Fn. 102), Rn. 538.

¹²⁸ *Momsen* (Fn. 70), § 41 Rn. 66; *Tiedemann* (Fn. 117), § 263 Rn. 43, 89; siehe auch zu § 263a StGB: *Waßmer* (Fn. 102), § 263a Rn. 49; siehe dagegen *Eisele* (Fn. 6), Rn. 544; *Rengier* (Fn. 6), § 13 Rn. 49.

¹²⁹ *Frisch* (Fn. 119), S. 125, 127 f., spricht insoweit von einem heuristischen Verfahren.

¹³⁰ *Hefendehl* (Fn. 120), § 263 Rn. 236; *Kindhäuser/Hoven* (Fn. 81), § 263 Rn. 126; *Tiedemann* (Fn. 117), § 263 Rn. 39.

¹³¹ Vgl. Bedingungen (Fn. 9), Nr. 8: „Die Eingabe der persönlichen Geheimzahl (PIN) oder die Nutzung der anderen vereinbarten Authentifizierungselemente darf nur durch den Karteninhaber erfolgen.“; siehe auch allgemein zum Missbrauchsverdacht AGB der BS PAYONE (Fn. 20), Nr. 3.1.

¹³² Vgl. zum Sparbuch: *Kindhäuser/Hoven* (Fn. 81), § 263 Rn. 135.

¹³³ Siehe auch zum Scheck mit Zahlungsgarantie: OLG Köln NJW 1978, 713 (714).

¹³⁴ BGHSt 33, 245 (249); BGH wistra 2005, 222; *Hoyer* (Fn. 69), § 263 Rn. 80; *Momsen* (Fn. 70), § 41 Rn. 66; *Saliger* (Fn. 118), § 263 Rn. 61; *Tiedemann* (Fn. 117), § 263 Rn. 43.

¹³⁵ BGH wistra 2007, 458 (460); LG Berlin wistra 1985, 241 (242); LG Hamburg wistra 1986, 227; ebenso *Kindhäuser/Hoven* (Fn. 81), § 263 Rn. 135; *Perron* (Fn. 102), § 263 Rn. 29a; *Saliger* (Fn. 118), § 263 Rn. 61, 100; *Tiedemann* (Fn. 117), § 263 Rn. 43, 89; siehe auch *Hefendehl* (Fn. 120), § 263 Rn. 200 Fn. 566.

¹³⁶ *Kindhäuser/Hoven* (Fn. 81), § 263 Rn. 135; *Saliger* (Fn. 118), § 263 Rn. 61; *Tiedemann* (Fn. 117), § 263 Rn. 43.

i.R.d. § 263 StGB) nicht davon abhängig zu machen, ob der Täter eine unechte Urkunde herstellt (§ 267 Abs. 1 Var. 1 StGB) oder eine unechte Datenurkunde erstellt (§ 269 StGB; s.o. 1 d).

d) Vermögensrelevanz der Berechtigung beim Dreiecksbetrug

Das Argument des OLG, dass der Händler keinen Anlass habe, sich über die Berechtigung des Kartennutzers Gedanken zu machen, und eine Täuschung und ein Irrtum des Händlers deshalb ausgeschlossen seien, ist darüber hinaus einem weiteren Einwand ausgesetzt. Da der Händler einen Zahlungsanspruch gegen die kartenausgebende Bank erwirbt, tritt der Vermögensschaden nicht beim Händler, sondern bei der kartenausgebenden Bank ein. Eine Strafbarkeit nach § 263 StGB kommt daher nur in Gestalt eines Dreiecksbetruges gegenüber dem Händler und zum Nachteil der Bank in Betracht (s.o. 2.). Eine täuschungs- und irrumsbedingte Verfügung des Händlers bezieht sich also nicht auf dessen eigenes Vermögen, sondern auf das der Bank. Für die Frage, welche Umstände für eine Verfügung aus der Sicht des Erklärungsadressaten relevant sind, ist daher beim Dreiecksbetrug nicht auf das Vermögen des Verfügenden, sondern auf das Vermögen des Geschädigten abzustellen. Exemplarisch: Bezahlt der Täter an der Ladenkasse Waren mit Falschgeld,¹³⁷ so ist die Vermögensrelevanz dieses Umstands nicht aus der Sicht des Kassenspersonals, das in der Regel nicht für den Schaden einzustehen hat, sondern aus der Sicht des geschädigten Ladeninhabers zu bestimmen.¹³⁸ Dementsprechend sind bei der Frage, ob der Händler über einen bestimmten Umstand getäuscht wird und einem entsprechenden Irrtum erliegt, nicht die Auswirkungen dieses Umstands auf sein eigenes Vermögen, sondern diejenigen auf das Vermögen der geschädigten Bank maßgeblich. Aus deren Sicht ist es wiederum entscheidend, ob die Karte vom Karteninhaber oder einem nichtberechtigten Dritten eingesetzt wird, denn in dem letztgenannten Fall besteht kein Aufwendungsersatzanspruch gegen den Kunden (s.o. II. 1.). Dem Erklärungsverhalten des Kartennutzers gegenüber dem Händler wäre mithin die gleiche Bedeutung beizumessen wie im Deckungsverhältnis.

Damit verlagert sich die entscheidende Frage auf das Tatbestandsmerkmal der Verfügung, d.h. das für einen Dreiecksbetrug erforderliche Näheverhältnis zwischen Verfügendem (Händler) und Geschädigtem (Bank). Zum Teil wird es für einen Dreiecksbetrug bereits als ausreichend angesehen, wenn die verfügende Person aufgrund von Rechtsscheinsgrundsätzen über das Vermögen des Geschädigten verfügen kann, wie z.B. der gutgläubige Erwerber über das Eigentums-

recht des Opfers (§ 932 BGB).¹³⁹ Dem wird allerdings entgegengehalten, dass vor der Verfügung keinerlei Rechtsverhältnis zwischen Verfügendem und Geschädigten besteht, auf das eine Zurechnungseinheit gestützt werden könnte.¹⁴⁰ Ein solches Rechtsverhältnis besteht allerdings nach Abtretung einer Forderung zwischen Schuldner und Zessionar; wenn der Schuldner gutgläubig an den Zedenten leistet und die Forderung des Zessionars dadurch erlischt (§ 407 Abs. 1 BGB), wird daher überwiegend eine Verfügung des Schuldners zum Nachteil des Zessionars bejaht.¹⁴¹ Auf dieser Linie liegt auch eine Entscheidung des BGH, wonach ein Angestellter, der unter Vorspiegelung einer Inkassovollmacht Forderungen seines Arbeitgebers einzieht, einen Dreiecksbetrug zum Nachteil seines Arbeitgebers begeht, der die Zahlungen des jeweiligen Schuldners (als Verfügung über sein Vermögen) nach § 56 HGB gegen sich gelten lassen muss.¹⁴² Da sich das Verhältnis zwischen Händler und der kartenausgebenden Bank nach den für den Einsatz der Kreditkarte bzw. für das POS-Verfahren geltenden Händlerbedingungen bestimmt, wäre das für die Zurechnung erforderliche Näheverhältnis nach den vorstehenden Grundsätzen zu bejahen. Dies gilt auch dann, wenn man Rechtsscheintatbestände nicht als ausreichend ansieht, da diese allein dem Verkehrsschutz dienen.¹⁴³ Eine Schutzfunktion gegenüber dem Vermögensinhaber kann sich nämlich insbesondere aus vermögensbezogenen Prüfungspflichten ergeben.¹⁴⁴ Der Händler ist verpflichtet, die sich aus den Vertragsbedingungen ergebenden Sicherheitsanforderungen beim Betrieb der Kartenlesegeräte zu beachten.¹⁴⁵ Bei Verdachtsmomenten, die auf einen Missbrauch der Karte hindeuten, darf der Händler die Karte nicht akzeptieren¹⁴⁶; bei einer Verletzung dieser Pflicht kann sich der Händler schadensersatzpflichtig machen (s.o. II. 1.). Ein Schutz- bzw. Näheverhältnis liegt damit vor, der Händler verfügt daher mit der Annahme des Angebots zum Abschluss eines abstrakten Schuldversprechens über das Vermögen der

¹³⁹ Fischer (Fn. 69), § 263 Rn. 84, 85; Kindhäuser/Hoven (Fn. 81), § 263 Rn. 212, 220; Momsen (Fn. 70), § 41 Rn. 82; Tiedemann (Fn. 117), § 263 Rn. 117.

¹⁴⁰ Eisele (Fn. 6), Rn. 570; Hoyer (Fn. 69), § 263 Rn. 178; Hefendehl (Fn. 120), § 263 Rn. 472; Mitsch (Fn. 106), S. 302; Perron (Fn. 102), § 263 Rn. 67; Rengier (Fn. 6), § 13 Rn. 136; Saliger (Fn. 118), § 263 Rn. 144; im Ergebnis ebenso RGSt 49, 16 (19 f.: keine Verfügung des Erwerbers).

¹⁴¹ OLG Celle NJW 1994, 142 (143); Eisele (Fn. 6), Rn. 571; AG Eggenfelden NSTZ-RR 2008, 242 (243); Perron (Fn. 102), § 263 Rn. 67; Rengier (Fn. 6), § 13 Rn. 137; ablehnend: Hoyer (Fn. 69), § 263 Rn. 178; Hefendehl (Fn. 120), § 263 Rn. 472; Saliger (Fn. 118), § 263 Rn. 145.

¹⁴² BGH wistra 1992, 299; zustimmend Saliger (Fn. 118), § 263 Rn. 145; siehe auch BGH NJW 1968, 1147 (1148).

¹⁴³ Hefendehl (Fn. 120), § 263 Rn. 472; siehe auch Satzger (Fn. 118), § 263 Rn. 200.

¹⁴⁴ Fischer (Fn. 69), § 263 Rn. 84; Saliger (Fn. 118), § 263 Rn. 143; Satzger (Fn. 118), § 263 Rn. 200.

¹⁴⁵ Vgl. Bedingungen (Fn. 9), nur Nr. 7.

¹⁴⁶ AGB zur Akzeptanz von Debit- und Kreditkarten der BS PAYONE (Fn. 20), Nr. 3.1.

¹³⁷ Vgl. BGH NSTZ 2014, 215.

¹³⁸ Damit soll nicht in Abrede gestellt werden, dass arbeitsvertragliche Pflichten das Kassenspersonal dazu anhalten, eine entsprechende Zahlung zurückzuweisen (vgl. BGH NSTZ 2014, 215 [216]); diese Pflichten sind jedoch nicht für die Tatbestandsmerkmale Täuschung und Irrtum, sondern erst für das Vorliegen einer Verfügung und das dafür erforderliche Näheverhältnis relevant, siehe dazu sogleich im Text.

kartenausgebenden Bank.¹⁴⁷ Dies gilt allerdings nur unter der Voraussetzung, dass das Vermögen der Bank durch das Verhalten des Händlers unmittelbar gemindert wird. Dies könnte mit dem Argument verneint werden, dass eine Vermögensminderung bereits durch das von der Bank abgegebene Angebot eintritt. Diese Frage betrifft das Konkurrenzverhältnis zum Betrugstatbestand und soll daher in diesem Kontext behandelt werden (s.u. 3.).

In Bezug auf den Eintritt eines Vermögensschadens, den Vorsatz und die Bereicherungsabsicht kann auf die Ausführungen zu § 263a StGB verwiesen werden (s.o. 1. f). Nutzt ein Nichtberechtigter eine Kredit- oder Debitkarte zum kontaktlosen Bezahlen, so erfüllt dieses Verhalten mithin auch den Tatbestand des Dreiecksbetruges (§ 263 Abs. 1 StGB).

e) Richtlinienkonforme Auslegung

Dieses Ergebnis entspricht wiederum zugleich dem Gebot der richtlinienkonformen Auslegung (s.o. 1. g). Art. 3 lit. a der Richtlinie zur Bekämpfung von Betrug und Fälschung bei unbaren Zahlungsmitteln¹⁴⁸ verpflichtet die Mitgliedstaaten, „die betrügerische Verwendung gestohlener oder in anderer Weise widerrechtlich angeeigneter oder erlangter unbarer Zahlungsinstrumente“ unter Strafe zu stellen. Der deutsche Gesetzgeber hat auch in Bezug auf diese Vorschrift keinen Umsetzungsbedarf gesehen, da die betrügerische Verwendung von gestohlenen oder auf andere Weise widerrechtlich erlangten Zahlungsinstrumenten umfassend nach § 263 StGB (ggf. auch § 263a StGB) mit Strafe bedroht sei.¹⁴⁹ Dieser Prämisse widerspräche eine Auslegung des § 263 StGB, wonach der Missbrauch einer dem berechtigten Karteninhaber abhandengekommenen Kredit- oder Debitkarte zum kontaktlosen Bezahlen gegenüber dem Händler nicht als „betrügerische“ Verwendung anzusehen wäre.

3. Verhältnis von Betrug und Computerbetrug

Als Zwischenergebnis ist damit festzuhalten, dass die Einwände des OLG Hamm gegen eine Strafbarkeit des Missbrauchs einer abhandengekommenen Kredit- oder Debitkarte zum kontaktlosen Bezahlen nach §§ 263, 263a StGB nicht durchgreifen. Da das Erfolgsunrecht nach beiden Tatbeständen in dem der Bank zugefügten Vermögensschaden liegt, stellt sich abschließend die Frage, ob der Täter wegen Betruges (§ 263 StGB) oder Computerbetruges (§ 263a StGB) zu bestrafen ist.

Nach einer Auffassung ist § 263a StGB als Auffangtatbestand gegenüber § 263 StGB subsidiär.¹⁵⁰ Nach der Gegen-

auffassung stehen beide Tatbestände zueinander in einem Exklusivitätsverhältnis; für die Abgrenzung ist entscheidend, ob die Vermögensverfügung auf einem automatisierten Datenverarbeitungsvorgang oder einem menschlichen Handeln beruht.¹⁵¹ Die Vermögensminderung wird durch den Vertragsschluss über das abstrakte Schuldversprechen (§ 780 BGB) bewirkt. Dieser Vertrag kommt nach überwiegender Auffassung durch die elektronische Autorisierung der Bank als Angebot und durch dessen Annahme durch den Händler zustande (s.o. II. 1. a). Da die rechtsgeschäftliche Bindung der Bank damit (auch) aus einer von dieser selbst abgegebenen Willenserklärung hervorgeht, bedarf es zur Begründung einer Vermögensverfügung keiner Zurechnung der (menschlichen) Willenserklärung des Händlers. Folgt man der letztgenannten Ansicht, so ist daher im Ergebnis nur eine Strafbarkeit wegen Computerbetruges anzunehmen.¹⁵²

IV. Ergebnis

Der Missbrauch einer abhandengekommenen Kredit- oder Debitkarte zum kontaktlosen Bezahlen ist nach alledem entweder als Betrug oder als Computerbetrug strafbar. Dieses Ergebnis ist angesichts der zunehmenden Bedeutung des unbaren Zahlungsverkehrs auch sachgerecht, insbesondere rechtfertigt der Verzicht auf eine starke Authentifizierung bei kleineren Zahlungsbeträgen keine Einschränkung des strafrechtlichen Vermögensschutzes. Eine ausschließliche Ahndung als Urkundendelikt (§§ 269, 274 Abs. 1 Nr. 2 StGB¹⁵³) ließe sich nicht widerspruchsfrei begründen (s.o. III. 1. d) zu § 269 StGB), wäre aber jedenfalls nicht geeignet, das verwirklichte Erfolgsunrecht (Vermögensschaden) vollständig zu erfassen. Die Ahndung als Vermögensdelikt entspricht schließlich auch den unionsrechtlichen Vorgaben (s.o. III. 1. g), 2. e). Dies gilt auch und erst recht für die Kartenzahlungen, bei denen sich der nichtberechtigte Zahler durch eine starke (z.B. Eingabe der PIN) oder eine einfache (z.B. Unterschrift) Authentifizierung legitimiert. Damit kommt es auch nicht mehr darauf an, ob eine starke Authentifizierung vom Zahlungsdienstleister selbst durchgeführt werden muss (s.o. II. 2. c), so dass auch der Missbrauch von Smartphones und anderen geeigneten Endgeräten zum kontaktlosen Bezahlen erfasst wird. Selbst wenn man bei elektronischen Zahlungsverfahren von einem Vorrang des § 263a StGB ausgeht (vgl. oben III. 3.), kommt eine Strafbarkeit nach § 263 StGB zumindest bei der Zahlung mit Kreditkarte im klassischen Belegverfahren in Betracht.

¹⁴⁷ Tiedemann (Fn. 117), § 263 Rn. 117; siehe auch zum Dreiecksbetrug beim Scheck mit Zahlungsgarantie: BGHSt 24, 386 (389); siehe ferner OLG Köln NJW 1978, 713 (714 f.); OLG Hamburg NJW 1983, 768 (769); a.A. Hoyer (Fn. 69), § 263 Rn. 171.

¹⁴⁸ Fn. 114; siehe auch bereits Rahmenbeschluss 2001/413/JI (Fn. 114), Art. 2 lit. d.

¹⁴⁹ BT-Drs. 19/25631, S. 7 f.; vgl. auch zu Art. 2 Rahmenbeschluss 2001/413/JI: BT-Drs. 15/1720, S. 7.

¹⁵⁰ Heger (Fn. 6), § 263a Rn. 27; Perron (Fn. 102), § 263a Rn. 41 f.; Tiedemann/Valerius (Rn. 69), § 263a Rn. 95.

¹⁵¹ Altenhain (Fn. 69), § 263a Rn. 32; Fischer (Fn. 69), § 263a Rn. 38; Hefendehl/Noll (Fn. 6), § 263a Rn. 220.

¹⁵² Vgl. auch Hefendehl/Noll (Fn. 6), § 263a Rn. 170 (zum POS-Verfahren).

¹⁵³ Siehe insoweit OLG Hamm BeckRS 2020, 9059 Rn. 33 ff.