

20. September 2023

## **Online-Banking-Betrug: Beweislast beim Kunden**

Spätestens seit den Bank-Datenlecks, bei denen die Kontodaten zahlloser Bankkunden abgefangen wurden, nehmen die Fälle von Online-Banking-Betrug weiter zu. Mit Anrufen von vermeintlichen Bankmitarbeitern, täuschend echten SMS und E-Mails sowie diversen persönlichen Informationen, die eigentlich nur der Bank vorliegen dürften, täuschen Betrüger zurzeit zahllose Bankkunden und verschaffen sich so Zugriff auf die Konten. Die Schäden sind häufig beträchtlich. Aber leider bleiben viele Betroffene auf ihren Verlusten sitzen.

### **Gefälschte SMS: Betrüger erbeuten Zugangsdaten von Bankkundin**

So auch in einem Fall in München, bei dem eine Sparkassen-Kundin einen Anruf von einem vermeintlichen Bankmitarbeiter erhielt. Der Mann kannte alle ihre Daten wie Adresse, Geburtsdatum und mehr. Der Anrufer fragte, warum die Frau ihre Push-Tan-Zugangsdaten nicht aktualisiert habe. Und tatsächlich hatte die Kundin zuvor von der Sparkasse eine Aktualisierungsaufforderung erhalten. Der angebliche Sparkassen-Mitarbeiter warnte die Frau, dass sie kein Online-Banking mehr durchführen könne, wenn sie nicht sofort die Aktualisierung vornehmen würde.

Der Mann schickte ihr noch während des Telefonats eine SMS. Diese sah genauso aus, als habe die Sparkasse sie verschickt. Daher klickte die Bankkundin auf den enthaltenen Link und gab neue Daten ein, ohne zu ahnen, dass sie damit den Betrügern Zugriff auf ihr Online-Konto gewährte. Sie erhielt von ihrer Sparkasse sogar eine Mail, in der die Änderung der Zugangsdaten bestätigt wurde. Umgehend griffen die Kriminellen auf das Online-Konto zu und zahlten damit diverse teure Reisen im Wert von über 4.600 Euro, bevor der Betrug bemerkt wurde. Zwar konnte die Sparkasse zwei Buchungen zurückholen, doch auf dem verbleibenden Schaden von mehr als 2.000 Euro blieb die Frau sitzen. Wie ihr ergeht es zurzeit vielen Bankkunden in ganz Deutschland. In vielen Fällen verweigern die Banken eine Entschädigung, weil die Kunden angeblich fahrlässig gehandelt hätten.

Ein Vorwurf, den zu entkräftigen oft sehr schwer ist.

## **Machen sich Opfer von Betrugsmaschen der Fahrlässigkeit schuldig?**

Grundsätzlich sollte gemäß der EU-Zahlungsdiensterichtlinie (PSD2) die Beweislast für eine angebliche Fahrlässigkeit im Falle von solchen Online-Zahlungen durch Dritte bei der Bank liegen. Doch nach der Umsetzung der EU-Richtlinie im deutschen Recht liegt in Betrugsfällen die Beweislast trotzdem häufig beim Kunden. Laut Bundesjustiz- und Bundesfinanzministerium erfordere die Rechtslage, „dass der Zahlungsdienstenutzer mit einem substantiierten und glaubhaften Vortrag über den Geschehensablauf darlegen kann, dass er trotz aufgezeichneter Authentifizierung den Zahlungsvorgang nicht autorisiert hat.“

Der Tatbestand der Fahrlässigkeit hängt also häufig von der Frage ab, ob der Kunde die Zahlung autorisiert hat oder nicht. Die Banken prüfen hier lediglich, ob eine Überweisung auch tatsächlich durch die erforderlichen Authentifizierungskomponenten autorisiert wurde, z. B. PIN und TAN. In Fällen wie dem hier Beschriebenen ist es für Betroffene daher überaus schwierig nachzuweisen, dass sie die betreffende Zahlung nicht selbst autorisiert haben.

## **Beweislast liegt meistens beim Bankkunden**

Wie soll ein Bankkunde also glaubhaft nachweisen, dass er die Autorisierung einer Zahlung nicht selbst veranlasst hat, wenn sich Betrüger mithilfe seiner Authentifizierungskomponenten Zugriff auf das Konto verschafft haben? Sobald eine Bank angibt, dass eine Überweisung angemessen autorisiert wurde, geht die Beweislast auf den Verbraucher über. Der muss dann beweisen, dass er nicht grob fahrlässig gehandelt hat. Das ist für Betrugsopfer aber extrem schwer nachzuweisen. Folglich bleiben viele Geschädigte auf ihren Verlusten sitzen.

Auch im Fall der Sparkassen-Kundin stellt sich also die Frage, ob sie fahrlässig gehandelt oder ob sie einen Rückzahlungsanspruch gegen ihre Bank hat. Für die Sparkasse Niederbayern-Mitte war die Sachlage klar. Auf Medienanfrage hieß es von dort, die Kundin habe selbst die SMS an die Betrüger geschickt, nicht umgekehrt. Man prüfe aber gerade, welche Möglichkeiten es zur Kulanzregelung in diesem Fall gebe.

## **Neue Zahlungsdiensterichtlinie soll besseren Verbraucherschutz ermöglichen**

Weil inzwischen klar ist, dass die aktuelle Zahlungsdiensterichtlinie (PSD2) die Verbraucher nicht angemessen schützt, arbeitet die EU-Kommission nun in Kooperation mit der Europäischen Bankenaufsichtsbehörde (EBA) an einer neuen Richtlinie. Es liegen seitens der EBA bereits zahlreiche Empfehlungen vor, wie die Richtlinie zu verbessern ist, z. B. in Bezug auf mangelnde Klarheit und abweichende Auslegungen in den Mitgliedstaaten sowie die unterschiedlichen Auslegungen bei den Banken. Eine dieser Empfehlungen ist außerdem eine genaue Definition von grober Fahrlässigkeit. Laut EBA tragen die Bankkunden etwa 70 Prozent der Schäden durch Online-Banking-Betrug.

Bis auf Weiteres müssen Betrugsopfer aber nachweisen, dass sie nicht fahrlässig gehandelt haben. Es empfiehlt sich daher, anwaltlichen Rat einzuholen, bevor der Bank Angaben zum Ablauf des

Betrugsfalls gemacht werden. Wir beraten Sie dazu in unserer Kanzlei gerne und kämpfen dafür, dass Sie nicht auf Ihren Verlusten sitzenbleiben. Vereinbaren Sie einfach kurzfristig einen Termin für ein kostenloses Erstgespräch.

[Guido Lenné](#)

Rechtsanwalt aus der Anwaltskanzlei Lenné.

Rechtsanwalt Lenné ist auch Fachanwalt für Bank- und Kapitalmarktrecht.

Wir helfen Ihnen gerne! [Kontaktieren](#) Sie uns. Oder vereinbaren Sie [hier online einen Termin](#) für eine telefonische kostenfreie Erstberatung.

- [Facebook](#)
- [Twitter](#)
- [WhatsApp](#)
- [E-mail](#)

[Zurück](#)