

## Betrug beim Online-Banking („Pharming“)

Muss eine Bank einer Kundin den Betrag ersetzen, den diese auf eine fingierte Aufforderung im Online-Banking an einen unbekanntem Betrüger überwiesen hat? Diese Frage hatte das Landgericht Koblenz zu entscheiden.

Urteil vom 01.06.2022, Az. 3 O 378/21 (nicht rechtskräftig)

### Der Sachverhalt

Die Klägerin nutzte als Kundin der beklagten Bank deren Online-Banking. Dabei muss jede Überweisung durch eine Sicherheitsnummer bestätigt werden, die von einem TAN-Generator erzeugt wird. Dieses Gerät zeigt auch die Nummer des Zielkontos und den zu überweisenden Betrag an.

Am 23.11.2020 loggte sich die Klägerin beim Online-Banking ein. Ein Schadprogramm auf ihrem Computer öffnete daraufhin ein Fenster mit der Aufforderung, eine „Demoüberweisung“ in Höhe von mehreren 10.000 € an einen Herrn Mustermann vorzunehmen. Die irritierte Klägerin startete die Anmeldung erneut, wieder öffnete sich das Fenster. Die Klägerin kam nun der Aufforderung nach und gab dazu die von ihrem TAN-Generator erzeugte Sicherheitsnummer ein. Das Schadprogramm nutzte diese Nummer für eine reale Überweisung in Höhe von 9.847,78 € von dem Konto der Klägerin. Anschließend wurde die Klägerin auf das echte Online-Banking der Beklagten umgeleitet, wo sie wie gewohnt ihre Bankgeschäfte abwickelte.

Die Klägerin vertrat im Prozess die Meinung, der überwiesene Betrag sei ihr von der Bank zu erstatten. Sie habe nicht erkennen können, dass es sich um eine Betrugsmasche – sogenanntes „Pharming“ – handelte. Ihren Computer habe sie mit einem Virenprogramm geschützt. Die Beklagte verweigerte die Zahlung mit dem Argument, das Verhalten der Klägerin sei grob fahrlässig gewesen, so dass sie ihren Schaden selbst zu tragen habe.

### Die Entscheidung

Das Gericht hat die Klage abgewiesen. Die Klägerin habe nämlich „in grob fahrlässiger Weise ihre Sorgfaltspflichten verletzt“, als sie die „Demoüberweisung“ mit einer echten Transaktionsnummer durchgeführt habe. Sie habe ganz naheliegende Überlegungen nicht angestellt und nicht beachtet, was jedem hätte einleuchten müssen. Von einem durchschnittlichen Computer-Nutzer könne erwartet werden, dass er die Nutzung des Online-Bankings einstellt, wenn die Umstände sehr zweifelhaft sind und auf ein fragwürdiges Geschehen hindeuten.

Das – so führte das Gericht weiter aus – sei hier der Fall gewesen. Es sei nämlich sehr ungewöhnlich, dass eine echte TAN einzugeben sei, obwohl keine reale Überweisung ausgeführt werden solle. Dies habe die Klägerin misstrauisch machen müssen. Auch die in der „Demoüberweisung“ genannte hohe Summe habe Anlass zu besonderer Vorsicht geben müssen. Die Klägerin habe ja selbst zugegeben, die Aufforderung zur Demoüberweisung sei ihr „gefühlsmäßig komisch vorgekommen“, weshalb sie zunächst von vorn begonnen habe. Sie habe auch sehen können, dass auf dem TAN-Generator die reale Ziel-Kontonummer und der tatsächliche Überweisungsbetrag angezeigt wurden. Dennoch habe die Klägerin die Transaktionsnummer für die „Demoüberweisung“ eingegeben. Dies hielt das Gericht

für einen derart groben Verstoß gegen die Sorgfaltspflichten eines Bankkunden, dass die Klägerin den Schaden selbst zu tragen habe.

#### Auszug aus dem Bürgerlichen Gesetzbuch

#### **§ 675u Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge**

Im Fall eines nicht autorisierten Zahlungsvorgangs hat der Zahlungsdienstleister des Zahlers gegen diesen keinen Anspruch auf Erstattung seiner Aufwendungen. Er ist verpflichtet, dem Zahler den Zahlungsbetrag unverzüglich zu erstatten und, sofern der Betrag einem Zahlungskonto belastet worden ist, dieses Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte.

...

#### **§ 675v Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsinstruments**

(1) Beruhen nicht autorisierte Zahlungsvorgänge auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Zahlungsinstruments, so kann der Zahlungsdienstleister des Zahlers von diesem den Ersatz des hierdurch entstandenen Schadens bis zu einem Betrag von 50 Euro verlangen.

(2) Der Zahler haftet nicht nach Absatz 1, wenn

1. es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Zahlungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder

2. der Verlust des Zahlungsinstruments durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Abweichend von den Absätzen 1 und 2 ist der Zahler seinem Zahlungsdienstleister zum Ersatz des gesamten Schadens verpflichtet, der infolge eines nicht autorisierten Zahlungsvorgangs entstanden ist, wenn der Zahler

1. in betrügerischer Absicht gehandelt hat oder

2. den Schaden herbeigeführt hat durch vorsätzliche oder grob fahrlässige Verletzung

- a) einer oder mehrerer Pflichten gemäß § 675l Absatz 1 oder
- b) einer oder mehrerer vereinbarter Bedingungen für die Ausgabe und Nutzung des Zahlungsinstruments.

...