VuR Verbraucher und Recht

vur.nomos.de

12 | 2025
40. Jahrgang
Seiten 441–480

Anlegerschutz | Konsumentenkredit | Versicherung | private Altersvorsorge | Verbraucherinsolvenz | Verbraucherschutz

EDITORIAL

Finger weg vom Online-Banking!

RA Arne Maier, Esslingen

RA Arne Maier, Esslingen

Nutzen Sie Online-Banking? Schnell, sicher, einfach und bequem? Sicherlich lesen Sie vor jeder Transaktion die aktuellen Sicherheitshinweise Ihrer Bank. Nein? Das ist schlecht. Dann verstoßen Sie nicht nur gegen Ihre Sorgfaltspflichten, sondern Sie handeln auch grob fahrlässig (OLG Dresden BKR 2025, 850, Rn. 130, 138). Jetzt können Sie nur noch hoffen, dass Sie kein Opfer eines Phishing-Angriffs werden. Sonst bleiben Sie nach der überwiegenden deutschen Rechtsprechung in der Regel auf Ihrem Schaden sitzen.

Das müsste, sollte und dürfte so nicht sein. Der EU-Gesetzgeber hat schon vor über zehn Jahren bei Erlass der Zweiten Zahlungsdienste-Richtlinie (EU) 2015/2366 erkannt, dass sich die Sicherheitsrisiken für elektronische Zahlungen in den letzten Jahren erhöht haben, zuverlässige und sichere Zahlungsdienste für einen gut funktionierenden Zahlungsverkehrsmarkt aber von entscheidender Bedeutung sind. „Daher“ (Erwägungsgrund 7) sollten die Nutzer von Zahlungsdiensten vor solchen Risiken angemessen geschützt werden. Durch immer professionellere und ausgefeiltere Angriffstechniken sind die Sicherheitsrisiken insbesondere im Online-Banking in den letzten zehn Jahren nochmals rapide angestiegen. Digitaler Bankbetrug bzw. „Social Engineering“ nimmt beständig zu (Buck-Heeb NJW 2025, 3079). Kontoinhaber werden immer wieder Opfer von Missbrauchsattacken über das Telefon (Linardatos BKR 2025, 848). Die Zahlen von Betrugs- und Missbrauchsfällen im Online-Banking sind in den vergangenen Jahren erheblich angestiegen (Böger WM 2025, 1872). Seit Anfang des Jahres 2021 lösten Kriminelle eine im Vergleich zu früheren Angriffswellen nie dagewesene Menge an Hacking-Angriffen auf Online-Banking-Systeme aus (Schulte am Hülse/Bremm/Steinsdörfer/Rößler/Kunz MMR 2025, 336). Umso wichtiger wäre ein erhöhter Schutz der Zahlungsdienstnutzer. Einen solchen Schutz sieht die deutsche Rechtsprechung aber kaum vor.

An den gesetzlichen Vorgaben liegt es nicht. Das Zahlungsdiensterecht stellt mit der groben Fahrlässigkeit als Voraussetzung für eine über 50 Euro (§ 675v Abs. 1 und 2 BGB) hinausgehende Haftung des Zahlungsdienstnutzers einen geeigneten Schutzmechanismus zur Verfügung (Art. 74 Abs. 1 UAbs. 3 Zweite Zahlungsdienste-Richtlinie, § 675v Abs. 3 Nr. 2 BGB).

In der Begründung des Gesetzes zur Umsetzung der (Ersten) Zahlungsdienste-Richtlinie 2007/64/EG hat der deutsche Gesetzgeber grobe Fahrlässigkeit nur dann angenommen, wenn ganz naheliegende Überlegungen nicht angestellt oder beiseite geschoben wurden und somit dasjenige unbeachtet geblieben ist, was sich im gegebenen Fall „jedem aufgedrängt hätte" (BT-Drs. 16/11643, 114 linke Spalte). Nach dieser Definition würde grobe Fahrlässigkeit ausscheiden, wenn zahlreiche Zahlungsdienstnutzer ähnlichen Angriffsmethoden zum Opfer fallen. Der Betrug hätte sich nicht jedem aufgedrängt.

Die BGH-Formel ist demgegenüber wertungsoffen. Demnach reicht es für grobe Fahrlässigkeit aus, wenn dasjenige unbeachtet geblieben ist, was im gegebenen Fall „jedem hätte einleuchten müssen" (zB BGH NJW 2025, 3076, Rn. 27). Nach dieser Formel können Zahlungsdienstnutzer reihenweise auf dieselbe Betrugsmasche hereinfallen und dennoch alle grob fahrlässig handeln. Dass sich der Betrug ihnen allen nicht aufgedrängt hat, ist dafür unerheblich. Sie hätten den Betrug eben alle erkennen müssen.

Auch weitere gesetzliche Schutzmechanismen greifen vor deutschen Gerichten nur sehr eingeschränkt. Wenn die Angreifer es technisch hinbekommen, die App-Anzeige für die Auftragsfreigabe zu überblenden, ändert dies im Ergebnis nichts an der Haftung des Zahlungsdienstnutzers. Das OLG Dresden hat diesem Vortrag des Klägers entgegengehalten, dass er während der Anrufe der vorgeblichen Sparkassenmitarbeiterin das Smartphone sowohl für das Telefonat als auch zur Bedienung der App verwendete. Hierzu habe er „das Gerät vom Ohr nehmen" müssen, um die App betätigen zu können. Sein Fokus habe deshalb nicht notwendigerweise auf der App-Anzeige gelegen (BKR 2025, 850, Rn. 117). Dass inzwischen jedes handelsübliche Telefon eine Freisprechmöglichkeit bietet, dass man das Gerät also nicht mehr ans Ohr halten muss, um zu telefonieren, und folglich auch nicht „vom Ohr nehmen" muss, um beim Telefonieren andere Dinge zu erledigen, ist beim OLG Dresden anscheinend nicht bekannt oder nicht von Bedeutung. Die Hoffnung, Barbara Schöneberger möge um die Ecke kommen, um es zum Spaß zu erklären, ist vergeblich. Es ist bitterer Ernst.

Der Zahlungsdienstnutzer entgeht auch dann nicht seiner Haftung, wenn die Angreifer sich vorab Zugang zu seinem nicht ausreichend geschützten Online-Banking-Konto verschafft haben, um mittels der dort ausgelesenen Daten sein Vertrauen zu gewinnen, dass ein Bankmitarbeiter anruft. Der Haftungsausschluss wegen fehlender starker Kundenauthentifizierung (§ 675v Abs. 4 Satz 1 Nr. 1 BGB) greife in diesem Fall nicht (BGH NJW 2025, 3076, Rn. 33-36). In solchen Fällen komme zwar ein Mitverschulden der Bank in Betracht (§ 254 Abs. 1 BGB). Dies sei vom Tatrichter zu beurteilen (BGH NJW 2025, 3076, Rn. 37-39). Im dortigen Verfahren hat das Berufungsgericht ein Mitverschulden der Bank mit der Begründung abgelehnt, die Klägerin hätte den Angriff abwehren müssen (OLG Naumburg BeckRS 2024, 26554, Rn. 73). Der Verursachungsbeitrag der Bank trete deshalb hinter den maßgeblichen und schwerwiegenden Verursachungsbeitrag der Klägerin zurück. Der BGH hat diese Begründung durchgewunken. Demnach soll ein (vermeintlich) grob fahrlässiger Verursachungsbeitrag des Zahlungsdienstnutzers nicht nur seine Haftung auslösen, sondern auch ein Mitverschulden der Bank ausschließen. Ein Mitverschulden der Bank steht aber erst in Frage, wenn der Zahlungsdienstnutzer haftet, wäre also regelmäßig ausgeschlossen. Das OLG Dresden hat in dieser Konstellation dennoch eine 20%ige Mithaftung der Bank angenommen (BKR 2025, 850, Rn. 145-149).

Auch ein Tageslimit oder ein bei derselben Bank geführtes Tagesgeldkonto können das Geld nicht vor fremdem Zugriff schützen. Der Zahlungsdienstnutzer haftet auch dann, wenn es den Angreifern gelingt, das Tageslimit zu erhöhen oder Guthaben vom Tagesgeldkonto auf das Girokonto umzubuchen (OLG Dresden BKR 2025, 850, Rn. 4; OLG Oldenburg BeckRS 2025, 21016, Rn. 2).

So bleibt im Ganzen die Erkenntnis: beim Online-Banking sollten Sie auf einen gerichtlichen Schutz nicht vertrauen. Verbraucheranwälte bemühen sich dennoch nach Kräften, Ihren gesetzlich vorgesehenen Schutz in gerichtlichen Verfahren durchzusetzen und zu retten, was zu retten ist, wenn Ihr Geld im Brunnen liegt bzw. vom Konto verschwunden ist (Poppelbaum/Jentsch VuR 2025, 451, in diesem Heft; Schulte am Hülse/Steinsdörfer VuR 2025, 172). Mit Glück und Mühe bekommen Sie dann womöglich ein 20%iges Nasenwasser des verlorenen Gelds zurück. Sie sollten sich aber bewusst sein, dass Sie das Online-Banking generell auf eigenes Risiko nutzen. Bevor Ihr Geld weg ist, stehen Sie deshalb vor der Frage, ob Sie darauf vertrauen wollen, dass Sie sich selbst schützen können, also auch ausgefeilte Betrugsversuche erkennen und professionelle Angriffe erfolgreich abwehren würden. Dann mögen Sie sich den Risiken des Online-Bankings aussetzen, um dessen Vorteile zu nutzen. Wenn Sie sich darauf aber lieber nicht verlassen wollen, gibt es nur eine Handlungsvariante, um Ihr Geld zu schützen: Finger weg vom Online-Banking!