29. April 2024

EBA-Op/2024/01

EBA-Stellungnahme zu neuen Arten von Betrug im Zahlungsverkehr und möglichen Abhilfemaßnahmen

Kurzfassung

1. Die EBA hat vor kurzem Betrugsdaten für das Jahr 2022 ausgewertet, die Ende 2023 zur Verfügung stehen, und ist dabei zu Erkenntnissen über Betrugsmuster und neue Betrugsarten gelangt, darunter, dass Sofortzahlungen deutlich höhere Betrugsraten aufweisen als herkömmliche Überweisungen und dass ein erheblicher Teil der Betrugsverluste von den Kunden getragen wird, insbesondere bei Überweisungen.

2. In Bezug auf die neuen Betrugsarten stellte die EBA fest, dass die obligatorische Anwendung der starken Kundenauthentifizierung (Strong Customer Authentication, SCA) zwar erfolgreich war, um Betrug zu verhindern, der auf dem Diebstahl von Kundendaten beruht, dass es den Betrügern aber gelungen ist, ihre Techniken anzupassen, so dass komplexere Betrugsarten entstanden sind, die insbesondere auf Social Engineering beruhen.

3. Auf der Grundlage der gewonnenen Erkenntnisse gelangte die EBA zu der Auffassung, dass zusätzlich zu den in den Vorschlägen der EU-Kommission für eine dritte Zahlungsdiensterichtlinie (PSD3) und eine Zahlungsdiensterichtlinie (PSR) sowie der kürzlich verabschiedeten Verordnung über Sofortüberweisungen vorgesehenen Sicherheitsmaßnahmen weitere Maßnahmen erforderlich sind, um dem dynamischen Charakter des beobachteten Betrugs zu begegnen. In der vorliegenden Stellungnahme werden Empfehlungen für solche zusätzlichen Maßnahmen formuliert, die auf den jüngsten Erfahrungen der zuständigen nationalen Behörden (NCAs) mit der Betrugsbekämpfung in ihrem Zuständigkeitsbereich beruhen.

4. Ziel dieser Stellungnahme ist es, einen Beitrag zur weiteren Stärkung des künftigen Rechtsrahmens im Rahmen der PSD3 und der PSR zu leisten, in dem die

Betrugsbekämpfungsvorschriften für Massenzahlungen für mehrere Jahre verankert werden sollen.

Einleitung und Rechtsgrundlage

5. Am 28. Juni 2023 veröffentlichte die Europäische Kommission ihre Vorschläge für eine Überarbeitung der bestehenden Zahlungsdiensterichtlinie (PSD2) in Form einer vorgeschlagenen PSD3 und einer Verordnung über Zahlungsdienste (PSR).

6. Die EBA begrüßt, dass die Vorschläge viele der über 200 Empfehlungen aufgreifen, die die EBA in ihrer Stellungnahme vom Juni 2022[1] an die EU-Kommission gerichtet hatte. Dies gilt insbesondere für die Empfehlungen, die auf eine weitere Verringerung des Betrugs im Zahlungsverkehr und die Verbesserung der Sicherheit von Massenzahlungen abzielen und die ihrerseits auf die Beobachtungen der EBA und der nationalen Wettbewerbsbehörden hinsichtlich der Einhaltung der in der PSD2 festgelegten Anforderungen durch die Zahlungsdienstleister (PSP) zurückgehen.

7. Seit der Veröffentlichung der EBA-Stellungnahme vom Juni 2022 hat die EBA weitere Arbeiten durchgeführt, um neue Betrugstrends und Arten von Betrug im Zahlungsverkehr zu bewerten, wobei sie die neuen Betrugsdaten nutzte, die der EBA und der Europäischen Zentralbank (EZB) Ende 2023 zur Verfügung standen. Diese Analyse wurde durch zusätzliche Datenerhebungen ergänzt, die 2023 mit den nationalen Wettbewerbsbehörden zu bestimmten Datenpunkten durchgeführt wurden, die in den EBA-Leitlinien (GL) zur Betrugsberichterstattung im Rahmen der PSD2[2] nicht verlangt werden, wie z. B. Daten zu Betrug bei Sofortüberweisungen und Betrug im Zusammenhang mit so genannten Post- oder Telefonbestellungen (MOTOs). Darüber hinaus stützt sich die Bewertung neuer Betrugsarten auf Beiträge von Behörden, die für die Beaufsichtigung von Zahlungsdienstleistern zuständig sind, sowie von Behörden, die für die Überwachung von Zahlungssystemen und -instrumenten verantwortlich sind, einschließlich der EZB.

8. Auf der Grundlage dieser Bewertung gelangte die EBA zu der Auffassung, dass insbesondere in Bezug auf die folgenden Punkte relevante Erkenntnisse gewonnen werden können:

    a. Die Auswirkungen der Sicherheitsanforderungen der PSD2 auf das Betrugsniveau in der EU;

    b. Beobachtete neue Betrugstrends und neue Arten von Zahlungsbetrug;

    c. Mögliche zusätzliche Maßnahmen zur Betrugsbekämpfung, die über die von der EU-Kommission in den Vorschlägen zu PSD3 und PSR vorgeschlagenen Maßnahmen zur Betrugsbekämpfung und den Dienst zur Überprüfung des Zahlungsempfängers bei Überweisungen in Euro (auch bekannt als IBAN/Namensprüfung), der in der Verordnung (EU) Nr. 260/2012 (SEPA-Verordnung) durch Art. 1(2) der Verordnung (EU) 2024/886 über Sofortüberweisungen in Euro (die

[1] Stellungnahme der Europäischen Bankenaufsichtsbehörde zu ihrer technischen Beratung über die Überprüfung der Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt (PSD2) - siehe https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2

%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

2 https://www.eba.europa.eu/sites/default/files/documents/10180/2281937/5653b876-90c9-476f-9f44-507f5f3e0a1e/Final%20report%20on%20Guidelines%20on%20fraud%20reporting%20under%20Article%2096%286%29%20PSD2%20%28EBA-GL-2018-05%29.pdf

"Instant Payments Regulation")[3] , die am 19. März 2024 im Amtsblatt der EU veröffentlicht wurde.

9. Diese Erkenntnisse werden im Folgenden unter "Allgemeine Anmerkungen" dargestellt, gefolgt von möglichen zusätzlichen Maßnahmen, die von den EU-Mitgesetzgebern und der Kommission unter "Spezifische Vorschläge" in Betracht gezogen werden sollten.

10. Die im nächsten Abschnitt dieser Stellungnahme enthaltenen Zahlen und Beobachtungen basieren auf ausgewählten Betrugsdaten, die von der EBA und der EZB für das Jahr 2022 im Rahmen der EBA-GL zur Betrugsberichterstattung im Rahmen der PSD2 erhoben wurden, mit Ausnahme der Zahlen zu MOTOs und Sofortzahlungen (in den Absätzen 15 und 17), die auf einer separaten Erhebung beruhen, die von der EBA über die nationalen Wettbewerbsbehörden und die nationalen Zentralbanken im Jahr 2023 durchgeführt wurde, wobei das erste Halbjahr 2022 als Bezugszeitraum diente.

11. Die Zuständigkeit der EBA zur Abgabe dieser Stellungnahme beruht auf Art. 1(5) und Art. 16a Absatz 1 der Verordnung (EU) Nr. 1093/2010 als Teil des Ziels der EBA, "zur Verbesserung des Kundenschutzes beizutragen" und "eine aktive Rolle beim Aufbau einer gemeinsamen Aufsichtskultur in der Union und kohärenter Aufsichtspraktiken sowie bei der Gewährleistung einheitlicher Verfahren und kohärenter Ansätze in der gesamten Union zu spielen".

[3] Verordnung (EU) 2024/886 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Änderung der

Verordnungen (EU) Nr. 260/2012 und (EU) 2021/1230 sowie der Richtlinien 98/26/EG und (EU) 2015/2366 in Bezug auf Sofortüberweisungen in Euro

Allgemeine Bemerkungen

Auswirkungen der Sicherheitsanforderungen der PSD2 auf das Betrugsniveau in der EU

12. Auf der Grundlage der Auswertung der im Rahmen der PSD2 gesammelten Daten zum Betrug im Zahlungsverkehr hat die EBA festgestellt, dass die SCA, ergänzt durch die Überwachung von Transaktionen sowie die anderen Sicherheitsmaßnahmen, die durch die PSD2 und die technischen Regulierungsstandards der EBA für eine starke Kundenauthentifizierung und gemeinsame und sichere offene Kommunikationsstandards im Rahmen der PSD2 (die RTS)[4] vorgeschrieben sind, den Betrug insgesamt erfolgreich eingedämmt hat.

13. So wurde beispielsweise die Betrugsquote bei Überweisungen auf 0,0008 % des Gesamtwerts (d. h. 8 Euro von 1 Million Euro) und bei Lastschriften auf 0,0020 % im Jahr 2022 begrenzt. Bei Kartenzahlungen ist die absolute Betrugsrate zwar höher, d. h. 0,029 % des Wertes (nach den vom Zahlungsverkehrsdienstleister des Zahlers gemeldeten Daten), aber die durchschnittliche betrügerische Transaktion beschränkt sich auf 80 €, während der entsprechende Wert bei Überweisungen 2 252 € beträgt. Bereits 2020-2021, in der Zeit der Umstellung auf SCA, hatte die EBA einen Rückgang der durchschnittlichen Betrugsrate zwischen 40 und 60 % allein bei Kartenzahlungen beobachtet[5] . In ähnlicher Weise zeigen die im Mai 2023 veröffentlichten Kartenbetrugsstatistiken der EZB[6] , dass die Einführung von SCA durch Zahlungsdienstleister und Händler im Jahr 2021 mit einem deutlichen Rückgang des Betrugs bei Kartenfernzahlungen einherging.

14. Parallel dazu stellt die EBA fest, dass SCA inzwischen in großem Umfang für die Authentifizierung elektronischer Ferntransaktionen, einschließlich solcher im elektronischen Geschäftsverkehr, verwendet wird. Zwar wurden in den RTS mehrere Ausnahmen von der Verwendung der SCA vorgesehen, um benutzerfreundliche und innovative Zahlungsmittel zu unterstützen und gleichzeitig die Sicherheit der Gelder und personenbezogenen Daten der Kunden zu gewährleisten, doch wurde die SCA im Jahr 2022 bei 70 % der Fernüberweisungen und 36 % der Fernkartentransaktionen (nach Angaben des Zahlungsverkehrsdienstleisters des Auftraggebers) angewandt, was einem Prozentsatz des Gesamtwerts von 77 % bzw. 55 % entspricht. Dementsprechend wurden die in den RTS vorgesehenen Ausnahmen von der SCA bei diesen beiden Zahlungsinstrumenten im Allgemeinen nur in begrenztem Umfang in Anspruch genommen. Insbesondere wurden SCA-Ausnahmen für 32 % der Fernkartentransaktionen genutzt.

15. Die EBA hat auch festgestellt, dass Zahlungsverkehrsdienstleister ein hohes Volumen nicht SCA-authentifizierter Transaktionen als "merchant-initiated transactions" (MITs)[7] gemeldet haben, was 13,1 % aller kartengestützten Fernzahlungen in der EU entspricht (wie vom Zahlungsverkehrsdienstleister des Zahlers gemeldet). Ähnlich verhält es sich mit Zahlungsvorgängen per Post- oder Telefonbestellung (so genannte MOTO-Transaktionen), die nicht in den Anwendungsbereich des SCA fallen

4Delegierte Verordnung (EU) 2018/389 der Kommission - https://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CELEX:32018R0389

5Siehe EBA-Bericht über die Angaben der Zahlungsdienstleister zu ihrer Bereitschaft, eine starke Kundenauthentifizierung für e-
kartengestützte Zahlungstransaktionen im Handel (https://www.eba.europa.eu/publications-and-media/press-releases/eba- publishes-report-data-provided-psps-their-readiness-apply)

[6] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.de.html

[7] MITs umfassen kartengestützte Zahlungen, die von einem Zahlungsempfänger ohne jegliche Interaktion oder Beteiligung des Zahlers auf der Grundlage einer Vereinbarung zwischen dem Zahler und dem Zahlungsempfänger initiiert werden, in der der Zahler den Zahlungsempfänger zur Initiierung dieser Transaktionen ermächtigt. Die EBA-Leitlinien zur Meldung von Betrugsdelikten im Rahmen der PSD2 sehen vor, dass eine Transaktion als MIT und damit als vom Zahlungsempfänger initiiert gilt und nicht unter die Anforderung von Art. 97 PSD2 zur Anwendung von SCA unterliegt, die von der EU-Kommission in den Q&As 2018 4131 und 2018 4031 genannten Bedingungen erfüllen muss.

Anforderung, waren auch vom Volumen her signifikant. Sowohl die MIT- als auch die MOTO-Transaktionen wiesen im ersten Halbjahr 2022 deutlich höhere Betrugsraten auf (d. h. mehr als 0,1 % des Wertes oder mehr als 1 Euro von 1000 übermittelten Euro), und zwar sowohl in Bezug auf Transaktionen mit SCA-Authentifizierung als auch auf Transaktionen, die von SCA ausgenommen sind.

Aufkommende Betrugstrends und neue Betrugsarten

16. Trotz der positiven Auswirkungen der SCA auf die Betrugsbekämpfung (siehe Ziffer 13) hat die EBA bei bestimmten Zahlungsinstrumenten, geografischen Dimensionen, Rechtsordnungen oder Kombinationen davon hohe Betrugsquoten festgestellt.

17. Die erste ist die Sofortüberweisung, auch Sofortzahlung genannt, für die die von 18 nationalen Wettbewerbsbehörden für das erste Halbjahr 2022 gemeldeten Daten zeigen, dass die wertmäßigen Betrugsraten nicht nur erhebliche Unterschiede zwischen den Mitgliedstaaten (MS) aufweisen, sondern im Durchschnitt etwa zehnmal höher sind als bei herkömmlichen Überweisungen.

18. Die EBA ist der Ansicht, dass es noch zu früh ist, um die Ursachen für diese Feststellungen eindeutig zu ermitteln, und dass die jüngsten Beobachtungen in einigen Mitgliedstaaten berücksichtigt werden müssen, dass Sofortzahlungen von Unternehmen weniger genutzt werden als herkömmliche Überweisungen. Dennoch ist die EBA der Ansicht, dass die erwähnte höhere Betrugsrate bei Sofortzahlungen zum Teil darauf zurückzuführen sein könnte, dass die Zahlungsdienstleister im Falle betrügerischer Sofortzahlungen nur begrenzte oder gar keine Möglichkeiten haben, Gelder zurückzufordern, da diese Zahlungen in weniger als 10 Sekunden ausgeführt werden - was Sofortzahlungen für Betrüger attraktiver machen könnte. Diese Feststellung könnte auch mit den technischen Einschränkungen zusammenhängen, die mit der Anwendung der Transaktionsüberwachung auf Sofortzahlungen und der anschließenden Behandlung verdächtiger Transaktionen durch die Zahlungsdienstleister verbunden sind. Die obigen Ausführungen machen deutlich, dass bei Sofortüberweisungen angemessene Sicherheitsvorkehrungen getroffen werden müssen, um das Betrugsrisiko zu mindern, zumal mit der Anwendung der Verordnung über Sofortüberweisungen zu erwarten ist, dass Sofortüberweisungen von den Kunden in der EU zunehmend genutzt werden.

19. Zweitens stellte die EBA fest, dass die Betrugsraten bei grenzüberschreitenden Transaktionen viel höher sind als bei inländischen Transaktionen (d. h. Transaktionen, bei denen der Zahlungsverkehrsdienstleister des Zahlers und der Zahlungsverkehrsdienstleister des Zahlungsempfängers im selben Mitgliedstaat ansässig sind), und zwar bei allen Zahlungsinstrumenten, die in den Melderahmen für Betrugsfälle im Zahlungsverkehr gemäß der PSD2 einbezogen sind. Dies gilt sowohl für grenzüberschreitende Transaktionen zwischen Ländern des Europäischen Wirtschaftsraums (EWR) als auch für grenzüberschreitende Transaktionen zwischen einem EWR-Land und einem Land außerhalb des EWR. Die von der EBA durchgeführte Analyse der aggregierten Daten auf EWR-Ebene für das Jahr 2022 deutet beispielsweise darauf hin, dass die Betrugsraten bei grenzüberschreitenden Transaktionen

sowohl bei Karten als auch bei Überweisungen gemessen am Volumen etwa neunmal höher sind als bei inländischen Transaktionen. Die Beobachtungen der nationalen Wettbewerbsbehörden und die von den Marktteilnehmern geäußerten Ansichten deuten darauf hin, dass dies in erster Linie auf eine unzureichende grenzüberschreitende Zusammenarbeit zwischen Zahlungsdienstleistern und anderen beteiligten Akteuren bei der Bekämpfung internationaler krimineller Aktivitäten sowie bei grenzüberschreitenden Transaktionen mit Beteiligung von Ländern außerhalb des EWR (Ein-Leg-Transaktionen) auf die uneinheitliche Anwendung der SCA zurückzuführen sein könnte.

20. Drittens: In der Praxis ist die Verteilung der Haftung für Betrugsverluste im EWR zwischen dem Zahlungsdienstnutzer (PSU) einerseits und dem Zahlungsdienstleister oder anderen Stellen andererseits je nach Zahlungsinstrument sehr unterschiedlich. Während beispielsweise im Jahr 2022 bei Kartenzahlungen die Verluste zu etwa gleichen Teilen zwischen Zahlungsdienstleistern und Zahlungsverkehrsdienstleistern sowie anderen Stellen aufgeteilt werden, liegt der Anteil der vom Zahlungsdienstleister getragenen Verluste bei Überweisungen bei 79 %, was in absoluten Zahlen 1,2 Mrd. EUR entspricht. Der Anteil der von den Zahlungsdienstleistern getragenen Verluste variiert auch innerhalb des EWR erheblich.

21. Dieser Befund könnte zum Teil dadurch erklärt werden, dass eine zunehmende Zahl von Zahlungsbetrügereien die Form der Manipulation des Zahlers annimmt, oder den sogenannten "Authorized Push Payment"-Betrug, bei dem der Zahler dazu gebracht wird, eine Zahlung an den Betrüger zu leisten. Darüber hinaus kann nach Ansicht der EBA das Fehlen einer klaren Abgrenzung zwischen autorisierten und nicht autorisierten Transaktionen in der PSD2, was zu einer unterschiedlichen Anwendung der einschlägigen Haftungsregeln in den Mitgliedstaaten führt, und die weite Auslegung des Begriffs "grobe Fahrlässigkeit" in einigen Mitgliedstaaten teilweise erklären, warum ein großer Prozentsatz der Verluste bei betrügerischen Überweisungen vom Zahlungsdienstleister getragen wird. In diesem Zusammenhang beobachtete die EBA die in einigen Mitgliedstaaten übliche Praxis von Zahlungsdienstleistern, alle SCA-authentifizierten Transaktionen als autorisiert zu betrachten, selbst im Falle von Social-Engineering-Betrug, und die Erstattung an Kunden in solchen Fällen zu verweigern, da sie der Ansicht sind, dass die Haftungsbeschränkung des Zahlers in Art. 74 PSD2 in solchen Fällen nicht gilt.

22. Darüber hinaus stellte die EBA fest, dass die Betrugsraten in den einzelnen EWR-Ländern bei allen betrachteten Zahlungsinstrumenten erheblich variieren, wobei in einigen Mitgliedstaaten die Gesamtbetrugsraten weit über dem EWR-Durchschnitt liegen. So liegen beispielsweise die Betrugsraten bei Überweisungen im Jahr 2022 in einigen Mitgliedstaaten um das Zehnfache oder mehr über den entsprechenden Zahlen für den gesamten EWR. Auch wenn es mehrere Gründe für diese Unterschiede zwischen den Mitgliedstaaten geben kann, darunter Unterschiede bei den von den Zahlungsdienstleistern in den verschiedenen Märkten angebotenen Zahlungsdiensten sowie die digitalen Fähigkeiten der Bürger in den einzelnen Mitgliedstaaten, ist die EBA der Ansicht, dass dieses Muster auch mit der unterschiedlichen Umsetzung der Sicherheitsanforderungen durch die Zahlungsdienstleister und den unterschiedlichen Aufsichtspraktiken in den Mitgliedstaaten zusammenhängen könnte.

23. Was die neuen Betrugsarten angeht, so hat die EBA festgestellt, dass die Betrüger - was nicht überrascht - damit begonnen haben, ihre Techniken an den veränderten technologischen und rechtlichen Kontext anzupassen. Während die SCA erfolgreich Betrugsarten verhindern konnte, die auf dem Diebstahl von Kundendaten beruhen, sind in den letzten Jahren neue, komplexere Betrugsarten aufgetaucht oder haben sich weiter verbreitet. Diese können in die folgenden drei Kategorien eingeteilt werden:

    A. Manipulation des Zahlers. Bei dieser Art von Betrug wird der Kunde von einem Betrüger manipuliert, damit er durch Social Engineering eine Zahlung an den Betrüger

leistet. Diese Betrugstechniken sind wohl weitgehend unabhängig von den technischen Sicherheitsmaßnahmen der Zahlungsdienstleister und stützen sich in der Regel auf Informationen über den Kunden, die z. B. über soziale Netzwerke gesammelt wurden, wobei häufig die Identität einer bekannten und vertrauenswürdigen Person wie eines Verwandten, eines Freundes, eines Geschäftspartners, der Steuerbehörden oder des Zahlungsdienstleisters selbst vorgetäuscht wird. Ein typisches Beispiel für diese Art von Betrug im Unternehmensbereich ist der so genannte "CEO-Betrug",
d.h. ein Betrug, der per Telefon oder Post von einem Betrüger durchgeführt wird, der sich als ein hochrangiger

Geschäftsführer oder leitender Angestellter, der einen Angestellten dazu bringt, eine Zahlung, häufig in Höhe eines hohen Betrags, zu veranlassen und zu genehmigen.

B. Gemischter Social Engineering- und technischer Betrug. Bei dieser Betrugsart kombinieren die Betrüger Phishing-Techniken (einschließlich Vishing und Smishing[8]), mit denen sie die persönlichen Sicherheitsdaten der Kunden stehlen, um Kontoinformationen zu sammeln und Zahlungsaufträge zu erteilen, mit Social Engineering, das darauf abzielt, die Zahlungsdienstleister zu manipulieren, damit sie die erteilten Zahlungsaufträge autorisieren. Auch wenn das Ausgeben der Identität z. B. eines Mitarbeiters eines Zahlungsdienstleisters oft Teil des Betrugs ist, unterscheidet er sich von der oben genannten Kategorie dadurch, dass die Betrüger einige Vorgänge direkt auf dem Konto des Opfers durchführen. Aus den von den nationalen Wettbewerbsbehörden gemeldeten und von der EBA bewerteten Betrugsfällen ging hervor, dass Zahlungsdienstleister bei der Meldung dieser Betrugsart gemäß der EBA-Leitlinien für die Meldung von Betrugsfällen im Rahmen der PSD2 diese häufig als "Manipulation des Zahlers" einstufen und die Transaktion als autorisiert betrachten, selbst wenn der Zahlungsauftrag von dem Betrüger erteilt wurde.

C. Kompromittierung des Anmeldevorgangs. Bei dieser Betrugsart handelt es sich um einen komplexen Betrug, der darauf abzielt, die Geräte des Betrügers als zweiten Faktor der SCA anzumelden, um sie zusammen mit den persönlichen Sicherheitsdaten des Kunden zu verwenden, die der Betrüger durch Phishing/Smishing/Vishing-Techniken gestohlen hat. Bei diesen Betrügereien, bei denen häufig spezifische Schwachstellen der Anmeldeverfahren ausgenutzt werden, besteht das Ziel des Betrügers darin, das Zahlungskonto vollständig zu übernehmen und so mehrere betrügerische Zahlungen zu ermöglichen.

[8] Während sich Phishing auf einen per E-Mail verübten Betrug bezieht, greifen die Betrüger beim Smishing auf SMS oder Sofortnachrichten zurück, und Vishing erfolgt über einen Telefonanruf. Andere von Betrügern eingesetzte Techniken umfassen gefälschte Anzeigen, die über gängige Suchmaschinen verbreitet werden und die Opfer auf gefälschte Websites führen, die die einer vertrauenswürdigen Einrichtung (z. B. einer Bank) nachahmen.

Spezifische Vorschläge

24. Die EBA begrüßt die neuen Sicherheitsbestimmungen, die in den PSD3/PSR-Vorschlägen der EU-Kommission und in der Verordnung über Sofortüberweisungen enthalten sind. Insbesondere begrüßt die EBA die mit der Verordnung über Sofortüberweisungen eingeführte obligatorische IBAN/Namen-Prüfung, vor allem, da sie auch für grenzüberschreitende Transaktionen gilt, sowie andere zusätzliche Maßnahmen zur Betrugsbekämpfung, die die EU-Kommission im PSR-Vorschlag vorschlägt - einschließlich einer verbesserten Transaktionsüberwachung, der Unterstützung des Austauschs betrugsbezogener Informationen zwischen Zahlungsdienstleistern und der Verpflichtung für Zahlungsdienstleister, Aufklärungsinitiativen durchzuführen, um Kunden und Mitarbeiter für Zahlungsbetrug zu sensibilisieren. All diese Maßnahmen können nützlich sein, um insbesondere den Betrug durch Manipulation des Zahlers und andere Betrügereien, die auf Nachahmung beruhen, einzudämmen. Darüber hinaus stellt die EBA fest, dass in einem Bericht des Wirtschafts- und Währungsausschusses des Europäischen Parlaments (ECON) zu den PSD3/PSR-Vorschlägen zusätzliche Bestimmungen zur Betrugsbekämpfung vorgeschlagen und vom Europäischen Parlament in einer Abstimmung im April 2024 angenommen wurden. Diese zielen beispielsweise darauf ab, Anbieter von elektronischen Kommunikationsdiensten außerhalb des Finanzsektors - z. B. Telekommunikations- und Internetanbieter, Social-Media-Unternehmen - ebenfalls für die Bekämpfung von Zahlungsbetrug verantwortlich zu machen.

25. Die EBA stellt jedoch auch fest, dass neun Monate nach Inkrafttreten der Verordnung über sofortige Zahlungen alle Zahlungsdienstleister im Euroraum verpflichtet sein werden, sofortige Zahlungen zu akzeptieren, aber nur ein Teil von ihnen die IBAN-/Namensprüfung unterstützen wird. Generell könnte die in der Verordnung über sofortige Zahlungen vorgesehene schrittweise Anwendung der IBAN-/Namensprüfung in den EWR-Ländern unter Berücksichtigung der in den Ziffern 17-18 genannten Aspekte in Bezug auf Betrug bei sofortigen Zahlungen zu einem Anstieg des Betrugsniveaus in dieser Zwischenzeit führen, sofern keine geeigneten Sicherheitsvorkehrungen getroffen werden.

26. In Anbetracht der beobachteten Dynamik von Betrug und der Fähigkeit von Betrügern, sich an neue Anforderungen zur Betrugsbekämpfung anzupassen, ist die EBA der Ansicht, dass zusätzliche Sicherheitsmaßnahmen - wie nachstehend beschrieben - in Betracht gezogen werden könnten, um einen umfassenden, einheitlichen und zukunftssicheren Rahmen für die Eindämmung und Kontrolle von Betrug im Zahlungsverkehr in der EU zu schaffen.

27. Auf der Grundlage der im vorangegangenen Abschnitt zusammengefassten Analyse und einer Bewertung relevanter Maßnahmen zur Betrugsbekämpfung, die nach Angaben einiger nationaler Aufsichtsbehörden in ihren Ländern bereits angewandt werden, hat die EBA die folgenden zusätzlichen Maßnahmen identifiziert, die von den EU-Mitgesetzgebern und der EU-Kommission bei der Verhandlung der PSD3/PSR-Vorschläge berücksichtigt werden sollten:

    1. Verschärfte Sicherheitsanforderungen für Zahlungsverkehrsdienstleister, die die Überprüfung von IBAN/Namen und die in den PSD3/PSR-Vorschlägen enthaltenen Maßnahmen zur Betrugsbekämpfung ergänzen und darauf abzielen, das Verfahren

zur Authentifizierung von Transaktionen weiter zu stärken, mögliche Schwachstellen, die in anderen Phasen des Zahlungsprozesses ausgenutzt werden, zu verringern sowie die Aufdeckung und Untersuchung von Betrug zu unterstützen;

2. Ein Rahmen für das Betrugsrisikomanagement, der von den Zahlungsdienstleistern zusätzlich zu den obligatorischen Sicherheitsanforderungen eingeführt werden muss;

3. Geänderte Haftungsregeln, einschließlich einer korrekten Abgrenzung zwischen genehmigten und nicht genehmigten Transaktionen sowie der Klärung des Begriffs der "groben Fahrlässigkeit";

4. Eine verstärkte und harmonisierte Aufsicht über das Betrugsmanagement, die auch die bereits im Rahmen der PSD2 erhobenen Betrugsdaten nutzt;

5. Angemessene Sicherheitsanforderungen für eine einzige EU-weite Plattform für den Informationsaustausch zur Verhinderung und Aufdeckung potenziell betrügerischer Zahlungsvorgänge.

28. Die fünf oben vorgeschlagenen Maßnahmen werden in den folgenden Unterabschnitten ausführlicher erläutert.

Verschärfte Sicherheitsanforderungen für PSPs

29. Die EBA ist zu der Auffassung gelangt, dass in Anbetracht der neuen und komplexeren Betrugsarten, die sich abzeichnen, ein breiteres Spektrum von Sicherheitsanforderungen für die Bereitstellung elektronischer Zahlungen erforderlich ist. In diesem Zusammenhang schlägt die EBA die folgenden Bestimmungen vor, die von den EU-Mitgesetzgebern und der EU-Kommission bei der Diskussion der PSD3/PSR-Vorschläge berücksichtigt werden sollten.

a) In Bezug auf den Zugang zu einem Zahlungskonto und die Erteilung von Zahlungsvorgängen/-aufträgen:

i. Änderung von Art. 85(12) im PSR-Vorschlag, um klarzustellen, dass die beiden SCA-Faktoren mindestens zwei verschiedenen Kategorien angehören sollten, um die positiven Auswirkungen der SCA auf die Betrugsbekämpfung nicht zu gefährden;

ii. Eine Verpflichtung für Zahlungsverkehrsdienstleister, den Zahlungsdienstnutzern die Möglichkeit zu bieten, tägliche oder pro Zahlung geltende Obergrenzen festzulegen, die unter oder über den vom Zahlungsverkehrsdienstleister für jedes Zahlungsinstrument festgelegten Standardwerten liegen, wobei eine angemessene Frist für das Inkrafttreten einer sich daraus ergebenden Erhöhung der Ausgabenobergrenzen vorzusehen ist, aber auch dem Geist von Erwägungsgrund 19 der Verordnung über Sofortzahlungen Rechnung zu tragen ist.

b) In Bezug auf die Transaktionsüberwachung (TM):

i. Eine Anforderung, dass TM vor der Ausführung der Transaktion durchgeführt werden muss
- d.h. für Sofortzahlungen und andere Zahlungen, die schnell und in Echtzeit abgewickelt werden;

ii. Eine Klarstellung, dass TM auf alle elektronischen Zahlungskanäle angewandt werden sollte, über die ein bestimmtes Zahlungsinstrument von dem Zahlungsdienstleister genutzt wird, u. a. über Geldautomaten und an

Verkaufsstellen (PoS), so dass der Zahlungsdienstleister verpflichtet werden kann, die für dieses Zahlungsinstrument verarbeiteten Transaktionen ganzheitlich zu betrachten;

iii. Die Anforderung, das vom Zahlungsverkehrsdienstleister des Zahlers durchgeführte TM durch das Screening der eingegangenen Zahlungsvorgänge durch den Zahlungsverkehrsdienstleister des Zahlungsempfängers zu ergänzen, um verdächtige Betrugsmuster aufzuspüren, die sich unter anderem auf den Betrag, die Herkunft und die Häufigkeit dieser Vorgänge in Bezug auf das Profil des Kontoinhabers sowie auf eine mögliche Abweichung des Namens des Zahlungsempfängers bei Vorgängen gegen den Namen des Zahlungsempfängers stützen

im Besitz des Zahlungsverkehrsdienstleisters des Zahlungsempfängers. Diese Maßnahme wird in der Tat als wichtig erachtet, um die gründliche Überwachung durch die Zahlungsverkehrsdienstleister zur Betrugsbekämpfung zu unterstützen.

iv. Eine Verpflichtung für alle Zahlungsverkehrsdienstleister, betrugsbezogene Informationen untereinander auszutauschen, um den TM zu verbessern. In diesem Zusammenhang könnten die Bestimmungen in Art. 83 der PSR weiter gestärkt werden, indem alle Zahlungsverkehrsdienstleister verpflichtet werden, betrugsbezogene Daten auszutauschen, die sich nicht nur auf eindeutige Kennungen/IBANs des Zahlungsempfängers beschränken, sondern auch Aspekte wie andere Identifizierungselemente von Personen, die im Verdacht stehen, Betrüger zu sein (einschließlich Namen, IP-Adressen und verwendete Telefonnummern), sowie Informationen über den *Modus Operandi der* Betrüger umfassen;

v. Eine Klarstellung, dass ein Zahlungsverkehrsdienstleister, der auf der Grundlage des TM feststellt, dass eine Sofortzahlung mit einem hohen Risiko behaftet ist, die Ausführung der Transaktion verweigern kann, wobei er den Zahlungsverkehrsdienstleister ordnungsgemäß zu benachrichtigen hat, einschließlich des Grundes für die Verweigerung und der Angabe der verfügbaren Optionen zur erneuten Erteilung des Zahlungsauftrags. Bei anderen Arten von Zahlungen sollte der Zahlungsverkehrsdienstleister, wenn das TM darauf hinweist, dass die Transaktion mit einem hohen Risiko behaftet ist, eine Untersuchung durchführen, an der auch der Gegenzahlungsverkehrsdienstleister beteiligt ist, und kann als Ergebnis dieser Untersuchung die Transaktion sperren. Die Einzelheiten hierzu können in die Stufe-2-Rechtsvorschriften aufgenommen werden.

c) Was das Verfahren für die Registrierung eines Kundengeräts als zweiten Faktor des SCA betrifft:

i. Sicherstellung einer angemessenen Zeitspanne ab dem Antrag des PSU, bevor das neue Kundengerät tatsächlich registriert wird;

ii. Im Falle der Registrierung eines weiteren Kundengeräts müssen die Zahlungsdienstleister rechtzeitig eine Warnmeldung an das bereits registrierte persönliche Gerät des Zahlungsdienstleisters senden.

d) Die Zahlungsverkehrsdienstleister müssen ihren Kunden Hilfestellung bei allen Sicherheitsaspekten des Dienstes und bei der Meldung von Anomalien und Betrugsverdacht leisten, einschließlich der Möglichkeit, dass sich das Zahlungsdienstleistungsunternehmen umgehend an geschultes Personal wendet und dass der betreffende Fall vom Zahlungsverkehrsdienstleister bei Bedarf zeitnah weiterverfolgt wird. Dieser Dienst sollte mindestens die Betriebszeiten des betreffenden Zahlungsdienstes abdecken (d. h. die Zeitspanne, in der der Zahlungsdienst dem Zahlungsdienstleister zur Verfügung steht). Dies gilt unbeschadet der Verpflichtung der Zahlungsdienstleister gemäß Art. 70(1)(c) der PSD2.

Ein von den Zahlungsdienstleistern einzurichtender Rahmen für das Betrugsrisikomanagement

30. Darüber hinaus rät die EBA den EU-Ko-Gesetzgebern und der Kommission, Anforderungen für einen Rahmen für das Betrugsrisikomanagement festzulegen, der von den Zahlungsdienstleistern als Teil des bestehenden umfassenderen Rahmens für Risikomanagementstrategien im Rahmen der PSD2 und der Verordnung (EU) 2022/2554 über die digitale operationelle Widerstandsfähigkeit des Finanzsektors (DORA) im Einklang mit dem Grundsatz der Verhältnismäßigkeit einzuführen ist. Ein solcher Rahmen könnte eine regelmäßige Bewertung des Betrugsrisikos vorsehen, die sich unter anderem auf die im Rahmen des PSR erhobenen Betrugsdaten stützt und Folgendes umfasst:

    a) Eine Erklärung der Zahlungsdienstleister zum Betrugsrisiko, in der die Ziele der Betrugsbekämpfung dargelegt werden und die regelmäßig zu überprüfen ist;

b) eine regelmäßige Überwachung des eigenen Betrugsniveaus durch die Zahlungsverkehrsdienstleister, sowohl auf der Seite der Zahlungsverkehrsdienstleister des Auftraggebers als auch auf der Seite der Zahlungsverkehrsdienstleister des Begünstigten.

c) die regelmäßige Aktualisierung der Sicherheitsmaßnahmen zur Minderung des Betrugsrisikos auf der Grundlage der aufgedeckten Betrugsquote und der Bewertung des jeweiligen Risikos.

Geänderte Haftungsregeln

31. Die EBA rät den EU-Mitgesetzgebern und der EU-Kommission, die Haftungsregeln im PSR-Vorschlag klarzustellen, und zwar insbesondere:

a) Klärung der Abgrenzung zwischen genehmigten und nicht genehmigten Transaktionen im Falle von Streitigkeiten über einen Betrugsverdacht zwischen dem PSU und dem PSP. Insbesondere könnten die folgenden Maßnahmen in Betracht gezogen werden:

i. in den PSR zu präzisieren, dass in Fällen, in denen ein Zahler bestreitet, einen Zahlungsvorgang autorisiert zu haben, die Verwendung der SCA allein nicht ausreichen sollte, um zu beweisen, dass der Zahlungsvorgang vom Zahler autorisiert wurde oder dass der Zahler in betrügerischer Absicht gehandelt hat;

ii. zu präzisieren, dass bei vom Zahler veranlassten Transaktionen (z. B. Überweisungen) eine vom Zahler verweigerte Transaktion nicht als autorisiert angesehen werden kann, wenn der Zahlungsauftrag von einem Betrüger veranlasst wurde, selbst wenn er anschließend vom Zahlungsdienstleister authentifiziert wurde;

iii. klarzustellen, dass unbeschadet von Art. 5 Buchstabe c Nummer 8 der Verordnung über Sofortüberweisungen eine vom Zahler verweigerte Transaktion nicht als autorisiert angesehen werden kann, wenn der Zahler nicht über eine Diskrepanz zwischen der IBAN und dem Namen des Begünstigten informiert wurde, z. B. weil der Betrüger die Mitteilung des Zahlungsdienstleisters des Zahlers gemäß Artikel 5 Buchstabe c Nummer 1 der Verordnung abgefangen hat. 5(c)(1) der genannten Verordnung.

b) Klärung des Begriffs der groben Fahrlässigkeit. In diesem Zusammenhang könnten die folgenden Maßnahmen in Betracht gezogen werden:

i. in den Erwägungsgründen der PSR klarzustellen, dass in Fällen, in denen ein Zahlungsdienstleister Opfer eines Social-Engineering-Betrugs wird, bei der Beurteilung, ob der Zahlungsdienstleister grob fahrlässig gehandelt hat, alle relevanten Faktoren berücksichtigt werden sollten, einschließlich, aber nicht beschränkt auf die Komplexität des Betrugs, die persönlichen Umstände des Zahlungsdienstleisters, die Frage, ob dieser berechtigte Gründe für die Annahme hatte, dass der Zahlungsdienstleister eine Zahlung an einen rechtmäßigen Zahlungsempfänger leistet, und die Frage, ob der Zahlungsdienstleister zusätzliche Schritte hätte unternehmen können, um den Betrug zu verhindern.

ii. in die Erwägungsgründe der PSR eine nicht erschöpfende Liste von Umständen aufzunehmen, die bei der Beurteilung der groben Fahrlässigkeit berücksichtigt werden könnten, wie z. B:

- das PSU eine Zahlung an einen Betrüger getätigt hat, ohne dass es hinreichende Gründe für die Annahme gab, dass der Zahlungsempfänger, für den die Zahlung bestimmt war, rechtmäßig ist;

- das PSU hat den Betrügern seine persönlichen Sicherheitsnachweise, gegebenenfalls einschließlich der für den zweiten Authentifizierungsfaktor verwendeten Geräte oder Elemente, offen und leicht zugänglich gemacht;
- Die PSU wurde bereits früher Opfer derselben Art von Manipulation des Zahlers oder von Social Engineering-Betrug und dessen *Modus Operandi*;
- das PSU hat Warnungen bezüglich der spezifischen Betrugsart missachtet, die vor kurzem an das PSU im Anschluss an die Ergebnisse von TM und/oder damit zusammenhängenden Untersuchungen des PSP gerichtet wurden;
- das PSU hat den Betrug dem PSP nicht rechtzeitig gemeldet, nachdem es davon Kenntnis erlangt hatte.

c) Es soll festgelegt werden, dass Zahlungsdienstleister unter anderem dann für Betrug haften, wenn:

i. Sie sind ihrer Verpflichtung nicht nachgekommen, dem PSU in Bezug auf die Sicherheit Unterstützung zu gewähren, wie in Ziffer 29(d) oben dargelegt, und zwar im Zusammenhang mit dem aufgetretenen Betrug;

ii. der Betrüger vor dem Betrug aufgrund einer Datenschutzverletzung bei diesem Zahlungsdienstleister, einschließlich der in Artikel 9 Absatz 3 Buchstabe c) DSGVO genannten Art, Zugang zu den persönlichen Daten oder Kontodaten des Zahlungsdienstleisters hatte.

32. Nach Ansicht der EBA würden die oben vorgeschlagenen Änderungen dazu beitragen, einen wirksameren Verbraucherschutz zu gewährleisten und gleichzeitig die Verantwortung der Zahlungsdienstleister für die Sicherheit der angebotenen Zahlungsdienste zu stärken. Diese Änderungen würden auch die entsprechenden Kosten für das Streitbeilegungsmanagement sowohl für Zahlungsdienstleister als auch für Kunden senken.

Verstärkung und Harmonisierung der Aufsicht über das Betrugsmanagement

33. Die EBA rät, die Aufsicht über das Betrugsmanagement zu stärken und zu harmonisieren und dabei die in einigen Mitgliedstaaten angewandten bewährten Aufsichtspraktiken sowie die im Rahmen des bereits im Rahmen der PSD2 umgesetzten Berichtsrahmens erhobenen Betrugsdaten zu nutzen. Um dies zu erreichen, könnten weitere Anforderungen in der PSR in Betracht gezogen werden, z. B. die Verpflichtung der NCAs zu:

a) die von den einschlägigen Zahlungsdienstleistern auf nationaler Ebene erhobenen Betrugsdaten regelmäßig zu überwachen - sowohl auf der Seite des Zahlungsdienstleisters des Zahlers als auch auf der Seite des Zahlungsempfängers - und dabei zu überprüfen, ob die Gesamtbetrugsraten für alle wichtigen Zahlungsinstrumente deutlich unter den auf EU-Ebene festgelegten maximal tolerierbaren Werten liegen, wobei die im Rahmen der EBA-GL verfügbaren statistischen Betrugsdaten zur Betrugsberichterstattung gemäß PSD2

zu berücksichtigen sind;

b) auf der Grundlage der Ergebnisse der oben genannten Überwachung mögliche Ausreißer, d.h. Zahlungsdienstleister mit einem Betrugsniveau, das über oder nahe den genannten tolerierbaren Höchstwerten liegt, zu verfolgen und gegebenenfalls Aufsichtsmaßnahmen zu ergreifen.

c) regelmäßig die korrekte Inanspruchnahme von MITs und MOTOs durch Zahlungsdienstleister sowie die Einhaltung der Anwendung von SCA und SCA-Ausnahmen durch Zahlungsdienstleister zu überwachen.

Sicherheitsanforderungen für eine einzige EU-weite Plattform für den Informationsaustausch

34. Zusätzlich zu den Vorschlägen in Absatz 29(b) oben in Bezug auf die Überwachung von Betrugstransaktionen und den Austausch von Betrugsdaten zwischen Zahlungsdienstleistern, wie er in Art. 83 des PSR-Vorschlags empfiehlt die EBA den EU-Ko-Gesetzgebern und der EU-Kommission, eine weitere Stärkung von Art. 83 des PSR-Vorschlags durch die Forderung nach einer einzigen EU-weiten Plattform für den Austausch von Betrugsdaten zwischen Zahlungsverkehrsdienstleistern zu ergänzen, die von den Zahlungsverkehrsdienstleistern unterhalten und betrieben werden muss, um die Vorteile der Maßnahme voll ausschöpfen zu können.

35. Darüber hinaus könnte in Erwägung gezogen werden, geeignete Sicherheitsstandards für die Behandlung von Kundenidentifikatoren von Zahlungsempfängern und anderen betrugsbezogenen Daten festzulegen, die von Zahlungsdienstleistern gemäß Art. 83 PSR ausgetauscht werden, unter Berücksichtigung der Anforderungen an den Schutz personenbezogener Daten. Insbesondere könnte in Erwägung gezogen werden, festzulegen, dass verdächtige eindeutige Kennungen (z. B. IBAN) oder andere personenbezogene Daten nicht zwischen Zahlungsdienstleistern ausgetauscht, sondern von diesen gemeldet und in der Plattform als kryptografische Hashes gespeichert werden sollten. Die Überprüfung der Übereinstimmung einer eingehenden persönlichen Kennung des Begünstigten einer bestimmten Transaktion könnte automatisch in der Plattform erfolgen, indem sie mit der Liste der bereits gespeicherten Hashes verglichen wird, ohne dass personenbezogene Daten zwischen den Zahlungsdienstleistern ausgetauscht werden und ohne dass personenbezogene oder sensible Kundendaten in der Plattform selbst verarbeitet werden.

36. Um die Zusammenarbeit zwischen den Zahlungsverkehrsdienstleistern bei der Verfolgung und Untersuchung von Betrugsfällen zu unterstützen, könnten die von den Zahlungsverkehrsdienstleistern über die oben genannte Plattform auszutauschenden Daten zusätzlich zu den in Absatz 29 Buchstabe b genannten Aspekten eine Liste der Kontaktstellen aller Zahlungsverkehrsdienstleister enthalten.