Bundesministerium
Arbeit, Soziales, Gesundheit,
Pflege und Konsumentenschutz

Bericht zu Phishing Betrugsfällen

Tätigkeitsbericht der Ombudsstelle für Zahlungsprobleme im BMASGPK zu Phishing Betrugsfällen im elektronischen Zahlungsverkehr für den Zeitraum 1. Jänner 2023 bis 31. Dezember 2025

Wien, Mai 2026

Inhaltsverzeichnis

1 Einleitung

Seit Sommer/Herbst 2022 gibt es in Österreich vermehrt Phishing Angriffe auf Konsument:innen, die zu **zahlreichen Missbräuchen im elektronischen Zahlungsverkehr** führen. Um den Schutz der Betrugsopfer zu verbessern, erklärte sich das BMASGPK bereit, **ab Jänner 2023** über die bei ihm eingerichtete **Ombudsstelle für Zahlungsprobleme**[1] als **Anlaufstelle** für Beschwerden zur Verfügung zu stehen.

Dadurch sollen Geschädigte bei der Geltendmachung und Durchsetzung ihrer Rechte bestmöglich beraten und unterstützt werden. Außerdem kann das BMASGPK in Fällen, in denen Banken zu keinen einvernehmlichen Lösungen bereit sind, beim Verein für Konsumenteninformation (VKI) **Verbandsklagen, Musterprozesse** und **Sammelklagen** anregen. Solche Verfahren dienen nicht nur der Rechtsdurchsetzung, sondern auch der Klärung der Rechtslage.

Vom **1. Jänner 2023 bis 31. Dezember 2025** haben sich insgesamt **717 Konsument:innen**, die Opfer eines Phishing Angriffs wurden, mit einer elektronischen oder schriftlichen Beschwerde an die Ombudsstelle gewandt. Telefonische Anfragen oder Beschwerden wurden nicht erfasst.

Der gegenständliche **Bericht enthält**

- eine **detaillierte statistische Auswertung** der von der Ombudsstelle bearbeiteten Beschwerdefälle,
- eine Darstellung der wesentlichen **rechtlichen Rahmenbedingungen** und
- die vom BM**A**SGPK für einen verbesserten Schutz der Konsument:innen vor Phishing Angriffen **vorgeschlagenen Maßnahmen**.

[1] Die Ombudsstelle für Zahlungsprobleme war aufgrund einer Entschließung des Nationalrats vom 15. Dezember 2021, 1189/E XXVII. GP, im BMSGPK eingerichtet worden und zunächst nur als Anlaufstelle für Konsument:innen tätig, die Probleme im Zusammenhang mit Krediten hatten.

2 Typischer Ablauf eines Phishing Angriffs

Phishing Angriffe sind **vielfältig**. Im Berichtszeitraum entfiel aber der Großteil der von der Ombudsstelle bearbeiteten Betrugsfälle auf eine der **drei** folgenden **Fallgruppen**:

2.1 Registrierung eines Geräts der Betrüger:innen

Das Opfer erhält eine SMS oder (seltener) eine E-Mail, in der es zu einer **Aktualisierung/ Bestätigung seiner Zugangsdaten** zum Online Banking oder zu seiner Zahlungs App aufgefordert wird. Die Aufforderung ist mit der Warnung verbunden, dass andernfalls der Zugang kurzfristig (meist bereits am nächsten Tag) gesperrt werden würde. Häufig kommt die Phishing SMS direkt **aus dem Nachrichtenverlauf mit der Bank selbst**, weshalb die Konsument:innen an der Authentizität der Nachricht nicht zweifeln.

In der SMS Nachricht ist ein Link enthalten, der auf eine **Phishing-Website** führt, die der Website der Bank **perfekt nachgebildet** ist. Man kann daher nur an der etwas anderen Adresszeile bemerken, dass man sich nicht auf der Website der Bank befindet. In einigen Browsereinstellungen wird das Anzeigen der Adresszeile außerdem standardmäßig unterdrückt, wenn man nicht extra in die Adresszeile hineinklickt oder zuvor den Link in der Nachricht überprüft.

Auf der Phishing-Website wird das Opfer zur Eingabe und Bestätigung seiner Zugangsdaten (Verfügernummer oder Benutzername und PIN bzw Passwort) aufgefordert. Mit diesen Daten erstellen die Betrüger eine Anfrage zum Login in das Konto des Opfers, welches vom in die Irre geführten Opfer im Glauben freigegeben wird, sich selbst einzuloggen. Nach erfolgreichem Login können die Betrüger eine Registrierung ihres eigenen Geräts für die App des Opfers beantragen. Das Opfer erhält dann eine mTAN auf sein Mobiltelefon oder eine Push Nachricht in seine App, um die Registrierung zu bestätigen. **In der Meinung, lediglich die Registrierung seines eigenen Geräts zu bestätigen, stimmt das Opfer ungewollt der Registrierung des Geräts der Betrüger zu,** die dadurch uneingeschränkten Zugriff auf das Zahlungskonto oder die Zahlungskarte des Opfers haben. Die Betrüger:innen können in der Folge mit ihrem Telefon und einem selbst gewählten Code, ihrem

Fingerabdruck oder ihrer Face-ID solange Zahlungen zu Lasten des Kontos des Opfers in Auftrag geben und auch die Limits für Überweisungen und Kartenzahlungen erhöhen, bis das Opfer den Betrug bemerkt und eine Sperre veranlasst.

Die Opfer werden zwar von der Registrierung des neuen Telefons von ihrer Bank in einer SMS-Nachricht und/oder E-Mail verständigt. Aber auch dann, wenn das Opfer bemerkt, dass es irrtümlich der Registrierung eines fremden Geräts zugestimmt hat, und unverzüglich reagiert, kann es den Missbrauch meist nicht mehr verhindern, weil die missbräuchlichen Zahlungen und allfälligen Limiterhöhungen von den Betrüger:innen innerhalb weniger Minuten nach der Registrierung des neuen Telefons veranlasst werden und eine **Sperre daher zu spät** kommt.

Diese Vorgangsweise der Betrüger:innen, die zu nicht autorisierten Zahlungsvorgängen und damit zu Erstattungsansprüchen des Opfers nach § 67 Abs. 1 ZaDiG 2018 führt, kam bis ca. Mitte 2025 am häufigsten vor. Die Betrüger:innen nutzten dabei **Sicherheitsmängel** aus, die vor allem bei der BAWAG PSK bei der Registrierung eines neuen Geräts bestanden (siehe Punkt 5.5. des Berichts). Seit diese Mängel von der BAWAG PSK im September 2025 behoben wurden, kommen Fälle nicht autorisierter Zahlungsvorgänge nur mehr relativ selten vor.

2.2 Vom Opfer irrtümlich freigegebene (Echtzeit-)Überweisungen

Die Betrüger:innen erlangen durch einen **ersten Phishing Angriff** auf die gleiche oder eine ähnliche Weise wie in der in Punkt 2.1. dargestellten Fallgruppe **Zugang zum Konto des Opfers** und können dadurch dessen Kontodaten einsehen und Aufträge für Umbuchungen vom Spar- auf das Zahlungskonto, Limiterhöhungen und Überweisungen zu Lasten des Zahlungskontos erstellen.

In einem **zweiten Angriff** wird das Opfer angerufen und dazu gebracht, die von den Betrüger:innen erstellten **Transaktionen selbst freizugeben**. Die Betrüger:innen geben sich dabei meist als Bankmitarbeiter:innen aus, die im Rahmen der Transaktionsüberwachung verdächtige Zugriffe auf das Konto des Opfers bemerkt hätten. Das Opfer wird angeleitet, die verdächtigen Aufträge durch eine Bestätigung von Push Nachrichten zu stornieren, die das Opfer auf seine Zahlungs App übermittelt erhält. Tatsächlich werden die betrügerischen Aufträge vom Opfer dadurch nicht storniert, sondern freigegeben.

Da die Registrierung eines neuen Geräts nunmehr – soweit ersichtlich – bei allen Banken weitgehend sicher ausgestaltet ist, bedienen sich die Betrüger **seit 2025 zunehmend dieser Angriffsmethode**.

2.3 Vom Opfer irrtümlich freigegebene Kartenzahlungen

Das Opfer erhält eine scheinbar von einem **Paketdienst** (österreichische Post, DPD, GLS) stammende Phishing Nachricht, in der es von einem wegen fehlerhafter/unvollständiger Adressangaben gescheiterten Zustellversuch informiert wird. Das Opfer wird über einen Link auf eine der Website des Paketdienstes perfekt nachgebildete Phishing Website geleitet, um dort seine vollständigen Adressdaten einzugeben und für eine nochmalige Zustellung einen **geringfügigen Betrag** mit seiner Kredit- oder Debitkarte zu bezahlen.

Mit den vom Opfer auf der Phishing Website eingegebenen Kartendaten können die Betrüger:innen einen Zahlungsauftrag über einen hohen Betrag an eine:n andere:n Empfänger:in erstellen, den das getäuschte Opfer dann in seiner **Zahlungs App freigibt**, weil es den in der Push Nachricht angegebenen Betrag und den:die Empfänger:in in der Meinung, es handle sich ohnehin nur um eine geringfügige Zahlung an den Paketdienst, nicht mehr kontrolliert.

Die gleiche Strategie wird von Betrüger:innen in Fällen angewandt, in denen die Phishing Nachricht scheinbar von einem **Telekommunikationsdienstleister** stammt, der seinen Kund:innen anbietet, gegen eine geringfügige Zahlung angesammelte Bonuspunkte einzulösen, die andernfalls in Kürze verfallen würden.

3 Auswertung der Beschwerdefälle

3.1 Zahl der Beschwerden und Interventionsfälle

Insgesamt haben sich im Berichtszeitraum **717 Phishing Betrugsopfer** mit einer Beschwerde an die Ombudsstelle gewandt:

- In **175 Fällen** kam es zu keiner Intervention der Ombudsstelle bei der kontoführenden Bank der Betrugsopfer, weil

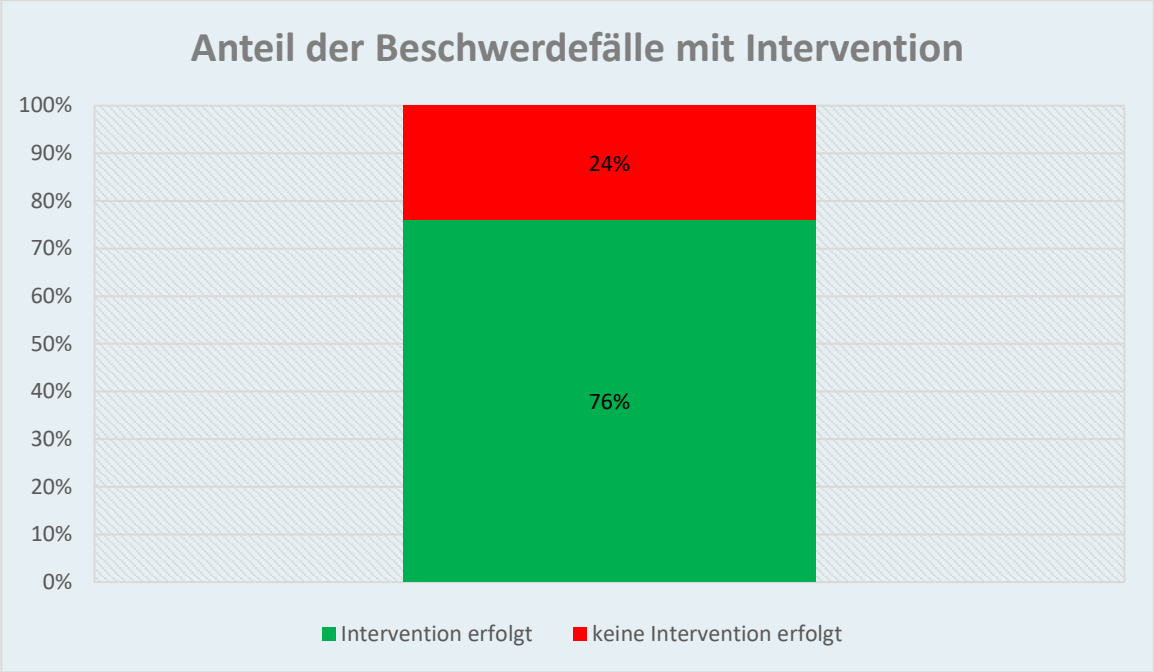
  - eine Überprüfung der Sach- und Rechtslage ergab, dass das Opfer **keine Erstattungs- oder Schadenersatzansprüche** mit Aussicht auf Erfolg geltend machen kann, insbesondere weil es sich um betrügerische Zahlungen mit relativ geringfügigen Beträgen handelte, die vom Opfer selbst freigegeben worden waren;

  - die Beschwerdeführer:innen der Ombudsstelle trotz Aufforderung **nicht alle für eine Intervention erforderlichen Unterlagen** übermittelten;[2]

  - es vor einer Intervention der Ombudsstelle zu einer **Einigung** zwischen dem:der Verbraucher:in und der Bank kam oder die Beschwerde aus anderen Gründen zurückgezogen wurde.

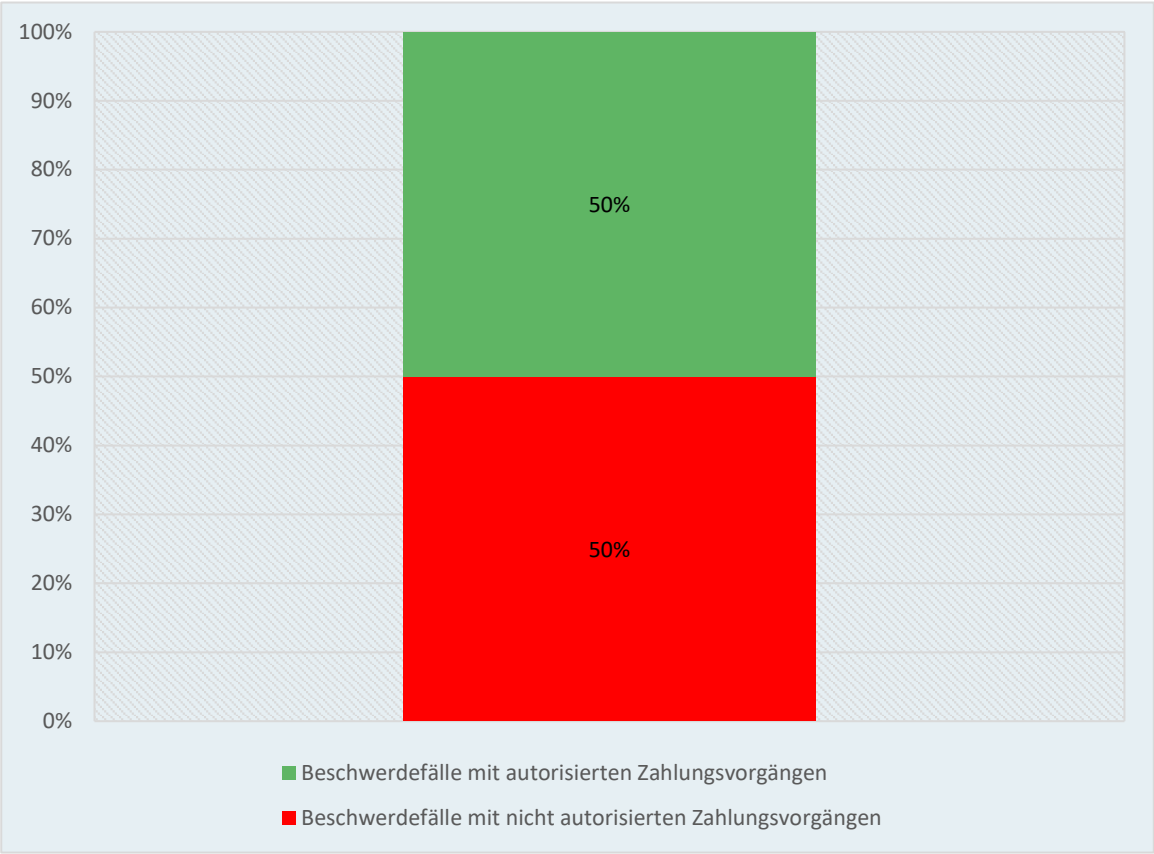
- In den restlichen **542 Fällen** intervenierte die Ombudsstelle für die Betrugsopfer bei ihrer Bank.

[2] Für eine Intervention benötigt die Ombudsstelle folgende Unterlagen: polizeiliche Anzeige, Kontoauszug mit den betrügerischen Transaktionen, Darstellung des Ablaufs des Phishing Angriffs, bisherige Korrespondenz mit der Bank sowie eine Entbindung vom Bankgeheimnis.



3.2 Nicht autorisierte und autorisierte Zahlungsvorgänge

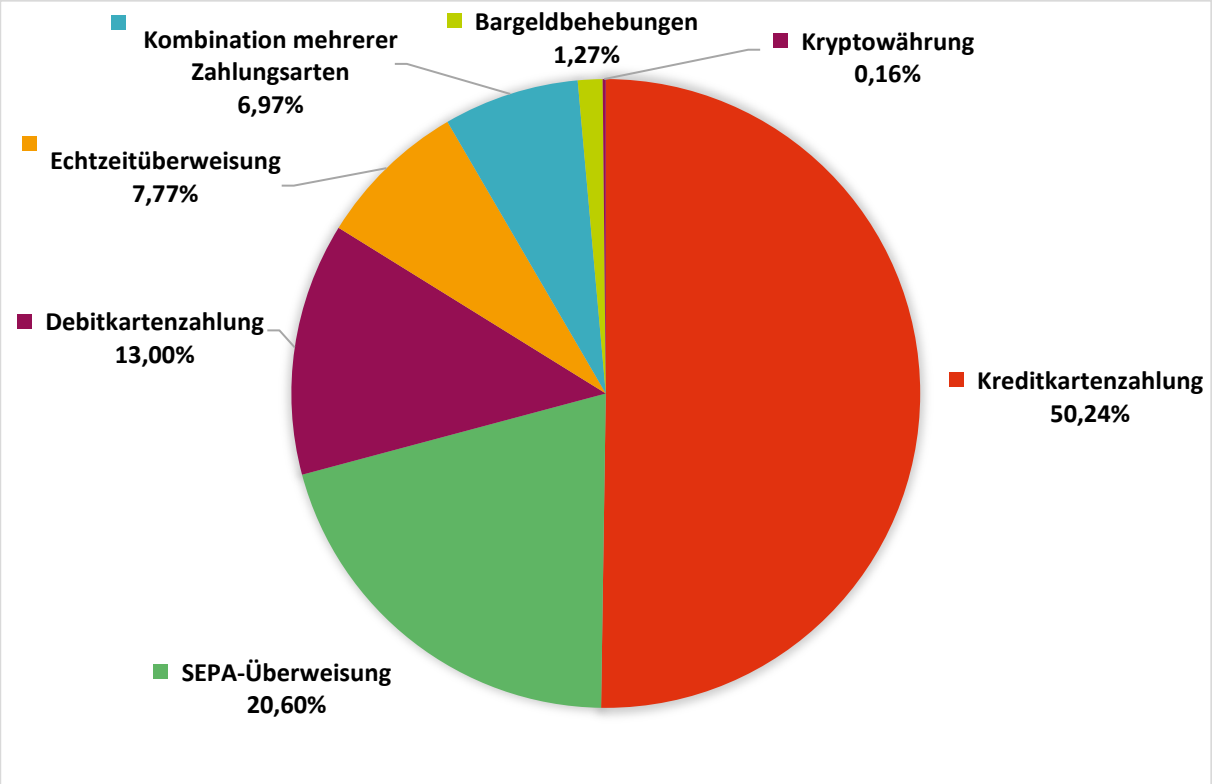
- **50 %** der Interventionsfälle lagen **nicht autorisierte Zahlungen** zugrunde.
- 50 % der Interventionsfälle lagen autorisierte Zahlungen zugrunde.



Eine Zahlung gilt dann als autorisiert, wenn sie **vom Opfer selbst** unter Verwendung der **vereinbarten Authentifizierungsmerkmale** (d.h. idR in der Zahlungs App mit dem App PIN oder einem biometrischen Merkmal) freigegeben wurde.[3] In den Fallgruppen Punkt 2.2. und 2.3. liegen daher autorisierte Zahlungen vor, in der Fallgruppe Punkt 2.1. hingegen nicht autorisierte Zahlungen.

Durch verstärkte Sicherheitsmaßnahmen der Banken, insbesondere der BAWAG PSK, ist der **Anteil nicht autorisierter Zahlungen** in den letzten Monaten des Berichtszeitraumes stark **zurückgegangen**. In den Jahren 2023 und 2024 lag der Anteil nicht autorisierter Zahlungen an den von der Ombudsstelle bearbeiteten Betrugsfällen noch bei 60 %.

3.3 Art der Zahlungen und Ort des Zahlungsempfängers/der Zahlungsempfängerin



[3] Siehe auch Punkt 4.1.

In **63,24 %** der Betrugsfälle kam es daher zu missbräuchlichen **Kartenzahlungen (Debit- und Kreditkarten)**, in **28,37 %** zu missbräuchlichen **Überweisungen (SEPA- und Echtzeitüberweisung)**.

Bei Betrugsfällen mit mehreren **verschiedenen Zahlungsarten** konnten Betrüger:innen mit ihrem für das Online Banking oder die Zahlungs App des Opfers **registrierten Mobiltelefon** (siehe Fallgruppe Punkt 2.1.) sowohl Überweisungen als auch Debitkartenzahlungen und/oder Bargeldbehebungen zu Lasten des Zahlungskontos des Opfers durchführen.

3.4 Land des Empfängers / der Empfängerin

- In **49 %** der Fälle befand sich der oder (bei mehreren) mindestens ein Zahlungsempfänger im **EU-Ausland**.
- In **28 %** der Fälle befand sich der oder (bei mehreren) mindestens ein Zahlungsempfänger in einem **Drittland.**
- In **23 %** der Fälle befanden sich der oder (bei mehreren) alle Zahlungsempfänger im **Inland**.

Ein **Großteil** der betrügerischen Zahlungen erfolgte daher an **Empfänger:innen im Ausland**.

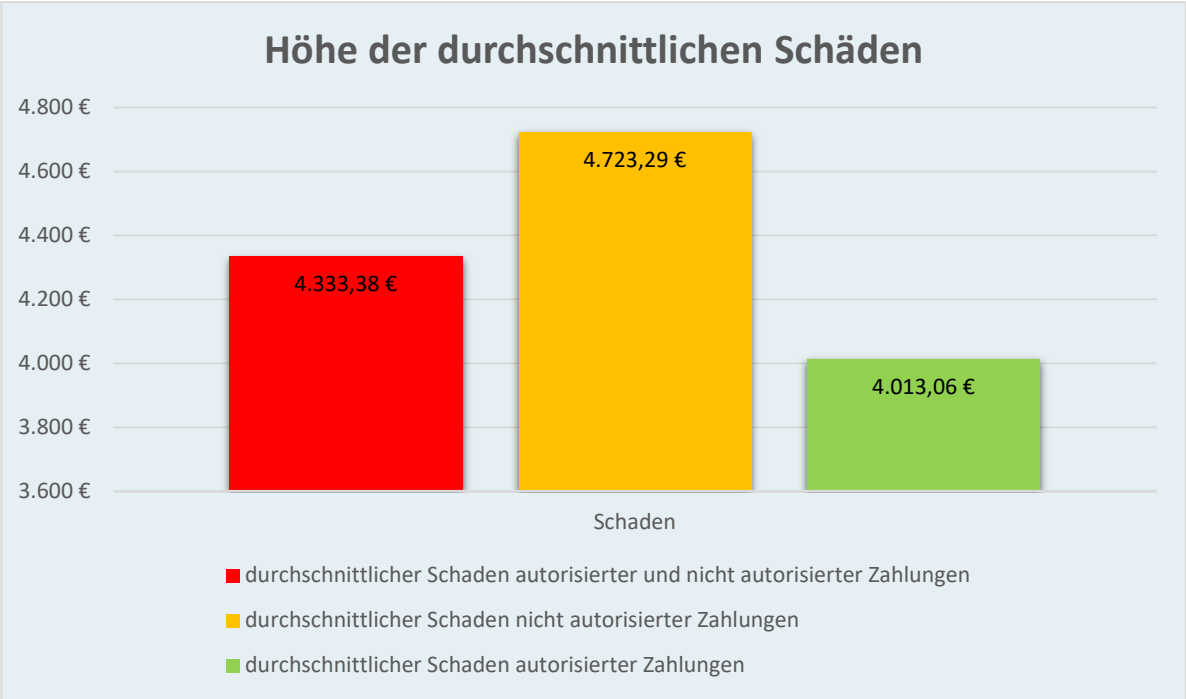
3.5 Anzahl der missbräuchlichen Zahlungen pro Beschwerdefall

- Bei den von der Ombudsstelle bearbeiteten Betrugsfällen kam es pro Fall zu zwischen einer und 140 missbräuchlichen Zahlungen.
- Im **Durchschnitt** kam es zu ca. **4,3 missbräuchlichen Zahlungen** pro Betrugsfall.

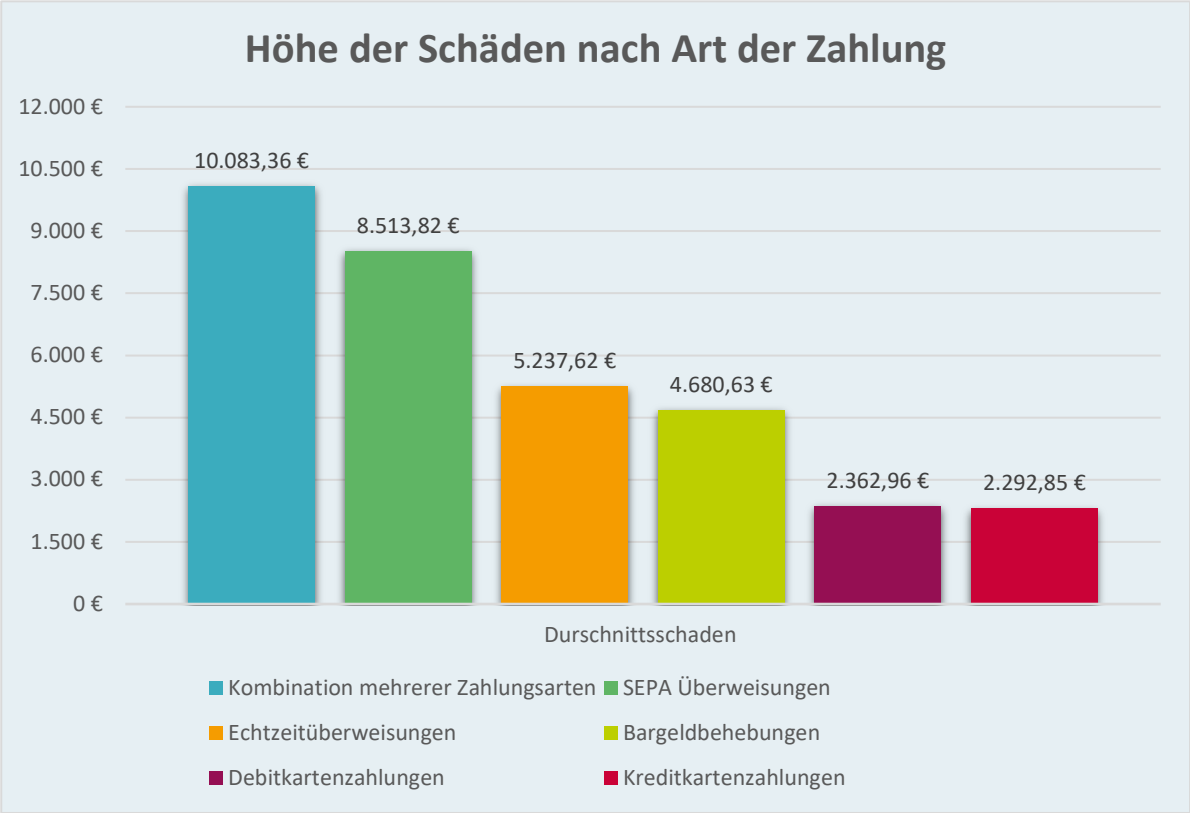
3.6 Höhe der Schäden (Durchschnitt und nach Art der Zahlung)

Der **Durchschnittsschaden** der Betrugsopfer betrug

- pro Beschwerdefall **4.333,38 Euro**
- bei Fällen mit nicht autorisierten Zahlungen 4.723,29 Euro
- bei Fällen mit autorisierten Zahlungen 4.013,06 Euro



Da die Betrüger:innen bei nicht autorisierten Zahlungen mit ihrem eigenen Telefon direkt und selbständig auf das Konto oder die Zahlungskarte des Opfers zugreifen konnten (siehe Fallgruppe Punkt 2.1.), ist der Durchschnittsschaden in solchen Fällen höher.



- Bei Betrugsfällen mit mehreren Arten von Zahlungen ist der Durchschnittsschaden daher am höchsten, was zu erwarten war.
- Obwohl Echtzeitüberweisungen als anfälliger für Missbräuche gelten, ist der Durchschnittsschaden bei Betrugsfällen mit SEPA Überweisungen wesentlich höher. Eine mögliche Erklärung wäre, dass Banken bei Echtzeitüberweisungen wegen der höheren Missbrauchsgefahr eine strengere Transaktionsüberwachung durchführen.
- Bei Kartenzahlungen ist der Durchschnittsschaden wegen der im Allgemeinen niedrigeren Limits wesentlich geringer als bei Überweisungen.

Der **Schaden** betrug in

- 26,47 % bis 1.000 Euro
- 55,04 % zwischen 1.001 und 5.000 Euro
- 14,44 % zwischen 5.001 und 20.000 Euro
- 4,05 % mehr als 20.001 Euro

Bei **Schäden über 20.001 Euro** kam es im Zuge des Phishing Angriffs meistens auch zu **Limiterhöhungen** und **Überträgen** vom Spar- auf das Zahlungskonto.

3.7 Geschlecht der Betrugsopfer

Bei den Betrugsopfern handelte es sich in

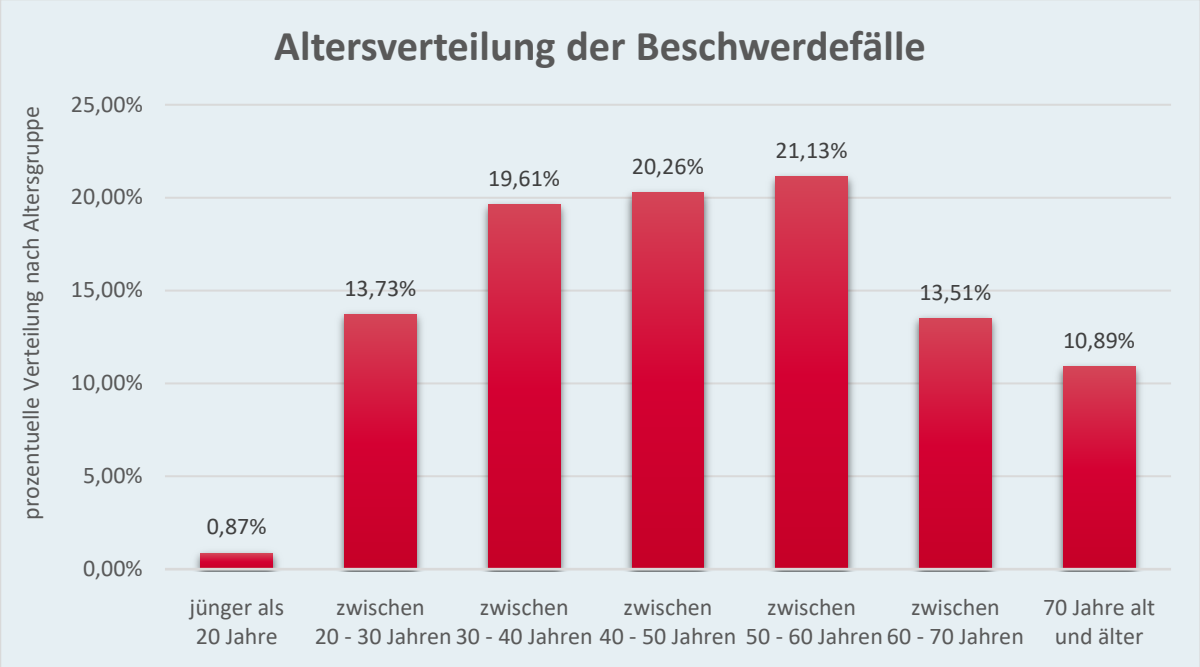
- 388 Fällen (= **54 %**) um **Frauen**
- 329 Fällen (= **46 %)** um **Männer**

Der **Anteil weiblicher Betrugsopfer** ist höher, weil ein Teil der Betrugsopfer Nutzer:innen von **Verkaufsplattformen** wie Vinted oder willhaben waren und es sich bei diesen Betrugsopfern zu 86,3 % um Frauen handelte.[4]

[4] 111 Fälle, davon 90 Frauen.

3.8 Alter der Betrugsopfer

Die Betrugsopfer waren zwischen 14 und 94 Jahren alt. Das **Durchschnittsalter** betrug **47,82 Jahre**,[5] wobei Frauen im Durchschnitt 46,4 und Männer im Durchschnitt 49,7 Jahre alt waren.



Das Durchschnittsalter der Betrugsopfer und ihre Altersverteilung entsprachen daher im Wesentlichen dem Durchschnittsalter und der Altersverteilung der Gesamtbevölkerung, wenn man Personen unter 14 Jahren nicht berücksichtigt. Da ältere Personen im Allgemeinen erheblich weniger oft elektronische Zahlungsinstrumente als jüngere nutzen, ist das **Risiko** des einzelnen Verbrauchers/der einzelnen Verbraucherin, Opfer eines Phishing Angriffs zu werden, **bei älteren Personen** aber **wesentlich höher**.

Bei den einzelnen Banken lag das Durchschnittsalter der Betrugsopfer

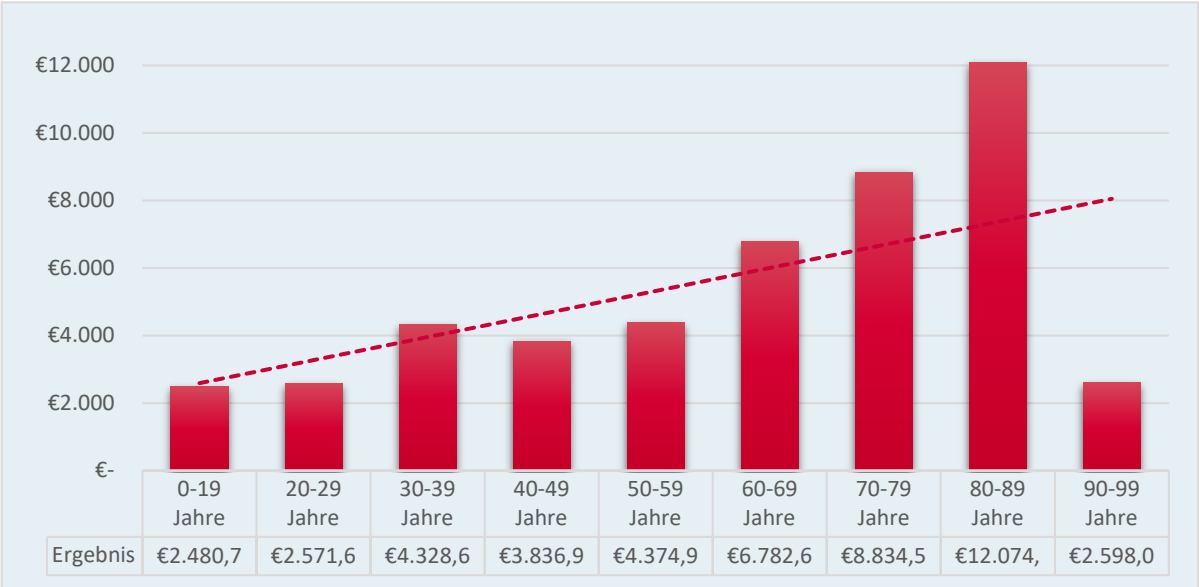
- bei der **BAWAG PSK** (inklusive easybank und PayLife) bei **51,58 Jahren**;
- bei der UniCredit Bank Austria (inklusive Card Complete) bei 49,86 Jahren;
- bei der ERSTE Bank und den Sparkassen bei 42,25 Jahren;

[5] Bei nicht autorisierten Zahlungen liegt das Durchschnittsalter des Opfers bei ca. 51 Jahren, bei autorisierten Zahlungen hingegen bei ca. 45 Jahren.

- beim **Raiffeisensektor** (Raiffeisen CardService, Raiffeisenlandesbanken und alle anderen Raiffeisenbanken) bei **39,89 Jahren**.

Das Durchschnittsalter der Betrugsopfer war daher bei Kund:innen der **BAWAG PSK** um **fast 12 Jahre höher** als bei den Kund:innen des **Raiffeisensektors.** Das könnte entweder am unterschiedlichen Durchschnittsalter der Kund:innen der jeweiligen Bank oder daran liegen, dass die elektronischen Zahlungsinstrumente der BAWAG PSK nicht ausreichend auf die Bedürfnisse von Nutzer:innen mit geringeren digitalen Fähigkeiten wie älteren Menschen ausgerichtet sind.

3.9 Durchschnittliche Schadenshöhe nach Alter der Opfer

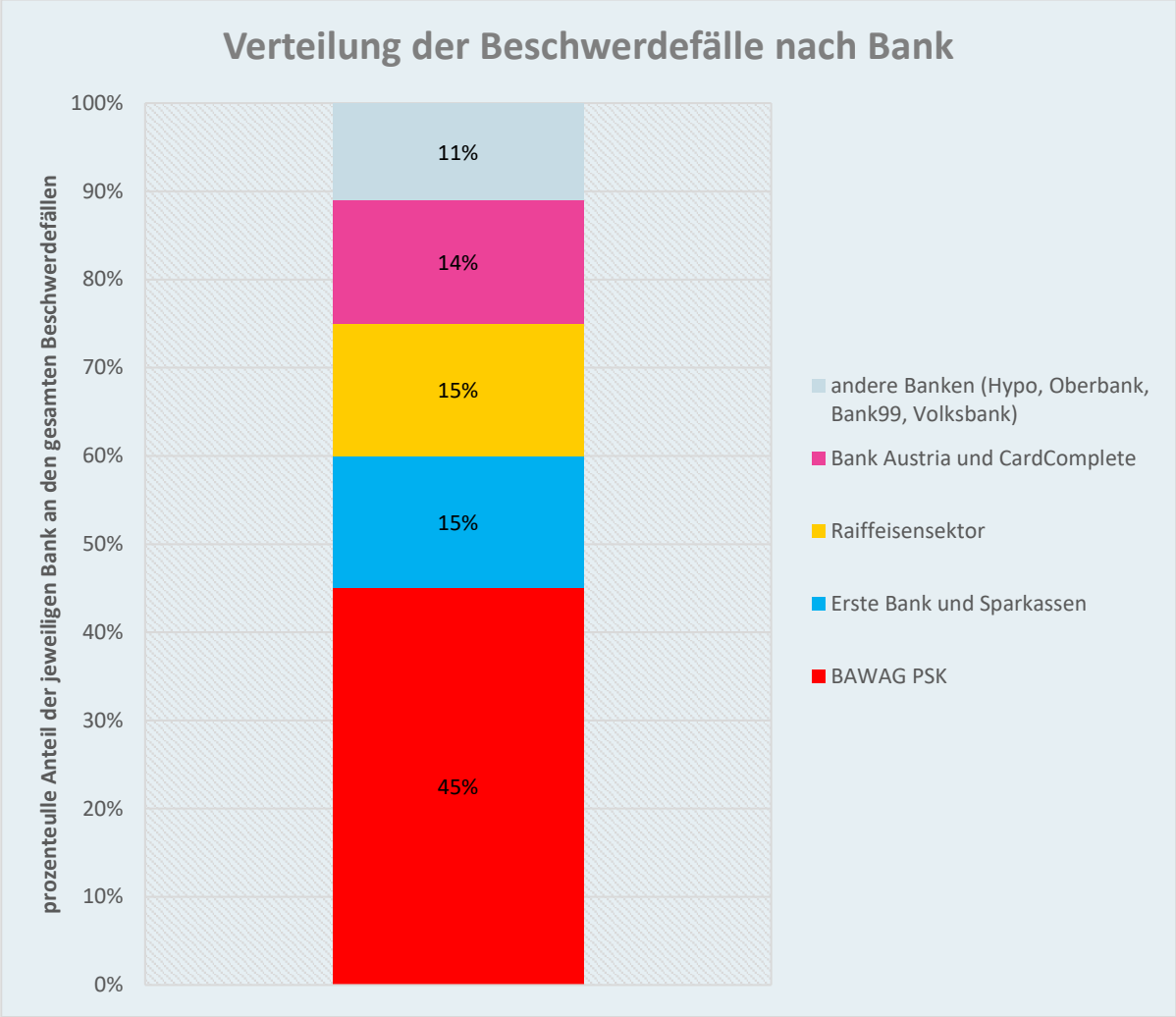


	0-19 Jahre	20-29 Jahre	30-39 Jahre	40-49 Jahre	50-59 Jahre	60-69 Jahre	70-79 Jahre	80-89 Jahre	90-99 Jahre
Ergebnis	€2.480,7	€2.571,6	€4.328,6	€3.836,9	€4.374,9	€6.782,6	€8.834,5	€12.074,	€2.598,0

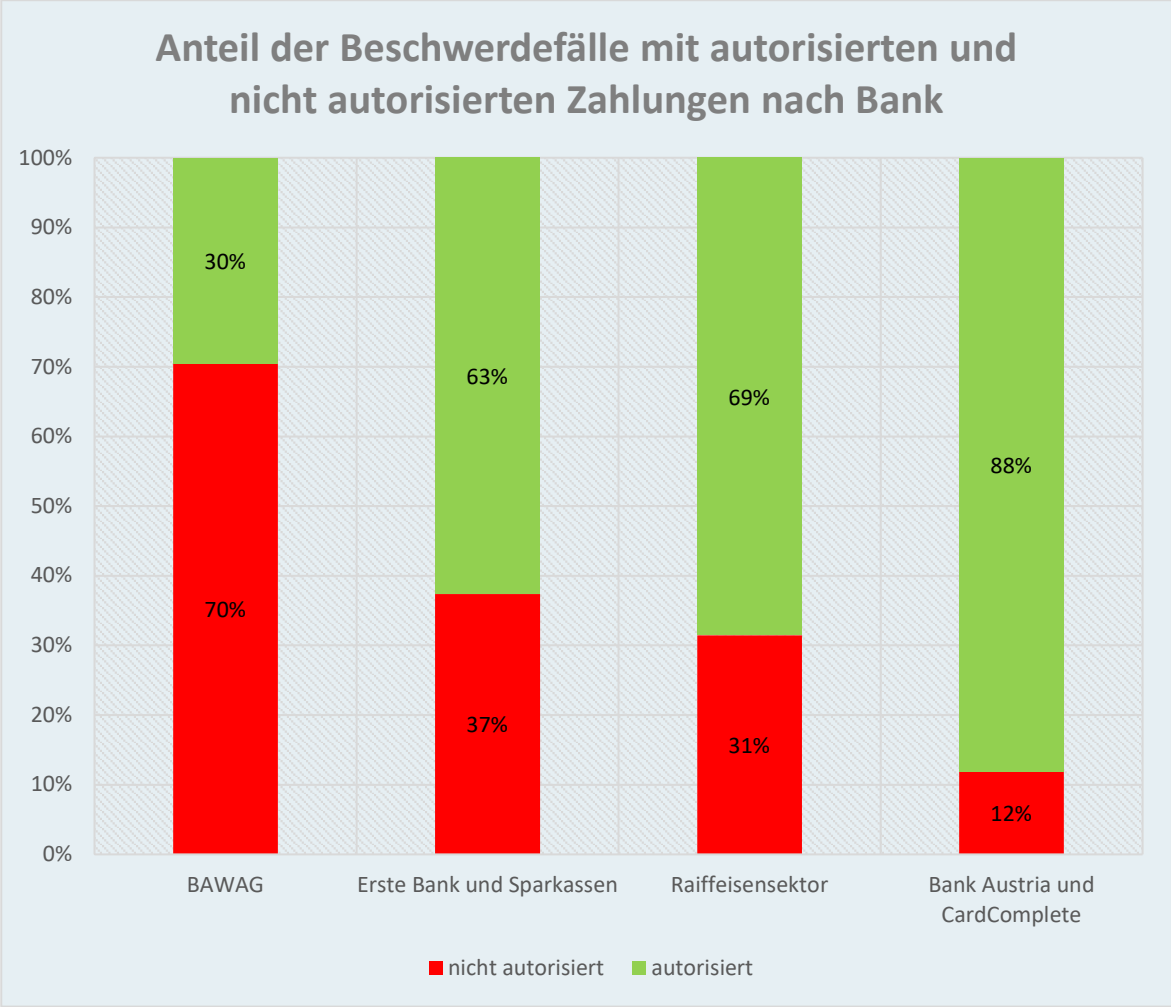
Eine Analyse der Daten nach Altersgruppen und der jeweils zugeordneten Schadenshöhe mit Hilfe einer linearen Trendlinie zeigt, dass **die durchschnittliche Schadenshöhe mit zunehmendem Alter tendenziell steigt.**

Der vergleichsweise niedrige Durchschnittsschaden in der Altersgruppe der 90- bis 99-Jährigen ist wegen der sehr geringen Fallzahl in dieser Altersgruppe statistisch nicht aussagekräftig.

3.10 Betroffene Banken und deren Sicherheit



Im Berichtszeitraum waren daher **fast die Hälfte** der Betrugsopfer **Kund:innen der BAWAG PSK**. Das lag offensichtlich an Sicherheitsmängeln bei der Registrierung neuer Geräte, da der Beschwerdeanteil der BAWAG PSK seit der Einführung neuer Sicherheitsanforderungen für die Registrierung im Herbst 2025 stark gesunken ist.



Da es bei nicht autorisierten Zahlungen den Betrüger:innen im Zuge des Phishing Angriffs gelingt, sich unmittelbaren Zugriff auf das Konto und/oder die Zahlungskarte des Opfers zu verschaffen und dadurch die von der Bank zum Schutz gegen Betrügereien getroffenen Sicherheitsmaßnahmen zu umgehen, ist der **Anteil solcher Betrugsfälle ein Indikator für das Sicherheitsniveau** bei der jeweiligen Bank.

Der Anteil von Beschwerdefällen mit nicht autorisierten Zahlungen war bei der **BAWAG PSK** im Berichtszeitraum im Vergleich zu den anderen Banken **mit 70 % außerordentlich hoch.** Der Grund waren (in der Zwischenzeit behobene) Sicherheitsmängel bei der Registrierung neuer Geräte.

3.11. Ergebnis der Interventionen und Klagen

In den insgesamt 542 Interventionsfällen konnte die Ombudsstelle in **363 Fällen (= 67 %)** eine **Einigung** zwischen dem Betrugsopfer und seiner Bank erreichten.

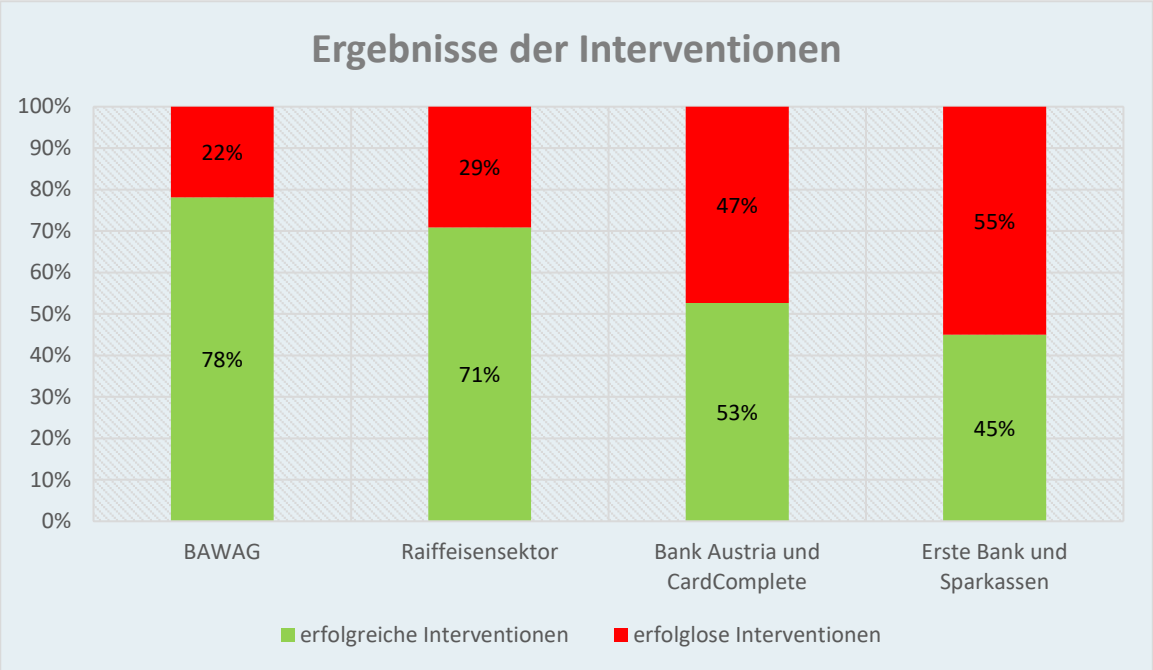
Für diese Einigung

- genügte in 305 Fällen eine außergerichtliche Intervention,
- war in 43 Fällen das Einbringen einer Sammelklage durch den VKI und
- in weiteren 15 Fällen das Einbringen von Individualklagen durch den VKI notwendig.

Im Fall einer Einigung nach einer **außergerichtlichen Intervention** konnte diese im Schnitt nach **15 Tagen** erreicht werden.

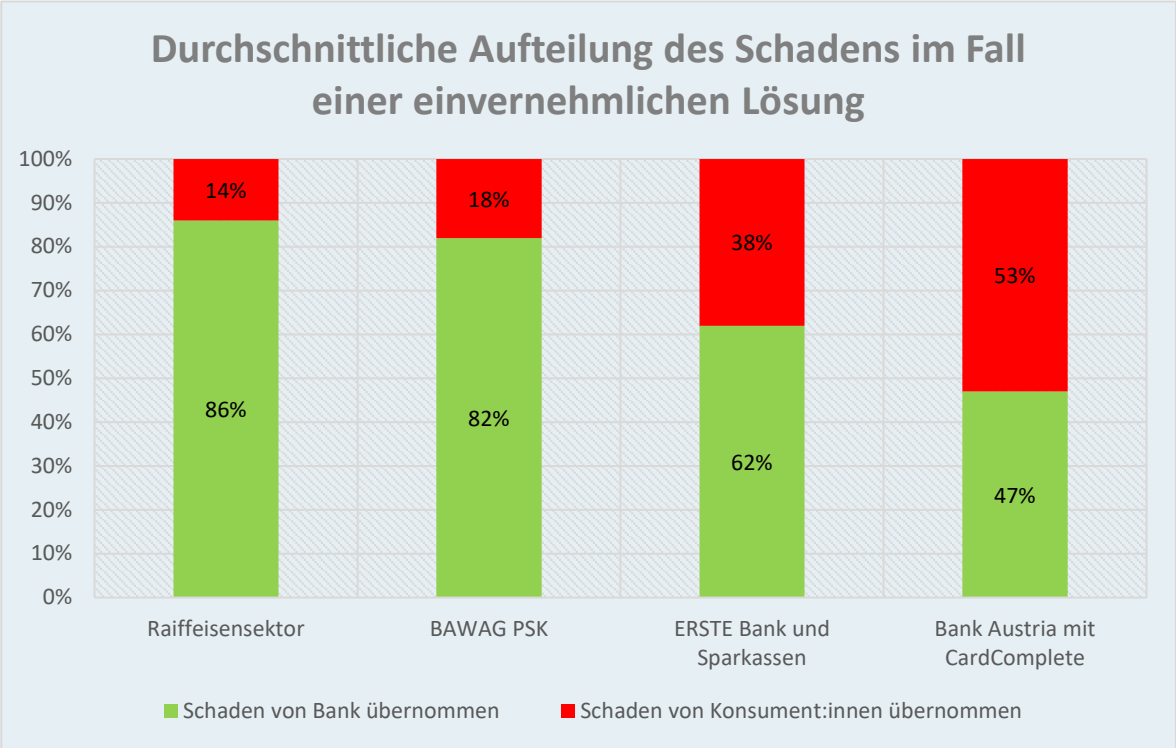
Die **Erfolgsquote** der Ombudsstelle ist bei den einzelnen Banken sehr unterschiedlich. Sie betrug

- bei der BAWAG PSK (mit easybank und PayLife) 78 %
- beim Raiffeisensektor 71 %
- bei der UniCredit Bank Austria (mit Card Complete) 53 %
- bei der ERSTE Bank und den Sparkassen 45 %



Die hohe Erfolgsquote bei der BAWAG PSK täuscht, da diese erst durch die Einbringung einer Sammelklage zu Gunsten von mehreren Geschädigten und 10 Einzelklagen erreicht werden konnte.

In den Beschwerdefällen, in denen eine **einvernehmliche Lösung** erzielt werden konnte, übernahmen die einzelnen Banken im Durchschnitt folgenden Anteil am Betrugsschaden:



Der **Raiffeisensektor** verhält sich daher bei Interventionen der Ombudsstelle **insgesamt am kundenfreundlichsten.** In 71 % der Fälle konnte eine außergerichtliche Lösung erzielt werden, wobei den Betrugsopfern vom Raiffeisensektor im Durchschnitt 86 % des Schadens ersetzt wurden.

4 Rechtliche Rahmenbedingungen[6]

4.1 Unterscheidung zwischen nicht autorisierten Zahlungen und autorisierten Zahlungen

Die Rechte der Opfer eines Phishing Angriffs hängen davon ab, ob die missbräuchlichen Zahlungen vom Opfer autorisiert wurden oder nicht.

Vereinfacht gesagt hat bei **nicht autorisierten Zahlungen** den **Schaden nach dem Gesetz die kontoführende Bank zu tragen**, die nur unter bestimmten engen Voraussetzungen Schadenersatzansprüche gegen den:die Verbraucher:in geltend machen kann.

Bei **autorisierten Zahlungen** hat hingegen **grundsätzlich der:die Verbraucher:in** den Schaden zu tragen, der:die aber allenfalls Schadenersatzansprüche gegen die Bank geltend machen kann.

Eine Zahlung ist nur dann autorisiert, wenn der:die Verbraucher:in der Zahlung unter Verwendung seiner:ihrer mit der kontoführenden Bank vereinbarten Authentifizierungsmerkmale **zugestimmt** hat (siehe § 58 ZaDiG 2018)[7] und ihm:ihr vor der Freigabe die notwendigen Informationen zum Zahlungsauftrag (Betrag, Empfänger, Währung) angezeigt wurden. Als **Authentifizierungsmerkmale** werden in der Regel das Mobiltelefon des Verbrauchers/der Verbraucherin in Verbindung mit dem geheimen PIN/dem Fingerabdruck/der Gesichtserkennung verwendet.

---

[6] Derzeit steht eine **Verordnung** des Europäischen Parlaments und des Rates über **Zahlungsdienste im Binnenmarkt** kurz vor ihrer Beschlussfassung (siehe https://data.consilium.europa.eu/doc/document/ST-8221-2026-INIT/en/pdf). Diese Verordnung wird 21 Monate und zwanzig Tage nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in den Mitgliedstaaten unmittelbar anwendbar sein (also voraussichtlich **ab Frühling 2028**); sie wird auch die hier dargestellten rechtlichen Vorgaben des ZaDiG 2018 und der Verordnung (EU) 2018/389 ersetzen und in fast allen relevanten Punkten **wesentlich verändern**. Die Auführungen in Punkt 4. dieses Berichts sind daher ausschließlich für Phishing Betrugsfälle relevant, die sich bereits ereignet haben oder die sich noch bis zum Frühling 2028 ereignen sollten.

[7] Gemäß § 48 Abs. 1 Z 2 lit. c ZaDiG 2018 hat der Zahlungsdienstleister dem Zahlungsdienstnutzer Informationen und Vertragsbedingungen betreffend die **Form und das Verfahren für die Zustimmung** zur Auslösung eines Zahlungsauftrags mitzuteilen.

Wenn es den Betrügern wie in der **Fallgruppe Punkt 2.1.** im Zuge des Phishing Angriffs gelingt, ihr Mobiltelefon für das Online Banking und/oder die Zahlungs App des Verbrauchers/der Verbraucherin registrieren zu lassen, und die missbräuchlichen Zahlungen dann mit dem Telefon der Betrüger beauftragt und freigegeben werden, liegen daher **nicht autorisierte Zahlungen** vor. [8]

Bei den Betrugsfällen der **Fallgruppe Punkt 2.2**. kommt es zwar zu einer missbräuchlichen Verwendung vertraulicher Authentifizierungsmerkmale, durch welche die Betrüger Zugang zum Zahlungskonto des Opfers erhalten. [9] Die Zustimmung zur Ausführung der missbräuchlichen Zahlungsvorgänge, auf die es nach dem Wortlaut des § 58 ZaDiG 2018 derzeit ausschließlich ankommt, wird aber durch das (arglistig in die Irre geführte) Opfer selbst erteilt. Es liegen daher bei dieser Fallgruppe nach der derzeit maßgeblichen Rechtslage wohl **autorisierte Zahlungsvorgänge** vor.[10]

Auch bei der **Fallgruppe Punkt 2.3.** stimmt das arglistig in die Irre geführte Opfer der Ausführung der missbräuchlichen Zahlungsvorgänge selbst zu. Es liegen daher **autorisierte Zahlungen** vor.

4.2 Rechte der Betrugsopfer bei nicht autorisierten Zahlungen

4.2.1 Berichtigungs-/Erstattungsanspruch

Zeigt die:der Konsument:in ihrer/seiner Bank eine von ihr:ihm nicht autorisierte Zahlung an, muss die Bank gemäß **§ 67 Abs. 1 ZaDiG 2018** bis zum Ende des auf die Anzeige **folgenden Bankarbeitstages** entweder eine Berichtigung des Kontos der:des Konsument:in vornehmen oder die nach § 66 Abs. 1 und 3 ZaDiG 2018 vorgeschriebenen Nachweise[11]

[8] Vgl *Fletzberger/Falke*, ZFR 2024, 364, 368; *Koch/Oppitz*, ÖBA 2024, 564.
[9] Gemäß § 87 Abs. 1 Z 1 ZaDiG 2018 muss die kontoführende Bank, sofern nicht ausnahmsweise die Voraussetzungen des Art. 10 VO (EU) 2018/389 vorliegen, auch dann eine starke Kundenauthentifizierung verlangen, wenn der Zahler online auf sein Zahlungskonto zugreift, sich also einloggt.
[10] Vgl *Fletzberger/Falke*, ZFR 2024, 364 und 368; *Koch/Oppitz*, ÖBA 2024, 564; aA: *Kriegner*, RdW 2025, 732; *Schmalenbach* in BeckOK BGB[77] § 675j Rz 2 f.
[11] Das sind Transaktionsprotokolle, die die ordnungsgemäße Authentifizierung und Ausführung der Zahlung durch eine sekundengenaue Darstellung der technischen Abläufe der Transaktion nachweisen.

vorlegen.[12] Eine Berichtigungs-/Erstattungspflicht nach Ablauf der Frist des § 67 Abs. 1 besteht gemäß § 67 Abs. 2 ZaDiG 2018 nur dann nicht, wenn berechtigte Gründe einen Betrugsverdacht stützen und die Bank diese Gründe der FMA schriftlich mitteilt.

4.2.2 Allfällige Schadenersatzansprüche der Bank schließen Berichtigungsansprüche von Konsument:innen nicht aus

In den meisten Beschwerdefällen der Fallgruppe 2.1. war es zwischen der Bank und den Konsument:innen idR **nicht strittig,** dass die reklamierten Zahlungen nicht vom berechtigten Karten- oder Kontoinhaber:innen autorisiert wurden, sondern von den Betrüger:innen. Es ergab sich nämlich aus den Transaktionsprotokollen, dass für die Zahlungen nicht das Gerät des Opfers, sondern ein fremdes Gerät verwendet wurde, das im Zuge des Phishing Angriffs neu registriert wurde.

In solchen Fällen ändert ein **Schadenersatzanspruch**, der der Bank gegenüber der Konsumentin/dem Konsumenten unter Umständen nach § 68 Abs. 3 ZaDiG 2018 wegen einer grob schuldhaften Verletzung von Sorgfaltspflichten zustehen könnte, nichts daran, dass das Konto sofort berichtigt werden muss.[13] Die Bank muss daher ihre allfälligen **Schadenersatzansprüche gesondert geltend machen**. Erst wenn die Bank ein rechtskräftiges Urteil erwirkt hat oder die:der Konsument:in die Schadenersatzforderung der Bank anerkannt hat, kann diese das Kundenkonto wieder mit der reklamierten Zahlung belasten.[14]

In den von der Ombudsstelle bearbeiteten Beschwerdefällen hielten sich die Banken regelmäßig **nicht an diese Vorgaben**, sondern lehnten eine Berichtigung des Kundenkontos mit Verweis auf ein angeblich grobes Verschulden des Betrugsopfers ab. Im Ergebnis rechneten die Banken daher mit ihrem eigenen (vermeintlichen) Schadenersatzanspruch gegen den Berichtigungs-/Erstattungsanspruch der Konsument:innen auf. Dadurch werden

---

[12] *Koch*, ÖBA 2019, 106 [113]; *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 67 Rz 21; *Zahrte*, NJW 2018, 337 (340).

[13] OGH 8 Ob 106/20a zu den Klauseln 4,5,7 und 8; *Koch*, ÖBA 2019, 106 (113 f); *Kodek*, ÖBA 2021, 19 (35 ff); *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 66 Rz 29 ff.; Leixner, ZaDiG 20183 (2023) § 67 Rz 9; Schlussanträge des Generalanwalts in der Rechtssache *Tukowiecka* C-70/25 (die Entscheidung des EuGH in diesem Verfahren steht noch aus).

[14] Schlussanträge des Generalanwalts in der Rechtssache *Tukowiecka* C-70/25; *Kodek*, ÖBA 2021, 19 (36); *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 67 Rz 24.

die gesetzlichen Vorgaben zum Schutz der Konsument:innen im Ergebnis vollständig entwertet.

4.2.3 Häufig kein grobes Verschulden der Konsumentin/des Konsumenten

Schadenersatzansprüche gemäß § 68 Abs. 3 ZaDiG 2018, die die Bank gesondert geltend machen müsste und die daher an ihrer Berichtigungspflicht nichts ändern, stehen der Bank nur dann zu, wenn die:der Konsument:in eine Pflicht gemäß § 63 ZaDiG **grob fahrlässig** oder **vorsätzlich** verletzt hat.

Grobe Fahrlässigkeit erfordert ein **erhebliches Ausmaß an Nachlässigkeit**. Sie darf daher nicht vorschnell bejaht werden, sondern muss die **Ausnahme** bilden, während die meisten in der Praxis in Betracht kommenden Sorgfaltspflichtverletzungen als leicht fahrlässig einzustufen sind.[15] Gibt die Kundin/der Kunde personalisierte Sicherheitsmerkmale im Zuge eines Phishing-Angriffs weiter, hängt es von den Umständen des Einzelfalls ab, ob ihm:ihr grobe Fahrlässigkeit zur Last fällt oder nicht.[16] Auch die vollständige Weitergabe von Verfügernummer und persönlichen Daten auf einer Phishing-Website ist daher nicht unbedingt grob fahrlässig.[17]

Grobe Fahrlässigkeit liegt jedenfalls nur dann vor, wenn es für die Kundin/den Kunden **erkennbar** war, dass sein/ihr Verhalten eine missbräuchliche Verwendung des Zahlungsinstruments wahrscheinlich macht.[18] Diese Voraussetzung ist unter Berücksichtigung der persönlichen Verhältnisse der betreffenden Kundin/des betreffenden Kunden und ihren:seinen Lebensgewohnheiten (insbesondere auch ihren:seinen bisherigen Erfahrungen mit solchen Zahlungsinstrumenten) zu beurteilen.[19]

Geht man von diesem Maßstab aus, liegt bei einem großen Teil der bei der Ombudsstelle für Zahlungsprobleme eingegangenen Beschwerdefällen wohl **keine grobe Fahrlässigkeit** vor, zumal es sich bei vielen Geschädigten um ältere Menschen ab ca. 50 Jahren handelt, die wenig Erfahrungen im Umgang mit elektronischen Zahlungsinstrumenten haben. Oft

[15] *Kodek*, ÖBA 2021, 19 (31 und 38).
[16] OGH 10 Ob 102/15w; *Kodek*, ÖBA 2021, 19 (32).
[17] OGH 8 Ob 108/21x.
[18] OGH 9 Ob 48/18a, Punkt 4.1.; RIS-Justiz RS0030303, RS0031127; RS0030644 und RS0030272.
[19] OGH 9 Ob 48/18a.

nutzen die Betrüger:innen auch gezielt die Unsicherheit der Opfer in unbekannten Situationen aus (z.B. beim Verkauf von Gebrauchtgegenständen auf Verkaufsplattformen).

4.2.4 Nichtbeachtung von Sicherheitswarnungen begründet für sich alleine noch kein grobes Verschulden

Zwar veröffentlichen die österreichischen Banken auf ihren Websites umfangreiche Informationen zu und Warnungen vor Phishing Angriffen. Auf diese Informationen wird immer wieder auch in Nachrichten hingewiesen, die in das Postfach der Kund:innen im Online Banking oder in der Zahlungs App eingestellt werden. Allerdings

- befanden sich beispielsweise im April 2026 auf der Website der BAWAG PSK[20] 56 derartige Sicherheitswarnungen, wobei in jeder einzelnen Warnung ein komplexes Betrugsszenario dargestellt wurde,
- nutzen die Banken das Online Banking, um ihre Kosten zu senken und den Absatz ihrer Zahlungsverkehrsprodukte zu fördern, und
- wird das Online Banking den Kund:innen mit dem Versprechen angedient, damit ihre Zahlungen rasch und bequem abwickeln zu können.

Angesichts dieser **Interessenlage**

- können die Banken wohl nicht berechtigterweise darauf vertrauen, dass die Verbraucher:innen bei der Nutzung des Online Banking einen Aufwand auf sich nehmen, der über das hinausgeht, was zur Abwicklung der Zahlungen unmittelbar notwendig ist, und
- handelt ein:e Verbraucher:in wohl nicht alleine bereits deshalb grob fahrlässig, weil er:sie es nicht auf sich nimmt, alle auf der Website seiner:ihrer Bank veröffentlichten Sicherheitswarnungen zu lesen, oder er:sie diese Warnung nach ihrer Lektüre wieder vergisst.

[20] Vgl https://www.bawag.at/bawag/sicherheit/alle-sicherheitswarnungen.

Aufgrund der wechselseitigen Interessen wäre es aus der Sicht des Verbraucherschutzes vielmehr die Verpflichtung des Zahlungsdienstleisters, mobile Zahlungsinstrumente so zu gestalten, dass sie auch von Verbraucher:innen **sicher verwendet werden können**, die es nicht auf sich nehmen können oder wollen, sich fortlaufend über neue Betrugsszenarien und Sicherheitswarnungen zu informieren, oder die solche Warnungen nach ihrer Lektüre wieder vergessen

Notwendig sind vor allem ausreichende **Sicherheitsvorkehrungen bei der Registrierung eines neuen Geräts** (siehe Punkt 5.4.) sowie eine **Überprüfung der einzelnen Transaktionen** in Echtzeit auf einen möglichen Betrugsverdacht (siehe Punkt 5.2.).

4.2.5 Haftungsbefreiung der Konsumentin/des Konsumenten wegen nicht ausreichender Sicherheitsvorkehrungen bei der Registrierung eines neuen Geräts

Nicht autorisierte Zahlungen kamen vor allem bei Banken vor, bei denen im Fall der Registrierung eines neuen Geräts nur die gleichen Sicherheitsmaßnahmen **wie bei jeder Einzelzahlung** zur Anwendung kamen, obwohl der Umfang des mit der Registrierung eines neuen Geräts verbundenen Betrugsrisikos wesentlich höher ist, wie die von der Ombudsstelle bearbeiteten Beschwerdefälle eindrücklich zeigen. Zu diesen Banken gehörte bis Herbst 2025 die BAWAG PSK, bei der man nach einer Registrierungsanfrage lediglich einen TAN auf das alte Gerät übermittelt erhielt, den man eingeben musste. Führte man die Registrierung über die Zahlungs App durch, erhielt man eine Push Nachricht auf die App, die man lediglich bestätigen musste. Weitere Sicherheitsmaßnahmen bestanden nicht.

Nach **Art. 25 DelVO (EU) 2018/389** muss allerdings der Zahlungsdienstleister Vorkehrungen ergreifen, die gewährleisten, dass **nur Geräte des rechtmäßigen Zahlungsdienstnutzers** als personalisierte Sicherungsmerkmale oder Authentifizierungsgeräte verwendet werden können und dass die vom Zahlungsdienstleister verwendete Software (d.h. die Zahlungs App) nur vom rechtmäßigen Zahlungsdienstnutzer verwendet werden kann. Die Registrierung eines neuen Geräts muss daher auch an das **gleichzeitige physische Vorhandensein** des neuen und alten Geräts beim rechtmäßigen Zahlungsdienstnutzer gebunden werden.[21] Erst dadurch wird mit ausreichender Sicherheit gewährleistet, dass

[21] Das wird beispielsweise bei der ERSTE Bank dadurch überprüft, dass der:die Kunde:in, der ein neues Gerät registrieren lassen will, auf das alte/bisherige Gerät einen QR-Code übermittelt erhält, den er:sie mit dem

sich auch das neue Gerät tatsächlich im Besitz des rechtmäßigen Zahlungsdienstnutzers befindet.

Zwar haben die Betrüger:innen Angriffsstrategien entwickelt, um auch diesen zusätzlichen Sicherheitsmechanismus zu umgehen. Allerdings reduziert er die Wahrscheinlichkeit eines Erfolgs eines Phishing Angriffs wesentlich, wie die statistische Auswertung der von der Ombudsstelle bearbeiteten Beschwerden zeigt. Die BAWAG PSK hatte im Berichtszeitraum einen Anteil an allen Beschwerden von 45 %, wobei es in 70 % der die BAWAG PSK betreffenden Betrugsfälle zur Registrierung eines Geräts der Betrüger:innen kam. Demgegenüber hatten die ERSTE Bank und die Sparkassen einen Beschwerdeanteil von 15 %, wobei es nur in 37 % dieser Fälle zur Registrierung eines Geräts der Betrüger:innen kam.[22]

Da die VO (EU) 2018/389 die Erfordernisse für eine sichere Kundenauthentifizierung in den verschiedenen Fallkonstellationen im Wege technischer Regulierungsstandards konkretisiert, wären Betrugsopfer gemäß **§ 68 Abs. 5 ZaDiG 2018** selbst im Fall eines groben Verschuldens **von einer Haftung nach § 68 Abs. 3 ZaDiG 2018 befreit**, sollte die Bank bei der Registrierung nicht die nach der VO (EU) 2018/389 erforderlichen Sicherheitsvorkehrungen eingehalten haben.[23]

4.2.6 Weitere mögliche Fälle einer Haftungsbefreiung der Konsumentin/des Konsumenten

Selbst wenn im Einzelfall grobe Fahrlässigkeit vorliegen sollte, **haftet der:die Konsument:in für den Schaden der Bank nicht**, wenn

- keine **starke Kundenauthentifizierung** (Zwei Faktor Authentifizierung) erfolgt ist,[24]

---

neuen Gerät scannen muss. Wurde das alte Gerät verloren oder gestohlen, ist für die Registrierung ein Besuch in einer Filiale der Bank und die Vorlage eines amtlichen Lichtbildausweises erforderlich.

[22] Siehe Punkt III.H.

[23] *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 68 Rz 69 und 83 ff; OGH 8 Ob 108/21x und 8 Ob 106/20a zu den Klauseln 4,5,7 und 8.

[24] Siehe § 68 Abs. 5 ZaDiG 2018.

- der:die Verbraucher:in **nicht die Möglichkeit** hatte, den **Missbrauch jederzeit anzuzeigen**, etwa weil er:sie längere Zeit warten musste, bevor der Anruf entgegen genommen wurde,[25]
- die nicht autorisierte Zahlung von der Bank durchgeführt wurde, **nachdem** der:die Verbraucher:in den **Missbrauch angezeigt hatte,** [26]
- **keine ordnungsgemäße Transaktionsüberwachung** stattfand,[27]
- **die mit der Konsumentin/dem Konsumenten vereinbarten Limits überschritten wurden.**[28]

4.3 Allenfalls Schadenersatzansprüche der Betrugsopfer bei autorisierten Zahlungen

Bei Zahlungen, die vom arglistig in die Irre geführten Betrugsopfer im Zuge des Phishing Angriffs selbst autorisiert wurden**,** steht der Bank ein **Aufwandersatzanspruch** gemäß § 1014 ABGB zu, der einen Berichtigungsanspruch des Verbrauchers/der Verbraucherin gemäß § 67 Abs. 1 ZaDiG 2018 ausschließt. Der Schaden ist daher grundsätzlich vom:von der Verbraucher:in zu tragen, der:die jedoch unter Umständen **Schadenersatzansprüche** gegen die Bank geltend machen kann, wenn diese **keine ordnungsgemäße Transaktionsüberwachung** gemäß **Art. 2 VO (EU) 2018/389** durchgeführt und dadurch den Betrug ermöglicht hat. [29] Die vom Zahlungsdienstleister einzusetzende Transaktionsüberwachung muss nämlich nach der ausdrücklichen Anordnung des Art. 2 nicht nur die Erkennung nicht autorisierter Zahlungsvorgänge ermöglichen, sondern auch die Erkennung (autorisierter) **betrügerischer** Zahlungsvorgänge.[30]

Führt die Transaktionsüberwachung zu einem Betrugsverdacht, muss die Bank die **Zahlung blockieren** und darf sie erst nach vorheriger Rückfrage beim:bei der Verbraucher:in durchführen.[31] Gemäß § 73 Abs. 1 Z 2 ZaDiG 2018 kann und muss der Zahlungsdienstleister die Ausführung eines autorisierten Zahlungsvorgangs ablehnen, wenn seine Ausführung

[25] Siehe § 68 Abs. 6 ZaDiG 2018.
[26] Siehe § 68 Abs. 6 ZaDiG 2018.
[27] Siehe Punkt 2.3.
[28] In diesem Fall ist der:die Konsument:in aber nur von der Haftung für den das vereinbarte Limit übersteigenden Teil des Schadens befreit.
[29] Vgl *Koch/Oppitz*, ÖBA 2024, 564 (584).
[30] Siehe Punkt 46 der Opinion EBA-Op-2018-04 vom 13.6.2018.
[31] *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 68 Rn 57 f mwN.

gegen eine unionsrechtliche Regelung – im vorliegenden Fall Art. 2 VO (EU) 2018/389 – verstoßen würde.[32]

Wie sich aus der rechtskräftigen **Entscheidung des OLG Linz zu 1 R 45/25f**[33] ergibt, ist es nicht zulässig, im Rahmen der Transaktionsüberwachung bei einer Serie von aufeinanderfolgenden Überweisungen/Zahlungen zu einer Verfügernummer die einzelnen Transaktionen isoliert auf eine mögliche Abweichung vom bisherigen Zahlungsverhalten des Kunden/der Kundin zu überprüfen.

In einem großen Teil der von der Ombudsstelle bearbeiteten Betrugsfällen mit formal autorisierten Zahlungen hatte das Opfer zuvor nie Zahlungen mit annähernd so hohen Beträgen in Auftrag gegeben. Außerdem hätte sich in einem Teil der Fälle auch aus der Person und dem Sitzstaat des Zahlungsempfängers, dem Ort der Zahlung oder einer unüblichen Währung ein Betrugsverdacht ergeben können oder müssen.

Hätte der Schaden bei Durchführung einer ordnungsgemäßen Transaktionsüberwachung verhindert werden können, stehen dem Verbraucher **Schadenersatzansprüche** gegen die Bank zu, [34] da die Verpflichtung zu einer Transaktionsüberwachung zu den nebenvertraglichen Schutz- und Sorgfaltspflichten des Zahlungsdienstleisters gehört. Es ergibt sich aus Art. 1 lit a iVm Art. 2 Abs. 1 DelVO (EU) 2018/389 und aus EG 1 dieser Verordnung, dass die Transaktionsüberwachung ein **notwendiger Bestandteil** der nach Art. 97 RL (EU) 2015/2366 und § 87 ZaDiG 2018 vorgeschriebenen **starken Kundenauthentifizierung** ist. Diese ist schon deshalb eine **nebenvertragliche Sorgfaltspflicht** des Zahlungsdienstleisters, weil § 87 im 4. Hauptstück des ZaDiG 2018 angesiedelt ist, das entsprechend seiner Überschrift Rechte und Pflichten der Vertragsparteien begründen soll, die unabhängig von einer allfälligen zusätzlichen aufsichtsrechtlichen Sanktionierung im Zivilrechtsweg vor ordentlichen Gerichten eingeklagt werden können.[35]

Aber selbst wenn man nur von einer aufsichtsrechtlichen Vorgabe ausginge, sehen § 87 Abs 1 ZaDiG 2018 und Art 2 DelVO (EU) 2018/389 ihrem Inhalt nach jedenfalls Verpflichtungen vor, die beim einzelnen Zahlungsvorgang zu erfüllen sind und die daher auch den einzelnen

---

[32] Vgl dazu auch *Koch/Oppitz*, ÖBA 2024, 564 (581).
[33] Abrufbar unter: RIS - 1R45/25f - Entscheidungstext - Justiz.
[34] OLG Linz 1 R 45/25f.
[35] ErläutRV 207 BlgNR 24. GP 31; *Haghofer* in Weilinger/Knauder/Miernicki, ZaDiG 2018 § 87 Rz 8; für D: *Omlor*, WM 2018, 57.

Zahlungsdienstnutzer schützen sollen. Insofern sind § 87 ZaDiG 2018 und Art 2 DelVO (EU) 2018/389 zumindest als **Schutzgesetze iSd § 1311 ABGB** einzuordnen, deren Verletzung den Zahlungsdienstleister schadenersatzpflichtig macht.

Ist der Zahlungsdienstleister wegen einer nicht ordnungsgemäßen Transaktionsüberwachung schadenersatzpflichtig, wird dem Betrugsopfer in den meisten Fällen aber ein **Mitverschulden** zur Last fallen, wodurch es letztendlich zu einer Teilung des Schadens nach Maßgabe des **§ 1304 ABGB** kommt.

Eine Verletzung der Vorgaben des § 2 VO (EU) 2018 kann beim Betrugsopfer auch zu einem **Irrtum** führen, der das Opfer zu einer **Anfechtung des Zahlungsauftrags** berechtigt.[36]

4.4 Verbands- und Musterklagen

Das BMASGPK hat den VKI bislang mit **Verbandsklagen** gegen drei Banken beauftragt. In diesen Verfahren wird die **Geschäftspraxis der Banken inkrimiert,** auch in Fällen, in denen nach den Transaktionsprotokollen unstrittig nicht autorisierte Zahlungsvorgänge vorliegen, eine Berichtigung des Kundenkontos mit der Begründung abzulehnen, der Bank stünden Schadenersatzansprüche gemäß § 68 Abs. 3 ZaDiG 2018 zu, weil das Opfer den Missbrauch grob schuldhaft ermöglicht habe. Eine solche Aufrechnung ist nach der Rechtsprechung des OGH zu § 67 Abs. 1 ZaDiG 2018 aber unzulässig.[37]

Das HG Wien und das OLG Wien haben der Klage des VKI i**n einem Verfahren** in den beiden ersten Instanzen stattgegeben. Dieses Verfahren ist seit Frühjahr 2024 zu 5 Ob 54/24p beim OGH anhängig und dort wegen eines seit 3. Februar 2025 beim EuGH zu C-70/25 anhängigen Vorabentscheidungsersuchen**s** unterbrochen. Die beiden anderen Verbandsverfahren sind noch beim Handelsgericht Wien in erster Instanz anhängig und derzeit ebenfalls unterbrochen. Im Vorabentscheidungsverfahren liegen seit 5. März 2026 die Schlussanträge des Generalanwalts vor, die den Standpunkt des Verbraucherschutzes vollinhaltlich bestätigen.[38]

[36] Vgl *Koch/Oppitz*, ÖBA 2024, 564 (583).
[37] OGH 8 Ob 106/20a zu den Klauseln 4,5,7 und 8; *Koch*, ÖBA 2019, 106 (113 f); *Kodek*, ÖBA 2021, 19 (35 ff).
[38] Schlussanträge des Generalanwalts in der Rechtssache *Tukowiecka* C-70/25.

Zusätzlich hat das BMASGPK den VKI bisher mit **15 Musterprozessen** gegen verschiedene Banken beauftragt, die bislang aber noch zu keinem Urteil geführt haben, da die Banken nach Einbringung der Klagen entweder den gesamten Schaden samt Kosten bezahlten oder ein für das Betrugsopfer günstiges Vergleichsangebot machten.

Im Mai 2025 brachte der VKI außerdem eine **Sammelklage** gegen die BAWAG PSK zu Gunsten von 24 Betrugsopfern ein und bereitete eine zweite Sammelklage für weitere 19 Opfer vor. In der Zwischenzeit ist eine für die Opfer günstige **Vergleichslösung** realistisch.

5 Vorgeschlagene Maßnahmen für einen verbesserten Schutz vor Phishing Angriffen

5.1 Informationen und Warnungen lösen das Problem nicht

Die österreichischen Banken und auch die Finanzmarktaufsicht (FMA) und die OeNB setzen derzeit in erster Linie auf eine verbesserte Information der Konsument:innen und auf Warnungen vor typischen Betrugsszenarien. Es hat sich aber auch bei den von der Ombudsstelle bearbeiteten Beschwerdefällen gezeigt, dass **bloße Warnmeldungen und Informationen nicht ausreichen**, um Konsument:innen wirksam vor Betrügereien im elektronischen Zahlungsverkehr zu schützen.

Ein großer Teil der Konsument:innen nutzt elektronische Zahlungsinstrumente, um Zahlungen möglichst schnell und bequem erledigen zu können. Warnungen werden daher, wie das auch mit anderen Informationen im elektronischen Geschäftsverkehr geschieht, meist weggeklickt oder ungelesen als gelesen bestätigt, zumal ihre Anzahl und ihr Umfang bei den meisten Banken überbordend sind. Außerdem beinhalten diese Warninformationen oft schwer nachvollziehbare Darstellungen oder sie sind zu allgemein gehalten.

Aus diesen Gründen wären aus der Sicht des Konsumentenschutzministeriums **in erster Linie andere Maßnahmen notwendig**, um Konsument:innen wirksam vor Phishing Angriffen zu schützen.

5.2 Verbesserung der Transaktionsüberwachung

In den meisten Beschwerdefällen mit nicht autorisierten Zahlungsvorgängen (Fallgruppe 2.1.) kam es unmittelbar nach der Registrierung eines neuen Telefons innerhalb weniger Minuten mit diesem Telefon zu mehreren Zahlungen mit häufig hohen Beträgen an (überwiegend ausländische) Empfänger, an welche die Opfer zuvor noch nie Zahlungen

getätigt hatten. Teilweise kam es zuvor auch zu Erhöhungen der vereinbarten Limits und/oder zu Umbuchungen vom Spar- auf das Zahlungskonto des Opfers.

Aber auch in vielen Fällen autorisierter Zahlungsvorgänge (Fallgruppen 2.2. und 2.3.) lagen **auffällige Abweichungen vom bisherigen Zahlungsverhalten** des Opfers und **Hinweise auf bereits bekannte Betrugsszenarien** vor. Trotzdem wurden die Zahlungen von der Bank nicht blockiert. Würden die Zahlungen in solchen Fällen erst nach einer Sicherheitsrückfrage beim Kunden/bei der Kundenin durchgeführt werden, könnte man einen **Großteil der Betrugsfälle verhindern**.

5.3 Ausrichtung der Zahlungsinstrumente auf die Bedürfnisse von Nutzer:innen mit geringeren digitalen Fähigkeiten

Die Wahrscheinlichkeit, Opfer eines Phishing Betrugs zu werden, und die Höhe der Schäden sind derzeit **bei älteren Nutzer:innen** von elektronischen Zahlungsinstrumenten und unerfahrenen Personen mit geringen digitalen Fähigkeiten **wesentlich höher** als bei digital erfahrenen Konsument:innen. Nutzer:innen mit geringen digitalen Fähigkeiten verstehen die Funktionsweise elektronischer Zahlungsinstrumente oft nur unzureichend und können dadurch leichter getäuscht werden.

Es wäre daher notwendig, elektronische Zahlungsinstrumente so auszugestalten und abzusichern, dass sie auch von Personen mit geringen digitalen Fähigkeiten **leicht verstanden** und **gefahrlos genutzt** werden können.

5.4 Neu registriertes Telefon kann erst nach einer Stunde für Zahlungen genutzt werden

Im Berichtszeitraum entstanden in 45 % der Fälle die Betrugsschäden durch nicht autorisierte Zahlungen, die mit dem Telefon der Betrüger **innerhalb weniger Minuten nach der Registrierung** dieses Telefons in Auftrag gegeben wurden.

Solche Schäden könnten daher verhindert werden, wenn nach der Registrierung eines neuen Geräts dieses **für eine bestimmte Zeit** noch nicht für Zahlungen und Limiterhöhungen verwendet werden könnte, wobei **eine verzögerte Nutzung von einer**

Stunde sachgerecht wäre. Dadurch hätte das Phishing Opfer eine erheblich höhere Chance, nach dem Erhalt der Information von der Registrierung des neuen Telefons den Betrug durch eine unverzügliche Sperrmeldung bei der Bank noch zu verhindern.

5.5 Zusätzliche Sicherheitsmaßnahmen bei der Registrierung eines neuen Mobiltelefons

Ein Teil der Banken wie vor allem die BAWAG PSK verlangte im Berichtszeitraum für die Registrierung eines neuen Mobiltelefons nur die gleiche Kundenauthentifizierung wie bei einzelnen elektronischen Zahlungen, obwohl das mit der Registrierung eines neuen Telefons verbundene **Missbrauchsrisiko**, soweit es um die Höhe des möglichen Schadens geht**, um ein Vielfaches höher** ist.

Zusätzliche Sicherheitsanforderungen für die Registrierung eines neuen Geräts verringern die Wahrscheinlichkeit erheblich, dass es Betrügern im Zuge eines Phishing Angriffs gelingt, ihr Telefon für das Online Banking oder die Zahlungs App des Opfers registrieren zu lassen.

5.6 Verbesserte Zusammenarbeit zwischen inländischen und ausländischen Zahlungsdienstleistern

In 77 % der Fälle ist zumindest ein:e Empfänger:in der betrügerischen Zahlungen im Ausland ansässig. Das zeigt, dass eine verbesserte Zusammenarbeit zwischen inländischen und ausländischen Zahlungsdienstleistern erforderlich ist, um die Wahrscheinlichkeit solcher Betrugsfälle zu verringern.

6 Zusammenfassung der wichtigsten Ergebnisse

- Im Zeitraum vom **1. Jänner 2023 bis zum 31. Dezember 2025** wandten sich insgesamt **717 Konsument:innen**, die Opfer eines Phishing Angriffs wurden, mit einer (schriftlichen oder elektronischen) Beschwerde an die Ombudsstelle. In 76 % dieser Fälle intervenierte die Ombudsstelle bei der Bank des Opfers.

- Die **Rechte der Opfer** hängen davon ab, ob es sich um vom Opfer **autorisierte oder um nicht autorisierte Zahlungen** handelt. Im Fall nicht autorisierter Zahlungen trägt den Schaden grundsätzlich die Bank, im Fall autorisierter Zahlungen grundsätzlich das Opfer.

- **50 %** der Interventionsfälle lagen **nicht autorisierte Zahlungen** zugrunde, 50 % der Interventionsfälle autorisierte Zahlungen.

- In **63,24 %** der Betrugsfälle kam es zu missbräuchlichen **Kartenzahlungen** (Debit- und Kreditkarten), in **28,37 %** zu missbräuchlichen **Überweisungen** (SEPA- und Echtzeitüberweisung).

- In **77 %** der Fälle befand sich der oder (bei mehreren) mindestens ein **Zahlungsempfänger im Ausland**.

- Im Durchschnitt kam es zu ca. **4,3 missbräuchlichen Zahlungen pro Betrugsfall**.

- Der **Durchschnittsschaden** betrug pro Betrugsfall **4.333,38 Euro**. Bei Fällen mit nicht autorisierten Zahlungen lag er bei 4.723,29 Euro, bei Fällen mit autorisierten Zahlungen bei 4.013,06 Euro.

- Bei den verschiedenen Zahlungsarten war der Durchschnittsschaden sehr unterschiedlich. Am höchsten war der Durchschnittsschaden bei missbräuchlichen **SEPA Überweisungen** mit **8.513,82 Euro**, am niedrigsten bei missbräuchlichen Kreditkartenzahlungen mit 2.292,85 Euro.

- Bei den Betrugsopfern handelte es sich zu **54 % um Frauen** und zu **46 % um Männer**.

- Das **Durchschnittsalter der Betrugsopfer** betrug **47,82 Jahre**, wobei Frauen im Durchschnitt 46,4 und Männer im Durchschnitt 49,7 Jahre alt waren.

- Bei den einzelnen Banken war das Durchschnittsalter der Betrugsopfer **sehr unterschiedlich**. Bei Kund:innen der BAWAG PSK war es **um fast 12 Jahre höher** als bei den Kund:innen des Raiffeisensektors.

- Das **Risiko des einzelnen Verbrauchers/der einzelnen Verbraucherin,** Opfer eines Phishing Angriffs zu werden, und die Höhe der Schäden sind **bei älteren Personen ab ca. 50 Jahren wesentlich höher.**

- **45 % der Betrugsopfer waren Kund:innen der BAWAG PSK**. Außerdem war der Anteil von Beschwerdefällen mit nicht autorisierten Zahlungen bei der BAWAG PSK im Berichtszeitraum mit 70 % außerordentlich hoch. Nachdem die BAWAG PSK im Herbst 2025 ihre Sicherheitsvorkehrungen verschärft hatte, ging ihr Anteil an den Beschwerden aber stark zurück.

- In **67 % der Interventionsfälle (= 363 Fälle)** kam es zu einer **Einigung** zwischen dem Konsumenten/der Konsumentin und der Bank. In 305 Fällen reichte dafür eine außergerichtliche Intervention aus, in **58 Fällen** war auch eine Beauftragung des VKI mit einer **Sammel- oder Einzelklage** notwendig.

- Im Fall einer Einigung übernahm der **Raiffeisensektor** im Durchschnitt **86 % des Schadens**, die BAWAG PSK 82 %, die ERSTE Bank und die Sparkassen 62 % und die UniCredit Bank Austria 47 %.

- Bloße Warnmeldungen und Informationen reichen für einen wirksamen Schutz der Konsument:innen vor Phishing Angriffen nicht aus. Notwendig wären vor allem eine **Verbesserung der Transaktionsüberwachung** und eine Ausrichtung der Zahlungsinstrumente auf die Bedürfnisse von **Nutzer:innen mit geringeren digitalen Fähigkeiten**.

- Außerdem sollte ein **neu registriertes Gerät** erst nach einer Stunde für Zahlungen genutzt werden können und es sollten **zusätzliche Sicherheitsmaßnahmen** bei der Registrierung eines neuen Geräts vorgesehen werden.

- Schließlich sollte die **Zusammenarbeit** zwischen inländischen und ausländischen Zahlungsdienstleistern verbessert werden.