ZStrR
RPS

Stämpfli

ZStrR 4/2021 | S. 385–408 **385**

Abhandlungen

Nora Markwalder, St. Gallen*

Eliane Täuber, St. Gallen**

Bestellbetrug im Onlinehandel

Charakterisierung eines unscheinbaren Delikts

Inhaltsübersicht

I. Einleitung

Die Digitalisierung hat unsere Lebensgewohnheiten grundsätzlich verändert. Dies betrifft auch unser Shoppingverhalten, kaufen wir doch immer häufiger im Internet ein. Im Rahmen einer Befragung des Bundesamtes für Statistik (BFS) aus dem Jahr 2019 gaben insgesamt 75% der Schweizer Bevölkerung im Alter zwischen 16 und 74 Jahren an, in den letzten drei Monaten etwas online eingekauft zu

haben, was die Schweiz im internationalen Vergleich auf Platz zwei der häufigsten Online-Shopper klassiert.[1] Die Tendenz zum Onlineshopping dürfte sich nun durch den Einfluss des Coronavirus akzentuiert haben, sind doch in den letzten Monaten auch Personen auf Onlineshoppingkanäle ausgewichen, die vorher noch nicht oder nur wenig online eingekauft haben. Mit dieser Verschiebung des Einkaufens vom analogen in den digitalen Raum liegt die Hypothese nahe, dass sich dadurch auch die Gelegenheiten der Deliktsbegehung im digitalen Raum vervielfacht haben. Diese Hypothese kann aus makrotheoretischer Perspektive damit erklärt werden, dass die Digitalisierung eine neue «Bresche» geschaffen hat, die sich Kriminelle zunutze machen, solange sie nicht mittels neuer Sicherungsmethoden geschlossen wird.[2] Als Erklärungsansatz für individuelles deliktisches Handeln kann die Theorie des «Routine-Activities-Ansatzes» von *Cohen* und *Felson* hinzugezogen werden, welche die Entwicklung und Verteilung der Kriminalität durch das Vorhandensein krimineller Gelegenheitsstrukturen erklärt. Eine Straftat wird demnach begangen, wenn ein potenzieller Täter auf ein geeignetes Tatobjekt trifft und dieses nicht geschützt ist.[3] Diese tat- und weniger täterbasierte situative Theorie verschiebt somit bei der Prävention den Fokus auf die Reduktion der Verfügbarkeit bzw. Attraktivität des Tatobjekts oder aber auf mögliche Schutzmechanismen des Tatobjekts.[4]

Die Messung von Onlinedelikten gestaltet sich allerdings als äusserst schwierig. Offizielle Statistiken erheben die Tatumstände erst für das Jahr 2020 und zudem nur sehr oberflächlich, weshalb dort nicht genau nachvollzogen werden kann, welche digitalen Hilfsmittel bei Betrugsdelikten zur Anwendung gelangt sind.[5] Und auch Umfragen bei den betroffenen Unternehmen wurden bisher nur punktuell durchgeführt. In einer nicht repräsentativen Studie aus dem Jahr 2020 gaben immerhin 95,4% der befragten Unternehmen an, dass sie in ihrem Onlineshop bereits einmal von Betrug betroffen gewesen sind, und dies, ob-

wohl praktisch alle Onlinehändler Sicherheitsmassnahmen zur Verhinderung von Betrugsdelikten anwenden. Jedoch wurde ebenfalls erwähnt, dass bei der Implementierung von Sicherheitsmassnahmen das richtige Kosten-Nutzen-Verhältnis zwischen Sicherheit mittels Methoden zur Vorbeugung von Betrugsdelikten einerseits und der Erfüllung der Kundenwünsche bei den Zahlungsverfahren andererseits entscheidend ist.[6]

Für die Erkennung und Verhinderung von solchen Onlinebetrugsdelikten ist Kenntnis über die Tatmotive und die Deliktsbegehung ein wichtiger Aspekt. Allerdings haben Betrugsdelikte im E-Commerce bislang kaum Beachtung in rechtlichen und kriminologischen Untersuchungen gefunden. Der vorliegende Beitrag bezweckt daher, das Phänomen des Bestellbetrugs rechtlich einzuordnen und danach mittels einer Datenanalyse bei einem St. gallischen Zahlungsdienstleistungs-Unternehmen auch empirisch zu untersuchen.

II. Bestellbetrug: Phänomenologie und rechtliche Grundlagen

1. Phänomenologie

Die Betrugsmöglichkeiten im E-Commerce sind vielseitig und oft vom Täter und von dessen Motivation abhängig. Dennoch lassen sich gewisse typische Vorgehensweisen in drei Hauptformen zusammenfassen.

Beim sogenannten *Eingehungsbetrug* bewirkt der Täter einen Vertragsabschluss mit dem Onlineanbieter, obwohl er weiss, dass er seine Leistungspflicht in Form der Bezahlung des Kaufpreises nicht erfüllen wird. Dabei täuscht der Täter seine Solvenz gegenüber dem Unternehmen vor, indem er eine Bestellung in dem Bewusstsein tätigt, die Rechnung nicht zu bezahlen.[7] Ein weiterer Modus Operandi besteht darin, eine vermutlich negativ ausfallende Bonitätsprüfung mit geringfügig abgeänderten oder teilweise erfundenen Personendaten zu umgehen, um das Sys-

tem im Glauben zu lassen, dass es sich beim Käufer um einen Neukunden handelt. Diese Veränderung der Daten kann bereits darin liegen, den Vor- und Nachnamen zu vertauschen, das Geburtsdatum um einen Tag anzupassen oder die Hausnummer leicht zu verändern.[8] Für ein automatisches Prüfsystem bedeuten diese leicht abgeänderten Angaben i.d.R. ein neues Kundenprofil, folglich können dieser Person keine negativen Zahlungserfahrungen zugeordnet werden, und eine Bestellung auf Kredit wird freigegeben. Rund 71% der befragten Schweizer Anbieter gaben 2020 bei einer Umfrage an, bereits mit dieser Betrugsform konfrontiert gewesen zu sein.[9]

Eine zweite Vorgehensweise betrifft die Situation, in welcher der mutmassliche Empfänger einer Lieferung entweder das Tätigen der Bestellung oder den Erhalt der Ware abstreitet *(Abstreiten der Bestellung).* Besondere Schwierigkeiten bereitet dabei der Umstand, dass i.d.R. jeweils der Onlineanbieter das Versandrisiko trägt und für abhandengekommene Pakete auf dem Postweg haftet. Die Unterscheidung von Betrugsfällen zu tatsächlichem Postversagen und somit der Nachweis eines Betrugs sind für den geschädigten Onlinehändler sehr schwierig.[10]

Die dritte Form betrifft den Betrug mittels *Identitätsdiebstahl bzw. -missbrauch.* Dieser liegt vor, wenn personenbezogene Daten von einer nicht autorisierten Person erworben, auf sie übertragen, von ihr besessen oder benutzt werden, um mittels eines fremden Benutzerkontos betrügerisch zu bestellen. Das Ziel des Identitätsdiebstahls ist die unrechtmässige Bereicherung auf Kosten eines Opfers, das hieraus einen Vermögensschaden erleidet, währenddem die eigene Anonymität gewahrt wird.[11] Durch die Warenbestellungen mittels falscher, gestohlener und teils erfundener Personendaten braucht der Täter ein Domizil für die Lieferung, wozu er Paketstationen, leere Wohnungen bzw. Briefkästen mit eigens angebrachten Namensaufklebern verwendet und günstige Zeitpunkte abwartet, um die Lieferungen an fremden Adressen abzufangen.[12] Je organisierter die Täterschaft bei der Tatausführung mit den fremden Daten und anonymen Domiziladressen vorgeht, desto weniger Hinweise gibt es auf die wahre Täterschaft.

2. Rechtliche Grundlagen

a) Abgrenzung zwischen Art. 146 StGB und Art. 147 StGB

Die Rechtsprechung im Bereich des Bestellbetrugs im Onlinehandel ist insofern uneinheitlich, als dass die Delikte nicht immer nach dem gleichen Straftatbestand beurteilt werden, was auch die statistische Erhebung des Phänomens zusätzlich erschwert. Die grosse Mehrheit dieser Delikte im E-Commerce wird unter den klassischen Betrugstatbestand nach Art. 146 StGB subsumiert, obwohl Art. 147 StGB den betrügerischen Missbrauch einer Datenverarbeitungsanlage (nachfolgend «DVA») unter Strafe stellt und damit eigentlich für den Computerbetrug konzipiert wäre.[13] Der betrügerische Missbrauch einer DVA stellt die unrichtige, unvollständige oder unbefugte Verwendung von Daten bzw. das Einwirken auf einen elektronischen oder vergleichbaren Datenverarbeitungsvorgang zwecks Herbeiführen eines Vermögensschadens bei jemand anderem unter Strafe. Diese betrügerische Manipulation muss somit in einem sachlich oder rechtlich unzutreffenden Ergebnis des Verarbeitungsvorganges resultieren.[14] Da beim Bestellbetrug häufig mittels falscher Angaben eine automatisierte Bonitätsprüfung umgangen wird, werden Daten unrichtig verwendet, was eine Subsumtion unter Art. 147 StGB nahelegt. In der Praxis wird dieser Tatbestand jedoch fast ausschliesslich für strafbare Manipulationen und unbefugte Bargeldbezüge am Bankomaten angewendet.[15] Der Grund für diese zurückhaltende Anwendung von Art. 147 StGB zugunsten des klassischen Betrugstatbestands von Art. 146 StGB liegt darin, dass Art. 147 StGB als Auffangtatbestand konzipiert wurde. Der klassische Betrugstatbestand setzt voraus, dass durch Vorspiegelung oder Unterdrückung von Tatsachen ein Mensch arglistig in die Irre geführt oder in einem Irrtum arglistig bestärkt wird und dadurch eine Vermögensdisposition vornimmt, die in einem Vermögensschaden resultiert (Art. 146 Abs. 1 StGB). Art. 147 StGB hingegen gelangt in all denjenigen Fällen zur Anwendung, in denen kein Mensch, sondern lediglich eine Maschine

getäuscht wurde.[16] Beeinflusst der Täter die Datenverarbeitung und täuscht dadurch einen Menschen, so kann die Frage der Anwendbarkeit von Art. 146 StGB bzw. Art. 147 StGB entweder im Sinne der Subsidiarität oder der Spezialität gelöst werden. In erster Linie soll jedoch vermieden werden, dass zwischen diesen beiden Straftatbeständen eine Strafbarkeitslücke entsteht.[17] Rechtsprechung und Lehre sprechen sich in solchen Konstellationen für die subsidiäre Anwendung von Art. 147 StGB aus, weshalb für alle Fälle einer Vermögensverschiebung, bei denen ein menschlicher Entscheidungsträger allein oder in Kombination mit einer Datenmanipulation getäuscht wird, Art. 146 StGB vorgehen soll.[18] Damit wird bereits ein breites Spektrum an Tathandlungen vom Anwendungsbereich von Art. 147 StGB ausgeschlossen. Eine weitere Einschränkung der Anwendbarkeit von Art. 147 StGB hat das Bundesgericht in einem älteren Entscheid vorgenommen. Darin geht das Bundesgericht davon aus, dass auch bei Angaben falscher Daten, die nur gegenüber einem Computer erfolgen, neben den automatisierten Vorgängen irgendwo im gesamten Versandprozess trotzdem eine natürliche Person beteiligt sei, weshalb diese anstelle des Computers getäuscht werde.[19] Allerdings stellt das Bundesgericht damit eine Fiktion der menschlichen Entscheidung auf und ignoriert mit dieser Argumentation die effektive Entscheidungskompetenz und die dementsprechende Willensbildung bei der getäuschten Partei. Meldet nämlich der Computer eine Autorisierung aufgrund der falschen Dateneingabe und führt eine natürliche Person ohne Entscheidungskompetenz diese Meldung lediglich aus, kann nicht Betrug, sondern nur ein Missbrauch nach Art. 147 StGB vorliegen.[20] Diese bundesgerichtliche Rechtsprechung dürfte demnach mit Blick auf die fortschreitende Digitalisierung und Entwicklung intelligenter Zahlungsabwicklungssysteme ohne menschliche Beteiligung überholt sein. Allerdings stellt sich dann die Frage nach der Eingrenzung der strafbaren Manipulationen, kennt Art. 147 StGB doch kein dem Betrugstatbestand analoges Arglisterfordernis,[21] weshalb jede unrichtige, unvollständige oder unbefugte Verwendung von Daten unter den Tatbestand fallen kann, unabhängig von der Komplexität der Manipulation bzw. des Abwehrdispositivs. In solchen Fällen wäre es stossend, das Ausfallrisiko einer grosszügigen und riskanten «Kauf-auf-Rechnung-Praxis» der Onlineshops der Allgemeinheit aufzubürden.

Soll daher nicht ständig die Fiktion eines menschlichen Entscheidungsträgers bemüht werden, um Art. 146 StGB und somit das Arglisterfordernis als anwendbar erklären zu können, wäre de lege ferenda auch bei Art. 147 StGB eine Einschränkung der Strafbarkeit aufgrund mangelhafter Sicherheitsvorkehrungen seitens der Betreiber des Computerprogramms sinnvoll.

b) Voraussetzungen von Art. 146 StGB

Die beim klassischen Betrugstatbestand vorausgesetzte Täuschung erfolgt beim Bestellbetrug vorwiegend über die Zahlungsunwilligkeit, wobei diese bereits zu Beginn der Tathandlung vorhanden gewesen sein muss.[22] Wie bereits erwähnt muss diese Täuschung – im Gegensatz zur Tathandlung in Art. 147 StGB – auch arglistig erfolgt sein, wobei Arglist definiert wird als Errichtung eines ganzen Lügengebäudes, besondere Machenschaften oder eine einfache Lüge, wenn deren Überprüfung nicht oder nur mit besonderer Mühe möglich oder nicht zumutbar ist, wenn der Täter den Irrenden von der Überprüfung abhält oder voraussieht, dass der Irrende die Überprüfung aufgrund eines besonderen Vertrauensverhältnisses unterlässt.[23] Die Umgehung einer negativen Bonitätsprüfung durch abgeänderte Daten, durch Missbrauch einer fremden Identität oder durch das Erstellen eines Kundenkontos unter falschen Angaben wird in der überwiegenden Mehrheit der Fälle als Lügengebäude bzw. besondere Machenschaften und dementsprechend als arglistig qualifiziert werden können. Das Bundesgericht hat in seiner Rechtsprechung jedoch auch das einfache Vortäuschen des Leistungswillens als arglistige einfache Lüge qualifiziert, da sie eine innere Tatsache betrifft, die vom Vertragspartner nicht direkt überprüft werden kann.[24] Dementsprechend erfüllen sowohl der simple Eingehungsbetrug ohne Datenmanipulation als auch das Abstreiten des Erhalts der Ware, d.h. die einfache Behauptung, keine Ware erhalten zu haben, ebenfalls grundsätzlich das Arglisterfordernis.

Allerdings kann unter dem Aspekt der Opfermitverantwortung eine Strafbarkeit wegen Betrugs entfallen, wenn eine so überwiegende Leichtfertigkeit des

Opfers bei den grundlegendsten Vorsichtsmassnahmen vorliegt, dass die arglistige Verhaltensweise des Täters in den Hintergrund gedrängt wird.[25] Zudem hat das Bundesgericht seine Rechtsprechung dahingehend präzisiert, dass Vortäuschung des Erfüllungswillens nicht in jedem Fall arglistig sei, sondern dass Arglist auch verneint werden könne, wenn sich aus der möglichen und zumutbaren Überprüfung der Erfüllungsfähigkeit ergeben hätte, dass der andere nicht erfüllungsfähig war.[26] Im Geschäftsverkehr kann diesbezüglich von Bedeutung sein, ob ein erfahrenes Opfer Kontrollen abbaut und damit elementare Schutzmassnahmen vernachlässigt oder trotz durchschauter Täuschung bzw. einer entsprechenden Warnung die Geschäfte mit dem Täter dennoch weiterführt.[27] Dieses Erfordernis dürfte insbesondere bei Fällen von Bestellungen auf Rechnung einschlägig sein, wenn Unternehmen ohne oder sogar im Falle einer negativen Bonitätsprüfung eine Bestellung auf Rechnung zulassen. Die Unternehmung ist somit gehalten, grundlegende Kontrollmechanismen zu implementieren, ansonsten die Täuschung nicht die genügende Qualität aufweist, um als arglistig zu gelten.[28] Allerdings sind solche Schutzmassnahmen oftmals teuer und aufwendig, weshalb sie für die betroffene Person bzw. Unternehmung zumutbar und wirtschaftlich tragbar bleiben müssen.[29] Bei einfachen falschen Aussagen hat das Bundesgericht die Arglist demnach nur als gegeben erachtet, wenn weitere Überprüfungen nicht handelsüblich seien, etwa weil sie sich im Alltag als unverhältnismässig erweisen und die konkreten Verhältnisse eine nähere Abklärung nicht nahelegen oder gar aufdrängen würden und dem Opfer diesbezüglich kein Vorwurf der

Leichtfertigkeit gemacht werden könne.[30] Im konkreten Fall, bei dem es um eine Onlinebestellung eines Druckers auf Rechnung für CHF 2000.– ohne weitere falsche Angaben des Beschuldigten ging, verneinte das Bundesgericht Arglist mit der Begründung, dass eine Lieferung auf Rechnung bei über das Internet bestellter Ware insbesondere mit höherem Warenwert generell eher unüblich sei und die Verkäuferin durch Lieferung auf Rechnung an eine ihr unbekannte Privatperson bewusst ein gewisses Risiko eingegangen sei. Zudem habe sie keinerlei Abklärungen hinsichtlich der Bonität des Bestellers getätigt, was ohne erheblichen zusätzlichen Aufwand möglich gewesen wäre und daher auch nicht als unverhältnismässig oder unzumutbar bezeichnet werden könne.[31] Aus dieser Rechtsprechung kann daher geschlossen werden, dass bei Onlinebestellungen gegen Rechnung das Risiko allgemein bei der Verkäuferin liegt und Unternehmen in solchen Fällen zumindest eine Bonitätsabklärung tätigen müssen, mangels

derer Arglist ausscheidet.[32] Wenngleich dieser Rechtsprechung im Ergebnis zuzustimmen ist, gilt es festzuhalten, dass heutzutage bei Onlinebestellungen die Zahlungsmodalität auf Rechnung entgegen der bundesgerichtlichen Einschätzung die beliebteste Zahlungsmethode darstellt und somit als geschäftsüblich qualifiziert werden kann, sich auf der anderen Seite aber Detailkontrollen als kostspielig erweisen, weshalb aus wirtschaftlichen Überlegungen ein gewisser «Ausfall» seitens der Unternehmen wohl in Kauf genommen wird.[33] Diese vielfach «simplen» Täuschungsverhalten bei Bestellung auf Rechnung dürften vermutlich auch der Grund sein, warum viele Unternehmen diese Delikte mangels Arglistvoraussetzung gar nicht erst zur Anzeige bringen.[34]

Weiter muss beim Betrug ein Vermögensschaden eintreten. Dieser dürfte – aufgrund der Häufigkeit der Bestellungen auf Rechnung – auch bei Missbrauch von fremden Personendaten weiterhin beim Unternehmen eintreten, weshalb allfällige natürliche Personen, die einen solchen «Identitätsdiebstahl» erlitten haben, aus rechtlicher Sicht keine Geschädigtenstellung wegen Betrugs haben. Mit geplanter Einführung des Tatbestands des Identitätsmissbrauchs in Art. 179^{decies} E-StGB dürfte sich diese Strafbarkeitslücke hingegen schliessen und bei solchen Konstellationen neben dem Betrugstatbestand auch eine Strafbarkeit wegen Identitätsmissbrauchs resultieren, in der dann auch dem Betroffenen des Identitätsmissbrauchs Geschädigtenstellung zukommt.[35]

Eine weitere Schwierigkeit bei der rechtlichen Einordnung des Bestellbetrugs liegt in der Tatsache, dass in der Praxis ein Onlineshop bei Bestellungen auf Rechnung seine gewährten Warenkredite über einen dritten Zahlungsdienstleister absichern kann und somit in solchen Konstellationen die Personen des Getäuschten und des Geschädigten auseinanderfallen. Es wird daher über Drittvermögen verfügt, weshalb geprüft werden muss, ob die Voraussetzungen für einen Dreiecksbetrug gegeben sind. Ein solcher wird jeweils nur angenommen, wenn ein Näheverhältnis zwischen dem Irrenden/Verfügenden und dem Geschädigten vorliegt.[36] Faktisch stellen die Rechnung und die damit aufgeschobene Fälligkeit der Zahlungsverpflichtung gegenüber dem Käufer einen Kredit des Onlinehändlers dar. Das Rechtsverhältnis zwischen dem Onlineshop und dem Zahlungsdienstleister ist i.d.R. ein Factoringvertrag. Dieser Vertrag setzt sich aus verschiedenen Elementen zusammen.

Zum einen handelt es sich um ein Dauerschuldverhältnis, wobei der Vertragspartner dem sogenannten Factor grundsätzlich sämtliche Debitorenforderungen aus den Onlineverkäufen zediert.[37] Neben dieser Abtretung übernimmt der Factor zusätzlich eine oder mehrere Funktionen im Zusammenhang mit den Forderungen. Möglich ist das Risikomanagement, also die Überprüfung von Bestellungen, die Übernahme der Buchhaltung und des Mahnwesens, die Finanzierungsfunktion, die Bevorschussung der zedierten Forderungen für eine sofortige

Warenauslieferung, oder die Delkrederefunktion, was die Übernahme des Delkredererisikos und somit die Absicherung des Onlinehändlers bei Zahlungsausfällen bedeutet.[38] Der Dienstleister ist auf diese Funktionen spezialisiert, kann bessere Betrugserkennungsmassnahmen einsetzen und verfügt über mehr Ressourcen, weshalb er gegenüber dem einzelnen Onlineanbieter klare Vorteile bei der Erledigung dieser Aufgaben hat.[39] Das Abtretungsverhältnis zwischen dem Onlineshop und dem Zahlungsdienstleister stellt daher ein Näheverhältnis zwischen der getäuschten und der geschädigten Person dar und begründet damit die Möglichkeit eines Dreiecksbetrugs. Der Täter löst mit einer falschen Dateneingabe einen Irrtum bzw. eine unrichtige Datenverarbeitung beim Onlineshop aus, wobei der Irrtum auch beim Onlineshop eintritt, wenn der Täter mittels falscher Angaben die vom Zahlungsdienstleister durchgeführte Bonitätsprüfung manipuliert. Aufgrund dieses Irrtums führt der Onlinehändler eine Vermögensverfügung, nämlich einen Versand von Waren auf Rechnung, aus. Bei vertraglicher Übernahme des Delkredererisikos nimmt der Zahlungsdienstleister die Refinanzierung vor und fügt sich damit einen Schaden zu.[40] Je nach Ausgestaltung der vertraglichen Pflichten zwischen dem Onlineshop und dem Zahlungsdienstleister kann somit die Täuschung bzw. der Schaden bei verschiedenen Parteien auftreten, oder er wird geteilt. In der Praxis ist in solchen Fällen oftmals auch umstritten, wer den Schaden zu tragen hat, gerade wenn eine der Parteien die nötigen Sicherheitsvorkehren beim Bestellvorgang missachtet hat.

Neben den objektiven Tatbestandsmerkmalen muss der Täter zudem in subjektiver Hinsicht (eventual)vorsätzlich und mit Bereicherungsabsicht gehandelt haben.[41] Dieser Nachweis dürfte in der Praxis insbesondere bei Fällen, in denen der Täter ohne Datenmanipulation die Ware nicht bezahlt, zu Schwierigkeiten führen, da sich das Vorhandensein eines Zahlungsunwillens zum Zeitpunkt der Bestellung wohl nur schwierig beweisen lässt.

Zusammengefasst bleibt festzuhalten, dass Bestellbetrüge im Onlinehandel de lege lata weiterhin unter Art. 146 StGB subsumiert werden, wobei heutzutage

bei automatisierten Bonitätsprüfungen kein menschlicher Entscheidträger mehr involviert ist, weshalb eine Anwendung von Art. 147 StGB in solchen Fällen sachgerechter erscheint. Eine solche rechtliche Einordnung würde allerdings dazu führen, dass kein Arglisterfordernis und somit keine Opfermitverantwortung mehr vorausgesetzt würden, was eine Strafbarkeit auch bei mangelhaften Schutzmassnahmen seitens der Onlineunternehmen bejahen liesse. Eine Einschränkung der strafbaren Handlungen mittels einer gewissen «Opfermitverantwortung» seitens der Unternehmen – so etwa bei fehlenden bzw. mangelhaften Sicherheitsvorkehren – wäre daher auch bei Art. 147 StGB angezeigt, um eine ausufernde Strafbarkeit zu vermeiden sowie die Analogie zum klassischen Betrugstatbestand aufrechtzuerhalten.

III. Empirische Untersuchung

1. Methode und Stichprobe

Die nachfolgende empirische Datenauswertung basiert auf einer Analyse von 180 Betrugsfällen, die in einem gesamtschweizerisch tätigen Dienstleistungsunternehmen für Zahlungsabwicklung im Onlinehandel aufgezeichnet worden sind. Dieses Unternehmen bietet für Onlinehändler die Abwicklung des Kaufs auf Rechnung an und identifiziert die Käufer in Echtzeit, um Betrugsrisiken weitestgehend zu reduzieren. Eine solche Analyse erlaubt, Informationen über Täter- und Tatumstände sowie die geschädigten Unternehmen bzw. Privatpersonen zu erheben, da die offiziellen Statistiken aufgrund der uneinheitlichen rechtlichen Erfassung der Delikte und der vermutlich hohen Anzahl an nicht zur Anzeige gebrachten Fällen nicht in der Lage sind, konkrete

Informationen zu diesem Phänomen zu liefern. Auch Opferbefragungen, die zwar auch das Dunkelfeld, sprich die nicht zur Anzeige gebrachten Delikte erheben können, vermögen die Betroffenheit von Unternehmen nicht zu messen, da sie sich grösstenteils auf die Befragung von natürlichen Personen beschränken.[42]

Tabelle 1: Zusammensetzung der Stichprobe

	N
Anzahl Fälle	180
Anzahl Täter	189
Anzahl Opfer: natürliche Personen	214
Anzahl Opfer: juristische Personen	146
Betrugsform	
– **Eingehungsbetrug**	36
– **Betrug mit Identitätsdiebstahl**	139
– **Kombination Eingehungsbetrug und Identitätsdiebstahl**	4
– **Abstreiten einer Bestellung**	1

Die in der vorliegenden Analyse berücksichtigten Fälle haben zwischen 2015 und 2018 stattgefunden und wurden im Juli und August 2018 beim vorgängig erwähnten Unternehmen erhoben. Als ein Fall wurden sämtliche Bestellungen eines Täters bzw. mehrerer zusammenwirkender Täter gewertet, unabhängig von der Menge der einzelnen Bestellungen. Es handelt sich somit nicht um eine für die gesamte Schweiz und sämtliche Branchen repräsentative Stichprobe, weshalb die erhaltenen Resultate diesbezüglich nicht verallgemeinerbar sind. Bei der Interpretation der Resultate der vorliegend analysierten Betrugsfälle muss zudem beachtet werden, dass es sich bei einem Grossteil um Verdachtsfälle und keine rechtskräftig abgeschlossenen Verfahren handelt, gewisse dieser Fälle also durchaus nicht strafrechtlich relevant sein können bzw. nicht zu einer strafrechtlichen Verurteilung führen werden (siehe dazu auch Kap. III.2.e)).

2. Untersuchungsresultate

a) Deliktsformen

Von den erläuterten Betrugsformen handelt es sich bei den untersuchten Fällen in 77,2% um einen Betrug mit gestohlener Identität, in 20% der Delikte um einen Eingehungsbetrug und in nur einem Fall (0,6%) um das Abstreiten einer Bestellung. Bei grösseren und länger andauernden Fällen sind auch Kombinationen der Betrugsformen möglich, wenn Täter anfänglich unter eigenem Namen einkaufen und, sobald dieser gesperrt ist, eine fremde Identität missbrauchen (2,2%). Die relativ geringe Anzahl von Konstellationen, in denen es sich um einen Eingehungsbetrug handelt, ist vermutlich der Tatsache geschuldet, dass in solchen Fällen i.d.R.

schwierig nachzuweisen ist, dass der Täter die Bestellung ohne Zahlungswillen getätigt hat, weshalb hier lediglich die eindeutigen Fälle, in denen allenfalls auch mehrfache Namensmanipulationen vorlagen, aufgeführt sind. Die Dunkelziffer dürfte hingegen um ein Vielfaches grösser sein. Die Überrepräsentation von Betrug mittels

gestohlener Identität hingegen könnte auch damit erklärt werden, dass sich hier die Betroffenen des Identitätsdiebstahls gemeldet haben, weshalb das Unternehmen diese Fälle danach als potenzielle Betrugsfälle aufführen musste.

b) Täterkomponenten

aa) Geschlecht

Von den 189 erfassten Täterinnen und Tätern sind rund 80% (N=152) bekannt. Von den 147 mit Geschlecht registrierten tatverdächtigen Personen sind 61% männlich. Damit sind weibliche Tatverdächtige mit 39% zwar in der Minderheit, jedoch im Vergleich zu ihrer aus der polizeilichen Kriminalstatistik ersichtlichen Vertretung bei der allgemeinen Delinquenz trotzdem übervertreten, machen sie doch dort im Durchschnitt lediglich rund 24% der Tatverdächtigen bei Delikten des StGB, 13% bei BetmG-Delikten und 20% bei AIG-Delikten aus.[43] Allerdings deckt sich dieser Anteil ziemlich gut mit der Vertretung weiblicher Tatverdächtiger bei gewissen anderen Vermögensdelikten wie beispielsweise Ladendiebstahl oder Betrug – im Jahr 2020 waren rund 37% bzw. 28% Frauen als Beschuldigte in der Kriminalstatistik aufgeführt.[44] Dieses relativ ausgeglichene Verhältnis der Geschlechter könnte damit erklärt werden, dass Frauen und Männer gleichermassen von den Reizen des Konsums angesprochen werden und jede Person mit Internetzugang diese Taten ausführen kann, unabhängig von der körperlichen Konstitution, dem Besitz von Tatmitteln oder der allfälligen Bereitschaft für gewaltsames Handeln. Die Hemmschwelle für die Deliktsbegehung könnte zudem gerade für Frauen noch tiefer als beim Laden- oder Taschendiebstahl liegen, da sich die Geschädigten nicht einmal im selben Raum befinden, das Delikt also aus der Distanz,

anonymer und weniger riskant ausgeführt werden kann. Ein genauerer Blick in die Fälle erweckt zudem den Eindruck, dass Frauen vermehrt für sich selbst Bestellungen tätigten, um sich Waren zu gönnen, die sie sich sonst finanziell nicht leisten könnten, wohingegen Männer vielmehr den Weiterverkauf und die Generierung eines Einkommens anstrebten. Diese These lässt sich an zwei typischen Beispielen aus der Stichprobe veranschaulichen, wobei eine weibliche Bestellerin beim Besuch eines Onlineshops in eine Art Kaufrausch geriet und innert kürzester Zeit verschiedenste über ihrem Budget liegende Haushalts- und Dekoartikel, Beautyprodukte sowie diverse Spielsachen für Kinder und Haustiere in den Warenkorb legte und demgegenüber ein männlicher Besteller mit geringem Einkommen in organisierter Art und Weise und unter Verwendung von fremden Identitäten mehrere iPhones, Laptops und Tablets bestellte, um diese anschliessend weiterzuveräussern und damit seine Lebenshaltungskosten zu decken.

bb) Alter

Junge männliche Personen treten am häufigsten als Tatverdächtige für ein Betrugsdelikt im Onlinehandel auf. Bei den untersuchten Betrugsfällen ist der Täter bzw. die Täterin im Schnitt 33 Jahre alt. Die Tatbegehung nimmt mit zunehmendem Alter auffällig stark ab, was einerseits mit der allgemein bekannten Übervertretung jüngerer Täter in der Kriminalität zu tun haben dürfte, hier aber vermutlich zudem mit der grundsätzlich weniger intensiven Nutzung des E-Commerce durch ältere Generationen erklärt werden kann. Auf der anderen Seite gibt es kaum minderjährige Täter, da Jugendliche aufgrund ihrer noch beschränkten Geschäftsfähigkeit meist keinen Zugang zu Bestellungen auf Rechnung haben, solange sie ihre Personaldaten wahrheitsgetreu angeben.

cc) Allein- oder Mittäterschaft

Die Untersuchung der Zusammensetzung der Täterschaft zeigt, dass in 92% der analysierten Betrugsfälle der Beschuldigte als Einzeltäter gehandelt zu haben scheint, und nur in wenigen Einzelfällen agierten mindestens zwei (5%) oder mehr als zwei Täter (3%) gemeinsam.

dd) Motivation und Tatausführung

Der entscheidende Tatumstand und Auslöser für einen Bestellbetrug (Eingehungsbetrug oder Identitätsdiebstahl) ist eine negative Bonität. In rund 80% der Fälle zeigt sich diese durch eine negative Bonitätsauskunft (Bonität «rot») bei der automatischen Prüfung des Bestellvorgangs und damit einhergehend der Verweigerung des Einkaufs auf Rechnung. Diese Prüfung fällt negativ aus, wenn der Besteller entweder im Betreibungsregister, im Inkasso oder auf der internen Schuldenliste bzw. der sogenannten Blacklist vermerkt ist. Für den potenziellen Täter

stellt sich somit die Frage nach der Umgehung dieser Bonitätsprüfung, um eine Bestellung dennoch ausführen zu können. In den restlichen 20% der erfassten Betrugsfälle meldete das System zwar keine negative Bonitätsprüfung, beispielsweise weil es sich um einen Erstbesteller handelte. Dennoch tätigten auch diese Täter aus finanziellen Motiven eine betrügerische Bestellung mit unterschiedlichen Tatausführungsmethoden.

Der übliche Umgehungsmechanismus einer negativen Bonität ist der Abschluss des Bestellvorgangs mit einer fremden Identität (knapp 80% der Bestellbetrüge werden mittels Identitätsdiebstahl begangen). Am einfachsten und somit am häufigsten (rund 54% der Fälle mit Identitätsdiebstahl) werden dazu die Personendaten eines Familienangehörigen oder eines Partners missbraucht, der im gleichen Haushalt wohnt und wo somit die automatisierte Adressprüfung positiv ausfällt. Andere, als Einzelfälle vorkommende Anreize zur Tatausführung mittels Identitätsdiebstahl und insbesondere zur Auswahl des Opfers sind ein vorgängiger Streit mit der geschädigten Person oder eine Trennung sowie der physische Diebstahl oder der Fund einer Identitätskarte, womit auf fremden Namen ein Paycard-Konto[45] eingerichtet und auf diesem Weg auf Rechnung eingekauft werden kann. Weitere bei der Untersuchung als Einzelfälle aufgetretene Tatumstände sind die Ausnutzung der Abwesenheit (längere Reise oder Gefängnisaufenthalt) eines Bekannten oder der Missbrauch der Identität einer effektiv minderjährigen Person (unter falscher Angabe des Geburtsdatums), da diese namentlich noch in keinem Betreibungsregister erfasst ist und somit keine negative Bonitätsauskunft möglich ist. Andere Tatmotivationen, die unabhängig von einer negativen Bonitätsauskunft auftreten, sind die dauerhafte Mittel- und Arbeitslosigkeit oder die unbemerkte Mitnutzung eines bereits aufgebauten Betrugsnetzwerks als Trittbrettfahrer, wobei mittels betrügerischer Bestellungen und anschliessenden Weiterverkaufs versucht wird, ein Einkommen zu generieren und damit den Lebensunterhalt zu finanzieren.

Damit ist zum einen festzuhalten, dass die Prüfsysteme der Onlinehändler im Grundsatz effizient sind, da die Täter in 80% der Fälle eine negative Bonitätsprüfung mittels fremder Identität umgehen mussten, und das System somit in den meisten Fällen Personen blockiert, die gerade zu Recht keine Lieferung auf Rechnung erhalten. Zum anderen lässt diese Analyse die Vermutung zu, dass – insbesondere im Gegensatz zu herkömmlichen Vermögensdelikten wie Ladendiebstahl

oder traditionellem Betrug – ein Grossteil der Täterinnen und Täter ohne eigentliche Betrugsabsicht einen Bestellvorgang initiiert und erst durch die Verweigerung des Kaufs auf Rechnung dazu «animiert» wird, mittels

Umgehungsmechanismus eine betrügerische Bestellung zu tätigen.

c) Opferkomponenten

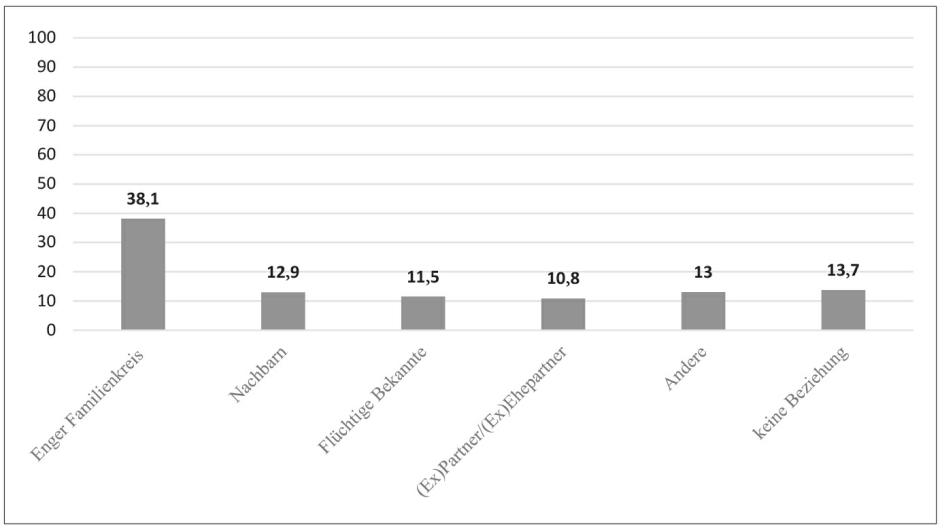
aa) Allgemeines

Auf der Geschädigtenseite gibt es bei Betrugsdelikten mit den natürlichen Personen, die Geschädigte eines Identitätsdiebstahls geworden sind, und den Onlinehändlern, die Zahlungsausfälle erlitten haben, i.d.R. zwei Arten von Betroffenen, nämlich natürliche und juristische Personen.[46] In der vorliegenden Stichprobe wurden in allen Betrugsfällen mit Identitätsdiebstahl (N=143; 79,4%) sowohl natürliche Personen als auch juristische Personen als Geschädigte vermerkt, was nicht unbedingt bedeuten muss, dass diese Personen auch tatsächlich aus rechtlicher Sicht geschädigt sind, da wie erwähnt nur bei derjenigen Person ein Betrug vorliegt, bei der ein Schaden auftritt. Die kriminologische Kategorie der «Opfer» eines Bestellbetrugs ist demnach nicht deckungsgleich mit der rechtlichen Definition der geschädigten Person eines Bestellbetrugs. Insgesamt wurden in den untersuchten Fällen 214 natürliche Personen Opfer eines Identitätsdiebstahls, und bei gesamthaft 146 Onlineshops wurden betrügerische Bestellungen getätigt.

bb) Charakteristika der geschädigten natürlichen Personen

In Bezug auf geschädigte natürliche Personen ist das Verhältnis zwischen weiblichen und männlichen betroffenen Personen mit 51,9% bzw. 48,1% ungefähr ausgeglichen. Hingegen lässt sich in Bezug auf das Alter eine Verschiebung nach oben feststellen, indem das durchschnittliche Opfer mit 44 Jahren rund elf Jahre älter ist als der durchschnittliche Tatverdächtige. Dieses Ergebnis lässt sich grösstenteils damit erklären, dass in vielen Fällen ein junger Erwachsener aufgrund fehlender Kreditwürdigkeit mit den Angaben eines Elternteils oder eines älteren Geschwisters einkauft (siehe dazu auch Unterkapitel cc)).

Abb. 1: Beziehung zwischen Täter und Opfer (natürliche Personen), in % der Opfer (N=139, ohne Angaben=75)



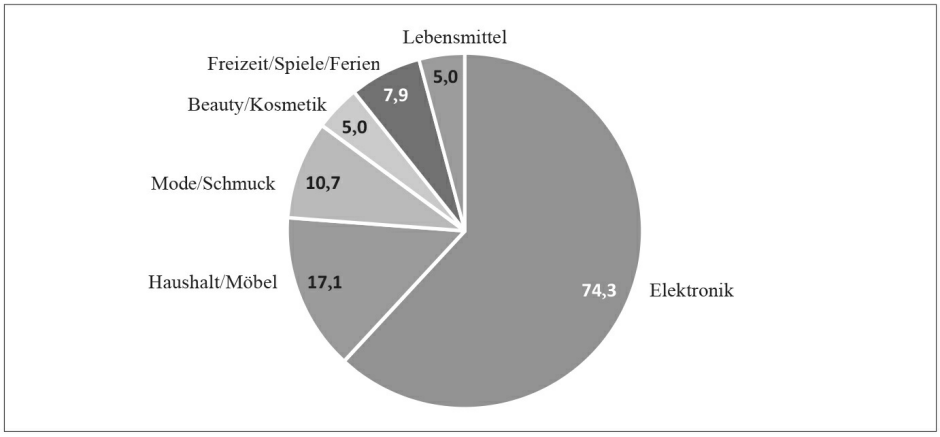
Bei den bekannten Opfer-Täter-Beziehungen (N=139) gab es in 13,7% der Betrugsdelikte mit Identitätsdiebstahl keine Beziehung zwischen dem Täter und der geschädigten Person. Es handelte sich somit um reine Zufallsopfer, an deren Identität der Täter beispielsweise über das Internet gelangte. In 86,3% der Fälle sind sich Opfer und Täter hingegen bekannt. In dieser Kategorie machen enge familiäre Beziehungsverhältnisse zwischen Eltern,

Kindern oder Geschwistern untereinander (38,1%), Nachbarn (12,9%) und zwischen aktuellen und vormaligen Ehe- oder Lebenspartnern (10,8%) den grössten Anteil aus. Dies lässt sich insbesondere dadurch erklären, dass die Wohnadressen in diesen Beziehungen meist übereinstimmen und dadurch eine Bestellung auf falschen Namen und das anschliessende Abfangen der Lieferung erheblich erleichtert werden. In einigen anderen Fällen benutzt der Täter die Identität von flüchtigen Bekannten (11,5%) wie beispielsweise ehemaligen Schulkameraden, wobei die Angaben meist über Social Media ausfindig gemacht werden. In der Untersuchung vereinzelt aufgetaucht und in Abb. 1 in der Kategorie «Andere» zusammengefasst ist auch der Identitätsmissbrauch von Freunden (3,6%), WG-Mitbewohnern (3,6%), Vermietern (2,9%) oder weiteren Verwandten (2,9%). Es lässt sich also feststellen, dass sich Täter und Opfer beim Bestellbetrug trotz den Möglichkeiten des Internets und des Datenhandels meist kennen und Zufallsopfer vergleichsweise selten sind.

cc) Geschädigte Onlineshops und betroffene Produkte

Gemäss den vorhandenen Lieferbestätigungen enthielten 74,3% der untersuchten Betrugsfälle bestellte elektronische Ware wie Smartphones, Laptops, Tablets, Fernsehgeräte, Kopfhörer, Kameras usw. Elektronikartikel sind bei der durchgeführten Untersuchung somit am häufigsten von betrügerischen Bestellungen betroffen und damit auch diejenigen Onlinehändler, die Heimelektronik und Multimedia verkaufen. An zweiter Stelle bei den von betrügerischen Bestellungen betroffenen Produkten folgen Haushaltsartikel oder Möbel (17,1%), sodann Modeartikel wie Schmuck und Bekleidung (10,7%), Spielwaren, Freizeitausrüstungen oder Reisen (7,9%) an vierter Stelle und schliesslich Beauty- und Kosmetikartikel (5%) sowie Lebensmittel, Alkohol oder Tabak (5%). Bei den Risikoartikeln im E-Commerce handelt es sich demnach typischerweise um Produkte, die einen hohen Marktwert aufweisen, problemlos transportiert werden können, wo bei Originalverpackung eine grosse Nachfrage am Wiederverkauf besteht und damit ein hoher Preis erzielt werden kann. Aus den Lieferbestätigungen ergab sich auch, dass Artikel wie Smartphones, Laptops oder Tablets meist in grösseren Mengen bestellt werden, da diese eher zum Weiterverkauf als zum Eigengebrauch vorgesehen sind.

Abb. 2: Betroffene Produkte betrügerischer Bestellungen, in % der Fälle (Mehrfachnennungen möglich, N=140, ohne Angaben=40)



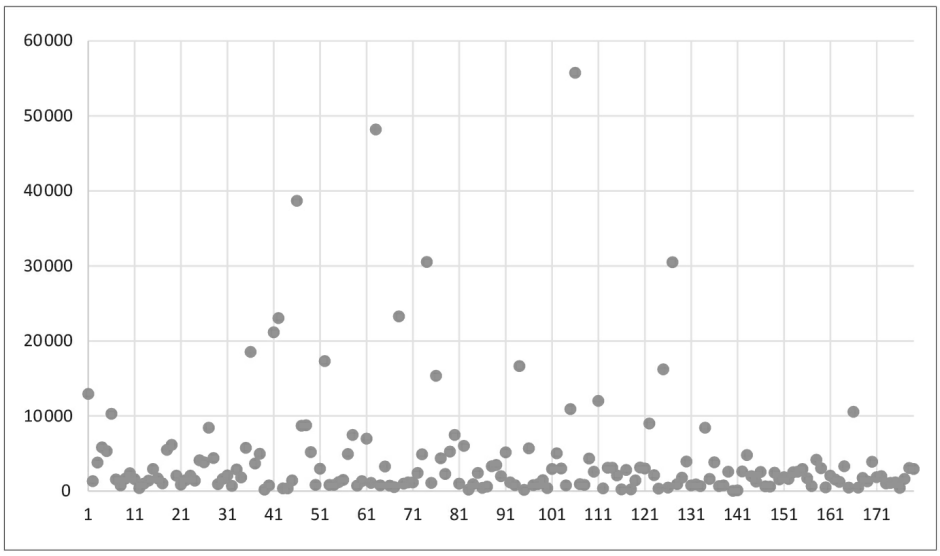
d) Schadenssumme

Den Vermögensschaden in einem konkreten Betrugsfall trägt je nach Ausgestaltung der Geschäftsbeziehungen entweder der betroffene Onlineshop oder der beauftragte Zahlungsdienstleister. Grundsätzlich übernimmt als Teil der vertraglichen Leistung immer das Dienstleistungsunternehmen das Delkredererisiko, solange der

Onlinehändler die vereinbarten Risikovorschriften bezüglich diverser Si-

cherheitsmassnahmen, Versandregeln usw. befolgt. In der vorliegenden Untersuchung geht der finanzielle Schaden in 60% aller Fälle zulasten des Onlinehändlers. Dies lässt den Schluss zu, dass der Zahlungsdienstleister als Zessionar in all diesen Fällen die Haftung ablehnte, weil das verkaufende Unternehmen die vereinbarten Sicherheitsmassnahmen beim Versand der Waren nicht eingehalten hat.

Abb. 3: Schadenssummen der Betrugsfälle, in CHF (N=179, ohne Angaben=1)



Der Gesamtschaden sämtlicher in der Analyse inkludierten Fälle betrug Fr. 785278.42. Wie aus Abb. 3 ersichtlich ist, ist beim Bestellbetrug die Schadenssumme pro Fall eher gering, übersteigt sie doch lediglich in einzelnen Fällen den Betrag von Fr. 10000.–. Die geringste Schadenssumme belief sich bei den untersuchten Fällen auf Fr. 24.90, die grösste Deliktssumme erreichte hingegen Fr. 55741.70. Diese Zahlen ergeben bei den analysierten Fällen einen durchschnittlichen Schaden von Fr. 4387.– pro Delikt und einen Medianwert von Fr. 1948.80. Diese Summen können sich je nach Fall aus einmaligen Bestellungen oder aus Serienbestellungen mit einzelnen geringen Beträgen zusammensetzen. Letzteres ist für die sogenannten Monitoringteams der Zahlungsdienstleister schwieriger erkennbar, da diese Teams eingehende Bestellanfragen nach gewissen Risikomerkmalen, wie beispielsweise einem verdächtig hohen Einkaufsbetrag, überprüfen. Problematisch bei diesen Delikten ist die Summe der vielen kleinen Einzelbestellungen und die unberechenbare Häufigkeit dieser Taten in der Zukunft.

Neben dem Verlust des Warenwertes müssen die Unternehmen auch die Kosten des gesamten Risikomanagements und die Reputationsschäden aufgrund

hoher Kreditausfälle zum finanziellen Schaden hinzuzählen. Dieses Risiko sowie die Kosten einer Implementierung von Sicherheitsmassnahmen stehen jedoch einer Umsatzsteigerung durch risikoreichere, aber attraktive Zahlungsoptionen gegenüber. Denn wie eine Studie aus Deutschland aufzeigt, kann aufgrund der hohen Beliebtheit des Kaufs auf Rechnung die Kaufabbruchquote um 54% reduziert werden, wenn der

Rechnungskauf als Zahlungsoption eingeführt wird.[47] Dies führt zu einer gefährlichen und gesellschaftlich nicht sehr verantwortungsvollen Kosten-Nutzen-Rechnung zwischen Umsatz und Kreditausfallrisiko seitens der Unternehmen.[48] Daher wird zwecks Umsatzsteigerung auch das Ausfallrisiko bei der Zahlungsart Rechnung durch die Unternehmen bewusst in Kauf genommen.

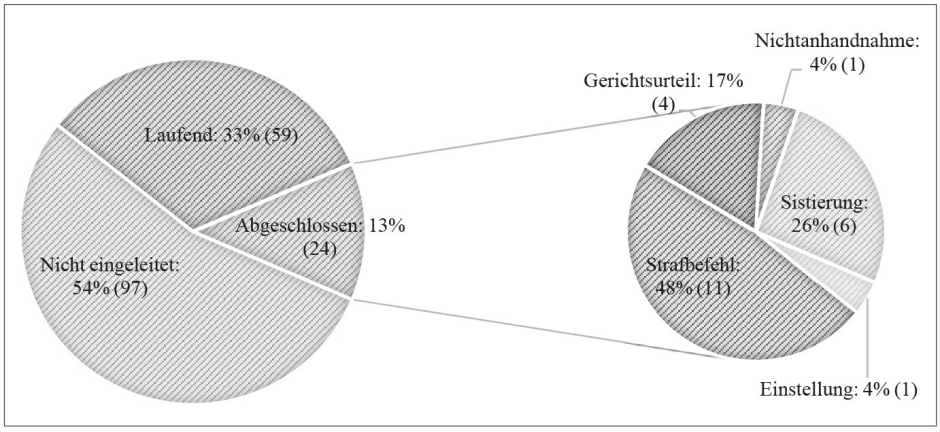
e) Verfahren und Verfahrensausgang

In der Hälfte aller Fälle (50%) erfolgte bis zum Abschluss der Untersuchung noch keine Reaktion des Opfers des Identitätsmissbrauchs. Dies kann daran liegen, dass der Identitätsmissbrauch vom Opfer gar nicht bemerkt wurde, dieses aus persönlichen Gründen gegen den Tatverdächtigen keinen Strafantrag stellen will oder es in der Strafanzeige gegen Unbekannt keine Erfolgsaussichten sieht. Dieses Geschädigtenverhalten ist auch ein Grund für die vermutlich hohe Dunkelziffer in diesem Deliktsbereich. In rund 42% der bemerkten Fälle wird hingegen bei der Polizei Strafanzeige erstattet, dies vor allem auch deshalb, weil eine Kopie der Anzeige für viele Onlinehändler als Beweis dafür dient, dass es sich tatsächlich um einen Betrugsfall handelt und das vermeintliche Opfer nicht einfach im Nachhinein die Bestellung abstreitet. Nur so wird das Opfer von der Pflicht zur Bezahlung der Rechnung aus der betrügerischen Bestellung befreit. Im Grundsatz bedeutsam ist die möglichst rasche Erkennung und Mitteilung von Betrugsdelikten, da diese bereits nach erfolgter Auslieferung der Ware schnell versickern und die Täterschaft mit fortschreitendem Zeitablauf immer seltener festgestellt werden kann.

Des Weiteren wurde bei den analysierten Betrugsfällen bis zum Erhebungszeitpunkt im Sommer 2018 in über der Hälfte der Fälle (54%) gar kein Strafverfahren eingeleitet. Von den aufgrund einer Strafanzeige eröffneten Verfahren wurden 29% bereits abgeschlossen, währenddem 71% noch laufend waren. Von den vollständig durchgeführten Strafverfahren endeten 35% ohne Verurteilung, obwohl kein einziger Freispruch zu verzeichnen war. Dies liegt daran, dass die Täterschaft oft generell unbekannt oder zumindest unbekannten Aufenthalts ist oder nicht ausreichend Beweise vorhanden sind. So wurden von den abgeschlossenen Verfahren 26% aufgrund unbekannter Täterschaft bzw. unbekannten Aufenthalts sistiert, und je 4%

der geführten Verfahren wurden mangels Beweisen oder überhaupt irgendwelcher Anhaltspunkte eingestellt bzw. nicht anhandgenommen. 65% der Strafverfahren führten hingegen zu einer Verurteilung. Von den mit Verurteilung abgeschlossenen Verfahren endeten 73% mit einem Strafbefehl, in den übrigen Fällen fand eine Gerichtsverhandlung statt, da diese Fälle entweder in die Zuständigkeit eines Jugendgerichts fielen oder die Anordnung einer Unterbringung, einer ambulanten oder stationären Behandlung bzw. einer Landesverweisung drohte und unter diesen Voraussetzungen ein Strafbefehl nicht in Betracht kommt. Von den mit Strafbefehl oder Gerichtsurteil ergangenen Schuldsprüchen qualifizierten 93% den Bestellbetrug als klassischen Betrug nach Art. 146 StGB und nur 7% als betrügerischen Missbrauch einer DVA nach Art. 147 StGB. Dieses Ergebnis bestätigt die dargelegten Unsicherheiten bei der Rechtsprechung und die Schwierigkeit, aus Kriminalstatistiken eine Angabe über die Häufigkeit des Bestellbetrugs herauszulesen, weil sich diese Verurteilungen nach Art. 146 StGB mit allen anderen Betrugsformen vermischen.

Abb. 4: Art des Verfahrensabschlusses, in % der Fälle (N=179, ohne Angaben=1)



IV. Diskussion und Fazit

Die Analyse der Betrugsfälle hat gezeigt, dass der Betrug mittels falscher Identität die grösste Kategorie der untersuchten Konstellationen darstellt. Täter sind dabei hauptsächlich junge Männer zwischen 18 und 37 Jahren, wobei im Vergleich zu anderen Deliktskategorien auch aussergewöhnlich viele weibliche Täter vorzufinden sind. Grund für die Betrügereien mittels falscher Identität sind hauptsächlich negative Bonitätsauskünfte, d.h., der Täter würde ohne falsche Identität die gewünschte Ware nicht auf Rechnung erhalten und versucht deshalb, die Sicherheitsvorkehren der Unternehmen zu umgehen. Dabei spielt sicherlich auch eine

Rolle, dass eine Bestellung mittels veränderter Angaben sehr leicht ausgeführt werden kann, aus situativer Kriminalitätsperspektive somit die Tatobjekte nur unzureichend geschützt sind bzw. vorhandene Schutzmassnahmen wie Bonitätsprüfungen sehr leicht umgangen werden können.[49] In Kombination mit der Möglichkeit des Kaufs auf Rechnung ist eine Tatbegehung somit sehr einfach, weshalb diese Gelegenheitsstrukturen dann auch ausgenutzt werden.

Opfer von Bestellbetrügereien hingegen können sowohl natürliche Personen sein, deren Identität gestohlen wurde, oder die betroffenen Unternehmen, die durch den Bestellbetrug einen Schaden erleiden. Bei den natürlichen Personen handelt es sich am häufigsten um Personen aus dem engsten Familienkreis, was vermutlich ebenfalls einen Grund darstellt, warum solche Fälle nicht häufiger zur Anzeige gelangen und die Dunkelziffer dementsprechend umso grösser sein dürfte. Die Schadenssumme beläuft sich bei Unternehmen pro Fall im Durchschnitt auf etwas über Fr. 4000.–, wobei die meisten Fälle unter der Schwelle von Fr. 10000.– zu liegen kommen. Es ist allerdings anzunehmen, dass die nicht entdeckten Fälle noch geringere Deliktssummen beinhalten, diese aber aufgrund ihres Bagatellcharakters einerseits von allfälligen Geschädigten nicht angezeigt oder vom Unternehmen selbst nicht untersucht werden, weil Letzteres nach einer Kosten-Nutzen-Analyse auf eine Untersuchung verzichtet und der Ausfall hingenommen wird. In unserer Stichprobe dürften daher Fälle mit höheren Schadenssummen überrepräsentiert sein.

Im Hinblick auf den Verfahrensausgang wurden viele Verfahren aufgrund unbekannter Täterschaft nicht abgeschlossen. Bei den abgeschlossenen Verfahren wurde am häufigsten, nämlich in 73% der Fälle, ein Strafbefehl erlassen, und lediglich 27% der Fälle wurden gerichtlich beurteilt. Diese Zusammensetzung widerspiegelt die Wichtigkeit des Strafbefehlsverfahrens in der Praxis, werden mittlerweile doch über 95% der Strafverfahren mittels Strafbefehl erledigt.[50]

Die Analyse der Betrugsfälle verdeutlicht, dass mit dem Opfer des Identitätsmissbrauchs, dem betroffenen

Onlineshop und einem allenfalls geschädigten Zahlungsdienstleister viele verschiedene Parteien von den Delikten betroffen sind und ein Interesse an der Erhöhung der Sicherheit im Internet haben. Eine Anpassung der materiellrechtlichen Rahmenbedingungen scheint allerdings nicht angezeigt, da verschiedene komplexere Formen des Bestellbetrugs bereits heute unter den Tatbestand des Betrugs nach Art. 146 StGB fallen und es auch nicht ersichtlich ist, warum ein von den Unternehmen bewusst in Kauf genommenes Ausfallrisiko durch Bestellungen auf Rechnung strafrechtlichen Schutz verdient. Prüft das Unternehmen daher die Bonität des Käufers gar nicht bzw. lediglich mangelhaft oder erlaubt es bei Erstbestellern den Kauf auf Rechnung, so hat es auch das Ausfallrisiko zu tra-

gen, und eine Strafbarkeit aufgrund von Art. 146 StGB entfällt mangels Arglist zu Recht. Anders sieht die Situation dann aus, wenn bei reinen Manipulationen automatisierter Kontrollsysteme die vom Bundesgericht eingeführte Fiktion, dass irgendwo im Bestellvorgang ein menschlicher Entscheidungsträger involviert war, aufgegeben und solche Fälle zukünftig unter Art. 147 StGB subsumiert würden. Dann müsste analog zum Betrugstatbestand auch in Art. 147 StGB eine gewisse Opfermitverantwortung eingeführt werden, damit allzu einfache Manipulationen, die vom Unternehmen zugunsten der allgemeinen Umsatzsteigerung bewusst in Kauf genommen werden, von einer allfälligen Strafbarkeit ausgeschlossen bleiben.

Eine solche rechtlich ausgestaltete Opfermitverantwortung kann auch situativen Präventionsansätzen Vorschub leisten, die eine Verbesserung von Präventions- und Betrugserkennungsmassnahmen durch die Unternehmen zum Inhalt haben. Den Onlinehändlern selbst kommt demnach die wichtigste Aufgabe zu, sich durch organisatorische und technische Massnahmen vor Betrug zu schützen, auch um einer allfälligen Opfermitverantwortung zu entgehen, den Kundinnen und Kunden aber dennoch ihre Konsumfreiheiten zu belassen.[51] Zu unterscheiden gilt es dabei zwischen der Prävention von Betrugsfällen mittels situativer Massnahmen technischer oder organisatorischer Art und der Erkennung von kriminellen Täuschungen bei Bestellvorgängen. Die Möglichkeiten hierzu sind vielfältig und beinhalten beispielsweise die manuelle Überprüfung von Bestellungen, das Führen von sogenannten Blacklists, wo Identitäten aufgrund von schlechten Zahlungserfahrungen festgehalten werden, oder die verbesserte Zusammenarbeit mit einem externen Zahlungsdienstleister und der dortigen Überprüfung von Adressen, Kontoinformationen und Bonitätsauskünften.[52] Viele Unternehmen nutzen Scoring-Verfahren, um Personen mit einer Risikobewertung zu versehen, die mittels mathematischer Methoden verschiedene Kennzahlen eines Käufers verknüpft und damit eine Prognose über die Zahlungsfähigkeit bzw. eine Abschätzung des Kreditrisikos ermöglicht.[53] Sobald eine Identität aufgrund veränderter Angaben oder durch einen Identitätsdiebstahl vom System nicht mehr zugeordnet werden kann, stossen diese Scoring-Verfahren jedoch an ihre Grenzen.[54] Dennoch erscheinen diese Präventionsmassnahmen für eine effektive Bekämpfung der Betrugskriminalität als unverzichtbar.

Aufgrund der laufenden Professionalisierung des Identitätsdiebstahls reichen die bisherigen Bonitätsprüfungen, Blacklists und Scoring-Verfahren zur Verhinderung der Delikte aber häufig nicht mehr aus. Eine mögliche Lösung für die Zukunft sind lernfähige Systeme, die aufgrund von Datenverknüpfungen und Mus-

ter- sowie Wahrscheinlichkeitsberechnungen Anomalien in Bestellvorgängen entdecken können. Dabei ist neu, dass bereits ein einzelnes Attribut ausschlaggebend für die Beurteilung eines Bestellvorgangs sein kann und dass Risiken aus der Verknüpfung von an sich unauffälligen Daten erkannt werden können.[55] Solche

Netzwerkanalysen werden zur Identifikation von Betrugsmustern entwickelt und dienen dazu, Identitäten durch die beim Bestellvorgang angegebenen Daten aufzuspüren, miteinander in Beziehung zu setzen und zu interpretieren. Die Grenzen des Systems liegen darin, dass es nicht möglich ist, einmalige Betrugsversuche abzubilden, da das Netzwerk auf dem Vergleich von Transaktionen beruht.[56] Solche lernfähigen Systeme stellen demnach eine grosse Verbesserung in der Betrugserkennung dar und sollten von den Unternehmen idealerweise als Ergänzung zu den klassischen Identifikationsmassnahmen eingesetzt werden.

Die aus situativer Perspektive immer noch einfachste, aber effizienteste Präventionsmassnahme würde im Verzicht der Option «Kauf auf Rechnung» liegen, da damit eine Bestellung ohne vorgängige Bezahlung faktisch verunmöglicht würde. Allerdings besteht hierbei einerseits das Risiko, dass der Gebrauch von Kreditkarten dadurch erhöht und damit das Ausfallrisiko teilweise auf die Kreditkartenfirmen verlagert wird, die allerdings basierend auf Art. 148 StGB ebenfalls verpflichtet sind, Massnahmen gegen den Kreditkartenmissbrauch vorzusehen. Zudem würde dies, wie bereits unter Kap. III.2.d) erläutert, zu einer Reduktion des Geschäftsvolumens führen, weshalb Unternehmen das Ausfallrisiko, das durch den Kauf auf Rechnung resultiert, von Anfang an einkalkulieren und sich diese Praxis nach einer Kosten-Nutzen-Abwägung betriebswirtschaftlich wohl immer noch lohnt. Solange die Unternehmen also aus Umsatzgründen nicht darauf verzichten möchten und das Ausfallrisiko durch mangelnde Liquidität oder betrügerische Bestellungen in Kauf nehmen, wird sich diese Lösung nicht durchsetzen.

Die Möglichkeiten zur Verhinderung von Betrugsdelikten sind also vielfältig, und die Onlinehändler sollten ihre gesellschaftliche Verantwortung wahrnehmen und im Rahmen ihrer Organisationsfreiheit Massnahmen finden, die potenziellen Tätern die Tatbegehung erschweren und dem Unternehmen selbst die Betrugserkennung erleichtern. Zur erfolgreichen Bekämpfung muss der Betrug im E-Commerce von allen Seiten als eine ernstzunehmende Problematik betrachtet werden, und es bedarf der gegenseitigen Unterstützung von Gesetzgeber, Strafverfolgungsbehörden, Unternehmen und Konsumenten. Wichtig für eine effiziente Prävention ist aber auch eine verbesserte Datenlage zum Phänomen des Bestellbetrugs. Nur wenn wir mehr über die Täter und deren Tathandlungen wissen, können wir daraus Risikofaktoren erkennen, die wiederum als Grundlage für Präventionsmassnahmen dienen. Weitere Forschung ist hier also dringend angezeigt.

---

* Prof. Dr., Assistenzprofessorin für Strafrecht, Strafprozessrecht und Kriminologie unter besonderer Berücksichtigung des Wirtschaftsstrafrechts an der Universität St. Gallen.

** M.A. HSG in Law, Auditorin Staatsanwaltschaft St. Gallen.

1 *BFS,* Online-Einkäufe und -Verkäufe, internationaler Vergleich, 2019, abrufbar unter: https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/e-commerce-e-banking.assetdetail.12307385.html (20.4.2021).

2 Zum Einfluss solcher Breschen auf die Kriminalität siehe *M. Killias,* The Opening and Closing of Breaches. A Theory on Crime Waves, Law Creation and Crime Prevention, European Journal of Criminology 2006, 11, 11 f.

3 Siehe *L. Cohen/M. Felson,* Social change and crime rate trends: A routine activity approach, American Sociological Review 1979, 588, 589, die diese Theorie ursprünglich aber auf Straftaten gegen die Person («direct-contact predatory violence») beschränkten.

4 Siehe dazu auch *M. Killias/M. Aebi/A. Kuhn,* Précis de criminologie, 4. Aufl., Bern 2019, N 436 ff.

5 Für einen erstmaligen Ausweis der digitalen Komponente in der Polizeilichen Kriminalstatistik siehe aber *BFS,* Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2020 der polizeilich registrierten Straftaten, Neuenburg 2021, 11 f.

6 *Crif,* Umfrageergebnisse Betrug im Online-Handel, Zürich 2020, 3 ff. Allerdings sind die Ergebnisse der Studie aufgrund der nicht repräsentativen Stichprobe sowie der geringen Rücklaufquote von lediglich rund 22% der befragten Unternehmen nur bedingt aussagekräftig. Gerade bei geringer Rücklaufquote besteht jeweils die Gefahr, dass von Delinquenz betroffene Unternehmen überrepräsentiert sind, da diese als vom Phänomen Betroffene häufiger geneigt sind zu antworten als solche, die nie in Kontakt mit Kriminalität gekommen sind. Zum Einfluss von Rücklaufquoten auf die Forschungsergebnisse siehe auch *Killias/Aebi/Kuhn/* (Fn. 4), N 105.

7 *Universum Group,* Betrug im Onlineshop: Die 3 erfolgreichsten Methoden vom 22.8.2016, abrufbar unter: https://www.universum-group.de/blog/universum-bietet/betrug-im-onlineshop-die-3-erfolgreichsten-methoden/ (8.2.2021), Abschnitt «Eingehungsbetrug – wenn der Kunde vorher weiss, dass er nicht zahlen kann».

8 *T. Marschall* et al., Netzwerkanalysen für die Betrugserkennung im Online-Handel, in: Tagungsband: 12. Internationale Tagung Wirtschaftsinformatik, O. Thomas/F. Teuteberg (Hrsg.), Osnabrück 2015, 1859, 1864.

9 *Crif* (Fn. 6), 7.

10 *Universum Group* (Fn. 7), Abschnitt «Ich habe nichts bekommen – Abstreiten des Erhalts der Ware».

11 *G. Borges* et al., Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte, Berlin/Heidelberg 2011, 197.

12 *Marschall* et al. (Fn. 8), 1864.

13 Siehe dazu auch Kap. III.2.e).

14 *G. Fiolka,* in: M. A. Niggli/H. Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht II, 4. Aufl., Basel 2018, Art. 147 N 9; *S. Grodecki,* in: A. Macaluso/L. Moreillon/N. Queloz (Hrsg.), Commentaire romand Code pénal II, Basel 2017, Art. 147 N 12.

15 *C. Schwarzenegger,* Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht, ZSR 2008, 399, 414; vgl. beispielsweise auch Urteil des Obergerichts des Kantons Zürich SB170126-O/U/cwo vom 27. April 2018, E. 6.2; Urteil des Obergerichts des Kantons Zürich SB170236-O/U/gs vom 12. Januar 2018, E. 3.3.3; Urteil des Obergerichts des Kantons Zürich SB150048-O/U/ad-cs vom 2. Juni 2015, E. 5.3.

16 BBl 1991 II 972; *S. Maeder/M.A. Niggli,* in: M.A. Niggli/H. Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht II, 4. Aufl., Basel 2018, Art. 146 N 126; *A. Donatsch,* Strafrecht III, Delikte gegen den Einzelnen, 11. Aufl., Zürich 2018, 254; *Grodecki* (Fn. 14), CR CP II, Art. 147 N 1.

17 BBl 1991 II 1020; *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 294.

18 BGE 129 IV 22, 32; *N. Schmid,* Das neue Computerstrafrecht, ZStrR 1995, 22, 35; *Fiolka* (Fn. 14), BSK StGB II, Art. 147 N 53; *Grodecki* (Fn. 14), CR CP II, Art. 147 N 23.

19 Vgl. BGE 96 IV 185, 188.

20 Für die österreichische Rechtslage *S. Reindl-Krauskopf,* Computerstrafrecht im Überblick, 2. Aufl., Wien 2009, 82.

21 So auch *Donatsch* (Fn. 16), 257.

22 So auch BGE 142 IV 153, 155; *K. D. Bussmann,* Wirtschaftskriminologie I: Grundlagen – Markt- und Alltagskriminalität, München 2016, Rz. 164 f. Dies dürfte allerdings nicht immer einfach von Fällen, in denen der Besteller seine finanziellen Möglichkeiten einfach überschätzt oder nicht bedacht hat, abzugrenzen sein, weshalb in solchen Fällen weitere Anhaltspunkte wie die Verwendung falscher Personalien, die Verschleierung des Aufenthalts oder die gleichartige serienmässige Begehung gegeben sein müssen, um auf den erforderlichen Zahlungsunwillen schliessen zu können; siehe dazu *D. Kochheim,* Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, München 2015, Rz. 824.

23 Statt vieler BGE 142 IV 153, 154 f.; siehe dazu auch *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 62 ff.; *A.M. Garbarski/B. Borsodi,* in: A. Macaluso/L. Moreillon/N. Queloz (Hrsg.), Commentaire romand Code pénal II, Basel 2017, Art. 146 N 35.

24 BGE 142 IV 153, 155.

25 BGE 135 IV 76, 81.

26 BGE 118 IV 359, 361.

27 *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 76.

28 *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 68 ff.

29 *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 80.

30 BGE 142 IV 153, 155.

31 BGE 142 IV 153, 157.

32 So auch *J. Francey,* L'escroquerie lors d'une commande sur Internet, LawInside vom 2.4.2016, abrufbar unter: https://www.lawinside.ch/215/ (8.2.2021).

33 Dies resultiert denn auch aus einer Befragung von Unternehmen, siehe dazu *Crif* (Fn. 6), 11.

34 Dies könnte auch erklären, warum lediglich ein geringer Anteil an potenziellen Betrugsfällen überhaupt an die Strafverfolgungsbehörder weitergeleitet wird, siehe dazu auch Abb. 4.

35 Zur Einführung des neuen Tatbestands des Identitätsmissbrauchs (Art. 179^{decies} E-StGB) sowie zur daraus folgenden Abgrenzung zu Art. 146 und 147 StGB siehe *Y. Reber,* Der neue Tatbestand des Identitätsmissbrauchs nach Art. 179^{decies} E-StGB, ex ante 2/2020, 33, 33 ff.

36 Siehe dazu *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 144 ff.

37 *B. Fässler,* Der Factoringvertrag im Schweizerischen Recht, Diss. St. Gallen 2010, Rz. 11 ff.

38 *Fässler* (Fn. 37), Rz. 10 ff.

39 Vgl. *Fässler* (Fn. 37), Rz. 92.

40 *Kochheim* (Fn. 22), Rz. 542.

41 *Maeder/Niggli* (Fn. 16), BSK StGB II, Art. 146 N 261 ff.; *Garbarski/Borsodi* (Fn. 23), CR CP II, Art. 146 N 120 ff.

42 Eine kürzlich ergangene Opferbefragung ergab immerhin, dass 3,2% der Befragten bereits einmal Opfer eines Internetbetrugs geworden sind, d.h. beim Nutzen des Internets betrogen und damit finanziell geschädigt wurden. Siehe dazu *D. Baier,* Kriminalitätsopfererfahrungen und Kriminalitätswahrnehmungen in der Schweiz: Ergebnisse einer Befragung, Winterthur 2019, 28. Auch in einer im Jahr 2015 durchgeführten Opferbefragung haben 3,7% der Befragten angegeben, Opfer eines Verbraucherschwindels geworden zu sein, wobei mit 28,6% die häufigste Viktimisierung beim Einkaufen im Internet stattgefunden hatte. Siehe dazu *L. Biberstein* et al., Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung. Analysen im Rahmen der schweizerischen Sicherheitsbefragung 2015, Lenzburg 2016, 16 f.

43 Siehe dazu *BFS,* Polizeiliche Kriminalstatistik, Beschuldigte, Kennzahlen 2020, abrufbar unter: https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/polizei/beschuldigte.html (8.2.2021). Für die Berechnung wurden die beschuldigten juristischen Personen sowie die Fälle ohne Geschlechtsangabe ausgeschlossen, wobei es sich dabei im Bereich des StGB um 548 Fälle, beim BetmG-Bereich um 2 und im AIG um 24 Fälle handelte.

44 *BFS,* Strafgesetzbuch (StGB): Straftaten und beschuldigte Personen, Schweiz Jahr 2020, abrufbar unter: https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/polizei/straftaten.assetdetail.15844440.html (8.2.2021). Prozentzahlen nach eigener Berechnung. Fälle mit juristischen Personen bzw. ohne Angaben des Geschlechts wurden für die Berechnung ausgeschlossen.

45 Die paycard ist ein Zahlungsmittel, womit auf Rechnung in über 600 Verkaufsstellen in der Schweiz sowie in zehn Onlineshops eingekauft werden kann. Dabei fallen keine Jahresgebühren an, und die Abrechnung erfolgt mittels Monatsrechnung mit flexiblen Teilzahlungsoptionen; weitere Informationen abrufbar unter: https://www.paycard.ch/ (8.2.2021).

46 *E. Hilgendorf,* Das Problem des Identitätsdiebstahls – Erscheinungsformen, internationale Entwicklungen und gesetzgeberischer Handlungsbedarf, in: Neuntes Zürcher Präventionsforum: Identitätsdiebstahl in der digitalen Welt – die Gefahren des Missbrauchs persönlicher Daten und Prävention, C. Schwarzenegger/R. Nägeli (Hrsg.), Zürich 2016, 7, 13.

47 *H. Seidenschwarz/N. Deichner/E. Stahl/G. Wittmann,* Erfolgsfaktor Payment – Der Einfluss der Zahlungsverfahren auf den Umsatz. Ergebnisse einer Befragung unter Endkunden. Ibi Research Studie Regensburg, 2020, 54.

48 *Bussmann* (Fn. 22), Rz. 176 ff.

49 Zu den Voraussetzungen des Routine-Activities-Ansatzes von *Cohen/Felson* siehe Kap. I.

50 Siehe dazu *M. Thommen,* Unerhörte Strafbefehle, ZStrR 2010, 373, 374 f.; *Th. Hansjakob,* Zahlen und Fakten zum Strafbefehlsverfahren, forumpoenale 2014, 160, 160.

51 *S. Beukelmann,* Prävention von Computerkriminalität: Sicherheit in der Informationstechnologie, Diss. Rostock 2000, Frankfurt am Main 2001, 100.

52 *Crif* (Fn. 6), 13.

53 *Bussmann* (Fn. 22), Rz. 200.

54 *Marschall* et al. (Fn. 8), 1861.

55 *Marschall* et al. (Fn. 8), 1861.

56 *Marschall* et al. (Fn. 8), 1859 ff.