VERBRAUCHERPROBLEME BEI BETRÜGERISCHEN KONTOZUGRIFFEN

Fallsammlung Marktbeobachtung Finanzmarkt

28. September 2022

NORMATIVE GRUNDLAGEN

Die Schaffung eines einheitlichen europäischen Zahlungsverkehrsraums war ein wichtiger Schritt für einen EU-weiten Binnenmarkt. Die hierzu grundlegende Zahlungsdiensterichtlinie definiert als Voraussetzung dafür in ihrer seit dem 13.01.2018 umgesetzten zweiten Fassung (Richtlinie 2015/2366 (EU)) die Verbraucherrechte für Zahlungen neu[1]. Hierzu zählt von jeher auch die Frage der Haftung bei betrügerischen Zugriffen auf ein Zahlungsverkehrskonto. Kernpunkte hierbei sind:

- Wenn Zahlungsdienstnutzer bestreiten, einen Zahlungsvorgang autorisiert zu haben, muss der Anbieter nachweisen, dass der Vorgang authentifiziert war, ordnungsgemäß ausgeführt wurde und nicht durch eine technische Panne beeinträchtigt wurde. (Art. 72, Abs. 1)
- Die aufgezeichnete Nutzung eines Zahlungsinstruments reicht nicht notwendigerweise aus, um eine Autorisierung nachzuweisen oder dem Zahler Betrug oder grob fahrlässiges Verhalten vorzuwerfen. (Art. 72, Abs. 2)
- Bei einem nicht autorisierten Zahlungsvorgang hat der Anbieter den Betrag spätestens bis zum Ende des folgenden Geschäftstags zu erstatten, zu dem er Kenntnis von der nicht autorisierten Zahlung erlangte. Eine Ausnahme wird nur für den Verdacht eines Betruges durch den Nutzer nach näheren Vorgaben zugelassen. (Art. 73, Absatz 1)
- Der Zahler trägt einen Schaden von höchstens 50 Euro, wenn er ein Zahlungsinstrument verloren hat oder es gestohlen oder missbräuchlich verwendet wurde, auch wenn er seine personalisierten Sicherheitsmerkmale nicht sicher aufbewahrt hat. (Art. 74, Abs. 1)
- Er trägt nur dann alle Schäden, wenn er in betrügerischer Absicht oder grob fahrlässig gehandelt hat. (Art. 74, Abs. 1)
- Verlangt der Zahlungsdienstleister vom Nutzer als Zahler keine starke Kundenauthentifizierung, so haftet der Nutzer – mit Ausnahme von betrügerischer Absicht – grundsätzlich nicht. (Art. 74, Abs. 2)

[1] Richtlinie (EU) 2015/2366, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32015L2366, abgerufen: 20.09.2022.

BEOBACHTUNGEN

Die Verbraucherrechte bei nicht autorisierten Zahlungsvorgängen wurden im Zuge der Schaffung des europaweiten Zahlungsverkehrsraums somit deutlich gestärkt. In der Praxis der Verbraucherzentralen zeigt sich allerdings, dass es in der Anwendung immer wieder zu Problemen kommt.

Im Folgenden werden Falltypen aufgezeigt, die wir aus Beschwerden extrahierten, mit denen sich Verbraucher:innen hilfesuchend an die Verbraucherzentralen wendeten. Ergänzend findet sich zu jedem Falltyp eine veranschaulichende Beispielbeschwerde. Die Fallkonstellationen stammen aus dem Frühwarnnetzwerk der Verbraucherzentralen und des vzbv [2]. Ausgewertet wurden Beschwerden aus den Jahren 2020 bis 2022.

Anbieter verweigert Kommunikation und blockiert

Eine Zahlungskarte wird infolge eines Identitätsdiebstahls missbräuchlich verwendet. Der Anbieter reagiert nicht oder bricht die Kommunikation ab. Er legt auch keine Beweise vor. Es erfolgt keine Erstattung des unautorisiert verfügten Betrags.

- Beispielbeschwerde:
  Es erfolgten unautorisierten Kreditkartenumsätze mit einem Schaden von knapp 1.400 Euro. Der Anbieter erstattet nicht. Es ist dem Verbraucher nicht möglich, mit dem Anbieter zu kommunizieren. In Summe stundenlange Wartezeiten in der Hotline. Beim äußerst seltenen Durchkommen ist keine direkte Lösung möglich. Anfragen per E-Mail oder Kontaktformular werden ignoriert. Es ist dem Kunden unmöglich, die Angelegenheit zu klären. Der Anbieter liefert keine Argumente und die angeforderten Nachweise werden seitens der Bank nicht geliefert.

Anbieter verweigert Erstattung, weil Verbraucher:innen angeblich auf Phishing hereingefallen sei

Es erfolgt eine unautorisierte Abbuchung vom Giro- oder Kartenkonto. Anbieter verweigert die Erstattung und behauptet, Verbraucher:innen seien auf Phishing-Angriff hereingefallen und daher sei die Buchung korrekt autorisiert worden. Verbraucher:innen bestreiten dies, stellen Strafanzeige gegen die Täter und verlangen vom Anbieter die Herausgabe der Transaktionsprotokolle. Es wird geschildert, dass Anbieter dies regelmäßig verweigern. Von Verbraucher:innen hingegen verlangen die Anbieter mitunter den kaum zu erbringenden Nachweis, dass sie nicht auf einen Phishing-Angriff hereingefallen sind. Die unautorisierten Abbuchungen zeigen deutliche Auffälligkeiten wie untypisch

[2] Beim Frühwarnnetzwerk (FWN) handelt es sich um ein qualitatives Erfassungs- und Analysesystem für auffällige Sachverhalte aus der Verbraucherberatung. Grundlage stellt eine ausführliche Sachverhaltsschilderung durch Beratungskräfte dar, die eine Kategorisierung sowie eine anschließende qualitative Analyse ermöglicht. Eine Quantifizierung der Daten aus dem FWN heraus bzw. ein Rückschluss auf die Häufigkeit des Vorkommens in der Verbraucherberatung oder in der Gesamtbevölkerung insgesamt ist daher nicht möglich.

hohe Überweisungen in kurzer Folge ins europäische oder nicht europäische Ausland. Mitunter werden zuvor noch eingestellte Überweisungslimite deaktiviert oder erhöht. Genutzt werden hierfür Authentisierungsinstrumente, die kurz zuvor erst registriert wurden und sonst noch nie für eine Aktion benutzt wurden. Die KI der Anbieter unterbindet diese Buchungen anscheinend nicht oder die vom Anbieter daraus gezogenen Maßnahmen sind unzureichend.

- Beispielbeschwerde:
  Ohne Zutun der Verbraucherin wurden von ihrem Konto schnell hintereinander drei Echtzeitüberweisungen für insgesamt über 23.000,00 Euro getätigt. Der Bankmitarbeiter meinte, es war bestimmt die Schuld der Verbraucherin und nicht der Bank. Die Verbraucherin glaubt das nicht. Das Überweisungslimit wurde einfach deaktiviert. Die ungewöhnlichen Geldbewegungen lösten bei der Bank keinerlei Alarm aus, der die Buchungen unterbunden hätte.

- *Nach unberechtigten Zugriffen auf das Online-Konto der Verbraucherin, wurde dieses gesperrt (Anruf vom Sicherheitsdienst). Das Geld wird der Verbraucherin nicht erstattet, mit der Begründung, es handele sich um von ihr autorisierte Überweisungen, dabei wurde ihr unterstellt, eine Phishingmail geöffnet zu haben. Des Weiteren wurde ihre Kreditkarte innerhalb von 1-2 Tagen mit mehr als 5.000 Euro belastet: Transaktionen in die Vereinigten Arabischen Emirate, Spanien, Kasachstan. Die Verbraucherin wurde bei diesen Auffälligkeiten nicht vom Sicherheitsdienst gewarnt. Als sie es bemerkt hat, sperrte sie die Karte sofort. Das war allerdings zu spät, um die Buchungen noch zu unterbinden. Ein von ihr eingereichtes Beschwerdeschreiben mit genauen Angaben der unberechtigten Transaktionen, sowie ein Schreiben über Anzeige bei der Polizei wurden mit der Begründung abgewiesen, dass alle Angaben korrekt seien (Kartennummer, Ablaufdatum, Prüfzahl) und damit von ihr autorisiert waren. Die Verbraucherin hat laut eigener Aussage nicht fahrlässig gehandelt: Sie gab die Karte nicht aus der Hand, sie wurde nicht verloren und die PIN war nirgends notiert und niemandem bekannt.*

Anbieter verweigert Erstattung komplett, weil Buchungen per TAN autorisiert waren

Nach einem Angriff durch Social Engineering erfolgen unautorisierte Buchungen vom Konto der Verbraucher:innen. Die Bank/Sparkasse bestreitet, dass die Buchungen nicht autorisiert waren.

- Beispielbeschwerde:
  Der Verbraucher hat bei ebay Kleinanzeigen Waren verkauft und die Zahlung über das Zahlungssystem des Portals abgewickelt (OPP). Das System ist so angelegt, dass die Zahlung zunächst beim Zahlungsdienst einbehalten wird und erst dann ausgezahlt wird, wenn Bestätigungen erfolgen. Der Verbraucher wurde per Whats-App aufgefordert, den Zahlungseingang zu bestätigen. Der Verbraucher bestätigte dies auf ebay-kleinanzeigen.eu. Da

es sich um die falsche Top-Level-Domain handelte, wurde damit vermutlich ein neues Authentisierungsinstrument freigeschaltet. Es folgten 22 nicht vom Verbraucher autorisierte Zahlungen. Die Umsätze erfolgten mittels einer Zwei-Faktor-Authentifizierung. Der Anbieter behauptet, dass alle betrügerischen Zahlungen bestätigt wurden. Er lehnt eine Erstattung mit der Begründung ab, dass die Umsätze mit starker Kundenauthentifizierung erfolgt seien.

Anbieter verweigert Erstattung und beruft sich pauschal auf die Sicherheit seiner Systeme

Es erfolgen unautorisierte Abbuchungen im Onlinebanking. Die Bank/Sparkasse verweigert eine Erstattung, da die Buchungen über die hauseigene App autorisiert worden seien und die App sicher sei.

- Beispielbeschwerde:
  Es erfolgen unberechtigte Zahlungen über das Onlinebanking des Anbieters, genutzt werden die Banking App und die pushTAN-App des Anbieters. Bank/Sparkasse verweigert Erstattung mit der Behauptung, dass die Nutzung der eigenen Apps konstruktionsbedingt sicher sei.

Anbieter gibt an, die Forderung sei berechtigt

Betrüger stehlen Kreditkartendaten und kaufen damit im Internet ein. Die Buchungen werden durch die Verbraucher:innen reklamiert. Das Chargeback-Verfahren scheitert allerdings, weil der Anbieter angibt, die Forderung sei berechtigt.

- Beispielbeschwerde:
  Der Verbraucher besitzt eine Mastercard-Kreditkarte und stellte auf seinem dazugehörenden Konto eine missbräuchliche Verwendung fest. Mit seiner Karte wurde ein Sofa in Boston bezahlt, obwohl er sich nicht dort aufhielt. Er leitete daraufhin ein Chargeback-Verfahren ein. Der Anbieter erstattet nicht und behauptet, die Forderung sei berechtigt.

Anbieter beruft sich auf Beweis des ersten Anscheins

Girocard oder Kreditkarte werden gestohlen. Im Vorfeld wird möglicherweise zusätzlich die PIN ausgespäht. Nachfolgend erfolgen unautorisierte Bargeldverfügungen, die der Anbieter nicht erstattet. Er führt an, die Verbraucher:innen müssten grob fahrlässig gehandelt und die PIN auf der Karte notiert haben. Es erfolgt keine Erstattung.

- Beispielbeschwerde:
  Einem Verbraucher wurde im Zug seine Geldbörse mit Bankkarten und Ausweisen von Taschendieben entwendet. Anschließend erfolgen Verfü-

gungen am Geldautomaten. Der Anbieter erstattet nicht, weil er davon ausgeht, dass die Täter ohne das Wissen seiner Geheimzahl nicht über sein Konto hätten verfügen können. Die Geheimzahl müsse der Verbraucher auf der Karte notiert haben.

BEWERTUNG

In den aufgeführten Konstellationen haben Verbraucher:innen immer wieder Schwierigkeiten, ihre Rechte durchzusetzen. Unabhängig von der Frage der endgültigen Haftung bringen die Anbieter in den genannten Konstellationen das Konto bis zur Klärung der Sachlage in den geschilderten Fällen nicht binnen eines Bankarbeitstages zurück auf den Stand vor der strittigen Verfügung. Das darf aber nur dann unterbleiben, wenn ein Betrugsverdacht gegen die Kontoinhaber selbst besteht. Der Wortlaut der Norm war diesbezüglich mit der zweiten Zahlungsdiensterichtlinie verschärft worden[3]. Das Ausbleiben der Erstattung bedeutet allerdings, dass die Anbieter den Verbraucher:innen grobe Fahrlässigkeit vorwerfen und abwarten, ob diese sich gegen diesen Vorwurf wehren können. Sie selbst legen nicht aktiv dar und beweisen, dass sie wegen einer groben Fahrlässigkeit der Kunden nicht haften.

Was die Frage der endgültigen Haftung betrifft, sehen die Regelungen[4] vor, dass die Kunden selbst nicht gänzlich fehlerfrei gehandelt haben müssen, da sie selbst bei einfach fahrlässigem Verhalten mit einer Haftungsbeschränkung auf 50 Euro geschützt bleiben sollen. Der Gesamtschaden ist nur bei eigenem Betrug und grober Fahrlässigkeit zu tragen. Grobe Fahrlässigkeit bedeutet allgemein einen besonders schweren Verstoß gegen die objektiv erforderliche Sorgfalt, was auch gleichgesetzt wird mit dem Fehlen geringster Vorsicht oder Aufmerksamkeit. Die aktuelle Richtlinie hat dies im Erwägungsgrund 72 bekräftigt. Zwar bleibt die Ausgestaltung danach dem nationalen Recht überlassen, als Anwendungsmaßstab wird aber ein offensichtliches Maß an Nachlässigkeit angeführt. Eine Erhöhung der Beweislast für Verbraucher:innen darf danach ebenso wenig zugelassen werden wie umgekehrt eine Minderung auf Seiten der Anbieter. Es sei demnach „angemessen, dass in bestimmten Situationen und insbesondere dann, wenn das Zahlungsinstrument bei der Verkaufsstelle nicht vorliegt, wie im Falle von Online-Zahlungen, die Beweislast für eine angebliche Fahrlässigkeit beim Zahlungsdienstleister liegt, da die entsprechenden Möglichkeiten des Zahlers in solchen Fällen sehr begrenzt sind[5].“ In der Praxis finden diese Gründe nicht immer hinreichend Anwendung.

Wenn sich Anbieter auf Social Engineering (Phishing) oder den Beweis des ersten Anscheins berufen, haben Verbraucher:innen kaum eine Möglichkeit, dies zu widerlegen – obgleich der Einsatz der korrekten PIN keineswegs immer bedeuten

---

[3] Basierend auf Rechtsprechung zur ersten Fassung der Richtlinie wird oft zusätzlich die Rechtsmeinung vertreten, ein Anspruch auf Rückbuchung bestehe auch dann nicht, wenn Verbraucher:innen die Haftung wegen grober Fahrlässigkeit zu übernehmen haben (vgl. BGH, Urteil vom 17.11.2020 - XI ZR 294/19 unter Verweis dort auf die Artikel 60, 61 der Richtlinie aus 2007).

[4] Vgl. §§ 675u ff. BGB.

[5] Vgl. Richtlinie (EU) 2015/2366 [Fn. 1], Erwägungsgrund 72.

muss, dass die PIN auf den Karten notiert war.[6] Auch die Behauptung, das eigene Onlinebanking und mobile Banking sei sicher, können Verbraucher:innen in der Regel nicht widerlegen, wenn die Anbieter beispielsweise die Herausgabe der entscheidenden Protokolldateien verweigern. Obgleich auch in diesen Fällen bekannt ist, dass Systeme angegriffen werden können.[7] Insbesondere bei den verbreiteten pushTAN-Apps konstatiert das Bundesamt für Sicherheit in der Informationstechnik „deutliche Schwächen bei Leaks des Dienstes und bei Real-Time-Phishing-Angriffen“. Hierbei haben „Verbraucherinnen und Verbraucher […] nicht bei jeder Implementierung eine Möglichkeit, sogenannte Man-in-the-Middle-Angriffe zu erkennen oder sich vor diesen zu schützen“.[8]

[6] Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond: Chip and PIN is Broken, in: Proceedings 2010 IEEE Symposium on Security and Privacy. Los Alamitos/Washington/Tokyo: 2010, S. 433-446.
[7] Vincent Haupert: Sicherheit mobiler Bankgeschäfte zwischen Innovation und Regulierung. Dissertation. Nürnberg: 2019. (abrufbar unter: https://opus4.kobv.de/opus4-fau/frontdoor/index/index/docId/11321)
[8] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html, abgerufen: 06.09.2022.

Kontakt

Verbraucherzentrale
Bundesverband e.V.

Team
Marktbeobachtung Finanzmarkt

Rudi-Dutschke-Straße 17
10969 Berlin

MBFinanzmarkt@vzbv.de

Der Verbraucherzentrale Bundesverband e.V.
ist im Deutschen Lobbyregister registriert.
Sie erreichen den entsprechenden Eintrag hier.