**4030/A(E)**
**vom 15.05.2024 (XXVII. GP)**

# ENTSCHLIESSUNGSANTRAG

der Abgeordneten Mag. Christian Drobits,
Genossinnen und Genossen

betreffend **Maßnahmen zum Schutz älterer Bankkund:innen vor Mißbrauch im elektronischen Zahlungsverkehr**

Auf Basis der Entschließung des Nationalrats vom 15. Dezember 2021, 1189/E XXVII. GP, wurde im Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz in der Abteilung III/A/4 die Ombudsstelle Zahlungsprobleme, eine Erstanlaufstelle zur Unterstützung von Konsument:innen mit Zahlungsschwierigkeiten bei Krediten, eingerichtet.

Der erste Tätigkeitsbericht der Ombudsstelle für Zahlungsprobleme für den Zeitraum 1. Jänner 2022 bis 20. Juni 2023 behandelt unter anderem auch den Bereich von Missbräuchen im elektronischen Zahlungsverkehr. Es käme vermehrt zu Phishing-Attacken auf österreichische Konsument:innen und dadurch zu zahlreichen Betrugsfällen im elektronischen Zahlungsverkehr im Zusammenhang mit Kreditkarten, Debit Karten oder Echtzeitüberweisungen. *„Opfer dieser Betrügereien wurden zum überwiegenden Teil ältere Konsument:innen ab ca. 50 Jahre, die wenig Erfahrungen mit elektronischen Zahlungsmöglichkeiten wie dem Mobile-Banking hatten. Diese Unerfahrenheit und die dadurch bedingte Unsicherheit im Umgang mit solchen Zahlungsinstrumenten nützen Betrüger:innen gezielt aus. Allerdings werden Phishing-Angriffe von den Betrüger:innen immer aufwändiger und geschickter inszeniert, wodurch ihnen immer wieder auch durchaus erfahrene Nutzer zum Opfer fallen“*, ist dazu im Bericht nachzulesen.

Die gesetzlichen Regelungen zu derartigen Fällen skizziert der Bericht folgendermaßen:

**a) 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 (ordnungsgemäße Authentifizierung und Aufzeichnung der Zahlung; keine Störung durch einen technischen Fehler) 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.

**b) Allfällige Schadenersatzansprüche der Bank schließen den Berichtigungsanspruch des Konsumenten/der Konsumentin nicht aus**

In den meisten Fällen war es zwischen der Bank und den Konsument:innen nicht strittig, dass die reklamierte Zahlung nicht vom berechtigten Karten- oder Kontoinhaber:innen autorisiert wurde, sondern von den Betrüger:innen. In solchen Fällen ändert ein Schadenersatzanspruch, der der Bank gegenüber der:dem Konsument:in unter Umständen nach § 68 Abs. 3 ZaDiG 2018 wegen einer Verletzung von Sorgfaltspflichten zustehen könnte, nichts daran, dass das Konto sofort berichtigt werden muss.

Die Bank muss daher ihre allfälligen Schadenersatzansprüche gesondert geltend machen. Erst wenn die Bank ein rechtskräftiges Urteil erwirkt hat oder die:der Konsument:in freiwillig zustimmt, kann die Bank das Kundenkonto wieder mit der reklamierten Zahlung belasten.

Wie sich aus den der Ombudsstelle vorliegenden Beschwerden ergibt, halten sich in der Praxis fast alle Banken derzeit nicht an diese gesetzlichen Vorgaben, sondern lehnen eine Berichtigung des Kundenkontos mit der Behauptung ab, die:der Konsument:in habe den Missbrauch durch eine Verletzung von Sorgfaltspflichten ermöglicht und der Bank stünden daher Schadenersatzansprüche zu, die eine Berichtigungspflicht ausschließen würden.

**c) 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. 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.

Auch die vollständige Weitergabe von Verfügernummern und persönlichen Daten auf einer Phishing-Website ist daher nicht unbedingt grob fahrlässig. 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. Diese Voraussetzung ist unter Berücksichtigung der persönlichen Verhältnisse der:des betreffenden Kund:in und ihren:seinen Lebensgewohnheiten (insbesondere auch seinen bisherigen Erfahrungen mit solchen Zahlungsinstrumenten) zu beurteilen.

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 beim großen Teil der Geschädigten um ältere Menschen ab ca. 50 Jahren handelte, die wenig Erfahrungen im Umgang mit elektronischen Zahlungsinstrumenten hatten.

**d) Transaktionsüberwachung**

Aber selbst wenn im Einzelfall grobe Fahrlässigkeit vorliegen sollte, wäre die:der Konsument:in gemäß § 68 Abs. 5 ZaDiG 2018 dann von einer allfälligen Haftung nach § 68 Abs. 3 befreit, wenn keine ordnungsgemäße Transaktionsüberwachung stattfand.

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. Dabei muss sich der Zahlungsdienstleister:innen 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:des betreffenden Kund:in zu überprüfen und bekannte Betrugsszenarien zu berücksichtigen.

Wäre bei der Authentifizierung ein technisches Verfahren zum Einsatz gekommen, das entsprechend den Vorgaben von Art. 2 der delegierten Verordnung (EU) 2018/389 auch eine ordnungsgemäße Transaktionsüberwachung miteingeschlossen hätte, hätten die nicht autorisierten Zahlungen in einem wesentlichen Teil der Ombudsstelle für Zahlungsprobleme vorliegenden Beschwerdefälle wohl nicht durchgeführt werden dürfen. Viele Geschädigte hatten zuvor nie Zahlungen mit auch nur annähernd so hohen Beträgen in Auftrag gegeben. Außerdem hätte sich in einem Teil der Fälle auch aus der Person und dem Sitzstaat der:des Zahlungsempfänger:in oder dem Ort der Zahlung ein Betrugsverdacht ergeben müssen.
Die Ombudsstelle hat von 01.2023- 20.6.2023 insgesamt 44 Betrugsfälle bearbeitet; nur in 16 Fällen hat sich die Bank bereit erklärt, den Schaden zur Gänze zu übernehmen. In 15 Fällen übernahm die Bank den Schaden zur Hälfte. In 13 Fällen war die Bank zu keinem freiwilligen Entgegenkommen bereit. Die Ombudsstelle hat daher den VKI in bisher fünf Fällen mit einer Musterklage beauftragt. Außerdem brachte der VKI im Auftrag des BMSGPK eine Verbandsklage gegen eine große österreichische Bank ein.

Wie der Tätigkeitsbericht der Ombudsstelle für Zahlungsprobleme sehr deutlich aufzeigt, halten sich in der Praxis fast alle Banken derzeit nicht an die gesetzlichen Vorgaben, sondern lehnen eine Berichtigung des Kundenkontos mit der Behauptung ab, die:der Konsument:in habe den Missbrauch durch eine Verletzung von Sorgfaltspflichten ermöglicht und der Bank stünden daher Schadenersatzansprüche zu, die eine Berichtigungspflicht ausschließen würden. Die Ombudsstelle schlägt daher weitere zielgerichtete Maßnahmen zum Schutz besonders vulnerabler Kund:innengruppen und eine generelle Verbesserung der Transaktionsüberwachung durch die Banken vor.

Die unterfertigten Abgeordneten stellen folgenden

**Entschließungsantrag**

Der Nationalrat wolle beschließen:

„Die Bundesregierung und insbesondere der Bundesminister für Finanzen sowie der Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz werden aufgefordert, unverzüglich in Gespräche mit den heimischen Banken einzutreten bzw. allenfalls durch ergänzende gesetzliche Regelungen folgende Punkte sicherzustellen:

- Nachdem zunehmend ältere Konsument:innen Opfer von Missbräuchen im elektronischen Zahlungsverkehr (Phishing-Attacken im Zusammenhang mit Kreditkarten, Debit Karten oder Echtzeitüberweisungen) werden, bedarf es zielgerichteter und effektiver Maßnahmen der Banken zum Schutz dieser besonders verletzlichen Kund:innengruppe.
- Wie die Erfahrung zeigt, reichen bloße Warnmeldungen und Informationen der Banken nicht aus, um Konsument:nnen wirksam vor Betrügereien im elektronischen Zahlungsverkehr zu schützen. Gerade Konsument:innen, die wenig Erfahrung mit elektronischen Zahlungsmöglichkeiten haben, sind meist auch nicht in der Lage, fortlaufend neue Informationen abzurufen und zu berücksichtigen. Daher sollen die Banken generell ihre Transaktionsüberwachung verbessern und mit den bestehenden rechtlichen Vorgaben in Einklang bringen."

In formeller Hinsicht wird um Zuweisung des Antrags an den Ausschuss für Konsumentenschutz ersucht.

| | | |
|---|---|---|
| | **Unterzeichner** | Parlamentsdirektion |
| | **Datum/Zeit-UTC** | 2024-05-15T14:53:43+02:00 |
| **Prüfinformation** | Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel | |