Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

Bericht zu Phishing Betrugsfällen

Tätigkeitsbericht der Ombudsstelle für Zahlungsprobleme im BMSGPK zu Phishing Betrugsfällen im elektronischen Zahlungsverkehr für den Zeitraum 1. Jänner 2023 bis 30. September 2024

Wien, Oktober 2024

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.

Obwohl das Risiko von Missbräuchen nach dem Gesetz grundsätzlich von den Banken zu tragen wäre, überwälzen diese in der Praxis die Schäden oft zur Gänze auf die Konsument:innen. Um den Schutz der Betrugsopfer zu verbessern, erklärte sich das BMSGPK daher bereit, **ab Jänner 2023** über die bei ihm eingerichtete **Ombudsstelle für Zahlungsprobleme**[1] (phishing@sozialministerium.at) als **Anlaufstelle** für solche Beschwerden zur Verfügung zu stehen.

Dadurch sollen die Geschädigten bei der Geltendmachung und Durchsetzung ihrer Rechte bestmöglich beraten und unterstützt werden. Außerdem hat das BMSGPK in Fällen, in denen Banken zu keinen einvernehmlichen Lösungen bereit sind, die Möglichkeit, beim Verein für Konsumenteninformation (VKI) **Verbandsklagen** und **Musterprozesse** in Auftrag zu geben.

Vom **1. Jänner 2023 bis 30. September 2024** haben sich insgesamt **457 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 BMSGPK 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**. In einem besonders häufig vorkommenden Szenario erhält das Opfer eine SMS oder (seltener) eine E-Mail, in der es zu einer **Aktualisierung 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 verständlicherweise 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.

Auf der Phishing-Website wird das Opfer zur Eingabe und Bestätigung seiner Zugangsdaten aufgefordert. **Tatsächlich stimmt das Opfer aber ungewollt der Registrierung des Mobiltelefons der Betrüger zu**, die dadurch uneingeschränkten Zugriff auf das Online Banking oder die Zahlungskarte des Opfers haben. Die Betrüger können dann 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.

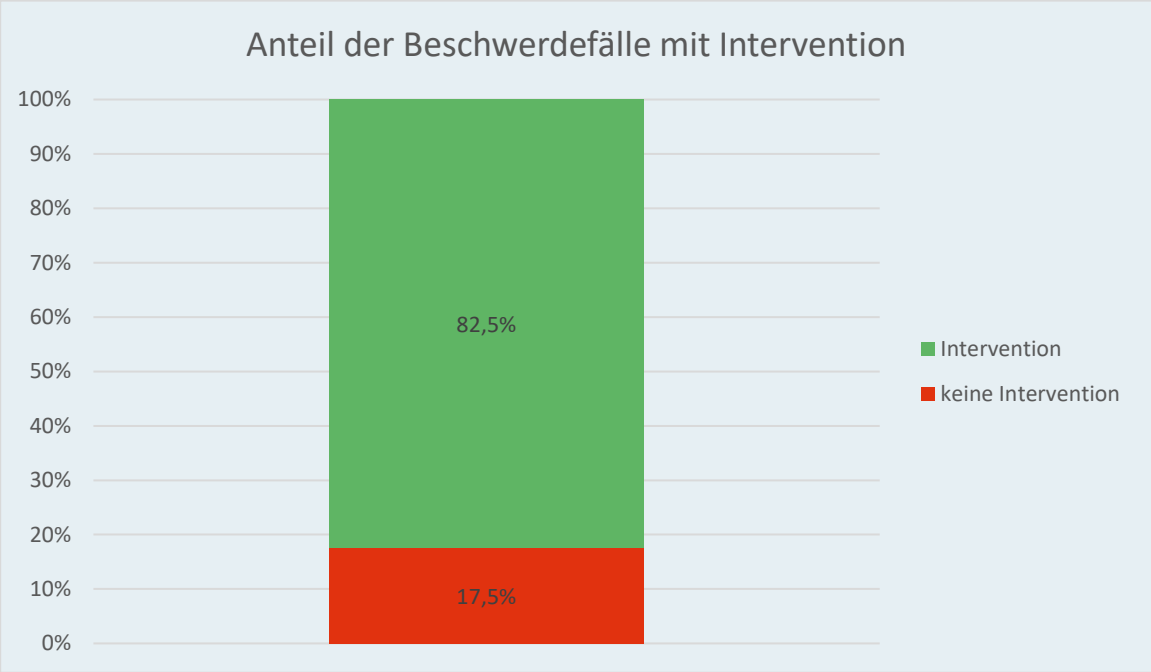
Die Opfer werden zwar in der Regel von ihrer Bank von der Registrierung des neuen Telefons in einer SMS-Nachricht und/oder E-Mail verständigt. Aber auch dann, wenn das Opfer unverzüglich reagiert, kann es den Missbrauch meist nicht mehr verhindern, weil die missbräuchlichen Zahlungen und allfälligen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

3 Auswertung der Beschwerdefälle

3.1 Zahl der Beschwerden und Interventionsfälle

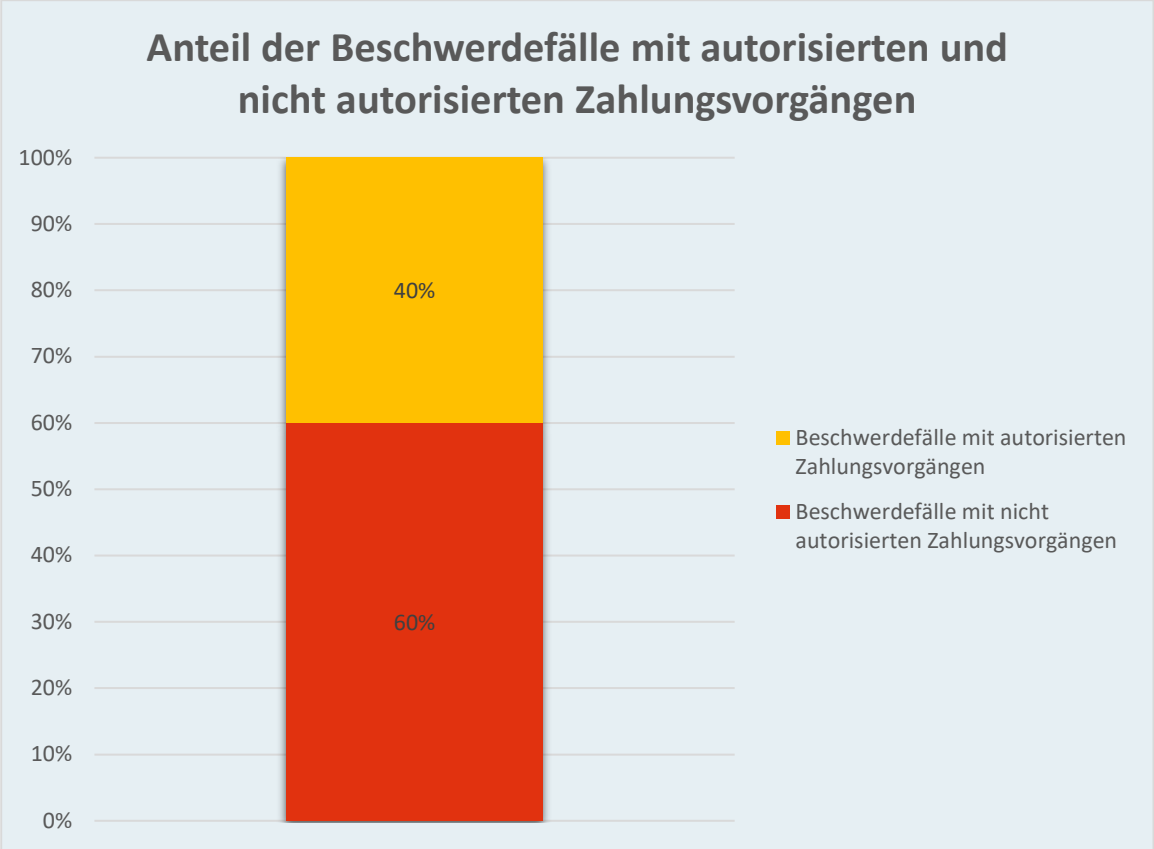
Insgesamt haben sich im Berichtszeitraum **457 Verbraucher:innen** mit einer Beschwerde zu einem Phishing Fall an die Ombudsstelle gewandt:

- In **377 Fällen** intervenierte die Ombudsstelle für die Betrugsopfer bei ihrer Bank.
- In **80 Fällen** kam es zu keiner Intervention, weil es bereits zuvor zu einer Einigung zwischen dem:der Kunden:in und der Bank gekommen war, die Opfer anwaltlich vertreten waren oder sie der Ombudsstelle nicht alle für eine Intervention notwendigen Unterlagen und Informationen übermittelten.



3.2 Nicht autorisierte und autorisierte Zahlungsvorgänge

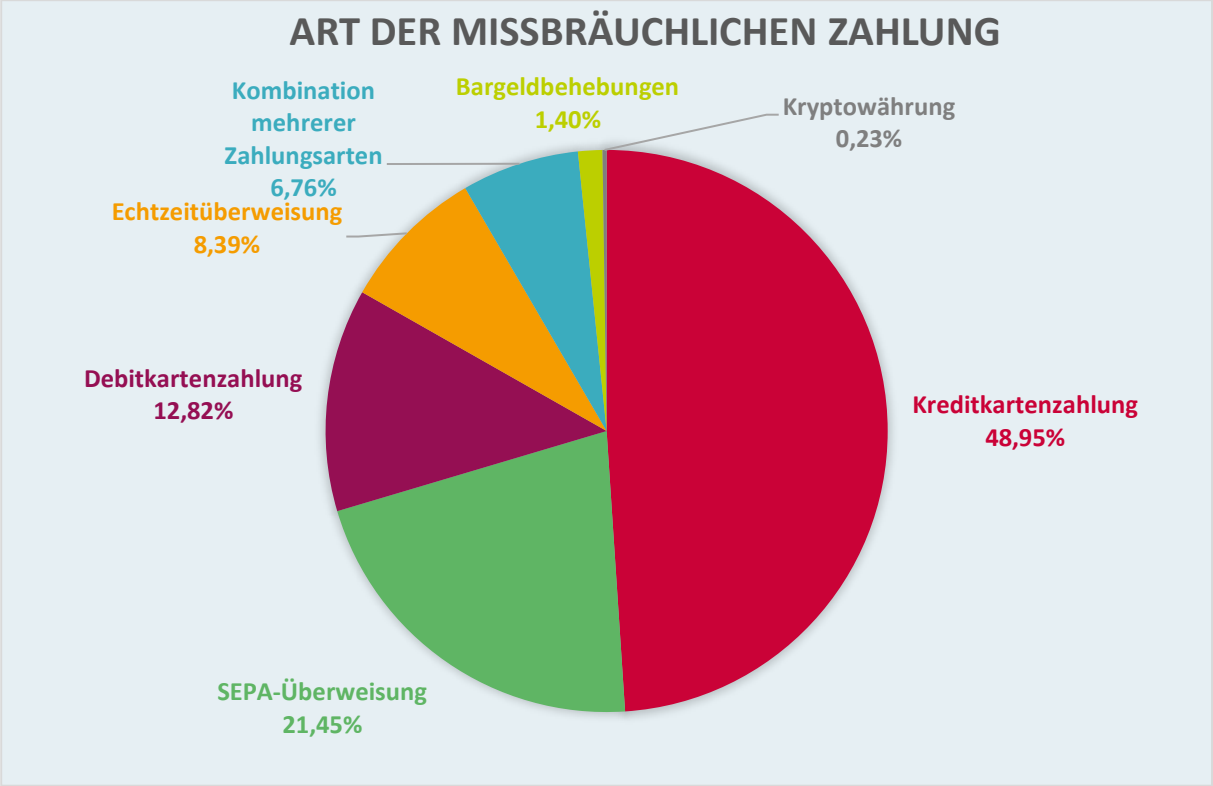
- 60 % der Interventionsfälle lagen nicht autorisierte Zahlungen zugrunde.
- 40 % der Interventionsfälle lagen autorisierte Zahlungen zugrunde.



3.3 Art der Zahlungen und Ort des Zahlungsempfängers

Bei den missbräuchlichen Zahlungen kann es sich handeln um:

- Kreditkartenzahlungen,
- SEPA Überweisungen,
- Debitkartenzahlungen,
- Echtzeitüberweisungen,
- mehrere verschiedene Zahlungsarten (z.B. Echtzeitüberweisungen + Debitkartenzahlungen),
- Bargeldbehebungen an Geldausgabeautomaten mit der auf dem Telefon der Betrüger digitalisierten Debitkarte oder physisch gestohlenen Debitkarte,
- Zahlungen in Kryptowährung



In 22 % der Fälle befand sich der oder (bei mehreren) mindestens ein Zahlungsempfänger im **Inland**. In 60 % der Fälle befand sich der oder (bei mehreren) mindestens ein Zahlungsempfänger im **EU-Ausland**. In 18 % der Fälle befand sich der oder (bei mehreren) mindestens ein Zahlungsempfänger in einem **Drittland**.

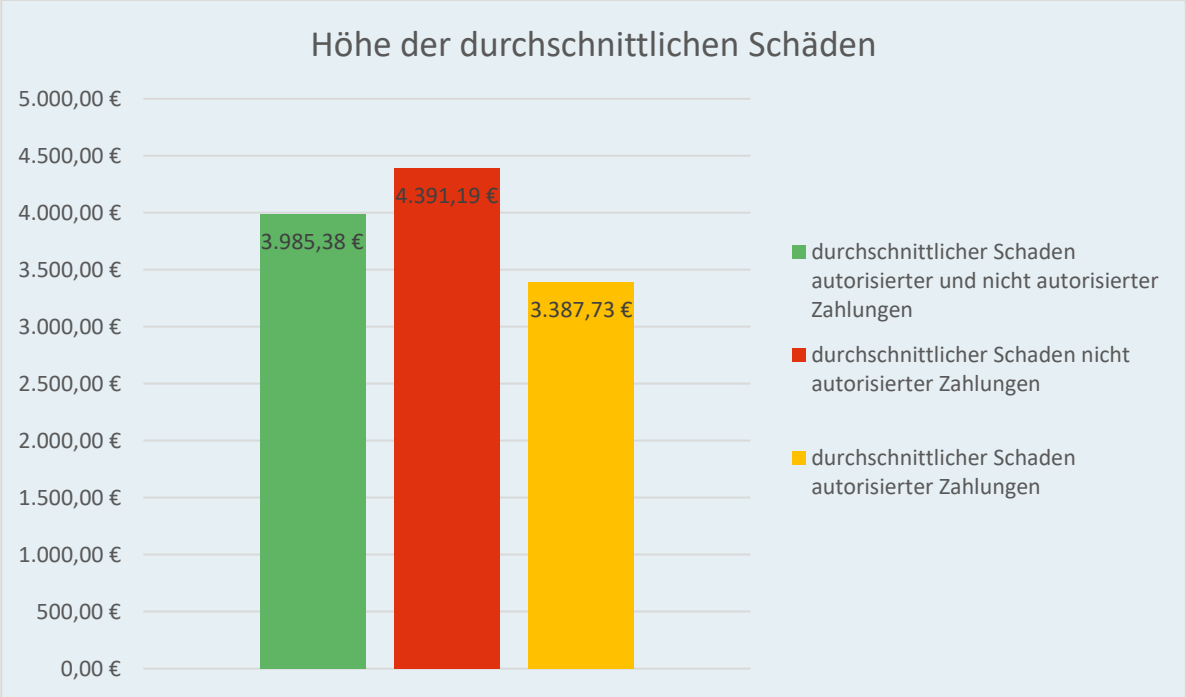
3.4 Anzahl der missbräuchlichen Zahlungen pro Beschwerdefall

- Bei den von der Ombudsstelle bearbeiteten Beschwerdefällen kam es pro Fall zu zwischen einer und 140 missbräuchlichen Zahlungen.
- Im **Durchschnitt** gelang es den Betrüger:innen pro Phishing-Angriff **5,08 missbräuchliche Zahlungen zu veranlassen**.

3.5 Höhe der Schäden

Der **Durchschnittsschaden** betrug

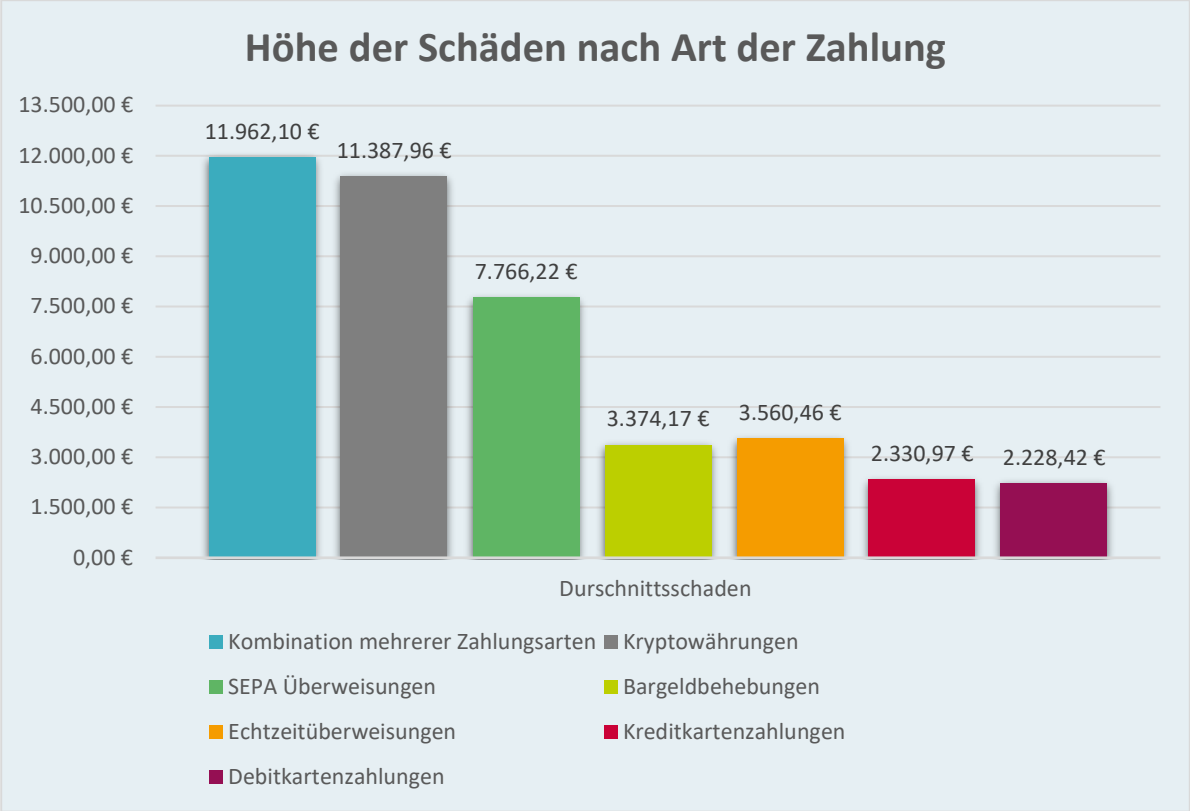
- pro Beschwerdefall 3.985,38 Euro;
- bei Fällen mit **nicht autorisierten Zahlungen 4.391,19 Euro**;
- bei Fällen mit **autorisierten Zahlungen 3.387,73 Euro**.



Da die Betrüger bei nicht autorisierten Zahlungen nach dem erfolgreichen Phishing Angriff mit ihrem eigenen Telefon direkt und selbständig auf das Konto oder die Zahlungskarte des Opfers zugreifen konnten, ist der Durchschnittsschaden in solchen Fällen wesentlich höher.

Der **Durchschnittsschaden** betrug bei Fällen

- mit mehreren verschiedenen Zahlungsarten 11.962,10 Euro;
- mit Kryptowährungen 11.387,96 Euro;
- mit SEPA Überweisungen 7.766,22 Euro;
- mit Echtzeitüberweisungen 3.560,46 Euro;
- mit Bargeldbehebungen 3.374,17 Euro;
- mit Kreditkartenzahlungen 2.330,97 Euro;
- mit Debitkartenzahlungen 2.228,42 Euro.



- Bei Betrugsfällen mit mehreren Arten von Zahlungen ist der Durschschnittsschaden daher am höchsten, was zu erwarten war.
- Da Echtzeitüberweisungen als anfälliger für Missbräuche gelten, ist es zumindest auf den ersten Blick überraschend, dass der Durchschnittsschaden bei Betrugsfällen mit SEPA Überweisungen um ein Vielfaches höher als bei Fällen mit Echtzeitüberweisungen war. Eine mögliche Erklärung wäre, dass die 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.

3.6 Geschlecht der Betrugsopfer

Bei den Betrugsopfern handelte es sich in

- 259 Fällen (= **56,67 %**) um **Frauen** und
- 198 Fällen (= **43,33 %)** um **Männer**.

Der **Anteil der weiblichen Betrugsopfer ist daher signifikant höher**. Das erklärt sich damit, dass sich ein wesentlicher Teil der Phishing Angriffe gegen Nutzer:innen von **Verkaufsplattformen** wie Vinted oder willhaben richtet, bei denen es sich überwiegend um Frauen handelt. Von den Betrugsopfern, die eine Verkaufsplattform nutzten, waren 86,3 % Frauen.

3.7 Alter der Betrugsopfer

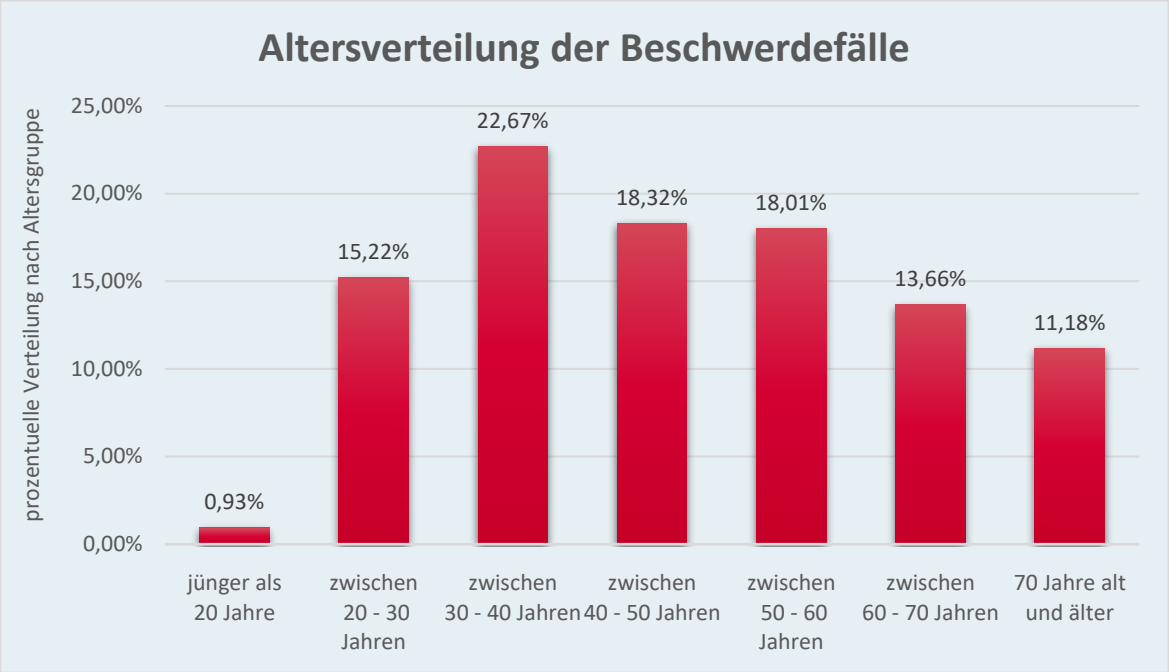
Die Betrugsopfer waren zwischen 14 und 94 Jahren alt. Das **Durchschnittsalter** betrug **47,13 Jahre**, wobei Frauen im Durchschnitt 45,6 und Männer im Durchschnitt 49,2 Jahre alt waren.

Das **Durchschnittsalter männlicher Betrugsopfer** ist daher um **3,6 Jahre höher** als das weiblicher Opfer. Eine mögliche Erklärung ist, dass bei älteren Personen innerhalb der Familie Zahlungen immer noch vorwiegend von Männern durchgeführt werden.

Von den Betrugsopfern waren

- 0,93 % jünger als 20 Jahre,
- 15,22 % zwischen 20 und 30 Jahre alt;
- 22,67 % zwischen 30 und 40 Jahre alt;
- 18,32 % zwischen 40 und 50 Jahre alt;

- 18,01 % zwischen 50 und 60 Jahre alt;
- 13,66 % zwischen 60 und 70 Jahre alt;
- 11,18 % 70 Jahre alt und älter.



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:der einzelnen Verbraucher:in**,** Opfer eines Phishing Angriffs zu werden, **bei älteren Personen ab ca. 50 Jahren** aber **wesentlich höher**.

Bei den einzelnen Banken lag das Durchschnittalter der Betrugsopfer

- bei der BAWAG PSK (inklusive easybank und PayLife) bei 52,29 Jahren;
- bei der UniCredit Bank Austria (inklusive Card Complete) bei 47,89 Jahren;
- bei der ERSTE Bank und den Sparkassen bei 40,55 Jahren;
- beim Raiffeisensektor (Raiffeisen CardService, Raiffeisenlandesbanken und alle anderen Raiffeisenbanken) bei 36,42 Jahren.

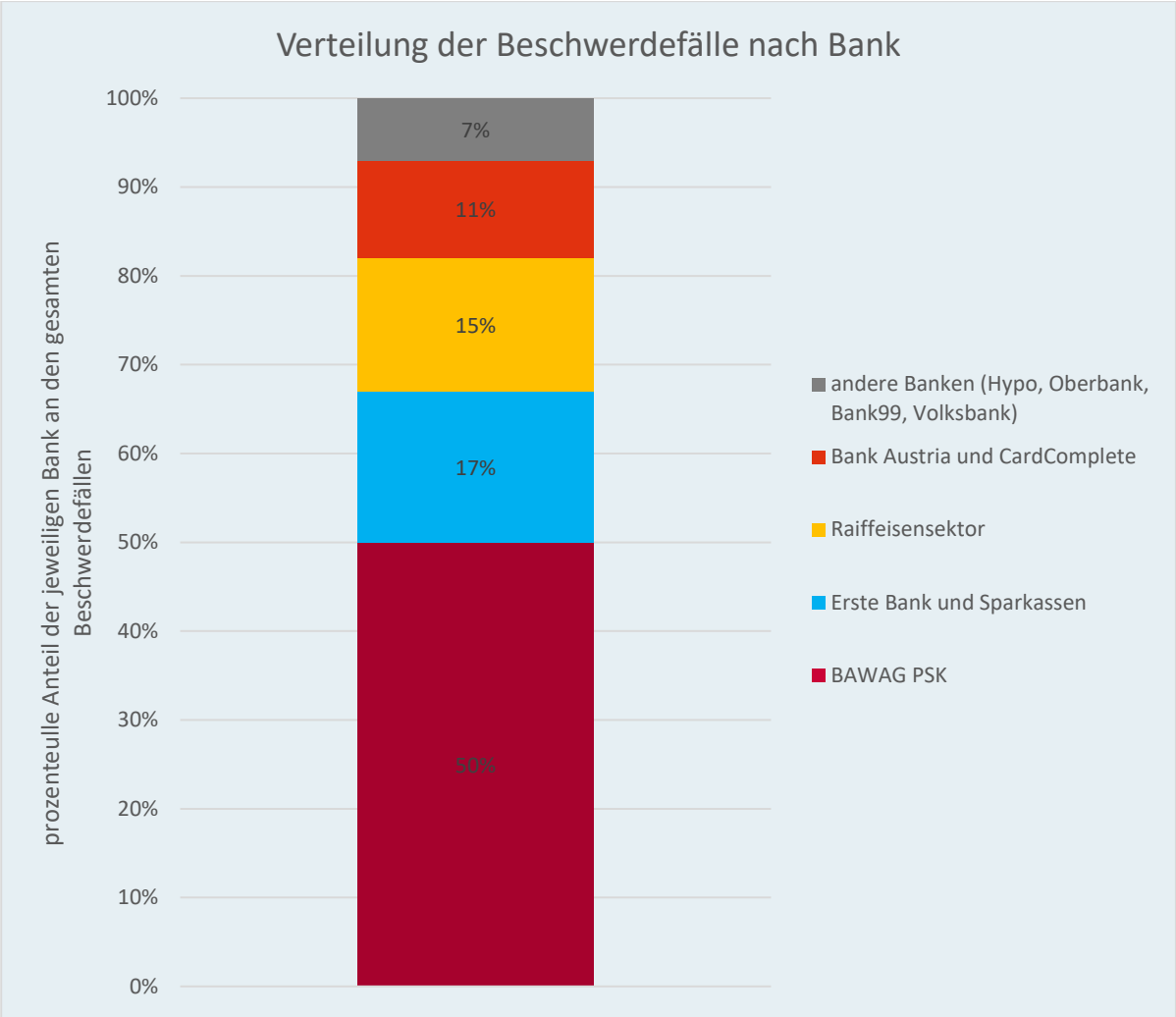
Die Kund:innen des **Raiffeisensektors**, die Opfer eines Phishing Angriffs wurden, hatten daher ein fast **16 Jahre geringeres Durchschnittsalter** als die der **BAWAG PSK**. Das könnte entweder am unterschiedlichen Durchschnittsalter der Kund:innen der jeweiligen Bank oder daran liegen, dass die elektronischen Zahlungsintrumente der BAWAG PSK nicht

ausreichend auf die Bedürfnisse von Nutzer:innen mit geringeren digitalen Fähigkeiten wie älteren Menschen ausgerichtet sind.

3.8 Betroffene Banken und deren Sicherheit

Die Beschwerdefälle teilten sich **auf die einzelnen Banken** wie folgt auf:

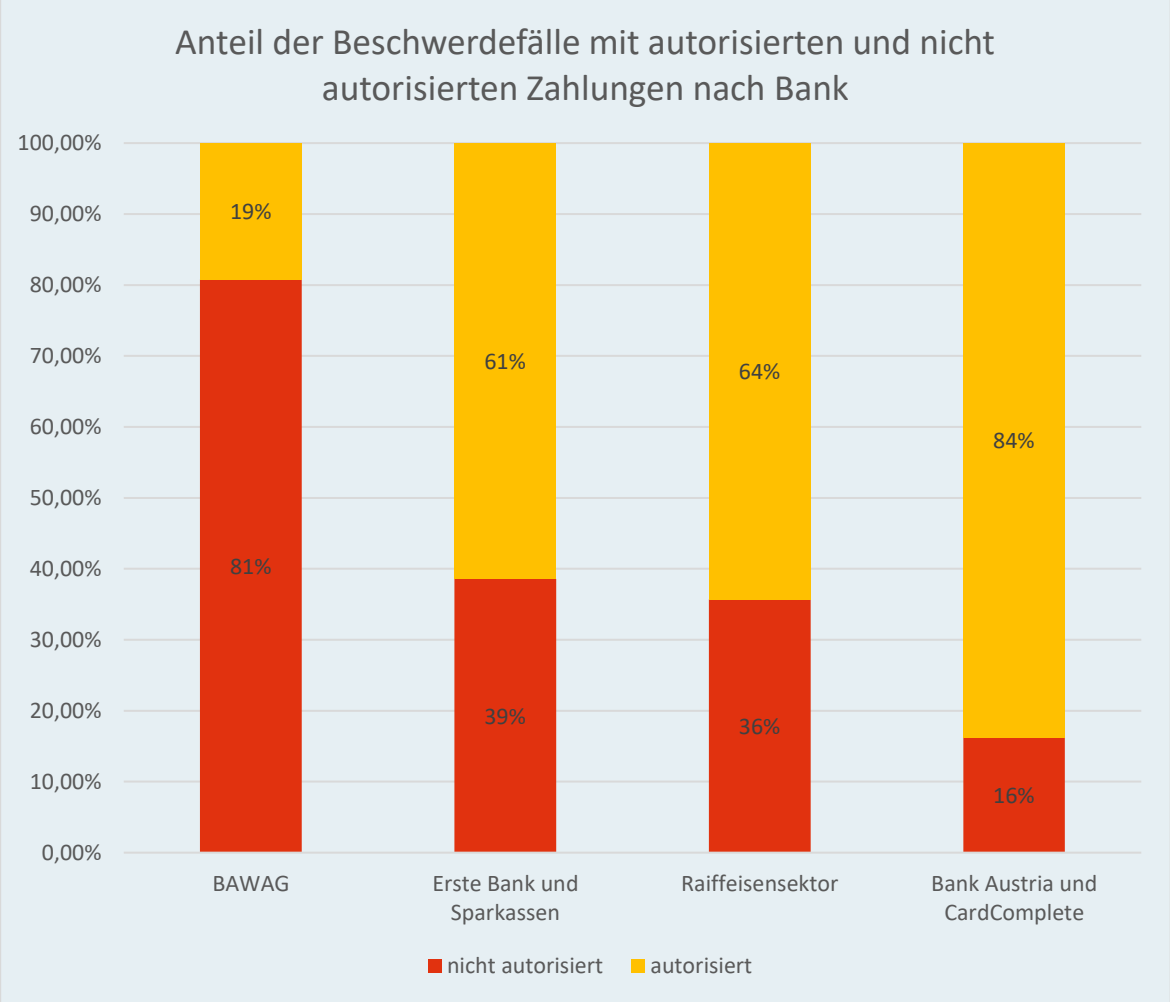
- **50 %** waren Kund:innen **der BAWAG PSK** (inklusive easybank und PayLife),
- 17 % waren Kund:innen der ERSTE Bank und Sparkassen,
- 15 % waren Kund:innen des Raiffeisensektors,
- 11 % waren Kund:innen der UniCredit Bank Austria mit Card Complete,
- 7 % waren Kund:innen anderer Banken (Hypo, Oberbank, bank99, Volksbank, etc).



Phishing Betrugsfälle sind daher in Österreich **zu etwa zur Hälfte ein Problem der BAWAG PSK** und ihrer Kund:innen, die wesentlich häufiger als Kund:innen anderer Banken Opfer eines Phishing Angriffs werden.

Der **Anteil der Beschwerdefälle mit nicht autorisierten Zahlungen** lag bei

- der **BAWAG PSK** (inklusive easybank und PayLife) bei **81 %**,
- der ERSTE Bank und Sparkassen bei 39 %,
- der Raiffeisensektor 36 %,
- der UniCredit Bank Austria mit Card Complete bei 16 %



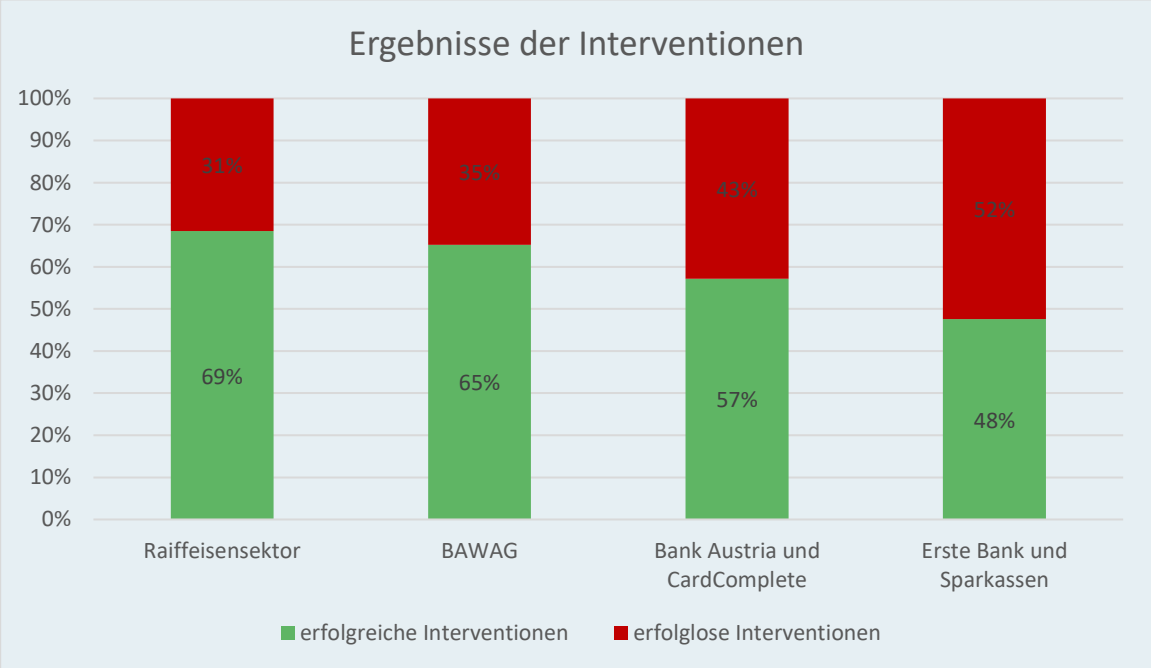
Da es bei nicht autorisierten Zahlungen den Betrügern im Zuge des Phishing Angriffs gelingt, sich unmittelbaren Zugriff auf das Konto und/oder die Zahlungskarte des Opfers zu verschaffen und dadurch die von der Bank zum Schutz gegen Betrügereien getroffenen Sicherheitsmaßnahmen zu umgehen, ist der Anteil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

Der Anteil von Beschwerdefällen mit nicht autorisierten Zahlungen war **bei der BAWAG PSK mit 81 % exorbitant hoch.** Er ist zum Beispiel ca. fünf Mal so hoch wie bei der UniCredit Bank Austria. Die betrugssichere Ausgestaltung der Zahlungsinstrumente und die Transaktionsüberwachung sind daher bei der BAWAG PSK offensichtlich erheblich schlechter als bei anderen Banken.

3.9 Ergebnis der Interventionen der Ombudsstelle

In **62 % der Beschwerdefälle** führte die Intervention der Beschwerdestelle zu einer **außergerichtlichen Einigung** zwischen dem:der Konsument:in und der Bank. Diese Einigung konnte im Schnitt nach 15 Tagen erreicht werden. Die Erfolgsquote bei den einzelnen Banken ist sehr unterschiedlich. Sie lag

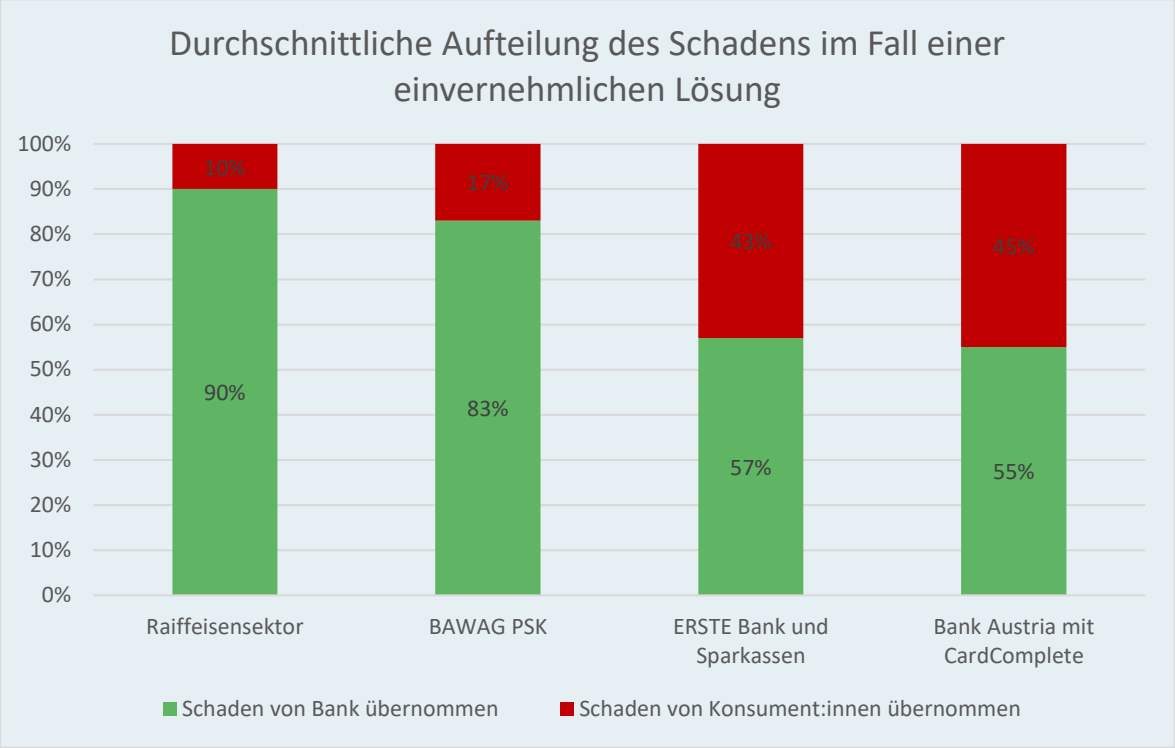
- beim **Raiffeisensektor** bei **69 %,**
- bei der BAWAG PSK (inklusive easybank und PayLife) bei 65 %,
- bei der UniCredit Bank Austria mit Card Complete bei 57 %,
- bei der ERSTE Bank und den Sparkassen bei 48 %.



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

- **Raiffeisensektor 90 %**

- BAWAG PSK 83 %
- ERSTE Bank und Sparkassen 57 %, und
- UniCredit Bank Austria mit Card Complete 55 %.



Bei der **ERSTE Bank** besteht daher die **geringste Bereitschaft, Betrugsopfer zu entschädigen**. Bei dieser Bank war nur in 48 % der Beschwerdefälle eine einvernehmliche außergerichtliche Lösung möglich. Außerdem übernahm die ERSTE Bank in solchen Fällen lediglich 57 % der Schäden.

4 Rechtliche Rahmenbedingungen

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 Authentifizierungsmerkmale **zugestimmt** hat 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:der Verbrauchers:erin in Verbindung mit dem geheimen PIN/dem Fingerabdruck/der Gesichtserkennung verwendet.

Wenn es den Betrügern im Zuge des Phishing Angriffs gelingt, ihr Mobiltelefon für das Online Banking des:der Verbrauchers:erin registrieren zu lassen oder die Kredit- oder Debitkarte des Opfers auf dem Telefon der Betrüger digital zu hinterlegen, und die missbräuchlichen Zahlungen dann mit dem Telefon der Betrüger autorisiert werden (siehe Punkt 2), liegen daher nicht autorisierte Zahlungen vor. Ebenso liegt eine nicht autorisierte Zahlung vor, wenn sie zwar vom:von der Verbraucher:in freigegeben wurde, ihm:ihr dabei aber der Betrag, der Empfänger und die Währung der Zahlung angezeigt wurden.

Bei den von der Ombudsstelle bearbeiteten Beschwerdefällen handelte es sich in

- **60 %** der Fälle um **nicht autorisierte Zahlungen** und
- **40 % der Fälle** um **autorisierte Zahlungen**.

4.2 Rechte der Betrugsopfer bei nicht autorisierten Zahlungen

4.2.1 Berichtigungsanspruch

Zeigt die:der Konsument:in 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 (das sind Transaktionsprotokolle, die die ordnungsgemäße Authentifizierung und Ausführung der Zahlung nachweisen) vorlegen. Eine Berichtigungspflicht nach Ablauf der Frist des § 67 Abs. 1 besteht gemäß § 67 Abs. 2 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 war es zwischen der Bank und den Konsument:innen **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 Telefon des Opfers, sondern ein fremdes Telefon verwendet wurde, das im Zuge des Phishing Angriffs neu registriert wurde.

In solchen Fällen ändert ein **Schadenersatzanspruch**, der der Bank gegenüber der:dem Konsument:in 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.[2] 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.

[2] 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).

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 ihren eigenen (vermeintlichen) Schadenersatzanspruch gegen den Berichtigungsanspruch der Konsument:innen auf, so dass die gesetzlichen Vorgaben zum Schutz der Konsument:innen im Ergebnis vollständig entwertet werden.

4.2.3 Häufig kein grobes Verschulden der:des Konsument:in

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.[3] Gibt die:der Kund:in personalisierte Sicherheitsmerkmale im Zuge eines Phishing-Angriffs weiter, hängt es von den Umständen des Einzelfalls ab, ob ihm grobe Fahrlässigkeit zur Last fällt oder nicht.[4] Auch die vollständige Weitergabe von Verfügernummer und persönlichen Daten auf einer Phishing-Website ist daher nicht unbedingt grob fahrlässig.[5]

Grobe Fahrlässigkeit liegt jedenfalls nur dann vor, wenn es für die:den Kund:in **erkennbar** war, dass sein Verhalten eine missbräuchliche Verwendung des Zahlungsinstruments wahrscheinlich macht.[6] Diese Voraussetzung ist unter Berücksichtigung der persönlichen Verhältnisse der:des betreffenden Kund:in und ihren:seinen Lebensgewohnheiten (insbesondere auch ihren:seinen bisherigen Erfahrungen mit solchen Zahlungsinstrumenten) zu beurteilen.[7]

---

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

Geht man von diesem Maßstab aus, liegt bei einem großen Teil der bei der Ombudsstelle für Zahlungsprobleme bisher 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 nutzen die Betrüger:innen auch gezielt die Unkenntnis der Opfer in unbekannten Situationen aus (zB beim Verkauf von Gebrauchtgegenständen auf Verkaufsplattformen).

4.2.4 Selbst bei grober Fahrlässigkeit haftet der:die Verbraucher:in in einer Reihe von Fällen nicht

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

keine **starke Kundenauthentifizierung** (Zwei Faktor Authentifizierung) erfolgt ist,[8]
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,[9]
die nicht autorisierte Zahlung von der Bank durchgeführt wurde, **nachdem** der:die Verbraucher:in den **Missbrauch angezeigt hatte,** [10]
keine ordnungsgemäße Transaktionsüberwachung stattfand;[11]
die mit dem Verbraucher vereinbarten Limits überschritten wurden.

4.3 Allenfalls Schadenersatzansprüche der Betrugsopfer bei autorisierten Zahlungen

Bei **autorisierten Zahlungen** steht der Bank ein **Aufwandersatzanspruch** gemäß § 1014 ABGB zu, der einen Berichtigungsanspruch des:der Verbraucher:in ausschließt. Der Schaden ist daher grundsätzlich vom:von der Verbraucher:in zu tragen, der:die jedoch

[8] Siehe § 68 Abs. 5 ZaDiG 2018.
[9] Siehe § 68 Abs. 6 ZaDiG 2018.
[10] Siehe § 68 Abs. 6 ZaDiG 2018.
[11] Welche genauen Rechts- und Haftungsfolgen eine nicht ordnungsgemäße Transaktionsüberwachung hat, ist derzeit aber noch strittig und muss erst ausjudiziert werden (siehe Punkt 2.3.).

unter Umständen Schadenersatzansprüche gegen die Bank geltend machen kann, wenn diese keine ordnungsgemäße Transaktionsüberwachung durchgeführt hat.

Gemäß **Art. 2 der delegierten Verordnung (EU) 2018/389** müssen Zahlungsdienstleister:innen über Transaktionsüberwachungsmechanismen verfügen, die ihnen die Erkennung nicht autorisierter oder betrügerischer Zahlungsvorgänge ermöglichen. Diese Überwachung muss bei jeder Kundenauthentifizierung automatisch und in Echtzeit stattfinden, um betrügerische Zahlungsvorgänge zu erkennen und zu verhindern.[12] Dabei muss sich der Zahlungsdienstleister am Leitbild eines normalen Zahlungsvorgangs orientieren und Abweichungen erkennen und auf diese reagieren. Zu den Minimalanforderungen gehört es, den Zahlungsbetrag auf Abweichungen gegenüber den bisherigen Zahlungsgewohnheiten der betroffenen Kund:innen zu überprüfen und bekannte Betrugsszenarien zu berücksichtigen.[13]

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. In vielen von der Ombudsstelle bearbeiteten Beschwerdefällen hatte der:die Geschädigte zuvor nie Zahlungen mit auch nur annähernd so hohen Beträgen in Auftrag gegeben. Außerdem hätte sich in einem Teil der Fälle wohl auch aus der Person und dem Sitzstaat der:des Zahlungsempfänger:in, dem Ort der Zahlung sowie einer häufig unüblichen Währung ein Betrugsverdacht ergeben müssen.

Hätte der Schaden bei Durchführung einer ordnungsgemäßen Transaktionsüberwachung verhindert werden können, stehen dem:der Verbraucher:in **Schadenersatzansprüche** gegen die Bank zu.[14] Da ihn:sie in den meisten Fällen ein **Mitverschulden** treffen wird, wird es in der Regel gemäß § 1304 ABGB zu einer **Teilung des Schadens** zwischen der Bank und dem:der Verbraucher:in kommen.

---

[12] Erwägungsgrund 1 der delegierten Verordnung; *Hofmann* in BeckOGK BGB § 675w Rz 24; *Baumbach/Hefermehl/Casper*, Recht des Zahlungsverkehrs24 Rz 416; *Linardatos* in MüKoHGB4 Online-Banking Rz 161).

[13] *Baumbach/Hefermehl/Casper*, Recht des Zahlungsverkehrs (2020) Rz 416; *Hofmann* in BeckOGK BGB § 675w Rz 24; *Mimberg* in Schäfer/Omlor/Mimberg, ZAG1 Rz 497; *Linardatos* in BeckOGK ZKG § 42 Rz 68.

[14] Es liegt entweder eine Verletzung einer nebenvertraglichen Sorgfaltspflicht oder zumindest eines Schutzgesetzes vor.

4.4 Vom Konsumentenschutzministerium in Auftrag gegebene Verbands- und Musterklagen

Das BMSGPK hat den VKI mit **Verbandsklagen** gegen drei große 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.[15]

Ein Verbandsklageverfahren befindet sich derzeit **bereits beim OGH**, nachdem die Unterinstanzen der Klage des VKI stattgegeben haben. Die beiden anderen Verfahren sind noch in erster Instanz anhängig.

Zusätzlich hat das Konsumentenschutzministerium den VKI mit einer Reihe von **Musterprozessen** beauftragt, die bislang noch zu keinem Urteil geführt haben. In den meisten Fällen bezahlte die Bank den gesamten Schaden samt Kosten nach Einbringung der Klage.

[15] 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).

5 Vorgeschlagene Maßnahmen für einen verbesserten Schutz vor Phishing Angriffen

5.1 Informationen und Warnungen lösen das Problem nicht

Die österreichischen Banken 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:nnen wirksam vor Betrügereien im elektronischen Zahlungsverkehr zu schützen.

Ein großer Teil der Konsument:innen nützt elektronische Zahlungsinstrumente, um Zahlungen möglichst schnell und bequem erledigen zu können. Warnungen werden daher wie andere Informationen im elektronischen Geschäftsverkehr auch weggeklickt oder ungelesen bestätigt, zumal ihre Anzahl und ihr Umfang bei den meisten Banken überbordend sind. Außerdem beinhalten diese Warninformationen oft nur 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

Die Banken müssten ihre **Transaktionsüberwachung verbessern**.

In den meisten Beschwerdefällen 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.

Es lagen daher **auffällige Abweichungen vom bisherigen Zahlungsverhalten** des Opfers und **eindeutige 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:bei der Kunden:in 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, ist 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

Ein großer Teil der Betrugsschäden entsteht durch nicht autorisierte Zahlungen, die mit dem Telefon der Betrüger **innerhalb weniger Minuten nach der Registrierung** dieses Telefons in Auftrag gegeben werden.

Solche Schäden könnten daher verhindert werden, wenn nach der Registrierung eines neuen Telefons 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

Die meisten Banken verlangen für die Registrierung eines neuen Mobiltelefons keine stärkere Kundenauthentifizierung als für einzelne elektronische 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.

Es wäre daher erforderlich, bei der Registrierung eines neuen Telefons entweder die Zwei Faktor Authentifizierung sicherer als bei einzelnen Zahlungen auszugestalten oder einen **zusätzlichen Faktor** zu verlangen. Das würde die Wahrscheinlichkeit erheblich verringern, dass es den Betrügern im Zuge eines Phishing Angriffs gelingt, ihr Telefon für das Online Banking oder die Zahlungskarte des Opfers registrieren zu lassen.

5.6 Verbesserte Zusammenarbeit zwischen inländischen und ausländischen Zahlungsdienstleistern

Da fast 80 % der betrügerischen Zahlungen einen Auslandsbezug haben, wäre eine verbesserte Zusammenarbeit zwischen in- und ausländischen Zahlungsdienstleistern erforderlich, um solche Fälle zu verringern.

6 Zusammenfassung der wichtigsten Ergebnisse

- Die im BMSGPK eingerichtete Ombudsstelle für Zahlungsprobleme ist **seit 1. Jänner 2023** Anlaufstelle für Phishing Opfer. Bis 30. September 2024 wandten sich insgesamt **457 Konsument:innen**, die Opfer eines Phishing Angriffs wurden, mit einer Beschwerde an die Ombudsstelle.
- 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. **60 %** der Interventionsfälle lagen **nicht autorisierte Zahlungen** zugrunde, 40 % der Interventionsfälle autorisierte Zahlungen.
- Der **Durchschnittsschaden** betrug pro Beschwerdefall **3.985,38 Euro**. Bei Fällen mit nicht autorisierten Zahlungen lag er bei 4.391,19 Euro, bei Fällen mit autorisierten Zahlungen bei 3.387,73 Euro.
- Bei den Betrugsopfern handelte es sich in zu **56,67 % um Frauen** und zu **43,33 % um Männer**. Der Anteil der weiblichen Betrugsopfer ist daher signifikant höher.
- Das **Durchschnittsalter der Betrugsopfer** betrug **47,13 Jahre**, wobei Frauen im Durchschnitt 45,6 und Männer im Durchschnitt 49,2 Jahre alt waren.
- Das **Risiko** des:der einzelnen Verbraucher:in**,** Opfer eines Phishing Angriffs zu werden, ist **bei älteren Personen ab ca. 50 Jahren wesentlich höher.**
- **50 % der Betrugsopfer waren Kund:innen der BAWAG PSK**, die wesentlich häufiger als Kund:innen anderer Banken Opfer eines Phishing Angriffs wurden.
- In **62 % der Beschwerdefälle** führte die Intervention der Ombudsstelle zu einer **außergerichtlichen Einigung** zwischen dem:der Konsument:in und der Bank.
- Die Bank mit der **geringsten Einigungsbereitschaft** war die **ERSTE Bank**, bei der trotz Intervention der Ombudsstelle nur in 48 % der Beschwerdefälle eine einvernehmliche außergerichtliche Lösung möglich war.
- Bloße Warnmeldungen und Informationen reichen für einen wirksamen Schutz der Konsument:innen nicht aus. **Notwendig wären** vor allem eine

Verbesserung der Transaktionsüberwachung und eine Ausrichtung der Zahlungsinstrumente an den Bedürfnissen von **Nutzer:innen mit geringeren digitalen Fähigkeiten**.

- Außerdem sollten **zusätzliche Sicherheitsmaßnahmen** bei der **Registrierung eines neuen Mobiltelefons** vorgesehen und die Zusammenarbeit zwischen inländischen und ausländischen Zahlungsdienstleistern verbessert werden.