Kommentar zu: Urteil: 4A_9/2020 vom 9. Juli 2020, zur Publikation vorgesehen
Sachgebiet: Vertragsrecht
Gericht: Bundesgericht
Spruchkörper: I. zivilrechtliche Abteilung
dRSK-Rechtsgebiet: Gesellschaftsrecht und Finanzmarktrecht

Transaktionen aufgrund einer gehackten E-Mail

Zur Pflichtverletzung von Finanzdienstleistern

Autor / Autorin

Pascal Zysset, Viktoriya Chernaya
walderwyss

Redaktor / Redaktorin

Dominik Rieder

Beat Brändli
Universität St.Gallen

In diesem Urteil befasste sich das Bundesgericht mit der Frage der Sorgfaltspflicht der Finanzdienstleister bei E-Mail-Zahlungsaufträgen und konkretisierte seine bisherige Rechtsprechung. Dabei legte es die Kriterien fest, welche bei der Beurteilung eines groben Verschuldens der Finanzdienstleisterin bei der Ausführung eines von einer gehackten E-Mail-Adresse des Kunden stammenden Auftrags zu prüfen sind. Das grobe Verschulden ist massgebend bei der Frage, ob die vereinbarte Risikotransferklausel zur Anwendung kommt.

Sachverhalt

[1] Am 6. November 2014 eröffnete der Kunde B., türkischer Staatsangehöriger und Geschäftsmann im Ruhestand, ein Konto bei einer Effektenhändlerin *[heute: Wertpapierhaus nach Art. 41 FINIG; nachfolgend: Finanzdienstleisterin]* und überwies einen Betrag in Höhe von rund EUR 850'000 auf dieses Konto. Gemäss dem Profilblatt des Kunden stammt das Geld aus seinen Ersparnissen und entsprach einem Drittel seines Vermögens (Sachverhalt A.a. und A.b.).

[2] Die Parteien gingen ein Execution-Only-Verhältnis ein, also weder ein Beratungs- noch ein Verwaltungsmandat. Im Kontoeröffnungsprozess unterzeichnete der Kunde ein Formular zur Freigabe der Kommunikation per Telefon, Fax sowie E-Mail und akzeptierte die Allgemeinen Geschäftsbedingungen (AGB) der Finanzdienstleisterin. Kraft Freigabe ermächtigte der Kunde die Finanzdienstleisterin, insbesondere per E-Mail übermittelte Zahlungsaufträge auch ohne seine schriftliche Bestätigung unverzüglich auszuführen. Er entband die Finanzdienstleisterin von der Haftung für Schäden, die ihm aus solchen Transaktionen entstehen könnten. Auch mit der Anerkennung der AGB und der darin enthaltenen «Risikotransferklausel» erklärte der Kunde, dass er die Finanzdienstleisterin von allen durch fehlende Legitimation oder aus der Übermittlung von Aufträgen per E-Mail resultierenden Schäden befreit, sofern die Finanzdienstleisterin kein grobes Verschulden trifft (Sachverhalt A.b.).

[3] Während rund eines Jahres nach der Kontoeröffnung kommunizierte der Kunde mit der Finanzdienstleisterin über zwei verschiedene E-Mail-Adressen. In diesem Zeitraum erteilte er lediglich zwei Zahlungsaufträge: Eine

Überweisung in Höhe von USD 10'000 zugunsten seiner Tochter in die USA und eine Überweisung in Höhe von EUR 44'000 auf sein eigenes Konto bei einer Bank in Istanbul (Sachverhalt A.c.).

[4] Im Dezember 2015 haben Hacker die Kontrolle über eine der besagten E-Mail-Adressen des Kunden übernommen. Es gelang ihnen nicht nur, in seine frühere Korrespondenz mit der Finanzdienstleisterin Einsicht zu nehmen, sondern auch E-Mails an die Finanzdienstleisterin zu versenden und die Korrespondenz danach zu löschen. Zwischen dem 1. Dezember 2015 und dem 4. Januar 2016 gaben die Hacker auf diese Weise acht Überweisungen in Auftrag und belasteten dem Konto des Kunden Beträge in Höhe von insg. EUR 34'000 und GBP 357'000 (Sachverhalt A.d.).

[5] Nachdem die Hacker sich am 6. und am 7. Januar 2016 mit einer leicht abweichenden E-Mail-Adresse an die Finanzdienstleisterin wandten, forderte die Finanzdienstleisterin den Absender auf, seine telefonischen Kontaktdaten anzugeben und versuchte auch selbst vergeblich, den Kunden telefonisch zu erreichen. Mangels Kontaktnahme seitens des Kunden wurde die weitere Ausführung von Aufträgen ohne die Validierung seiner Identität und Adresse verboten, weshalb die später eingegangenen Aufträge vom 8. und 13. Januar 2016 nicht mehr ausgeführt wurden. In der Folge konnte die Finanzdienstleisterin mit dem Kunden in Kontakt treten. Der Kunde bestritt alle getätigten Überweisungen, mit Ausnahme der Überweisungen an seine Tochter und das auf ihn lautende Konto in Istanbul (Sachverhalt A.e.).

[6] Angesichts dieser Umstände forderte die Finanzdienstleisterin die zahlungsausführende Bank auf, die strittigen Transaktionen zurückzuüberweisen oder zu blockieren. Der Kunde verlangte seinerseits von der Finanzdienstleisterin die Rückzahlung der fraglichen Überweisungen. Eine vom Kunden beauftragte Expertenfirma bestätigte schliesslich, dass sich auf dem Computer des Kunden keine Phishing-Mails befanden und auch sonst keine Hinweise auf unsachgemässe Verwendung der IT ausgemacht werden konnten (Sachverhalt A.e.).

[7] Der Kunde stellte am 21. April 2016 ein Betreibungsbegehren. Die Finanzdienstleisterin erhob daraufhin Rechtsvorschlag (Sachverhalt A.f.).

[8] Nach dem Scheitern des Schlichtungsversuchs am 19. Oktober 2016 reichte der Kunde am 26. Januar 2016 Klage beim erstinstanzlichen Genfer Gericht gegen die Finanzdienstleisterin ein und forderte die Rückerstattung der seinem Konto belasteten, strittigen Beträge samt Zinsen. Mit Urteil vom 4. Dezember 2018 wurde die Klage in erster Instanz abgewiesen, da der Finanzdienstleisterin keine grobe Sorgfaltspflichtverletzung nachgewiesen werden konnte (Sachverhalt B).

[9] Auf Berufung des Kunden hin hob die Zivilkammer des Genfer Cour de Justice mit Urteil ACJC/1603/2019 vom 31. Oktober 2019 das erstinstanzliche Urteil auf und verurteilte die Finanzdienstleisterin zur Rückzahlung der strittigen Beträge. Sechs der acht in Frage stehenden Überweisungsaufträge seien ungewöhnlich gewesen und ihre Ausführung durch die Finanzdienstleisterin stelle eine grobe Sorgfaltspflichtverletzung dar (Sachverhalt B).

[10] Gegen dieses Urteil reichte die Finanzdienstleisterin am 9. Januar 2020 Beschwerde in Zivilsachen beim Bundesgericht ein (Sachverhalt C). Das Bundesgericht hiess die Beschwerde gut und verweigerte die Rechtsöffnung (E. 7).

Erwägungen des Bundesgerichts

[11] Das Bundesgericht hielt in seinen Erwägungen zunächst fest, dass in einer dreistufigen Prüfung zu eruieren sei, wer die Folgen der fehlenden Auftragslegitimation zu tragen habe. Dabei sei in einem ersten Schritt (i) zu prüfen, ob überhaupt ohne Kundenauftrag eine Transaktion ausgeführt worden sei. In einem zweiten Schritt (ii) sei zu prüfen, ob die Finanzdienstleisterin dem Kunden mittels Risikotransferklausel das Risiko überbunden habe. Falls keine entsprechende Klausel vereinbart worden ist oder diese in einem konkreten Fall nicht zur Anwendung kommt, habe der Richter schliesslich in einem dritten Schritt (iii) das kausalitätsunterbrechende Mitverschulden sowie die Schadensminderungsobliegenheit des Kunden in Betracht zu ziehen (E. 4).

[12] Zu den Grundlagen des ersten Prüfschritts führte das Bundesgericht aus, dass eine Finanzdienstleisterin, welche im Auftrag eines Kunden Geld an einen Dritten überweise, einen Rückzahlungsanspruch gegen den Kunden erwerbe (Art. 402 OR), welchen sie wiederum mit dem Restitutionsanspruch des Kunden verrechnen

könne. Werde hingegen ohne Kundenauftrag eine Überweisung vorgenommen, fehle es der Finanzdienstleisterin an einem Rückzahlungsanspruch, womit kein Verrechnungssubstrat zur Verfügung stehe und die Buchung rückgängig zu machen sei. Im vorliegenden Fall kam das Bundesgericht zum Schluss, dass die sechs noch strittigen Zahlungsaufträge von unbekannten Dritten in betrügerischer Absicht und somit ohne Auftrag des Kunden erteilt worden seien (E. 5).

[13] Betreffend den zweiten Prüfschritt müssten gemäss Bundesgericht zuerst die Gültigkeit und die Modalitäten der Risikotransferklausel angesehen und in dieser Hinsicht insbesondere geprüft werden, ob die Finanzdienstleisterin grobfahrlässig gehandelt habe. Einleitend machte das Gericht allgemeine Ausführungen zur Risikotransferklausel und bezeichnete diese als allgemein übliches Mittel, Schäden aus fehlender Legitimation oder nicht zuordenbaren Fehlern – schweres Fehlverhalten der Finanzdienstleister vorbehalten – den Kunden zu übertragen. Die Klausel habe zwar nicht eine Haftungsbeschränkung bei Nichterfüllung oder mangelhafter Erfüllung des Vertrags durch die Finanzdienstleisterin zum Gegenstand, wohl aber eine Risikoübertragung bei Handlungen unbefugter und nicht legitimierter Drittpersonen auf den Kunden. In Übereinstimmung mit der ständigen Rechtsprechung habe sich die Gültigkeit einer solchen Klausel anhand von Art. 100 und Art. 101 Abs. 3 OR zu orientieren. Die Anwendung erfolge dabei analog, da die Risikotransferklausel keine vertragliche Nichterfüllung im Sinne der Art. 97 ff. OR betreffe. Demnach sei insbesondere bei vorsätzlichem oder grobfahrlässigem Verhalten der Finanzdienstleister ein Risikotransfer ausgeschlossen. Dieselben Grundsätze seien anwendbar, wenn die Parteien eine Freigabe der Kommunikation per Telefon, Telefax oder E-Mail vereinbart hätten (E. 6.1).

[14] Das Bundesgericht rief in Erinnerung, dass ein grobes Verschulden der Finanzdienstleisterin nur vorliege, wenn elementare Vorsichtsgebote missachtet würden, die jede vernünftige Person unter den gleichen Umständen befolgt hätte (E. 6.2). Dabei habe die Finanzdienstleisterin die Echtheit der ihr zugestellten Zahlungsaufträge nur dann zu überprüfen, wenn dies zwischen den Parteien so vereinbart worden oder gegebenenfalls aufgrund gesetzlicher Vorgaben vorgeschrieben sei (E. 6.2.1). Die Finanzdienstleisterin habe jedoch weder ausserordentliche Massnahmen zur Prüfung der Auftragserteilung vorzunehmen noch habe sie systematisch vom Vorliegen eines Falschauftrags auszugehen. Zusätzliche Prüfungen seien nur dann anzustreben, wenn ernsthafte Hinweise auf eine Fälschung vorlägen, wenn ein vertraglich nicht vorgesehener oder unüblicher Auftrag erteilt werde oder wenn sonst besondere Umstände einen Zweifel aufkommen liessen (E. 6.2.1.1). Dieselben Prinzipien seien gemäss Bundesgericht dann anwendbar, wenn unter den Parteien die Auftragserteilung per E-Mail vereinbart worden sei. Insbesondere habe die Finanzdienstleisterin nicht systematisch davon auszugehen, dass die ihr von der E-Mail-Adresse des Kunden übermittelte Nachricht nicht vom Kunden stamme. Aufgrund der vereinbarten Risikotransferklausel läge es vielmehr in der Verantwortung des Kunden, alle notwendigen Vorsichtsmassnahmen zu ergreifen, um einen solchen Missbrauch zu vermeiden. Die Haftung des Kunden erstrecke sich dabei auch auf höhere Gewalt. Ein grobes Verschulden der Bank könne folglich nur dann vorliegen, wenn eine notwendigerweise durchzuführende kurze Authentizitätsprüfung ernsthafte Hinweise auf das Vorliegen einer Fälschung oder einen Missbrauch ergebe und für jeden vernünftigen Menschen ersichtlich wäre, dass der übermittelte Auftrag aufgrund der Adresse, der Sprache, des Inhalts oder eines exotischen Bestimmungslandes unter Berücksichtigung der konkreten Umstände des Kunden nicht vom Kunden stamme (E. 6.2.1.2).

[15] Im vorliegenden Fall hätten sich die Parteien – mit Ausnahme schweren Fehlverhaltens der Bank – auf zwei Risikotransferklauseln geeinigt: Zum einen sei das Risiko in den AGB bei Legitimationsmängeln und unerkannten Fälschungen und zum anderen bei Übermittlungsfehlern der elektronischen Post auf den Kunden überwälzt worden. Mittels gesondert unterzeichneter Freigabevereinbarung sei die Finanzdienstleisterin vorliegend ausdrücklich ermächtigt worden, die E-Mail-Weisungen entgegenzunehmen und die entsprechenden Aufträge unverzüglich auszuführen, ohne dass vorgängig eine systematische Kontaktnahme per Telefon hätte erfolgen müssen (E. 6.3.1).

[16] Das Bundesgericht zog weiter in Erwägung, dass bei der Beurteilung, ob vorliegend ein nicht übertragbares Risiko grobfahrlässigen Verhaltens der Finanzdienstleisterin einschlägig sei, auf die Umstände des Einzelfalls abgestellt werden müsse (E. 6.3.2). Demnach habe die Vertragsbeziehung zwischen den Parteien bis zu den fraglichen Überweisungen lediglich ein Jahr gedauert. Während dieser Zeit habe der Kunde immer per E-Mail bzw. per Telefon kommuniziert. Dabei seien vorgängig zu den fraglichen Überweisungen bereits zwei Zahlungsaufträge

erteilt worden. Bevor die fraglichen acht Transaktionen ausgeführt worden seien, habe das Kundenkonto einen Saldo von ca. EUR 850'000 aufgewiesen. Als die Hacker eine leicht geänderte E-Mail-Adresse verwendet hätten, seien die offenen Transaktionen von der Finanzdienstleisterin gesperrt worden und der Kunde sei aufgefordert worden, sich mit der Finanzdienstleisterin telefonisch in Verbindung zu setzen. Erst dann habe man festgestellt, dass die Hacker Kontrolle über die Kunden-E-Mail übernommen und so die Aufträge erteilt hatten. Wie diese Kontrolle übernommen worden war, sei – so das Bundesgericht – ungeklärt und folglich sei auch nicht ersichtlich, welche Massnahmen notwendig gewesen wären, um diese Kontrollübernahme zu verhindern (E. 6.3.2.1).

[17] Während die ersten zwei Transaktionen vom Kunden nicht beanstandet worden seien, habe die kantonale Vorinstanz in den folgenden sechs Aufträgen ein schweres Fehlverhalten der Finanzdienstleisterin erblickt. Gemäss Vorinstanz könne nicht davon ausgegangen werden, dass eine Kontrollübernahme der Mailbox durch die Hacker notwendigerweise eine Sorgfaltspflichtverletzung des Kunden impliziere. Demgegenüber stelle sich die Finanzdienstleisterin auf den Standpunkt, keinerlei schwerwiegendes Fehlverhalten an den Tag gelegt zu haben (E. 6.3.2.2).

[18] Das Bundesgericht erläuterte, dass der rechtlichen Würdigung der kantonalen Vorinstanz nicht beigepflichtet werden könne. Die Auftragserteilung per E-Mail ohne telefonische oder schriftliche Rückbestätigung sei zwischen den Parteien explizit so vereinbart worden, inklusive damit verbundener Risikotransferklausel. Ohne ernsthafte Hinweise auf einen Missbrauch habe die Finanzdienstleisterin daher die erteilten Aufträge nicht verdächtigen müssen. Dabei würden die von der Vorinstanz berücksichtigten Elemente gerade keine entsprechenden Anhaltspunkte liefern und daher die Bedingung eines schweren Fehlverhaltens nicht erfüllen, da keine elementaren Sorgfaltspflichten verletzt worden seien. Einerseits seien die in Frage stehenden E-Mails von der vom Kunden angegebenen E-Mail-Adresse abgeschickt worden. Andererseits habe auch das von den Hackern verwendete, grobe Englisch keinen Hinweis auf die fehlende Legitimität gegeben. Die Hacker hätten den Zugang zur bisherigen Korrespondenz des Kunden mit der Finanzdienstleisterin geschickt ausgenutzt, um die Formulierung bisheriger Zahlungsaufträge zu imitieren. So habe der Kunde bereits in seinen früheren E-Mails auf Englisch kommuniziert, Fehler gemacht und häufig auf Höflichkeitsfloskeln verzichtet. Sodann seien die Überweisungen an eine bekannte Bank im Vereinigten Königreich gerichtet gewesen und damit mitnichten in ein exotisches Land. Zudem habe sich die Finanzdienstleisterin nicht dazu verpflichtet, die Identität des Endbegünstigten zu überprüfen. Weiter sei auch der dritte Transfer im beträchtlichen Umfang von GBP 100'000 mit «*urgent business deal*» bezeichnet und mit einer Liquiditätsbeschaffung durch den Verkauf von Wertpapieren begründet worden, was gemäss Bundesgericht keinen Anlass zur Überprüfung durch die Finanzdienstleisterin gegeben habe, zumal ein solches Geschäft auch für einen ehemaligen Geschäftsmann im Ruhestand mit einem Vermögen von rund EUR 850'000 bei der Finanzdienstleisterin plausibel erscheine. Zwar seien die nächsten fünf strittigen Aufträge innerhalb eines Monats und mit einer Gesamtsumme von GBP 357'000 erteilt worden, jedoch sei es nicht möglich, aus dieser Auftragsfrequenz und diesem Auftragsvolumen bereits auf ein schweres Fehlverhalten der Finanzdienstleisterin zu schliessen. Da die Risikotransferklausel zufällige Ereignisse miteinschliesse, gehe vorliegend der Schaden zu Lasten des Kunden, selbst wenn ihn kein Verschulden treffe, dass die Hacker die Kontrolle über seine Mailbox übernahmen. Nach Ansicht des Bundesgerichts wäre die Situation anders zu beurteilen, wenn das Computersystem der Bank gehackt worden wäre (E. 6.3.2.3).

[19] Demnach hat die Finanzdienstleisterin nach höchstrichterlicher Auffassung kein schwerwiegendes Fehlverhalten an den Tag gelegt, weshalb das Risiko des E-Mail-Missbrauchs vom Kunden zu tragen sei (E. 6.3.3). Somit hiess das Bundesgericht die Beschwerde gut und hob das angefochtene Urteil der Vorinstanz auf, wodurch die Rechtsöffnung verweigert wurde (E. 7).

Kurzkommentar

[20] Das vorliegende Urteil des Bundesgerichts behandelt die Frage, wer im Auftragsverhältnis für unverschuldete *Cyber*-Risiken haftet in der Konstellation, in welcher eine sog. Risikotransferklausel vereinbart wurde (vgl. zur Risikotransferklausel, insb. BSK OR I-Corinne Widmer Lüchinger/Wolfgang Wiegand, 5. Aufl., Basel 2016, Art. 100 N 2a m. w. H.). *In casu* nahm der Kunde die Leistungen einer Effektenhändlerin in Anspruch, wobei im Rahmen des (in analoger Anwendung) geprüften Art. 100 Abs. 1 OR nicht die regulatorische Klassifizierung entscheidend ist, sondern vielmehr die vertragliche Grundlage des Execution-Only-Geschäfts. Aus diesem Grund wird vorliegend der weite Begriff des Finanzdienstleisters nach Art. 3 lit. d FIDLEG verwendet (a. M. Martin

RAUBER, 4A_9/2020: Sorgfaltspflichten von Banken und anderen Finanzgesellschaften bei Transaktionsaufträgen via E-Mail (amtl. Publ.), swissblawg vom 29. Juli 2020, der untechnisch von der «Finanzgesellschaft» schreibt; unklar z. T. das Bundesgericht im zugrundeliegenden Urteil, wenn es primär von der *«société de négoce»*, häufig aber von der – in der Rechtsprechung zu dieser Thematik oft vorkommenden – *«banque»* ausgeht).

[21] Der Anwendungsbereich des vorliegenden, höchstrichterlichen Urteils ist abzugrenzen von Anlageberatungs- und Vermögensverwaltungsverhältnissen. Da beim reinen Anlageberatungsverhältnis die Ausführungskompetenz in der Sphäre des Kunden bleibt, kann sich dieselbe Konstellation der missbräuchlichen Auftragserteilung gar nicht stellen. Auf der anderen Seite verbleibt im Vermögensverwaltungsverhältnis die Ausführungskompetenz beim Finanzdienstleister, womit jegliche Ausführungshinweise des Kunden im Lichte der vordefinierten Anlagestrategie kritisch zu würdigen sind. Demnach liesse sich das Risiko derartiger betrügerischer Anweisungen kaum in derselben Weise auf den Kunden abwälzen, da Änderungen in der Strategie als wesentliche Auftragsanpassung zu betrachten sind, bei welchen eine Verifizierung oder gar ein persönliches Gespräch geboten sind. Hingegen wählte der Kunde mit dem Execution-Only-Verhältnis gerade eine rein ausführende Dienstleistung, wobei in der Praxis kundenseitig ein grosses Bedürfnis besteht, solche Anweisungen möglichst einfach erteilen zu können. Dies erklärt, warum im vorliegenden Fall die im heutigen Geschäftsverkehr übliche Freigabevereinbarung betreffend elektronische Kommunikation unterzeichnet wurde.

[22] Das Bundesgericht wendete zur Einordnung des Sachverhalts ein dreistufiges Prüfschema an, wonach zu prüfen ist, ob (i) tatsächlich ein rechtsgültiger Auftrag erteilt worden ist, ob (ii) eine gültige Risikotransferklausel vorliegt und ob (iii) ein Mitverschulden des Kunden bzw. eine Verletzung der Schadensminderungsobliegenheit ausgemacht werden kann (abweichend NICOLAS BRACHER, Legitimationsprüfung und Risikotransfer bei E-Mail-Zahlungsaufträgen, SZW 2018, 161 f., der bei gewöhnlichen E-Mail-Transaktionen davon ausgeht, dass Risikotransferklauseln *per se* nicht anwendbar sind). Das zugrundeliegende Urteil befasste sich dabei intensiv mit dem zweitgenannten Punkt (ii) der Risikotransferklausel und der Frage, ob grobe Fahrlässigkeit der Finanzdienstleisterin der Gültigkeit dieser Klausel entgegensteht (Art. 100 Abs. 1 OR analog). Bei dieser Prüfung setzte sich das Bundesgericht mit den verschiedenen Kriterien zur Abgrenzung der groben zur leichten Fahrlässigkeit auseinander (ähnlich bereits BGer 4A_386/2016 vom 5. Dezember 2016, E. 2.4.2 und jüngst das vorliegende Urteil bestätigend BGer 4A_178/2019 und 4A_192/2019 vom 6. August 2020, E. 6.3.3.3). Diese Kriterien werden in der Praxis der Finanzdienstleister grosse Wellen schlagen. Im Einzelnen sind demnach zu berücksichtigen:

1. **Umstände der Geschäftsbeziehung**: Die vorliegend kurze Geschäftsbeziehung (rund ein Jahr) und die Tatsache, dass nur ein Teil des Vermögens übertragen wurde, sprachen gegen grobe Fahrlässigkeit. Nicht berücksichtigt wurden vom Bundesgericht persönliche Umstände wie die IT-Erfahrenheit des Kunden.
2. **Autorisierte E-Mail-Adresse**: Die verwendeten E-Mail-Adressen müssen von den Parteien vorgängig definiert werden. Wird eine abweichende Adresse benützt – wie *in casu* von den Hackern aus unerklärlichen Gründen nach den ersten acht Transaktionen – besteht bei Ausführung des Auftrags kaum mehr Spielraum für ein leichtes Verschulden der Finanzdienstleisterin.
3. **Sprache**: Die angewendete Sprache darf betreffend Stil, Orthografie und Formulierungen keine Auffälligkeiten aufweisen. Wenn sich die Hacker wie vorliegend Zugang auf frühere Konversationen verschaffen können und die Ausführungen geschickt imitieren, muss sich die Finanzdienstleisterin nichts vorwerfen lassen. Viele Missbräuche dürften aber nach wie vor anhand des Sprachkriteriums aufgedeckt werden.
4. **Inhalt der Transaktion**: Dabei berücksichtigt das Bundesgericht den angegebenen Zahlungsgrund der Transaktion sowie den Ort und das Finanzinstitut des Begünstigten. Kritisch sind dabei Überweisungen in ferne oder exotische Länder sowie an unbekannte Finanzinstitute. Vorliegend wendete das Bundesgericht für den Zahlungsgrund keinen strengen Massstab an, indem der Hinweis *«business deal»* auch auf den pensionierten Kunden noch nicht zu einem groben Verschulden der Finanzdienstleisterin führte.
5. **Transaktionsvolumen**: Das angestrebte Transaktionsvolumen muss in einem angemessenen Verhältnis zum gesamten, der Finanzdienstleisterin bekannten Vermögen stehen und hinsichtlich des angegebenen Zahlungszwecks plausibel erscheinen. Unter Berücksichtigung dieser Umstände können auch grössere Transaktionsvolumina, vorliegenden Falles etwa in der Höhe von GBP 100'000 (3. Transaktion), ohne

grobes Verschulden der Finanzdienstleisterin durchgeführt werden.

6. **Transaktionsfrequenz**: Schliesslich sind Auffälligkeiten einer geänderten Transaktionsfrequenz zu berücksichtigen. Dabei wendet das Bundesgericht wiederum einen nicht allzu strengen Massstab an, indem fünf Transaktionen innerhalb eines Monats als unproblematisch angesehen wurden, selbst wenn zuvor während eines Jahres lediglich zwei Überweisungen in Auftrag gegeben worden waren.

[23] Aus den definierten Kriterien wird klar, dass sich Finanzdienstleister keinesfalls zurücklehnen dürfen und die obgenannten Punkte in ihr Compliance-Konzept einbauen müssen. Andererseits lässt sich aus dem Urteil schliessen, dass das Rechtsrisiko des Finanzdienstleisters – anders als bisweilen befürchtet – durchaus ersichtliche Grenzen aufweist, nicht zuletzt, weil das Bundesgericht in der Anwendung der Kriterien nicht seinen strengsten Massstab ansetzte und die Anforderung (*«manquement absolument inexcusable»,* E. 6.3.2.3) beim Wort nahm.

[24] Das Urteil ist in diesem Punkt zu begrüssen. Finanzdienstleister sollen bei vereinbartem Risikotransfer nicht für *Cyber*-Schäden haften, welche sich in der Sphäre des Kunden abspielen, solange keine klaren Signale die Finanzdienstleister hätten stutzig machen sollen. Diese Auslegung des groben Verschuldens ist letztlich die einzige mit der Digitalisierung zu vereinbarende. Nachdenklich macht diese Seite der Technologieneutralität nur deshalb, weil des Menschen liebste Digitallösung nur schwerlich mit seiner tiefen Risikotoleranz zu vereinbaren ist. Im Ergebnis haben sich die Risiken aber nur verschoben: Während früher analoge Täter ihre Opfer auf der Strasse ausraubten, befinden sich die heutigen, digitalen Täter hinter Bildschirmen.

[25] Unklar ist, wie die Intensität des vom Bundesgericht angewendeten Verschuldensmassstabs zu verstehen ist. Auffällig ist, dass das höchste Gericht zwar die analoge Anwendung des gesamten Art. 100 OR auf die Risikotransferklausel stützt (so in E. 6.1; vgl. dazu auch die Vorinstanz in E. 5.1.4, wobei diese aufgrund der Bejahung des schweren Verschuldens nicht weiterprüfen musste), jedoch bei der Prüfung der groben Fahrlässigkeit nach Abs. 1 aufhört. Obwohl es sich bei der Finanzdienstleisterin um ein bewilligtes Institut (Effektenhändlerin nach BEHG, heute Wertpapierhaus nach FINIG) handelt, prüfte das Bundesgericht die Zulässigkeit des Risikotransfers für leichtes Verschulden gemäss Art. 100 Abs. 2 OR nicht, obschon es diese Bestimmung seit BGE 112 II 450 auf Banken anwendet. Ist das der Beginn einer Abkehr von der teilweise kritisierten Rechtsprechung? Oder wollte das Gericht beim Effektenhändler nicht ganz so weit gehen wie bei Banken? Oder wurde dieser Aspekt schlicht übersehen? Oder bezog sich die analoge Anwendung doch nur auf Art. 100 Abs. 1 OR (trotz offenem Wortlaut «Art. 100 OR»)? Oder hatte es der Kunde versäumt, diesen Aspekt eventualiter vorzubringen (Dispositionsmaxime)? Oder hat das Gericht lediglich von ihm gemäss Art. 100 Abs. 2 OR zustehenden Ermessen Gebrauch gemacht (zum Ermessen BSK OR I-Corinne Widmer Lüchinger/Wolfgang Wiegand, 7. Aufl., Basel 2020, Art. 100 N 15)? Dies ist eine Reihe von offenen Fragen bzw. von Alternativbegründungen für die bloss teilweise Anwendung von Art. 100 OR, aufgelistet nach u. E. absteigender Wahrscheinlichkeit ihres Zutreffens. Aufgrund der diversen möglichen Erklärungen scheint es (noch) zu früh, dem Bundesgericht eine Abkehr dieser Rechtsprechung in den Mund zu legen. In jedem Fall darf aber gespannt auf die weitere Entwicklung geblickt werden.

Dr. iur. Pascal Zysset, Rechtsanwalt und Notar, Walder Wyss AG.

MLaw Viktoriya Chernaya, Substitutin Walder Wyss AG.

Zitiervorschlag: Pascal Zysset / Viktoriya Chernaya, Transaktionen aufgrund einer gehackten E-Mail, in: dRSK, publiziert am 12. November 2020

ISSN 1663-9995. Editions Weblaw

Weblaw AG | Schwarztorstrasse 22 | 3007 Bern

T +41 31 380 57 77 info@weblaw.ch