Nicolas Bracher
Dr. iur. | LL.M. | Rechtsanwalt
Tel.: +41 (58) 958 58 58
n.bracher@wengervieli.ch

Mathias Müller
MLaw, Rechtsanwalt
Tel.: +41 (58) 958 58 58
m.mueller@wengervieli.ch

Wenger & Vieli AG Rechtsanwälte
CH – 8034 Zürich
www.wengervieli.ch

HACKERANGRIFFE AUF BANKKUNDEN: WER TRÄGT DEN SCHADEN?

Nicolas Bracher

Mathias Müller

Zahlungsverkehr im Visier von Hackern

In jüngerer Zeit haben sich Medienberichte über Fälle gehäuft, in denen es Hackern gelang, über das Internet betrügerische Banküberweisungen auszulösen. In einigen Fällen verschafften sich Hacker Zugriff auf E-Mail-Accounts von Bankkunden und erteilten Banken in der Folge über diese Accounts per E-Mail betrügerische Zahlungsaufträge. Teilweise gelang es Hackern auch, Computer von Bankkunden mit einer Schadsoftware (z. B. einem Trojaner) zu infizieren, die nach Offline-Zahlungssoftware suchte und darüber betrügerische Fehlüberweisungen auslöste.

Wird ein Bankkunde Opfer eines derartigen Hackerangriffs, stellt sich aus rechtlicher Sicht die Frage, ob der Kunde oder die Bank den aus einer Fehlüberweisung resultierenden Schaden tragen muss. Letzteres steht vor allem dann zur Diskussion, wenn der Bank bei der Ausführung einer betrügerischen Fehlüberweisung Fahrlässigkeit vorwerfbar ist, weil der Betrug für sie bei Anwendung der gebotenen Sorgfalt erkennbar gewesen wäre.

In letzter Zeit wurden in diesem Zusammenhang mehrere kundenfreundliche Urteile gefällt. Auf den ersten Blick legt dies den Schluss nahe, das Haftungsrisiko der Banken bei betrügerischen Fehlüberweisungen sei sehr gross. Allerdings betrafen diese Urteile ausschliesslich Privatkunden, die ihren Banken jeweils mittels persönlicher Kommunikation mit einem Kundenberater Zahlungsaufträge per E-Mail erteilt hatten. Zudem verhielten sich die Hacker in den beurteilten Fällen meist überaus verdächtig, indem sie beispielsweise im Gegensatz zum Kunden nur in gebrochener Sprache mit dem Kundenberater kommunizierten oder – für einen Privatkunden – ungewöhnlich hohe Zahlungen in fremde Länder auslösten. Der vorliegende Beitrag beleuchtet, inwiefern die erwähnten Urteile auf die Situation von Firmenkunden übertragbar sind, die den Zahlungsverkehr mit ihrer Bank per E-Banking abwickeln.

Grundsätzliche Risikoverteilung bei Fehlvergütungen

Der Kunde, der gestützt auf einen Kontovertrag Geld bei einer Bank hinterlegt, gilt rechtlich nicht als Eigentümer des hinterlegten Geldes, sondern als Gläubiger der Bank. Diese ist gestützt auf den Kontovertrag verpflichtet, ein positives Guthaben auf Verlangen des Kunden an ihn selbst oder einen von ihm bezeichneten Zahlungsempfänger auszubezahlen. Wenn die Bank Geld überweist, überweist sie folglich nicht das Geld des Kunden, sondern ihr eigenes Geld. Erfolgt eine Überweisung allerdings im Auftrag des Kunden, erfüllt die Bank durch die Überweisung ihre vertragliche Auszahlungspflicht und das Guthaben des Kunden gegenüber der Bank verringert sich entsprechend. Bezahlt die Bank das Guthaben oder einen Teil davon hingegen irrtümlich einem Betrüger aus, stellt dies keine Vertragserfüllung gegenüber dem Kunden dar, weshalb dieser weiterhin die Auszahlung des gesamten Guthabens verlangen kann. Nach ständiger Rechtsprechung des Bundesgerichts erleidet bei betrügerischen Fehlüberweisungen deshalb grundsätzlich nicht der Kunde, sondern die Bank einen Schaden. Dies gilt im Grundsatz selbst dann, wenn der Bank keinerlei Verschulden bezüglich der Fehlvergütung vorgeworfen werden kann und sie gutgläubig an einen Betrüger geleistet hat.

Abwehrklauseln in Bankverträgen

Dieses Risiko der Doppelzahlung versuchen Banken vertraglich auszuschliessen oder zu minimieren. Daher enthalten die einschlägigen Bankverträge sowie die dazugehörigen AGB verschiedene branchenübliche Klauseln, die den Auszahlungsanspruch des Kunden nach einer Fehlüberweisung ausschliessen oder dessen Durchsetzung jedenfalls erschweren.

Im Fokus stehen zwei Arten von Klauseln: Sogenannte Risikoverteilungsklauseln regeln, dass im Falle einer Fehlüberweisung nicht die Bank, sondern der Kunde den Schaden zu tragen hat, sofern die Bank ihrerseits nicht grobfahrlässig gehandelt hat. Die Folge davon ist, dass die Bank dem Kunden bei einer Fehlüberweisung den Betrag nicht ein «zweites Mal» ausbezahlen muss. Risikoverteilungsklauseln sind nicht unbeschränkt gültig. Im Verhältnis zu Firmenkunden

setzt ihre Gültigkeit im Wesentlichen voraus, dass damit ein legitimes Ziel verfolgt wird, namentlich die Absicherung der Bank gegen schwer vermeidbare Risiken, die nicht in ihrem Machtbereich liegen, wie beispielsweise ein Hackerangriff auf die IT-Infrastruktur des Kunden. Unzulässig ist die Risikoüberwälzung auf den Kunden aber in jedem Fall dann, wenn die Fehlüberweisung einer groben Fahrlässigkeit der Bank zuzuschreiben ist. Eine solche liegt vor, wenn die Bank elementare Vorsichtsregeln nicht beachtet, die ein Kunde berechtigterweise erwarten darf. Grundsätzlich gilt allerdings, dass sich die Bank bei der Prüfung der Echtheit von Zahlungsaufträgen auf die vertraglich festgelegte Authentizitätsprüfung beschränken darf. Da ein rascher Zahlungsverkehr gewährleistet werden muss, hat sie Fälschungen nicht systematisch zu vermuten. Erst wenn bei ordnungsgemässer Prüfung ernsthafte Indizien für eine Fälschung bzw. einen Hackerangriff vorliegen, muss die Bank zusätzliche Abklärungen vornehmen, beispielsweise indem sie den Auftrag vom Kunden telefonisch rückbestätigen lässt. Solche Indizien liegen insbesondere vor, wenn vertraglich nicht vorgesehene oder für den Kunden unübliche Handlungen verlangt werden oder andere ungewöhnliche Umstände vorliegen. Ignoriert die Bank solche Verdachtsmomente und tätigt sie in der Folge eine Fehlüberweisung, hat sie den Schaden auch bei Vorhandensein einer Risikoverteilungsklausel selbst zu tragen.

Für den Fall, dass die Risikoverteilungsklausel nicht greift, enthalten die von den Banken für den Zugriff auf ihre E-Banking-Systeme verwendeten Standardverträge und AGB jeweils detaillierte Regeln betreffend die Verwendung und Verwahrung persönlicher Legitimationsmittel (wie Passwörter, Vertragsnummern etc.) für den Online-Zugriff auf das jeweilige E-Banking-System. Liegt einem erfolgreichen Hackerangriff ein Verstoss des Kunden gegen solche Regeln zugrunde (z. B. die unsichere Verwahrung eines Passworts), kann dies nach der Rechtsprechung zu einem Schadenersatzanspruch der Bank gegenüber dem Kunden führen, den diese mit dem Auszahlungsanspruch des Kunden verrechnen kann, so dass im Ergebnis wiederum der Kunde das Risiko der Fehlüberweisung trägt.

Unsichere Rechtslage beim E-Banking-Verkehr zwischen Banken und Firmenkunden

Die kundenfreundlichen Urteile zu E-Mail-Hacking-Fällen sollten nicht darüber hinwegtäuschen, dass die Gerichte erstens jeden Einzelfall sorgfältig prüfen, und dass zweitens wichtige Rechtsfragen nicht höchstrichterlich geklärt sind. Letzteres gilt etwa für die Frage, welche Authentizitätsprüfung die Banken bei der Entgegennahme und Ausführung von per E-Banking übermittelten Zahlungsaufträgen vornehmen müssen, und welches Verhalten in diesem Zusammenhang als grobfahrlässig gilt. Die bisherige Rechtsprechung zu den Anforderungen an die Prüfung einer physischen Unterschrift kann hier nur bedingt weiterhelfen. Dasselbe gilt für die Rechtsprechung zu den Verdachtsmomenten, die eine weitergehende Überprüfungspflicht der Bank auslösen. Die diesbezüglich in den E-Mail-Hacking-Fällen als relevant betrachteten Umstände sind entweder bei der Kommunikation zwischen Computersystemen irrelevant (z. B. gebrochene Sprache in einer E-Mail-Kommunikation) oder im Verkehr mit Firmenkunden wohl meistens weniger verdächtig als im Verkehr mit Privatkunden (z. B. hohe Überweisungssummen ins Ausland). Der im Streitfall vom Kunden zu erbringende Beweis einer groben Fahrlässigkeit seitens der Bank ist deshalb nicht leicht zu führen. Misslingt er, greift grundsätzlich die Risikoverteilungsklausel, was einem Auszahlungsanspruch des Firmenkunden gegen seine Bank entgegensteht.

Weitgehend offen erscheint zurzeit, inwieweit die übrigen von den Banken verwendeten Abwehrklauseln wirksam sind. Dies gilt insbesondere für die den Kunden vertraglich auferlegten Regeln betreffend den Zugriff auf E-Banking-Systeme. Dazu hat das Bundesgericht nämlich festgehalten, dass in einer Zeit, in der selbst Regierungen gehackt würden, aus einem erfolgreichen Hackerangriff nicht ohne weiteres auf eine Sorgfaltspflichtverletzung des Opfers geschlossen werden könne. In der Tendenz scheinen die Gerichte zurzeit abgeneigt, den Kunden in diesem Zusammenhang einschneidende Sorgfaltspflichten aufzuerlegen.

Fazit

Das Doppelzahlungsrisiko von Banken bei Fehlüberweisungen im Zahlungsverkehr ist grundsätzlich hoch, wird aber in der Praxis durch die standardmässig verwendeten Abwehrklauseln erheblich reduziert. Im Bereich des elektronischen Zahlungsverkehrs über E-Banking und Offline-Zahlungssoftware sind die jeweiligen Sorgfaltspflichten von Banken und Kunden bis anhin nicht höchstrichterlich geklärt. Die Rechtslage hängt deshalb stark von den Umständen des Einzelfalls ab. Die Rechtsprechung ist tendenziell kundenfreundlich, betrifft aber bis anhin primär Privatkunden und ist nur punktuell auf die Verhältnisse bei Firmenkunden übertragbar.