

Banken müssen Phishing-Opfern ihr Geld zunächst erstatten – auch bei grober Fahrlässigkeit

Wer Opfer eines Phishing-Angriffs wird und anschließend feststellt, dass unberechtigte Überweisungen vom eigenen Bankkonto vorgenommen wurden, sieht sich häufig mit einer zweiten Belastung konfrontiert: Das kontoführende Kreditinstitut verweigert die Erstattung des verlorenen Geldes mit dem Argument, der Kunde habe durch die Preisgabe seiner Zugangsdaten grob fahrlässig gehandelt.

Der Europäische Gerichtshof (EuGH) hat dieser Vorgehensweise mit Urteil vom 15. Oktober 2026 in der Rechtssache C-70/25 – Tukowiecka eine wesentliche Grenze gesetzt.

Die zentrale Aussage des Urteils lautet: Der bloße Vorwurf grober Fahrlässigkeit berechtigt die Bank nicht dazu, die gesetzlich vorgesehene unverzügliche Erstattung einer nicht autorisierten Zahlung zu verweigern.

Damit stellt der EuGH klar, dass der Erstattungsanspruch des Kunden und eine mögliche spätere Haftung für den entstandenen Schaden rechtlich getrennt zu beurteilen sind. Die Entscheidung ist insbesondere für Verbraucher von erheblicher Bedeutung, die durch Phishing, gefälschte Bankwebseiten oder vergleichbare Betrugsmaschen finanzielle Verluste erlitten haben. Sie kann darüber hinaus Auswirkungen auf laufende Auseinandersetzungen mit Banken und Sparkassen haben.

Der Ausgangsfall: Phishing über eine gefälschte Bankwebseite

Dem Verfahren lag ein typischer Fall des modernen Onlinebanking-Betrugs zugrunde. Eine Kundin einer polnischen Bank wollte einen Artikel über eine Online-Verkaufsplattform veräußern. Ein vermeintlicher Kaufinteressent übersandte ihr einen Link, der den Eindruck erweckte, der Bestätigung des Verkaufs zu dienen. Tatsächlich führte dieser Link auf eine betrügerische Internetseite, die der Webseite ihrer Bank nachempfunden war.

Die Kundin gab dort ihre Onlinebanking-Zugangsdaten ein. Dadurch gelangten die Daten in die Hände des Täters, der anschließend eine nicht autorisierte Zahlung von ihrem Konto veranlasste.

Nachdem die Kundin den Vorgang bei ihrer Bank gemeldet hatte, verweigerte das Kreditinstitut die Erstattung. Zur Begründung führte es an, die Kundin habe ihre Zugangsdaten grob fahrlässig preisgegeben und dadurch den Betrug ermöglicht. Die entscheidende Rechtsfrage war deshalb, ob ein Zahlungsdienstleister die unverzügliche Erstattung mit dem Hinweis auf eine grob fahrlässige Pflichtverletzung des Kunden ablehnen darf.

Der EuGH verneinte dies.

Die Entscheidung des EuGH: Erst Erstattung, dann gegebenenfalls Haftungsprüfung

Der Gerichtshof hatte die einschlägigen Bestimmungen der Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt, der sogenannten Zweiten Zahlungsdiensterichtlinie (PSD2), auszulegen.

Im Mittelpunkt standen insbesondere Art. 73 Abs. 1 und Art. 74 Abs. 1 PSD2.

a) Die Erstattungspflicht nach Art. 73 PSD2

Nach Art. 73 Abs. 1 PSD2 muss der Zahlungsdienstleister bei einem nicht autorisierten Zahlungsvorgang grundsätzlich den Betrag unverzüglich, spätestens bis zum Ende des auf die Kenntnismeldung beziehungsweise Anzeige des Vorgangs folgenden Geschäftstags, erstatten. Das Zahlungskonto ist gegebenenfalls wieder auf den Stand zu bringen, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte.

Die Richtlinie sieht eine eng begrenzte Ausnahme vor: Der Zahlungsdienstleister darf von der unverzüglichen Erstattung absehen, wenn er berechtigte Gründe für den Verdacht hat, dass der Zahlungsdienstanutzer in betrügerischer Absicht gehandelt hat, und diese Gründe der zuständigen nationalen Behörde schriftlich mitteilt.

Entscheidend ist die Abgrenzung zwischen Betrugsverdacht und grober Fahrlässigkeit.

Der Vorwurf, der Kunde habe durch unvorsichtiges Verhalten den Zugriff auf sein Konto ermöglicht, ist nicht mit dem Verdacht gleichzusetzen, der Kunde selbst habe betrügerisch gehandelt. Die bloße Behauptung grober Fahrlässigkeit eröffnet daher keine zusätzliche Ausnahme von der Erstattungspflicht.

b) Grobe Fahrlässigkeit beseitigt den Erstattungsanspruch nicht automatisch

Banken argumentieren in Phishing-Fällen häufig, dass Kunden ihre Zugangsdaten niemals auf einer fremden Webseite eingeben oder Sicherheitswarnungen ignorieren dürften. Je nach konkretem Sachverhalt kann ein entsprechendes Verhalten tatsächlich eine erhebliche Pflichtverletzung darstellen.

Der EuGH stellt jedoch klar, dass diese Frage nicht mit der vorgelagerten Erstattungspflicht vermischt werden darf.

Die Bank kann sich nicht allein auf die Behauptung stützen, der Kunde habe grob fahrlässig gehandelt, um die gesetzlich vorgeschriebene Erstattung zunächst vollständig zu verweigern. Damit trennt der Gerichtshof zwei rechtlich unterschiedliche Prüfungsschritte: zunächst die Wiederherstellung des Kontostands und anschließend gegebenenfalls die Frage, wer den wirtschaftlichen Verlust endgültig zu tragen hat.

Die entscheidende Einschränkung: Grobe Fahrlässigkeit bleibt rechtlich relevant

Das Urteil bedeutet ausdrücklich nicht, dass Bankkunden bei Phishing unter allen Umständen vor finanziellen Verlusten geschützt sind.

Art. 74 Abs. 1 PSD2 regelt die Haftung des Zahlungsdienstanutzers bei vorsätzlicher oder grob fahrlässiger Verletzung bestimmter Pflichten, insbesondere der Pflichten zum Schutz personalisierter Sicherheitsmerkmale nach Art. 69 PSD2.

Nach der Entscheidung des EuGH kann der Zahlungsdienstleister deshalb grundsätzlich auch nach erfolgter Erstattung geltend machen, dass der Kunde den Verlust wegen einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung selbst zu tragen hat.

Hierfür müssen jedoch die gesetzlichen Voraussetzungen erfüllt sein. Der Zahlungsdienstleister kann sich nicht mit einer pauschalen Behauptung begnügen, der Kunde hätte den Betrug erkennen müssen.

Die wesentliche Neuerung liegt damit nicht in einem vollständigen Haftungsausschluss zugunsten der Verbraucher, sondern in der rechtlichen Trennung zwischen sofortiger Erstattung und endgültiger Verlustzuweisung.

Diese Unterscheidung ist für die außergerichtliche und gerichtliche Durchsetzung von Ansprüchen von erheblicher Bedeutung.

Bedeutung für das deutsche Recht: §§ 675u, 675v und 675w BGB

Die Entscheidung des EuGH ist auch für die Beurteilung vergleichbarer Sachverhalte nach deutschem Recht maßgeblich.

§ 675u BGB: Anspruch auf Erstattung bei nicht autorisierten Zahlungsvorgängen

§ 675u BGB verpflichtet den Zahlungsdienstleister, bei einem nicht autorisierten Zahlungsvorgang den Zahlungsbetrag grundsätzlich unverzüglich zu erstatten und das Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung befunden hätte.

Die Vorschrift bildet den zentralen Ausgangspunkt für Ansprüche von Bankkunden, deren Konten durch unberechtigte Zahlungen belastet wurden.

Die Auslegung des europäischen Zahlungsdienstrechts durch den EuGH ist bei der Anwendung der entsprechenden nationalen Regelungen zu berücksichtigen. Eine pauschale Leistungsverweigerung allein mit dem Argument grober Fahrlässigkeit lässt sich daher nicht ohne Weiteres mit dem gesetzlichen Erstattungsregime vereinbaren.

§ 675v BGB: Mögliche Haftung des Zahlungsdienstnutzers

Von der Erstattungspflicht zu unterscheiden ist die Frage, ob der Kunde nach § 675v BGB für den entstandenen Schaden haftet.

Hierbei kommt es auf die gesetzlichen Haftungsvoraussetzungen, die konkrete Art der Pflichtverletzung und die jeweiligen Umstände des Einzelfalls an.

Ob die Preisgabe von Zugangsdaten, die Freigabe einer Transaktion oder die Bestätigung einer Zahlung eine Haftung begründet, muss anhand des tatsächlichen Geschehensablaufs geprüft werden. Nicht jede erfolgreiche Phishing-Attacke belegt bereits eine grobe Fahrlässigkeit des Kunden.

§ 675w BGB: Nachweis und Beweislast

Besondere Bedeutung kommt außerdem § 675w BGB zu. Die Vorschrift regelt die Anforderungen an den Nachweis der Authentifizierung und ordnungsgemäßen Aufzeichnung eines Zahlungsvorgangs sowie an den Nachweis einer behaupteten Autorisierung oder einer vorsätzlichen beziehungsweise grob fahrlässigen Pflichtverletzung.

Die bloße technische Erfassung einer Zahlung oder die ordnungsgemäße Verwendung von Authentifizierungsdaten genügt nicht ohne Weiteres, um eine Autorisierung durch den Kunden oder dessen grob fahrlässiges Verhalten zu beweisen.

Für die anwaltliche Praxis bedeutet dies: Die tatsächlichen Umstände des Zahlungsvorgangs, die verwendeten Authentifizierungsverfahren, die Kommunikation mit der Bank und die konkreten Sicherheitsvorkehrungen müssen sorgfältig aufgearbeitet werden.

Welche Fälle sind besonders betroffen?

Die Entscheidung ist insbesondere bei folgenden Konstellationen relevant:

- **Phishing über gefälschte Bankseiten:** Kunden geben ihre Zugangsdaten auf einer täuschend echt gestalteten Webseite ein.
- **Betrug über Verkaufsplattformen:** Täter geben sich als Käufer aus und veranlassen Verkäufer dazu, vermeintliche Zahlungs- oder Verkaufsbestätigungen vorzunehmen.
- **Social Engineering:** Betrüger erschleichen sich Zugangsdaten oder Transaktionsfreigaben durch manipulative Kommunikation.
- **Gefälschte Bankmitarbeiter und Telefonbetrug:** Täter geben sich als Mitarbeiter des Kreditinstituts aus und versuchen, Kunden zur Herausgabe von Sicherheitsinformationen oder zur Freigabe von Zahlungen zu bewegen.
- **Unberechtigte Onlineüberweisungen:** Ein Dritter veranlasst eine Zahlung, ohne dass der Kontoinhaber diese tatsächlich autorisiert hat.

Allerdings muss in jedem Einzelfall geprüft werden, ob überhaupt ein nicht autorisierter Zahlungsvorgang vorliegt. Hat ein Kunde eine Überweisung selbst bewusst freigegeben, kann die rechtliche Einordnung anders ausfallen als bei einer vollständig ohne seine Autorisierung vorgenommenen Transaktion.

Auch die Frage, ob ein Kunde eine Zahlung selbst autorisiert oder lediglich eine Sicherheitsmaßnahme im Vertrauen auf eine Täuschung bestätigt hat, bedarf einer differenzierten Prüfung der konkreten Umstände.

Was sollten Betroffene jetzt tun?

Wer durch Onlinebanking-Betrug Geld verloren hat und von seiner Bank eine Ablehnung der Erstattung erhalten hat, sollte die Angelegenheit rechtlich überprüfen lassen.

Dabei empfiehlt sich folgendes Vorgehen:

1. Betrug unverzüglich melden

Der Zahlungsdienstleister sollte über den Vorfall informiert werden. Nicht autorisierte Zahlungen sind möglichst umgehend zu beanstanden. Bei fortbestehendem Zugriff der Täter müssen die erforderlichen Sicherheitsmaßnahmen getroffen werden.

2. Sämtliche Beweismittel sichern

Dazu gehören insbesondere Kontoauszüge, Transaktionsdaten, Nachrichten, E-Mails, SMS, Screenshots der betrügerischen Webseite und die bisherige Korrespondenz mit der Bank.

3. Erstattung ausdrücklich verlangen

Betroffene sollten die konkrete Belastung benennen und die Wiederherstellung des Kontostands nach den einschlägigen gesetzlichen Vorschriften verlangen. Eine pauschale Ablehnung der Bank sollte nicht ungeprüft akzeptiert werden.

4. Die Begründung der Bank rechtlich überprüfen

Beruft sich das Kreditinstitut auf grobe Fahrlässigkeit, ist zu prüfen, ob es lediglich die Erstattung verweigert oder ob es einen eigenständigen Anspruch wegen einer behaupteten Pflichtverletzung geltend macht. Diese Unterscheidung ist nach dem EuGH-Urteil von zentraler Bedeutung.

5. Verjährung und Fristen beachten

Auch wenn das Urteil die Rechtsposition betroffener Bankkunden stärkt, sollten mögliche Verjährungsfristen und sonstige rechtliche Fristen geprüft werden. Das Urteil ersetzt nicht die erforderliche Einzelfallprüfung.

8. Konsequenzen für die anwaltliche Praxis

Für die anwaltliche Beratung und Vertretung eröffnet das Urteil neue Argumentationsmöglichkeiten bei der Durchsetzung von Erstattungsansprüchen gegen Banken und Sparkassen.

Im Vordergrund steht zunächst die Frage, ob ein nicht autorisierter Zahlungsvorgang vorliegt und ob die Voraussetzungen des gesetzlichen Erstattungsanspruchs erfüllt sind.

Ein pauschaler Hinweis des Kreditinstituts auf grobe Fahrlässigkeit darf nicht dazu führen, dass die vorgelagerte Erstattungspflicht und die nachgelagerte Haftungsfrage miteinander vermengt werden.

Zugleich bleibt die sorgfältige Sachverhaltsaufklärung unverzichtbar. Insbesondere bei behaupteter Autorisierung, Freigabe mittels Zwei-Faktor-Authentifizierung, manipulierten Überweisungen oder telefonischer Täuschung muss geprüft werden, welche konkrete Handlung der Kunde vorgenommen hat und welche rechtlichen Folgen sich daraus ergeben. Für laufende Verfahren kann das Urteil Anlass geben, die bisherige rechtliche Argumentation zu überprüfen und Erstattungsansprüche unter Berücksichtigung der unionsrechtlichen Vorgaben neu zu bewerten.

Fazit: Banken dürfen die Erstattung nicht mit dem bloßen Vorwurf grober Fahrlässigkeit verweigern

Mit dem Urteil vom 15. Oktober 2026 in der Rechtssache C-70/25 (Tukowiecka) hat der EuGH eine wichtige Klarstellung zum Schutz von Bankkunden getroffen.

Die gesetzliche Pflicht zur unverzüglichen Erstattung nicht autorisierter Zahlungsvorgänge ist von der Frage zu trennen, ob der Kunde den entstandenen Verlust wegen vorsätzlicher oder grob fahrlässiger Pflichtverletzungen später selbst tragen muss.

Für Betroffene bedeutet dies: Wer Opfer eines Phishing-Angriffs geworden ist, sollte eine Ablehnung der Bank nicht allein deshalb hinnehmen, weil ihm grobe Fahrlässigkeit vorgeworfen wird.

Das Urteil begründet allerdings keinen uneingeschränkten Erstattungsanspruch für sämtliche Betrugsfälle. Entscheidend bleiben die fehlende Autorisierung, die einschlägigen gesetzlichen Voraussetzungen und die konkreten Umstände des Einzelfalls.

Gerade deshalb empfiehlt sich eine rechtliche Prüfung, wenn eine Bank die Erstattung verweigert oder lediglich mit pauschalen Hinweisen auf vermeintliche Sorgfaltspflichtverletzungen argumentiert.

Rechtsgrundlagen: Art. 69, 73 und 74 der Richtlinie (EU) 2015/2366 (PSD2); §§ 675u, 675v und 675w BGB.

Rechtsprechung: EuGH, Urteil vom 15. Oktober 2026, C-70/25 – Tukowiecka, ECLI:EU:C:2026:852.

Quellen:

- [EuGH – Pressemitteilung Nr. 147/26 vom 15. Oktober 2026 \(PDF\)](#)
- [EuGH – Verfahrensübersicht C-70/25 \(Tukowiecka\)](#)
- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62025CJ0070>