verbraucherzentrale
Bundesverband

DEN ZAHLUNGSVERKEHR SICHERER MACHEN

Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zum Legislativvorschlag der Europäischen Kommission zur Überarbeitung der Zweiten Zahlungsdiensterichtlinie – Payment Services Regulation

28. Juli 2023

Impressum

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

Team Finanzmarkt
finanzen@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

I. ZUSAMMENFASSUNG 3

II. EINLEITUNG 4

III. IM EINZELNEN 5

1. Artikel 43 – Data access management by payment service users 5
2. Artikel 44 – Prohibited obstacles to data access 5
3. Artikel 47 – Specific obligations of and other provisions concerning account information service providers 5
4. Artikel 50 – Discrepancies 6
5. Artikel 51 – Limits and Blocking of the use of the payment instrument 6
6. Artikel 53 – Obligation of the payment service provider in relation to payment instruments 7
7. Artikel 55 – Evidence on authorisation and execution of payment transactions 7
8. Artikel 56 – Payment service provider’s liability for unauthorised payment transcations 8
9. Artikel 59 – Payment service provider’s liability for ‘impersonating bank emplyee fraud’ 8
10. Artikel 80 – Data protection 9
11. Artikel 82 – Fraud reporting 9
12. Artikel 83 – Transaction monitoring and fraud data sharing 9
13. Artikel 84 – Payment fraud risks and trends 9
14. Artikel 88 – Accessibility requirements regarding strong customer authentication 10
15. Artikel 96 ff. – Administrative sanctions 10

I. ZUSAMMENFASSUNG

Die Europäische Kommission hat am 28. Juni 2023 einen Legislativvorschlag für eine künftige Payment Services Regulation (PSR)[1] vorgelegt. Diese sieht eine Reihe von Verbesserungen für Verbraucher:innen vor, die dazu beitragen können, den Zahlungsverkehr sicherer und inklusiver zu machen. Während einige der Maßnahmen in die richtige Richtung weisen, besteht jedoch noch Luft nach oben, um Daten und Ersparnisse der Verbraucher:innen tatsächlich besser zu schützen.

Der vzbv begrüßt unter anderem:

- die verpflichtende Bereitstellung eines Dashboards durch Account Servicing Payment Service Providers (Kreditinstitute), was die Kontrolle über durch Drittdienste abgerufene Datenströme verbessern kann,
- die Einführung eines „IBAN-checks“, der fehlgeleitete Überweisungen verhindern kann,
- klarere Haftungsregeln bei social engineering-Betrug,
- Vorgaben für inklusiv gestaltete starke Kundenauthentifizierung und
- die obligatorische Einführung von Sanktionen durch nationale Aufsichtsbehörden gegenüber Zahlungsdienstleistern.

Der vzbv fordert:

- den Ausbau der Dashboards zur echten Kontrollinstanz inklusive genereller Sperrung und Kündigung von Drittdiensten,
- ein Bonitätsscoring-Verbot für Kontoinformationsdienste,
- die Durchsetzung harter Transaktionslimits zur Betrugsprävention,
- den Ausschluss des Anscheinsbeweises,
- ein Aufrechnungsverbot,
- eine starke Kundenauthentifizierung, die auch wirtschaftlich niemanden ausschließt und
- obligatorische Sanktionen und Entschädigungsleistungen für Zahlungsdienstleister, die ihrer Pflicht zur unverzüglichen Erstattung bei Betrugsfällen nicht nachkommen.

[1] Europäische Kommission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367, 26.07.2023

II. EINLEITUNG

Verbraucher:innen müssen sich darauf verlassen können, dass ihre Zahlungen und Ersparnisse sicher sind, Zahlungsdienstleister ordentlich beaufsichtigt werden und Daten über ihr Zahlungsverhalten vertraulich behandelt werden. Der Zahlungsverkehr ist essenziell für wirtschaftliche Teilhabe und sollte deshalb allen Verbraucher:innen dienen. Im Fokus der Verbraucherberatung, der Rechtsdurchsetzung und der Verbraucherpolitik stehen deshalb seit Inkrafttreten der Zweiten Zahlungsdiensterichtlinie (Revised Payment Services Directive, PSD2) insbesondere die Themen Sicherheit, Betrug und Haftung, sowie finanzielle Inklusion, Kontoinformationsdienste und die behördliche Aufsicht.

Die PSD2 sieht ein Haftungssystem vor, bei dem Verbraucher:innen nur für fehlerhafte Transaktionen haften müssen, wenn sie diese selbst verschuldet haben. Der Gesetzgeber hat somit aus gutem Grund die Last hin zu den Zahlungsdienstleistern verschoben. Die Durchsetzung dieses Grundsatzes findet leider nach Erkenntnissen des Verbraucherzentrale Bundesverbands (vzbv) und der Verbraucherzentralen nur eingeschränkt statt. In der Folge bleiben Verbraucher:innen, entgegen der Regelungsintention, zu oft auf teils existenzbedrohenden Schäden sitzen. Dieses Problem gewinnt durch immer ausgefeiltere Betrugsmethoden („social engineering“) an Brisanz.

Die PSD2 hat die starke Kundenauthentifizierung (Strong Customer Authentication, SCA) für Zahlungen grundsätzlich obligatorisch gemacht. Dies hat einerseits die Sicherheit befördert, andererseits den Zahlungsverkehr verkompliziert. SCA bedeutet im Alltag vieler Menschen erhebliche Hürden, selbstständig am Zahlungsverkehr teilhaben zu können. Der Preis der technologieoffenen Regulierung ist die Benachteiligung all jener Verbrauchergruppen, die digitale Geräte, wie Smartphones, nicht nutzen können oder wollen.

Die PSD2 hat Open Banking reguliert und die neuen Zahlungsdienste, Kontoinformationsdienste und Zahlungsauslösedienste eingeführt. Der Zugriff von Kontoinformationsdiensten auf Zahlungskontodaten hat erhebliche datenschutzrechtliche und damit gesellschaftliche Implikationen. Vorteilen von Multibanking-Apps und ähnlichen Anwendungen stehen die Risiken für Verbraucher:innen gegenüber, die die Preisgabe der vertraulichen Informationen mit sich bringen kann: darunter Betrug (insbesondere social engineering), wirtschaftliche und soziale Nachteile durch Bonitätsscoring und tiefe Eingriffe in die informationelle Selbstbestimmung.

Verbraucher:innen müssen darauf vertrauen können, dass die Zahlungsdienstleister, denen sie Geld und Daten anvertrauen, wirksam beaufsichtigt werden. Letztlich tragen regelmäßig Verbraucher:innen den Schaden bei Defiziten in der grenzüberschreitenden Zusammenarbeit im Binnenmarkt und in der behördenübergreifenden Zusammenarbeit; etwa zwischen Finanzaufsicht und Datenschutzbehörden.

Die Europäische Kommission hat am 28. Juni 2023 einen Legislativvorschlag für eine künftige Payment Services Regulation (PSR) sowie eine neue PSD3[2] vorgelegt. Die

[2] Europäische Kommission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0366, 26.07.2023

aus Verbraucherperspektive relevanten Aspekte werden künftig in der PSR behandelt, auf die sich diese Stellungnahme konzentriert.

Die Stellungnahme bezieht sich auf die vorliegende englische Fassung, weswegen teilweise die englischen Begriffe Verwendung finden.

Der Verbraucherzentrale Bundesverband (vzbv) bedankt sich beim Bundesministerium der Finanzen für die Gelegenheit, zum Legislativvorschlag der Europäischen Kommission zur Überarbeitung der Zweiten Zahlungsdiensterichtlinie Stellung nehmen zu können.

III. IM EINZELNEN

1. ARTIKEL 43 – DATA ACCESS MANAGEMENT BY PAYMENT SERVICE USERS

Der vzbv begrüßt die verpflichtende Bereitstellung eines Dashboards durch ASPSPs gegenüber Zahlungsdienstnutzern. Dieses kann dazu beitragen, dass Verbraucher:innen einen besseren Überblick über erteile Zugriffsberechtigungen erhalten und diese zentral managen können. Dies fördert Kontrolle über die potenziellen Zugriffe auf die persönlichen Zahlungsverkehrstransaktionsdaten.

> Verbraucher:innen sollten unter Absatz 2 die Möglichkeit erhalten, mithilfe des Dashboards von vornherein den Zugriff von Kontoinformationsdiensten und Zahlungsauslösediensten zu sperren.

Davon würden Verbraucher:innen, die diese Drittdienste nicht nutzen wollen und sichergehen wollen, dass niemals ein Zugriff auf ihre Kontodaten erfolgen kann, profitieren. Dadurch könnten Verbraucher:innen sich wirksam gegen versehentlich erteilte Einwilligungen schützen. Die Sperrmöglichkeit würde die Gefahr bannen, dass Verbraucher:innen ohne Kenntnis der Konsequenzen in den Datenzugriff einwilligen.

> Das Dashboard sollte ebenfalls darstellen, wann Payment Service Provider (PSP, Zahlungsdienstleister) auf Kontoinformationen zugegriffen und welche Daten(-kategorien) sie hierbei abgerufen haben.

2. ARTIKEL 44 – PROHIBITED OBSTACLES TO DATA ACCESS

Der Artikel regelt, dass ASPSPs keine Hürden für den Datenzugang gegenüber Drittdienstleistern errichten dürfen.

> Die Norm sollte klarstellen, dass Maßnahmen und Instrumente von ASPSPs in Reaktion auf begründeten Betrugsverdacht und zur Einhaltung der Datenschutzgrundverordnung keine Hindernisse darstellen.

3. ARTIKEL 47 – SPECIFIC OBLIGATIONS OF AND OTHER PROVISIONS CONCERNING ACCOUNT INFORMATION SERVICE PROVIDERS

Kontoinformationsdienste können für Verbraucher:innen nützlich sein, zum Beispiel in Gestalt von Multibanking-Anwendungen. Sie bergen aber auch relevante Risiken. Diese Risiken sind besonders erheblich mit Blick auf Bonitätsscoring durch Wirtschaftsauskunfteien. Hier sind die drohenden negativen Auswirkungen so erheblich, dass der negative gesellschaftliche Effekt möglichen individuellen Nutzen überwiegt. Durch den

Eingang von Kontotransaktionsdaten in Bonitätsscoring müssten Verbraucher:innen rationalerweise bei jedem Zahlvorgang überlegen, wie dieser sich auf ihren Score auswirken könnte und ihre Lebensführung dementsprechend anpassen. Durch diesen Chilling-Effekt droht eine Überwachungsmentalität und Verbraucher:innen könnten davon Abstand nehmen, ihre Grundrechte (insbesondere informationelle Selbstbestimmung und allgemeine Handlungsfreiheit) auszuüben.

Der Einwand, dass zur Datenverarbeitung eine Einwilligung erforderlich sei, verliert an Überzeugungskraft, wenn man bedenkt, dass die Datenpreisgabe zu Bonitätsscoring-Zwecken nicht nur das Individuum betrifft, sondern Auswirkungen auch und gerade auf diejenigen hat, die keine Daten preisgeben. Denn im Umkehrschluss lässt sich ja durchaus schließen, dass diejenigen, die „nichts zu verbergen haben“, deutlich eher den Datenzugriff einräumen werden. Dadurch kann nicht länger von einer freiwilligen, selbstbestimmten Einwilligung ausgegangen werden.

Aus sozialen Gesichtspunkten wird sich der Druck der Datenfreigabe nicht homogen entlang der Bevölkerung verteilen, sondern insbesondere bereits marginalisierte Gruppen treffen.

> Bonitätsscoring durch Wirtschaftsauskunfteien mithilfe von Kontoinformationsdiensten sollte aus diesen Gründen verboten werden.
>
> Davon unberührt bleiben sollte die Pflicht zur Kreditwürdigkeitsprüfung nach § 505a BGB. Es kann im Sinne des Wettbewerbes und des Verbraucherschutzes sein, wenn Kreditinstitute in effizienter Weise, zweckgebunden und dem Datensparsamkeitsprinzip folgend, die saldierten Ein- und Ausgaben zur Kreditwürdigkeitsprüfung heranziehen können

4. ARTIKEL 50 – DISCREPANCIES

Der vzbv begrüßt die verpflichtende Einführung des als „IBAN-Checks“ bekannten Verfahrens auch jenseits von Echtzeitüberweisungen, für welche dies die EU-Kommission bereits vorgeschlagen hat[3]. Es ist zu erwarten, dass dieses Instrument insbesondere zu einem Rückgang von irrtümlichen Überweisungen an einen nicht gewünschten Empfänger beitragen wird.

Gleichzeitig ist zu bedenken, dass Betrüger:innen auch beim „IBAN-Check“ Mittel und Wege finden dürften, die neue Sicherheitsvorkehrung zu umgehen, sodass der Einfluss auf Betrugsinzidenzen weniger Gewiss ist. Somit verlieren die notwendigen Verbesserungen im Haftungssystem durch diese Maßnahmen keinesfalls an Dringlichkeit.

5. ARTIKEL 51 – LIMITS AND BLOCKING OF THE USE OF THE PAYMENT INSTRUMENT

Verschaffen sich Betrüger:innen Zugriff zu einem Bankkonto, ist es ihnen immer wieder möglich, die vorher zur Sicherheit eingerichteten Überweisungslimits kurzfristig zu erhöhen. Der Schutzmechanismus wird somit ausgehöhlt und Verbraucher:innen ein untaugliches Mittel an die Hand gegeben.

---

[3] Europäische Kommission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro, 2023, https://ec.europa.eu/finance/docs/law/221026-proposal-instant-payments_en.pdf, 26.07.2023

> Die Verordnung sollte Instrumente vorsehen, die diese Schwachstelle beheben. Beispielsweise könnte eine verpflichtende Wartefrist vorgesehen werden, nach derer Erhöhungen von Überweisungslimits erst wirksam werden

6. ARTIKEL 53 – OBLIGATION OF THE PAYMENT SERVICE PROVIDER IN RELATION TO PAYMENT INSTRUMENTS

Problematisch für Verbraucher:innen ist es, wenn Zahlungsdienstleister Praktiken anwenden, vor denen sie ihre Kund:innen gleichzeitig warnen. Zu beobachten ist beispielsweise, dass Zahlungsdienstleister per Mail Links auf eigene Portale verschicken oder selber mehrere TANs im Zuge der starken Kundenauthentifizierung abfordern.

> Zahlungsdienstleister sollten dazu verpflichtet werden, solche Praktiken nicht anzuwenden.

Buchstabe c regelt, dass Zahlungsdienstleister, die Zahlungsinstrumente ausgeben, für Verbraucher:innen erreichbar sein müssen. Dies ist heute immer wieder nicht der Fall, wie eine Untersuchung der Marktbeobachtung Finanzmarkt erst kürzlich ergeben hat.

> „Appropriate means“ sollte ausgeführt werden. Zumindest eine Erreichbarkeit 24/7 per Telefon ist erforderlich.

7. ARTIKEL 55 – EVIDENCE ON AUTHORISATION AND EXECUTION OF PAYMENT TRANSACTIONS

Die bisherige Rechtslage bleibt weitestgehend bestehen. Beweisbelastet ist grundsätzlich der Zahlungsdienstleister. Dieser muss, wenn die Autorisierung eines Zahlungsvorgangs streitig ist, den Nachweis führen, dass der Zahlungsvorgang authentifiziert war, ordnungsgemäß aufgezeichnet und verbucht und nicht durch eine technische Panne oder einen anderen Mangel des von dem Zahlungsdienstleister erbrachten Dienstes beeinträchtigt wurde, wobei aus den Unterlagen allein nicht (hier wurde „notwendigerweise“ gestrichen) zu schließen ist, dass der Zahlungsvorgang autorisiert oder der Zahler seine Sorgfaltspflichten verletzt oder vorsätzlich oder grob fahrlässig gegen weitere Pflichten verstoßen hat.

Die Streichung des Einschubs „notwendigerweise“ könnte den Raum für den Anscheinsbeweis verkleinern. Dies wäre aus Verbrauchersicht sehr zu begrüßen. Allerdings fehlt eine dahingehende Klarstellung in den Erwägungsgründen. Ohne klare Anpassung droht die deutsche Rechtsprechung weiter Bestand zu haben, wonach in bestimmten Teilen des zu führenden Beweises dem Zahlungsdienstleister der Beweis des ersten Anscheins zugutekommt.

Dies wäre verbraucherschädlich; denn häufig können Verbraucher:innen vor Gericht den Anschein nicht entkräften, dass die fehlerhafte Autorisierung ihrer Fahrlässigkeit und nicht Fehlern aufseiten des Zahlungsdienstleisters zuzurechnen sei. Diese Beweislastverteilung konterkariert den Zweck des Artikel 72 PSD2 und würde auch den Zweck des Artikel 55 PSR konterkarieren. In der Praxis sind faktisch viel zu häufig Verbraucher:innen in der Beweispflicht und nicht wie intendiert Zahlungsdienstleister.

8. ARTIKEL 56 – PAYMENT SERVICE PROVIDER'S LIABILITY FOR UNAUTHORISED PAYMENT TRANSCATIONS

Der Vorschlag sieht kein Aufrechnungsverbot vor. Zumindest eine Klarstellung, dass dieses gilt, wäre dringend geboten. Denn die deutsche Rechtsprechung hat allerdings noch unter Geltung der PSD 2007 entschieden, dass die Bank dem Anspruch auf sofortige Wiedergutschrift einen Schadensersatzanspruch gegen den Verbraucher entgegensetzen kann, der auf grobe Fahrlässigkeit des Verbrauchers gestützt wird. Eigentlich ist aufgrund der Fassung der PSD2 und der PSR klar, dass der Zahlungsdienstleister nur dann die Wiedergutschrift verweigern kann, wenn der begründete Verdacht auf betrügerisches Handeln besteht. Da diese Praxis dennoch Fortbestand hat, sollte eindeutig formuliert werden, dass die Zahlungsdienstleister dem Erstattungsanspruch nicht einen Schadensersatzanspruch wegen angeblich grober Fahrlässigkeit entgegenhalten dürfen, um so die Erstattung zu vermeiden.

Artikel 56 sollte um folgende Formulierung erweitert werden:

> „Gegen die sich aus diesem Artikel ergebenden Ansprüche des Zahlers ist eine Aufrechnung nicht zulässig."

9. ARTIKEL 59 – PAYMENT SERVICE PROVIDER'S LIABILITY FOR 'IMPERSONATING BANK EMPLYEE FRAUD'

Diese Regelung ist grundsätzlich zu begrüßen, stellt sie doch klar, dass Zahlungsdienstleister bei Spoofing-Angriffen und verwandten social engineering-Angriffen haften müssen, wenn sich der Betrüger als Mitarbeiter des Zahlungsdienstleisters ausgibt.

Ziffer 1 sollte ergänzt werden um die Imitation von Websites oder Apps der Banken. Dies ist relevant, wenn Nutzer über eine Suchmaschine auf Fake-Websites geleitet werden, die jene ihres Zahlungsdienstes imitieren. Dort werden sie zum Beispiel durch eine vorgebliche Identitätsüberprüfung dazu bewogen, ihre Sicherheitsmerkmale einzugeben, während im Hintergrund zeitgleich Zahlungen ausgeführt oder gar Authentifizierungsinstrumente übernommen werden. Zahlungsdienstnutzer müssen sich auch bei solchen Betrugsmaschen auf den Ausgleich ihrer Schäden verlassen können.

Grundsätzlich bleibt die Problematik, dass der Vorwurf der groben Fahrlässigkeit seitens der Zahlungsdienstleister erhoben werden kann. Die Auslegung des unbestimmten Begriffs der groben Fahrlässigkeit liegt bei den nationalen Gerichten, die ihre nationalen Regeln anwenden.

Da das Beweisrecht in der nationalen Zuständigkeit bleibt, wird es auch beim Beweis des ersten Anscheins bleiben.

Deshalb steht zu befürchten, dass die gut gedachte und wohl intendierte neue Regelung in der Praxis folgenlos bleiben könnte, weil Zahlungsdienstleister die bestehenden Lücken ausnutzen können.

> Diese Lücke gilt es zu schließen, indem der Anscheinsbeweis ausgeschlossen wird (vgl. Artikel 55).

10. ARTIKEL 80 – DATA PROTECTION

Dass der effizient und störungsfrei funktionierende Zahlungsverkehr im Binnenmarkt im öffentlichen Interesse ist, steht außer Zweifel. Fraglich ist jedoch, ob diese Einordnung auch für Kontoinformationsdienste zutrifft und dieses vermeintliche Interesse verbraucherschützende Regeln, wie die Pflicht zur Einholung einer ausdrücklichen Einwilligung bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 DSGVO, übertrumpfen können sollte

11. ARTIKEL 82 – FRAUD REPORTING

Es ist essenziell, dass National Competent Authorities (NCAs) und die European Banking Authority (EBA) ein genaues Bild von Betrug im Zahlungsverkehr haben, um ihren Aufsichtsaufgaben wirksam nachkommen zu können.

Auch der öffentliche Diskurs leidet unter einer schlechten Datenlage.

> Zahlungsdienstleister sollten alle Betrugsfälle an die NCAs melden müssen, damit diese schnell und zielgenau die Prozesse nachhalten können.
>
> Daneben sollte ebenfalls eingeben werden müssen, ob die Unternehmen gehaftet haben oder der Zahlungsdienstnutzer den Schaden zu tragen hatte und mit welcher Begründung.
>
> NCAs sollten jährlich aggregierte Statistiken zur Betrugsdaten veröffentlich müssen.

12. ARTIKEL 83 – TRANSACTION MONITORING AND FRAUD DATA SHARING

Der vzbv begrüßt den Ausbau des Transaktionsmonitoring durch Zahlungsdienstleister und hält den Austausch bestimmter Nutzerdaten für den konkreten Zweck der Betrugsprävention für angemessen.

> Zahlungsdienstleister sollten ausnahmslos haften müssen in Betrugsfällen, wenn sie für eine involvierte IBAN bereits eine Warnung erhalten haben.
>
> Der Informationsaustausch sollte darüber hinaus obligatorisch sein, um ein effizientes Transaktionsmonitoring und die Teilnahme gerade derjenigen Zahlungsdienstleister sicherzustellen, bei denen sich Betrugsfälle häufen.

13. ARTIKEL 84 – PAYMENT FRAUD RISKS AND TRENDS

> Zahlungsdienstleister sollten nicht nur ihre Kund:innen informieren, sondern auch gehalten werden, selbst ihre Prozesse auf dem letzten Stand zu halten. Die Anwendung von Praktiken, vor denen Zahlungsdienstleister ihre Kund:innen selber warnen, sollten ausgeschlossen sein.

Dazu gehört unter anderem, keine Links per Mail auf eigene Portale zu verschicken oder nicht mehrere TANs im Zuge der starken Kundenauthentifizierung anzufordern.

14. ARTIKEL 88 – ACCESSIBILITY REQUIREMENTS REGARDING STRONG CUSTOMER AUTHENTICATION

Dass der Vorschlag anerkennt, dass starke Kundenauthentifizierung zum Ausschluss bestimmter Verbrauchergruppen führen kann, ist ein großer Fortschritt. Ihre Gestaltung kann daher nicht völlig technologieoffen und den Anbietern anheimgestellt werden.

Es ist zu begrüßen, dass starke Kundenauthentifizierung nicht alleine von einem Gerätetyp und implizit einem Smartphone abhängen dürfen soll.

> Angesichts des fortlaufenden technischen Fortschritts und um den Regelungszweck nicht zu unterlaufen sollte „Smartphone“ ergänzt werden um „oder ähnliche smarte Geräte“, wie Smartwatches.

Auch heute bieten in Deutschland Kreditinstitute regelmäßig alternative SCA-Verfahren an. Allerdings sind diese für Verbraucher:innen regelmäßig teuer und nicht zuverlässig, weil Institute immer wieder die Verfahren ändern. Durch den notwendigen Kauf dedizierter Geräte entstehen Kontowechselhürden, die den Wettbewerb unterminieren können.

> Der Artikel sollte deshalb dringend um eine Vorgabe ergänzt werden, dass die alternativen Verfahren zu gleichen Entgelten ermöglicht werden müssen.
>
> ASPSPs sollten außerdem den Einsatz interoperabler Geräte ermöglichen müssen, sodass Verbraucher:innen nach Kontowechsel kein neues Gerät erwerben müssen.

15. ARTIKEL 96 FF. – ADMINISTRATIVE SANCTIONS

Der vzbv begrüßt die obligatorische Einführung von Sanktionen gegenüber PSPs, wenn diese gegen Vorgaben der Verordnung verstoßen. Insbesondere Art. 97 Abs. 1 lit. e kann den Anreiz von PSPs erhöhen, Verbraucher:innen bei Betrugsfällen fristgerecht zu entschädigen.

> Es bedarf jedoch einer Präzisierung: Nationale Aufsichtsbehörden sollten nicht nur die Einhaltung der Frist beaufsichtigen, sondern auch, ob PSPs überhaupt ihren Vorgaben nach Artikel 56 ff nachkommen und Verbraucher:innen bei Betrugsfällen entschädigen. Wenn nicht, sollten Aufsichtsbehörden Sanktionen gegenüber PSPs verhängen müssen.
>
> Darüber hinaus sollten Zahlungsdienstleister nach französischem Vorbild zu Entschädigungszahlungen gegenüber ihren Kund:innen verpflichtet werden, wenn sie Erstattungen verspätet geleistet haben.