SORGFALTSPFLICHTEN BEI ZAHLUNGS-DIENSTLEISTERN

Erkenntnissammlung Marktbeobachtung

10. Oktober 2024

Impressum

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

Team Marktbeobachtung Finanzmarkt
MBFinanzmarkt@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.

INHALT

VERBRAUCHERRELEVANZ

Die Angriffe auf Bankkonten nehmen stetig zu. Phishing-Nachrichten, Meldungen von vermeintlichen Familienmitgliedern in Messenger-Apps, Anrufe von angeblichen Mitarbeiter:innen der eigenen Bank oder ungewöhnliche SMS-Benachrichtigungen – täglich werden Verbraucher:innen vielfach Angriffsziele von Betrüger:innen. Die Schadenssummen steigen, und Geschädigte bleiben immer wieder auf den Verlusten sitzen. Dabei wird den Verbraucherzentralen wiederholt gemeldet, dass Zahlungsdienstleister den Verbraucher:innen vorwerfen, grob fahrlässig gehandelt zu haben, weil sie angeblich ihren Sorgfaltspflichten nicht nachgekommen seien. Sorgfaltspflichten werden dabei von den Zahlungsdienstleistern sehr breit interpretiert: keine Links anzuklicken, Mitarbeiter:innen keine TANs zu nennen, sich immer auf der Internetseite der jeweiligen Bank mit den aktuellen Sicherheitswarnungen vertraut zu machen und niemandem zu glauben, dass er auch wirklich von der Nummer aus anruft, die auf dem Display angezeigt wird. Die Begründungen für angebliche grobe Fahrlässigkeit sind vielfältig und scheinen nach Belieben eingesetzt werden zu können.

Doch betrogene Verbraucher:innen berichten wiederholt, dass die Betrüger:innen auf ihren Konten seltsame Aktionen durchgeführt hätten, wie Limite erhöhen und ungewöhnliche Überweisungen beauftragen, dass sie ihre Banken nur schlecht erreichen konnten, um die Überweisungen zu stoppen, oder dass die Anbieter selbst genau zu den Dingen auffordern, von denen sie behaupten, dass man sie nie tun dürfte. Wenn Anbieter von Verbraucher:innen die Beachtung von umfangreichen Sorgfaltspflichten abverlangen, wie stellt sich das Verhalten der Anbieter ihrerseits in den Betrugsfällen dann dar? Kommen die Zahlungsdienstleister ihren eigenen Sorgfaltspflichten denn uneingeschränkt nach und welchen Pflichten müssen sie überhaupt genügen?

ZUSAMMENFASSUNG

Bei der zunehmenden Zahl von Betrugsfällen im Onlinebanking berufen sich Zahlungsdienstleister (Anbieter von Bankkonten) immer wieder auf die Verletzung von Sorgfaltspflichten durch die Verbraucher:innen. Sie lehnen damit Erstattungsansprüche ab. Beschwerden aus den Verbraucherzentralen und eigene Untersuchungen der Marktbeobachtung Finanzmarkt werfen aber ein kritisches Licht auf die Sorgfaltspflichten, denen die Anbieter selbst nachkommen sollten, und damit auf die Frage nach deren potenziellem Mitverschulden. Im Bericht werden sechs Problemfelder thematisiert:

1. **Inkonsistentes Verhalten:** Anbieter verhalten sich nicht in einer Weise, die leichtes Erkennen von Betrug erlauben würde. Sie widersprechen teilweise eigenen Warnungen und schreiben verwirrende Passagen auch in ihren AGB nieder.
2. **Unverständlichkeit von Texten und Prozessen:** An Kund:innen gerichtete Texte oder Prozessschritte bewerten diese mitunter als unverständlich und verwirrend. Warnungen können somit nicht angemessen wahrgenommen werden und helfen zwar den Anbietern bei der Haftungsabwehr gegen die Verbraucher:innen, haben aber einen unzureichenden Nutzen für die Betrugsprävention.
3. **Ungenügende Erreichbarkeit:** Verbraucherbeschwerden schildern immer wieder, dass Anbieter in dringenden Anliegen schlecht oder gar nicht telefonisch erreichbar seien.
4. **Unzureichende Transaktionsanalysen:** Abläufe, wie sie aus Beschwerden hervorgehen, zeigen in Betrugsfällen regelmäßig auffällige Verwaltungseingriffe in Konten, wie beispielsweise Limit- und Dispoerhöhungen und ungewöhnliche Buchungsvorgänge oder im Ausland sitzende Zahlungsempfänger. Diese Vorgänge werden von Seiten der Anbieter mitunter nicht blockiert und lösen auch keine Nachfragen an die Betroffenen aus.
5. **Unangemessene technische Konstruktion:** Beschwerden zeigen, dass Banksysteme anscheinend nicht resilient genug gegen Social Engineering konstruiert sind. Sie können mit dieser Technik zu leicht erfolgreich angegriffen werden. Auch gibt es Systemkonfigurationen, beispielsweise in den Apps der Anbieter, die nur beschränkte Wirkung haben, ohne dass dies den Verbraucher:innen hinreichend klar würde.
6. **Verbraucherschädigendes Verhalten:** Verbraucher:innen berichten, dass ihnen Mitarbeiter:innen der Anbieter nicht immer kompetent weiterhelfen können und teilweise sogar Verhaltensweisen nahegelegen, die der Dringlichkeit im Betrugsfall nicht gerecht werden und unnötig wertvolle Zeit verstreichen lassen.

Nach aktueller Rechtslage werden Sorgfaltspflichten für Anbieter kaum und nur unscharf definiert. Ausnahmen bilden lediglich die jederzeitige telefonische Erreichbarkeit im Betrugsfall und die Beweispflicht der Autorisierung eines Zahlungsvorgangs. In der Rechtsprechung führt dies immer wieder dazu, dass Sorgfaltspflichtverletzungen einseitig zulasten der Verbraucher:innen angeführt werden sowie dass Pflichten der Anbieter – etwa zur Wiederherstellung des Kontostands binnen eines Bankarbeitstags im Falle eines Betrugs – mit der Forderung eines Schadenersatzes aufgerechnet werden. Immer wieder gelingt es Anbietern auch, ihrer Pflicht zum Nachweis der Autorisierung durch faktische Umkehr des eigentlich vorgesehenen Klagewegs zu entgehen. Sie erreichen dies ohne Vorlage handfester Beweise mit einer mittelbaren Beweisführung des ersten Anscheins vor Gericht.

1. PROBLEMLAGE BEI FINANZDIENSTLEISTUNGEN

Die Nutzung von Onlinebanking nimmt an Bedeutung zu. Im Jahr 2023 nutzten in Deutschland 57 Prozent der Bevölkerung Onlinebanking.[1] Gleichzeitig sind die Konten von Verbraucher:innen immer stärker im Fokus von Betrüger:innen. Der Betrug mit Konten und Karten stieg laut Bundeskriminalamt von 2018 bis 2023 um 45 Prozent auf 90.000 Fälle im Jahr.[2] Banken und Sparkassen warnen deshalb vor Betrugsmaschen an unterschiedlichen Stellen auf ihren Internetseiten: als Meldung auf der Startseite[3], auf der Loginseite zum Onlinebanking[4], im Service-Bereich der Website[5], bei jeder Anmeldung in der Banking-App[6] oder als Schulung mit verschiedenen Kapiteln in einem eigenen Bereich[7]. Um sich bei einem erfolgreichen Angriff auf ihre Gelder nicht in die Gefahr des Vorwurfs einer Verletzung ihrer Sorgfaltspflichten zu begeben, wird von Verbraucher:innen regelmäßig verlangt, sich die Internetseiten und die entsprechenden Meldungen genau anzusehen.[8] Andernfalls könnte es sein, dass Banken und Sparkassen ihnen jegliche Erstattung verlorener Gelder versagen.

Doch welchen Sorgfaltspflichten müssen die Zahlungsdienstleister selbst nachkommen, um es Betrüger:innen nicht allzu leicht zu machen, die Konten der Kund:innen zu leeren? Warum haben Betrüger:innen anscheinend immer noch ein so leichtes Spiel, obwohl die Sicherheitsmaßnahmen in den letzten Jahren deutlich erhöht wurden, beispielsweise durch Einführung der Zwei-Faktor-Authentifizierung? Erkenntnisse aus Verbraucherbeschwerden[9] und eigene Analysen der Marktbeobachtung Finanzmarkt deuten auf einige Problemfelder hin. Ohne Anspruch auf Vollständigkeit sind das: ein inkonsistentes Verhalten durch Anbieter von Bankkonten, Unverständlichkeit von Texten und Prozessen, die ungenügende Erreichbarkeit der Anbieter sowie möglicherweise unzureichende Transaktionsanalysen und technische Konstruktionen.

1.1 Inkonsistentes Verhalten

Die Verfahrensweisen und Prozesse für sicheres Onlinebanking sind nur in geringem Ausmaß definiert. Ein Verhalten, das ein Anbieter ausschließt, kann ein anderer durch-

[1] Eurostat: Individuals – internet activities, https://ec.europa.eu/eurostat/databrowser/view/ISOC_CI_AC_I__custom_5475301/bookmark/table?lang=en&bookmarkId=b96fab00-944e-4d02-94e7-b910bc79f103, 02.08.2024.

[2] Atzler, Elisabeth: Betrug mit Karten und Konten wächst, in: Handelsblatt 24.07.2024.

[3] https://tfbank.de/, 23.07.2024.

[4] https://meine.deutsche-bank.de/trxm/db/, 23.07.2024.

[5] https://www.haspa.de/de/home/service/sicherheit-im-internet.html?n=true&stref=sitemap, 23.07.2024.

[6] so bei der ING-DiBa.

[7] https://wissen.consorsbank.de/t5/Ihre-Sicherheit-im-Online/tkb-p/finanzcoach-sicherheit, 23.07.2024.

[8] Vgl. Verbraucherzentrale Bundesverband: Bank oder Betrüger? Erhebung zur Erkennbarkeit von Betrug im digitalen Zahlungsverkehr, 2024, S. 5f, https://www.vzbv.de/sites/default/files/2024-05/24-05-09%20Bericht_vzbv_Betrugserkennung.pdf, 23.07.2024.

[9] Verbraucherbeschwerden entstammen den Einzelfallschilderungen aus den Beratungsstellen der Verbraucherzentralen. Hierbei handelt es sich um ausführliche Beschreibungen besonders auffälliger Sachverhalte aus der Verbraucherberatung, die qualitativ ausgewertet werden können. Rückschluss auf die Häufigkeit des Vorkommens entsprechender Fälle in der Verbraucherberatung oder in der Gesamtbevölkerung sind nicht möglich.

aus anwenden. Selbst eine sehr gängige Warnung wie die, nicht mehrere TANs hintereinander einzugeben[10], da dies als Erkennungsmerkmal für Betrug gilt[11], ist keineswegs ein sicheres Indiz für einen Betrug. So haben regulierte Kontoinformationsdienste in einem normalen Prozessablauf bis zu drei TANs hintereinander abgefragt.[12] Entgegen anderslautender Ansagen verlinken Anbieter in E-Mails auch zu ihrem Onlinebanking oder senden Links zum Anklicken per SMS. Angesichts dieses inkonsistenten Verhaltens ist es nicht verwunderlich, dass Verbraucher:innen betrügerische Angriffe nicht zuverlässig erkennen können. In einer Untersuchung hatten sie sogar bei 38 Prozent der Verhaltensweisen von echten Anbietern den Verdacht, es könnte sich um einen Angriff auf ihr Konto handeln.[13]

1.2 Unverständlichkeit von Texten und Prozessen

Neben der fehlenden klaren Definition von Prozessen beklagen Verbraucher:innen auch, dass Texte von Anbietern unverständlich oder nicht eindeutig seien. So bewerteten Teilnehmer:innen der eben genannten Untersuchung Warnmeldungen, die sie über die Übernahme ihres Authentifizierungsinstruments durch Betrüger:innen informieren sollten, als „verwirrend“ und „unverständlich“. In der Folge erreichten die Warnmeldungen ihren Zweck nicht, nämlich die Betroffenen vor betrügerischem Handeln zu warnen. Nur 16 Prozent der Befragten verstanden den Inhalt dieser Warnmeldungen korrekt.[14] Auch die Freigabetexte in Authentisierungsinstrumenten sind mitunter verwirrend. Wenn Verbraucher:innen beispielsweise ein Überweisungslimit in ihrem Onlinebanking anpassen oder einen Freistellungsauftrag ändern wollen, wurde in der App einer Direktbank als freizugebender Auftrag „Online-Abschluss“ angezeigt, obwohl hierbei kein Produkt abgeschlossen wurde.

Neben den Texten sind auch die Prozessabläufe nicht immer klar und nachvollziehbar. So bewerteten Befragte der oben genannten Untersuchung die dargestellten Abläufe von Anbietern als „umständlich“, „kompliziert“, „verwirrend“ und „nicht einfach“. Sie beklagten eine „komische Reihenfolge“ und äußerten Verunsicherung und Überforderung.[15]

1.3 Ungenügende Erreichbarkeit

Verbraucherbeschwerden aus dem laufenden Jahr 2024 zeigen, dass Anbieter mitunter im Notfall schwer erreichbar sind. Ein Verbraucher beklagte, dass er Opfer eines Phishing-Angriffs wurde, dies aber sofort merkte und seine Bank telefonisch kontaktierte. Bis zur Kontosperre dauerte es nach Angaben des Verbrauchers allerdings 25 Minuten, was die Betrüger:innen nutzten, um 4.800 Euro abzubuchen. Ein anderer Verbraucher schilderte:

> *Durch eine Phishing-Attacke gelang es kriminellen Personen, Zugang zu meinen Bankdaten, Online-Banking, Login-Daten sowie Kreditkarten-Informationen*

---

[10] Siehe beispielsweise https://www.volksbank-buehl.de/banking-service/service/tipps-sicheres-online-banking.html, 23.07.2024.

[11] Siehe Bundesamt für Sicherheit in der Informationstechnik: Was tun im Ernstfall?, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Banking/Was-tun-im-Ernstfall/was-tun-im-ernstfall_node.html, 23.07.2024.

[12] Siehe Verbraucherzentrale Bundesverband: Übersicht zur Erhebung bei Kontoinformationsdiensten, 2022, S. 4, https://www.vzbv.de/sites/default/files/2022-06/2022-06-14%20KID_Ergebnispapier-final.pdf, 23.07.2024.

[13] Verbraucherzentrale Bundesverband (2024) (wie Anm. 8), S. 16.

[14] Ebd., S. 14.

[15] Ebd., S.16f.

zu erhalten. […] Ich verbrachte fast den ganzen Samstag damit, die Bank zu erreichen, und musste mehrere Stunden in der Warteschleife warten, bis ich einen Mitarbeiter am Telefon hatte, der mir nun auch die virtuelle Kreditkarte sperrte. Insgesamt dauerte es über sechs Stunden, jemanden in der Service-Hotline der Bank zu erreichen.

Ein weiterer Verbraucher erklärte, drei Stunden benötigt zu haben, um einen Mitarbeiter einer anderen Bank wegen einer entdeckten unautorisierten Überweisung zu erreichen.

In einem Verbraucheraufruf der Marktbeobachtung zu Problemen bei der telefonischen Erreichbarkeit des Kundenservices der Zahlungsdienstleister meldeten Betroffene verschiedenste Gründe, weshalb sie ihre Anbieter nicht erfolgreich kontaktieren konnten. Darunter fallen endlose Warteschleifen, das Fehlen eines telefonischen Kontaktkanals oder dass sie aus der Leitung geworfen wurden. Trotz hartnäckiger weiterer Anrufversuche gelang nur bei 52 von 178 Rückmeldungen irgendwann eine erfolgreiche Kontaktaufnahme. Elf Meldungen besagten, dass Betroffene einen unautorisierten Kontozugriff nicht mit einem Anruf melden konnten.[16] Wie eine Untersuchung aus dem vergangenen Jahr bei Neobanken und Direktbanken zeigte, sind die Anbieter in dringenden Fällen nicht jederzeit telefonisch erreichbar. Und vier von zehn betrachteten Neobanken stellten gar keine Telefonnummer zur Verfügung oder nur für ein einziges Anliegen.[17]

1.4 Unzureichende Transaktionsanalysen

Betrugsopfer melden in den Verbraucherzentralen immer wieder, dass Täter:innen in einer Weise über ihr Vermögen verfügt hätten, die von ihrem üblichen Nutzungsverhalten stark abweicht: Überweisungslimite wurden erhöht, Zahlungen flossen in schneller Abfolge an unterschiedliche Personen in ungewöhnlich hohen Beträgen, Kreditrahmen wurden beantragt und sofort vollständig ausgeschöpft, Guthaben umgebucht oder es wurden mehrere Echtzeitüberweisungen beauftragt, obwohl Verbraucher:innen nie zuvor derartige Überweisungen durchgeführt hatten. Folgende Schilderungen aus den Beratungsstellen verdeutlichen dies anhand einiger Beispiele:

- *Ende Januar wurde das Konto des Verbrauchers online leergeräumt. Eine fremde Person hat sich Zugang zu seinem Online Konto verschafft. […] Kurz darauf war sein Konto leer. Dabei handelte es sich um vier Flüge ins Ausland und Zahlungen in Dubai (mit einer Kreditkarte der Bank, die der Täter sich auch noch hat erstellen lassen). Diese Transaktionen sind keine üblichen Transaktionen des Verbrauchers und wurden nicht von seinem üblichen Endgerät beauftragt.*
- *Das Konto des Verbrauchers wurde via Phishing-SMS gekapert, ein Dispo wurde eingerichtet und für mehrere Überweisungen ausgereizt.*
- *Verbraucher schildert: Ich erhielt einen Anruf mit der Nummer meiner Bank von einem vermeintlichen Mitarbeiter. Man hätte einen Betrug festgestellt. […] Es wurden dann jeweils zehn Sofortüberweisungen über knapp 2.000 Euro von*

[16] Verbraucherzentrale Bundesverband: Verzweifelte Anrufe. Wie Banken ihre Kunden am Telefon im Regen stehen lassen. Ergebnisse eines Verbraucheraufrufs, 2024, https://www.vzbv.de/pressemitteilungen/banken-lassen-kundinnen-mit-problemen-allein, 16.08.2024.

[17] Verbraucherzentrale Bundesverband: Im Notfall schwer erreichbar? Erhebung zu telefonischen Kontaktmöglichkeiten bei Neobanken und Direktbanken, 2023, https://www.vzbv.de/sites/default/files/2023-07/23-05-10_Ergebnispapier_ServicetelefoneNeobanken_final.pdf, 24.07.2024.

meinem Depot-Verrechnungskonto und vom Tagesgeldkonto auf ein spanisches Konto überwiesen. Nachmittags wurde ich misstrauisch, Anruf bei der Bank, Warteschleife von einer Stunde. Das Auslandsüberweisungslimit wurde von Unbekannten auf 100.000 Euro erhöht.

- *Verbraucherin erhielt eine Mitteilung, angeblich von „netflix“ […] Danach gab es mehrere Abbuchungen vom Kreditkartenkonto in der Währung AED (Vereinigte Arabische Emirate).*
- *Kriminelle haben von den Girokonten der Verbraucher insgesamt 43 Buchungen per Blitztransfer nach Frankreich an einen einzelnen Empfängernamen überwiesen. In Summe handelt es sich dabei um einen Schaden in Höhe von 43.000 Euro.*
- *Verbraucher wurde von vermeintlichem Bankmitarbeiter kontaktiert […] Es wurden in der Folge fast 50 Einkäufe mit Apple Pay getätigt. Der Schaden beträgt fast 10.000 Euro.*
- *Die Kreditkarte des Verbrauchers wurde missbräuchlich genutzt. Sie wurde an einem einzigen Tag in Italien, Marokko und London eingesetzt.*
- *Ein vermeintlicher Bankmitarbeiter fragte die Verbraucherin, ob sie in der letzten halben Stunde Aufträge getätigt hätte – Erhöhung des Überweisungslimits auf 3.900 Euro, eine Überweisung über 2.300 Euro und drei Überweisungen über knapp 500 Euro. Da die Verbraucherin in der letzten halben Stunde mit ihrem Hund spazieren ging, verneinte sie die Frage. Der angebliche Mitarbeiter hatte Einblick in das Konto, denn er gab der Verbraucherin noch Details zu vorherigen von der Verbraucherin beauftragten Überweisungen. […] Der Anrufer sagte dann, dass sie nun die falschen Beträge 'stornieren' müssten. Tatsächlich kamen danach entsprechende Aufträge. Als Empfänger war der Name der Verbraucherin angegeben. Darauf wies der Anrufer auch noch genau hin. Der Anrufer erklärte, dass dies für die Rückbuchung erforderlich sei.*
- *Vom Konto des Verbrauchers wurden per Debitkarte über 4.000 Euro (Konto/Dispo) abgebucht. […] Auf Fragen des Verbrauchers bei der Bank, warum die Karte bei über 20 abgelehnten Buchungsversuchen von der Bank nicht gesperrt wurde, erfolgte keine Reaktion.*

1.5 Unangemessene technische Konstruktion

Weitere Verbraucherbeschwerden werfen die Frage auf, wie Anbietersysteme technisch konstruiert werden und von welchem Verbraucherleitbild her dabei gedacht wurde. So zeigen beispielsweise Fälle, bei denen von der scheinbar korrekten Telefonnummer des Anbieters bei Verbraucher:innen angerufen wird, um einen vermeintlichen Betrug rückabzuwickeln, dass schon mit einem einzigen falschen Klick in der App ganze Konten an Betrüger:innen übergeben werden. Verbraucher:innen werden von Betrüger:innen in eine Stresssituation versetzt und es kann auch nicht davon ausgegangen werden, dass jede Person umfassend in Zahlungsverkehrstermini und -vorgängen gebildet ist. Betrüger:innen wird es so mit einer plausiblen Geschichte und geschickten kommunikativen Fähigkeiten vermutlich immer wieder gelingen, diesen einen Klick auszulösen. Technische Systeme, mit denen unterschiedlichste Menschen interagieren, sind aus Sicht des vzbv aber fehlkonstruiert, wenn ein einziger falscher Klick bereits derart gravierende Auswirkungen haben kann. Kritische Anwendungen, die

nicht nur an Experten gerichtet sind, sollten technisch so konstruiert werden, dass sie auch bei Angriffsszenarien resilient sind.[18]

Umso mehr gilt dies, wenn Betrüger:innen Systeme selbst ohne Techniken des Social Engineerings übernehmen können, wie die folgenden Beschreibungen von Verbraucherbeschwerden nahelegen:

- *Es erfolgte eine unautorisierte Verfügung durch Kreditkartenmissbrauch. Der Verbraucher erhielt eine Aktivierungs-SMS für Apple Pay, hat auf diese aber nicht reagiert. Wochen später fand Betrug durch Warenkauf im stationären Laden statt.*
- *Verbraucherin hatte im Januar 2024 Probleme beim Onlinebanking bzw. technische Probleme mit der TAN-App. Daraufhin erhielt sie einen Aktivierungsbrief von der Bank. Mit diesem konnte sie die TAN-App jedoch immer noch nicht neu registrieren, Insgesamt erhielt die Verbraucherin neun Aktivierungsbriefe. Im Nachgang stellte sich heraus, dass durch die Freigabe der Aktivierungscodes Sicherheitsverfahren für fremde Dritte installiert wurden.*
- *Auf die Frage der Berater, ob ich Phishing E-Mails oder SMS erhalten habe, antwortete ich mit einem klaren Nein. Bei Bankdaten bin ich so sorgfältig, dass noch nicht mal mein eigener Mann meine Zugangsdaten kennt. Daraufhin stellte die Beraterin fest, dass Ende Mai 2024 auf einem neuen Android-Handy die TAN-App installiert wurde. Ich erinnere mich, dass ich kurz vorher eine Überweisung tätigen wollte. Wie üblich wurde ich vom Online-Banking-System der Bank nach der TAN gefragt und wie üblich öffnete ich die TAN-App, um den Auftrag freizugeben. Bei diesem Erstellungsvorgang kam direkt von der App eine Fehlermeldung. Ich versuchte es erneut, aber es kam eine erneute Fehlermeldung. Ich versuchte auf SMS-TAN umzustellen, aber auch das ging nicht, da es nicht aktiviert war. Als ich las, dass ich einen neuen Aktivierungsbrief benötige, um den Vorgang ins Laufen zu bringen, brach ich den Vorgang ab. Drei Tage später tätigte ich eine neue Überweisung, die funktioniert hat. Am nächsten Tag wurde mein ganzes Konto geplündert.*

Selbst wenn Verbraucher:innen Technik vermeintlich korrekt anwenden, scheint diese nicht immer zu den naheliegenden Ergebnisse zu führen. Dies kann eine Fehlfunktion oder aber konstruktionsbedingt angelegt sein. So zum Beispiel, wenn Kreditkarten in einer App nur für künftige Zahlungen in der App gesperrt werden können, das aber nicht bedeutet, dass die Karte generell, also auch außerhalb der App gesperrt wird. Verbraucherbeschwerden beleuchten auch dieses Problemfeld:

- *Laut Verbraucher kam es im Dezember 2023 zu Kreditkartenmissbrauch. Er erwähnt, per Online-Banking-App die Kreditkarte gesperrt und Missbrauch als Grund angekreuzt zu haben. […] Später sprach er mit einem Mitarbeiter der Bank. Der Mitarbeiter sah die Kreditkartensperrung online nicht. Deswegen hat der Mitarbeiter dann noch selbst die Kreditkartensperrung veranlasst.*
- *Verbraucherin hat seit 1990 das Girokonto und erhält im Februar 2024 einmal nachts und einmal morgens vom Kreditkartenservice der Bank per SMS eine Nachricht, dass eine Kreditkarte und eine Digitale Karte mit Limit von 1.000*

[18] Siehe hierzu Zimmermann, Verena; Renaud, Karen: Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset, in: International Journal of Human-Computer Studies, 2019, S. 169–187.

Euro aktiviert wurden. Verbraucherin hat dann taggleich das Konto sperren lassen, weil Sie keine Karten beantragt hatte. Das Konto wurde dennoch über die beiden Karten belastet, da die Karten nicht mitgesperrt wurden.

1.6 Verbraucherschädigendes Verhalten

Frustrierende Erfahrungen erleben Verbraucher:innen auch fortwährend, nachdem sie Betrüger:innen zum Opfer fielen. Melden sie dies den betreffenden Anbietern, erfahren sie nicht immer die Unterstützung, die sie bekommen sollten: Sie werden auf einen späteren Zeitpunkt vertröstet, auf Formulare und Prozesse verwiesen oder ihnen wird Hilfestellung schlichtweg verweigert. Folgende Fallschilderungen veranschaulichen dies:

- *Verbraucherin ist Opfer eines Kreditkartenbetruges geworden. Als sie gesehen hat, dass in ihrem Onlinebanking der Zahlungsbetrag von fast 1.500 Euro zur Abbuchung vorgemerkt wurde, rief sie sofort beim Notfallservice an, um diesen Vorgang zu stoppen. Ihr wurde gesagt, dass man den Vorgang nicht stoppen könne, dass sie abwarten müsse, bis das Geld abgebucht wurde und sie die Zahlung dann innerhalb von 30 Tagen reklamieren könne. Ihr Konto wurde zusätzlich gesperrt. Gesagt, getan. Das Geld wurde abgebucht, und sie wollte den Vorgang reklamieren, Das ging aber nicht, „aus technischen Gründen gerade nicht möglich“. Sie rief sofort bei der Bank an: Es sei ja kein Notfall und sie solle das bereitgestellte Formular verwenden.*
- *Verbraucher ist auf Phishing eingegangen und hatte danach Bedenken. Er rief gleich seine Bank an, um sein Konto zu sperren. Diese hat ihn jedoch auf den darauf folgenden Tag vertröstet. Vier Tage später wurde dann von seinem Konto eine Überweisung nach Großbritannien getätigt, die er nicht autorisiert hatte (über 5.000 Euro).*
- *Verbraucher-Ehepaar war in Südafrika und wurden unter Vortäuschen einer Sicherheitskontrolle an einen Geldautomaten gelockt, der offenbar manipuliert war. Er hat die Kreditkarte behalten. Verbraucher haben umgehend die Kreditkarte innerhalb von zehn Minuten sperren lassen. Am kommenden Tag war ersichtlich, dass 200 Euro abgehoben wurden, was in der Regel dem maximalen Betrag an einem Geldautomaten in Südafrika entspricht. Einige Tage später wurden nochmals zwei Beträge auf dem Konto verbucht, im Wert von 5.000 Euro. Obwohl die Karte schon mehrere Tage gesperrt war, war es den Dieben möglich, damit Geld zu bewegen. Es gab keine TAN, keine E-Mail, keine Rückfragen, ob diese ungewöhnlich hohen Bewegungen im Ausland tatsächlich von Ihnen stammten.*
- *Die Kreditkarte des Verbrauchers wurde missbräuchlich genutzt. […] Die Bank weigert sich, den Schaden zu regulieren und ebenso ein Chargeback-Verfahren bei Mastercard einzuleiten. Angeblich hätte der Verbraucher die Zahlungen über die App freigegeben, was nicht der Fall war.*

2. AKTUELLE RECHTSLAGE

Die gesetzlichen Regelungen zum Umgang mit unautorisierten Zahlungen haben ihren Ursprung in den Vorgaben der EU-Zahlungsdienste-Richtlinie.[19] Das Regelwerk gibt für

[19] Aktuell gilt die zweite Zahlungsdienste-Richtlinie (EU) 2015/2366; ohne nähere Angabe beziehen sich Artikel-Normen im Folgenden auf diese Richtlinie.

unbefugte Buchungen vor, dass primär die Zahlungsdienstleister für die wirtschaftlichen Folgen von durch die Berechtigten nicht „autorisierten“ Buchungen verantwortlich sind.

Unbefugte Buchungen sind danach in der Regel kurzfristig zu erstatten (Artikel 73 beziehungsweise § 675u BGB). Auch eine technisch korrekte Verbuchung soll in der Regel nicht den Schluss zulassen, dass Betroffene Pflichten verletzt oder gegen Bedingungen für die Ausgabe und Nutzung dieser Zahlungsinstrumente vorsätzlich oder grob fahrlässig verstoßen haben (Art. 72, § 675w BGB). Beruht die Abbuchung auf der Nutzung eines abhandengekommenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Zahlungsinstruments und hätte dies bemerkt werden können, haften Betroffene Kontoinhaber zunächst auch nur mit 50 Euro. Sie sind zum Ersatz des gesamten Schadens vollends verpflichtet, wenn der Schaden durch eine vorsätzliche oder grob fahrlässige Verletzung ihrer gesetzlichen Pflichten[20] nach § 675l Absatz 1 BGB oder von Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments verursacht worden ist.

2.1 Unscharfe Definition der Pflichten

Die Diskussion der Pflichten zur Prävention von Betrug fokussiert sich zunächst auf die Zahlungsdienstnutzenden.[21] Erst ihre Pflichtverletzung bewirkt eine Haftung der Zahlungsdienstnutzenden. Für Laien sind die Vorgaben zu ihren Pflichten jedoch nicht immer so einfach zu verstehen, wie es auf den ersten Blick scheint.

Normen schaffen grobe Vorgaben und AGB sowie Nutzungsbedingungen formulieren Regelbeispiele. Dabei müssen klare Vorgaben auch wieder formal aufgehoben werden[22], weil zum Beispiel ein klares Verbot zur Nichtweiterleitung von TANs außerhalb des Online-Bankings nicht gegenüber Kontoinformations- und Zahlungsauslösediensten sowie sonstigen Diensten formuliert werden darf.[23] Dadurch sind Bedingungen für das Online-Banking für Verbraucher:innen beispielsweise verwirrend gestaltet, wenn sie einerseits vorschreiben, dass „die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Online-Bankings mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden“ dürfen.[24] Andererseits werden diese Vorgaben zwei Absätze weiter unter bestimmten Bedingungen wieder aufgehoben. Deswegen sind immer gültige Vorgaben auch normativ schwierig. Es muss weiter der Einzelfall bewertet werden.[25]

Für Betroffene bleibt bei derart verwirrenden Regelungen die Unterscheidung von regulärem, nicht betrügerischem Verhalten und betrügerischen Angriffen eine Herausforderung. So ist beispielsweise die Behauptung, die Eingabe mehrerer TANs sei immer

---

[20] Die Normen schützen ferner nicht Betrügende, zur Vereinfachung wird auf die explizite Erwähnung dieses Sachverhalts hier verzichtet.

[21] Siehe beispielsweise MüKoBGB/Jungmann, 9. Aufl. 2023, BGB § 675l Rn. 34, Beck Online. Kommentiert werden dann detaillierte Beispiele, die aber nicht in jeder Situation eine Verallgemeinerung erlauben vgl. etwa aaO Rn. 36.

[22] Exemplarisch zum Beispiel Ziffer 7.1 (2) b der Bedingungen für das Online-Banking, 182 410.000 D1 (Fassung Sep. 2022) v4.1 der S-Management-Services – DSV Gruppe via Sparkasse Köln-Bonn

[23] Gemäß Artikel 33 der Delegierten Verordnung (EU) 2018/389 vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 haben Drittdienste das Recht, bei Störungen ihres eigentlichen Zugriffs zur Bank auf die Kunden-Schnittstellen zurückzugreifen. Was bedeutet, dass sie dann den Zugang zur Bank mit den Daten des Nutzers übernehmen dürfen.

[24] Exemplarisch zitiert aus Ziffer 7.1 (2) b der Bedingungen für das Online-Banking, 182 410.000 D1 (Fassung Sep. 2022) v4.1 der S-Management-Services – DSV Gruppe via Sparkasse Köln-Bonn

[25] So auch im Ergebnis. Maihold in: Ellenberger/Bunte BankR-HdB, § 33. Bankgeschäfte online Rn. 248, beck-online

eine grobe Pflichtverletzung der Verbraucher:innen, jedenfalls in dieser Pauschalität nicht korrekt.

2.2 Faktische Umkehr des Klageweges

Ginge es nach Art. 73 der Zahlungsdienste-Richtlinie müssten Anbieter unbefugte Buchungen dem Wortlaut nach „*auf jeden Fall*“[26] zunächst dem Konto wieder erstatten. In der Folge müsste dann eigentlich die Bank beweisen, dass Nutzer:innen sich grob fahrlässig verhalten haben, um sie – nötigenfalls als Kläger vor Gericht – in Regress nehmen zu können. Das ist aber nicht der Fall, weil sich höchstrichterlich etabliert hat, dass Betroffene unbefugter Buchungen nicht erst von der Bank die Erstattung verlangen können sollen, wenn sie diese anschließend als Schadensersatz ohnehin zurückzahlen müssten. Was dem BGH und zuletzt auch wieder dem OLG Frankfurt am Main andernfalls treuwidrig erscheint[27], wirft die Frage auf, warum es aber in der Folge zulässig sein soll, dass eine Bank sich mit der Prüfung eines Falls mitunter mehrere Wochen Zeit lassen darf, ohne währenddessen für Kontodeckung zu sorgen. Ergäbe die Prüfung am Ende, dass doch keine grobe Fahrlässigkeit vorlag, wäre klar gegen den § 675u BGB verstoßen worden.

In Folge dieser Umkehrung muss sich die Bank keine Mühe geben, den schwerwiegenden Vorwurf grob fahrlässiger Pflichtverletzungen gegen die Kund:innen zur Überzeugung des Gerichts darzulegen und zumindest im Anschein nachzuweisen. Es sind betroffene Nutzer:innen von Zahlungsdienstleistern, die immer wieder gezwungen sind, ihr Recht auf unverzügliche Erstattung aufwendig und wesentlich verspätet zur Vorgabe des § 675u BGB durchzusetzen. Was zu einer regelmäßig planwidrigen Verschlechterung der Lage von Zahlungsdienstnutzern führt.

2.3 Pflichten der Bank und die Mitverschuldens-Thematik

Pflichtverstöße der Banken können den Ersatzanspruch wegen grob fahrlässiger Pflichtverstöße auf Nutzerseite nach § 675v BGB ausschließen. Die in diesem Fall relevanten Pflichten auf Seiten der Zahlungsdienstleister ergeben sich aus § 675m Absatz 1 Ziffer 3 und 5 BGB und werden in § 675v Absatz 5 BGB[28] aufgegriffen: Die Haftung der Zahlungsdienstnutzer:innen bei grober Fahrlässigkeit entfällt bei fehlender Erreichbarkeit des Anbieters sowie ab der Meldung des Sicherheitsvorfalles für folgende Buchungen.

Kritisch ist, dass der Wortlaut des § 675v Absatz 5 BGB scheinbar nicht bei fehlender Erreichbarkeit des Anbieters vor den Folgen grober Fahrlässigkeit schützt. Denn hier fehlt ein Verweis im Text auf den richtigen Absatz 3. In der Lehre wird von einem Redaktionsversehen ausgegangen.[29] Artikel 74 der Zahlungsdienste-Richtlinie schließt die Haftung wegen grober Fahrlässigkeit auch bei mangelnder Erreichbarkeit der Anbieter aus.

---

[26] Exklusive genau definiertem Betrugsverdacht

[27] Vgl. BGH Urteil vom 17.11.2020 (Az.: XI ZR 294/19) Randnummer 25 oder auch OLG Frankfurt am Main Urteil vom 6.12.2023 – 3 U 3/23 Randnummer 46

[28] Ein weiterer Ausschluss der Haftung wegen grober Fahrlässigkeit für Zahlungsdienstnutzer ergibt sich bei fehlendem Einsatz starker Kundenauthentifzierung nach Absatz 4. Das ist aber nicht als Pflichtverletzung, sondern Formvorgabe ausgestaltet.

[29] Siehe auch Maihold in: Ellenberger/Bunte BankR-HdB, § 33. Bankgeschäfte online Rn. 400, beck-online

Nicht besonders kodifiziert sind die weiteren Pflichten der Zahlungsdienstleister, die im Sinne der allgemeinen Schadensminderungspflicht nach § 254 BGB der Bank aufgeben, einen Schaden selbst dann klein zu halten, wenn ein grob fahrlässiges Kundenverhalten festgestellt werden kann. In diesem Zusammenhang geht es auch um die unzureichende Beobachtung und Reaktion auf Angriffsmuster vor dem Hintergrund erkannter neuer Gefährdungslagen.[30]

Angesichts dessen sind Schilderungen der Verbraucher:innen bedenklich, wenn Banken die Erstattung von Buchungen verweigern, weil Zahlungsinstrumente nicht oder nicht mehr rechtzeitig „gesperrt“ werden konnten oder die Betroffenen vertröstet wurden. Denn nur auf die Meldung, nicht auf die Sperrung kommt es beim Entfallen der Haftung an. Ein Gericht müsste den Schadenersatz für solche Buchungen versagen.

Kritisch ist es auch, wenn die Banken trotz Kenntnis von klassischem Verhalten von Betrüger:innen Buchungen nicht stoppen, die diesen Mustern folgen und zum Beispiel nach dem Einrichten eines neuen Zahlungsinstruments unübliche Buchungen zur Kontoleerung vorbereiten und beauftragen. Ein Gericht müsste in diesen Fällen einen Ersatz mindestens reduzieren und sogar versagen, wenn die Pflichtverletzung der Bank schwerwiegender erscheint. Bisher wurde ein Mitverschulden aber auch immer wieder abgelehnt, weil eine Überwachung von Kontobewegungen oder eine Risikobewertung von Zahlungsvorgängen nicht als Pflicht der Zahlungsdienstleister angesehen wurden.[31] Der BGH[32] setzte dazu noch 2012 „massive Verdachtsmomente“ voraus. Die Vorgaben der höchstrichterlichen Rechtsprechung laufen den Gefahren und auch den technischen Möglichkeiten hinterher.

FAZIT

Bei der Betrachtung des Gesamtbildes im Zusammenhang mit Sorgfaltspflichten bei betrügerischen Aktivitäten fällt auf, dass Anbieter von Bankkonten an unterschiedlichsten Stellen und immer wieder vor Betrug warnen, teilweise auch bei jedem Zahlungsvorgang ohne jeglichen Verdachtsmoment. Von Verbraucher:innen wird erwartet, alle diese Informationen an unterschiedlichen Stellen jederzeit wahrzunehmen, in der jeweiligen Situation kritisch auf den jeweiligen Sachverhalt hin zu überprüfen und abzuwägen, ob Bestimmungen beispielsweise in den AGB der Anbieter ein unübliches Verhalten nicht doch erlauben. Dieser Aufgabe werden auch informierte Verbraucher:innen nur sehr schwer gerecht werden können. Informationen, die von Anbietern unter diesen Bedingungen bereitgestellt werden, scheinen auch dazu zu dienen, geschädigten Verbraucher:innen am Ende vorzuwerfen, dass sie diese Information nicht wahrgenommen hätten und deshalb keine Erstattung erhalten könnten. Zudem scheinen Warnungen auch nicht immer ausreichend verständlich zu sein, um ihren Zweck zu erfüllen. Ein nicht zielgerichteter informationeller Overload in Kombination mit zwar zielgerichteten, aber unverständlichen Warnungen hat aus Sicht des vzbv kaum einen Nutzen für Verbraucher:innen, sondern dient eher der Schadensabwehr der Anbieter. Wollten Anbieter wirklich Sorgfaltspflichten nachkommen, wäre es ihre Aufgabe, Informationen punktgenau bereitzustellen und in einer Weise zu formulieren, die für eine breite Verbraucherschicht auch verständlich ist.

[30] So auch Maihold in: Ellenberger/Bunte BankR-HdB, § 33. Bankgeschäfte online Rn. 380, beck-online

[31] Vgl. BeckOK BGB/Schmalenbach, 70. Ed. 1.5.2024, BGB § 675v Rn. 19, beck-online

[32] BGH, Urt. v. 24. 4. 2012 − XI ZR 96/11, NJW 2012, 2422, 2425 Rn. 32f. beck-online

Darüber hinaus scheint die Technik für digitales Banking zwar gesetzlichen Anforderungen zu entsprechen, aber aus Sicht des vzbv nicht hinreichend resilient gestaltet zu sein, um kommunikativ versierten Betrüger:innen kein Einfallstor zu bieten.

Insgesamt scheinen Sorgfaltspflichten für Anbieter kaum definiert zu sein. Eine der wenigen Anforderungen ist deren jederzeitige telefonische Erreichbarkeit im Betrugsfall. Ist diese aber nicht vorhanden und werden dann zudem mitunter noch unsachgemäße Anweisungen gegeben, ist dies für Verbraucher:innen im Zweifel schwer nachweisbar. In der Rechtsprechung wird vielmehr noch regelmäßig eine weitere Pflicht der Anbieter – die Beweisführung bei grober Fahrlässigkeit – durch die Annahme des Anscheinsbeweises minimiert – gestützt durch vermeintliche Sorgfaltspflichtverletzungen auf Seiten der Verbraucher:innen bei Nichtbeachtung von Warnhinweisen.

Wenn Betrüger:innen aber Zugriff auf Bankkonten erlangt haben und dort Einstellungen verändern, verschiedenste Aktionen hintereinander ausführen, ungewöhnlich hohe Beträge in untypischer Häufigkeit hintereinander an neuartige Empfänger versenden, besteht rechtlich keine Verpflichtung der Banken, dies im Sinne einer Schadensminderung zu erkennen und zu unterbinden. Die Überwachung auffälliger Transaktionen und Kontoaktivitäten sowie eine technisch resiliente Gestaltung der eigenen Instrumente scheint eine rein freiwillige Leistung der Zahlungsdienstleister zu sein. Und dieser kommen sie aus Sicht des vzbv nur unzureichend nach.