www.jusletter-it.eu

Simon Schlauri

Risikoüberwälzung im E-Banking

Category: News
Region: Switzerland
Field of law: E-Taxation und FinanceOnline

Citation: Simon Schlauri, Risikoüberwälzung im E-Banking, in: Jusletter IT 24 November 2016

[Rz 1] Am Montag, 7. November 2016 stellte die britische Tesco-Bank ihr Online-Banking vorläufig ein, nachdem über das vorausgehende Wochenende Hacker rund 20'000 Konten der Bank geplündert hatten.[1] Wie sind die Risiken in solchen und ähnlichen Fällen nach Schweizer Recht verteilt?

[Rz 2] Elektronische Daten eignen sich oftmals schlecht als Beweismittel. Organisatorische und technische Massnahmen müssen getroffen werden, um den Beweis zu sichern. Der Kunde soll nicht abstreiten können, eine bestimmte Transaktion getätigt zu haben, und er soll sich umgekehrt keine Gedanken zur Sicherheit seines Bankkontos machen müssen.

[Rz 3] In der Schweiz gibt es verschiedene E-Banking-Legitimationsmittel, beispielsweise die Mobile TAN, TAN-Generatoren oder das bankenübergreifende Paymit-System. Letzteres begnügt sich mit Benutzerkennung und Passwort oder einer Betätigung des Fingerabdrucksensors des Gerätes, lässt dafür aber nur Zahlungen bis 500 Franken zu. Gleiches gilt für manche E-Banking-Apps.

[Rz 4] Aus rechtlicher Sicht bleibt es der Bank und ihren Kunden im Grundsatz unbenommen, für den Einsatz solcher Legitimationsmittel im Rahmen der gesetzlichen Schranken eine eigene vertragliche Legitimationsordnung und damit eine vom Gesetz abweichende Risikoverteilung zu vereinbaren. Im Bankgeschäft werden gewisse Risiken, die gemäss Gesetz bei der Bank liegen, regelmässig per Allgemeine Geschäftsbedingungen (AGB) auf den Kunden überwälzt.

[Rz 5] Die Risikoabwälzung ist indessen bestimmten Schranken unterworfen. Diese Schranken liegen im Auftragsrecht, in der analogen Anwendung der Haftungsregelung nach Art. 100 und 101 OR sowie insbesondere in der relativ neuen Norm von Art. 8 UWG. Die Schweiz kennt indessen bislang, bis auf ein geldwäschereirechtlich motiviertes Rundschreiben der FINMA zur Video- und Online-Identifizierung bei der Aufnahme von Geschäftsbeziehungen[2] keine spezifische Regulierung der Legitimation im Bankenbereich.

[Rz 6] Vorliegend soll das Augenmerk hauptsächlich auf Art. 8 UWG gerichtet werden, der die Verwender von allgemeinen Geschäftsbedingungen gegenüber Konsumenten bei deren Gestaltung einschränkt.

[Rz 7] Zur Risikoüberwälzung nach Art. 8 UWG im Bereich des E-Banking findet sich eine grosse Bandbreite juristischer Meinungen:

[Rz 8] Schott und Kut/Stauber gehen davon aus, dass die neue Norm keinerlei Änderungen gegenüber der alten Rechtslage[3] mit sich brachte, gemäss der die Bank das Risiko auf den Kunden abwälzen konnte, so lange sie sich nur an die branchenübliche Sorgfalt hielt.[4] Diese Position ist allerdings angesichts der Entstehungsgeschichte der Norm wenig plausibel.Sie wurde denn auch als aus Bankensicht riskant kritisiert.[5]

---

1 NZZ Online vom 7. November 2016, tinyurl.com/hb382f3.

2 FINMA-RS 16/7 «Video- und Online-Identifizierung».

3 BGE 132 III 449 = Pra 2007, 195; vgl. auch Simon Schlauri, Elektronische Signaturen, ZIK Bd. 19, Zürich 2002 = Diss. Zürich 2002, N 719 ff.

4 Ansgar Schott, Missbräuchliche Allgemeine Geschäftsbedingungen, in: Der Schweizer Treuhänder 2012, 78 ff., 80; Ahmet Kut/Demian Stauber, Die UWG-Revision vom 17. Juni 2011 im Überblick, in: Jusletter 20. Februar 2012, Rz. 124 f.

5 Zum Ganzen etwa Thomas Koller, Art. 8 UWG: Eine Auslegeordnung unter besonderer Berücksichtigung von Banken-AGB, AJP 2014, 19 ff., 20.

[Rz 9] Widmer plädiert für eine Haftungsverteilung gemäss der sogenannten Sphärentheorie, die besagt, dass die Haftung für Zufall nur gemäss der jeweiligen Sphäre aufgeteilt werden darf, in der sie auftritt. Eine Risikoabwälzung sei dann gerecht, wenn jeder Vertragspartner diejenigen Risiken übernehme, die aus seinem Einflussbereich stammen, und die er entsprechend kontrollieren könne. Für den Fall, dass dem Kunden seine Bankkarte gestohlen wird (Sphäre des Kunden), dürfte die Bank das Risiko auch dann dem Kunden zuweisen, wenn diesen kein Verschulden trifft. Findet indessen ein Hackerangriff auf die Bank statt (wie im Fall der Tesco-Bank), müsste auf jeden Fall die Bank haften, selbst wenn sie kein Verschulden trifft, d.h. selbst wenn sie ihre Systeme korrekt abgesichert hat.[6] Die Sphärentheorie kommt dem Konzept des «cheapest cost avoider» nahe, das sich in der Theorie der Ökonomischen Analyse des Rechts findet: Eine Übertragung des Risikos für Verschulden der Bank auf den Kunden scheint ineffizient und ist damit aus dieser Sicht abzulehnen.[7]

[Rz 10] Rusch geht noch weiter als Widmer und lehnt selbst die Sphärentheorie ab, weil eine Zufallshaftung im Sinne einer verschuldensunabhängigen Schadensüberwälzung dem Schweizer Vertragsrecht fremd sei. Nach seiner Auffassung darf dem Kunden die Haftung nur für Fälle überwälzt werden, in denen ihn ein Verschulden (d.h. zumindest leichte Fahrlässigkeit) trifft.[8] Ein Kartendiebstahl ohne Verschulden des Kunden könnte demnach für den Kunden nicht haftungsbegründend sein. Diese Position entspricht zugleich dem geltenden (dispositiven) Obligationenrecht, gemäss dem der Kunde nur bei Verschulden haftet.[9]

[Rz 11] Angesichts des breiten Meinungsspektrums stellt sich die Frage, welchen Weg ein Finanzinstitut bei der Ausgestaltung seiner AGB gehen soll.

[Rz 12] Zu beachten ist, dass eine Verletzung von Art. 8 UWG zu Nichtigkeit der betreffenden AGB-Klauseln führt und damit zur Anwendbarkeit des für die Bank ungünstigen dispositiven Gesetzesrechts.[10] Dieses Risiko scheint bei AGB, die nur dem alten Recht genügen, erheblich. Nachdem Ruschs Position bereits dem dispositiven Gesetzesrecht entspricht, dürfte es sich umgekehrt rechtfertigen, auf die Sphärentheorie abzustellen: Denn greift auch eine Ausgestaltung gemäss Sphärentheorie nicht, fällt man ohnehin auf das dispositive Gesetzesrecht zurück.

[Rz 13] Ebenfalls nach Art. 8 UWG ungültig dürften ferner Beweisregeln in AGB sein, gemäss denen jedes Login mit den Legitimationsmitteln des Kunden als genügender Beweis für die Urheberschaft des Kunden an einer Transaktion gelten soll.[11]

---

6 Esther Widmer, Missbräuchliche Geschäftsbedingungen nach Art. 8 UWG, Unter besonderer Berücksichtigung der Allgemeinen Geschäftsbedingungen von Banken, Zürich/St. Gallen 2015 = Diss. Bern 2014, N 426 ff.

7 Auf die «cheapest cost avoider»-Regel stellt das Bundesgericht in BGE 126 III 20 E. 3 c) ab, in dem es um einen fehlerhaft erteilten Überweisungsauftrag ging: Das Gericht fand, es sei der Bank möglich und in Anbetracht ihrer auftragsrechtlichen Sorgfaltspflicht zumutbar, die im Überweisungsauftrag gemachten Angaben zum Zweck der korrekten Ausführung zu überprüfen, weshalb diesbezügliche Fehler ihrem Kontroll- und Risikobereich unterlägen. Vgl. für Deutschland etwa auch Stefan Grundmann, in: Carsten Thomas Ebenroth/Karlheinz Boujong/Detlev Joost/Lutz Strohn (Hrsg.), Handelsgesetzbuch: HGB, 3. Auflage, München 2015, Band 2, 341, gemäss dessen Darstellung der Grundsatz des «cheapest cost avoider» als Begründung für eine durch die Spezialnorm von § 675 v Abs. 2 BGB geschaffene Gefährdungshaftung in Höhe von maximal 150 EUR dient.

8 Arnold Rusch, Schadenabwälzungsklauseln in der Inhaltskontrolle, SZW 2012, 439 ff.

9 Gemäss BGE 132 III 449 (=Pra 2007, 195) ist es grundsätzlich die Bank, die das Risiko einer zu Lasten des Kontos zu Gunsten einer nicht berechtigten Person ausgeführten Leistung trägt; sie allein erleidet einen Schaden, denn sie ist gehalten, ihrem Kunden den betreffenden Betrag ein zweites Mal zu bezahlen.

10 Koller (FN 5), 34.

11 Daniel Markwalder, Public Key Infrastructure, ZIK Bd. 45, Zürich 2009 = Diss. Zürich 2009, N 807; vgl. auch Bst. q des Anhangs der europäischen AGB-Richtlinie 93/13/EWG (Klauselkatalog), der für die Auslegung von Art. 8 UWG von Bedeutung sein dürfte. Anders (zum alten Recht) noch Schlauri (FN 3), N 561, 566.

[Rz 14] Weniger problematisch dürfte der Einsatz von Legitimationsmitteln geringerer Sicherheit (Benutzerkennung und Passwort ohne TAN, Fingerabdrucksensoren[12] o.dgl.) dort sein, wo die Summen beschränkt sind (wie bei Paymit) oder wo andere Sicherheitsmechanismen greifen (bspw. Zahlungen nur auf bereits früher verwendete Empfängerkonti).[13] Die Begründung hierfür liegt darin, dass der Kunde gerade bei kleinen Risiken ebenfalls ein Interesse an weniger kompliziert anzuwenden Legitimationsmitteln hat.

[Rz 15] Die Tesco-Bank hätte den aus dem Hacker-Angriff resultierenden Schaden nach Schweizer Recht also selber zu tragen. Nach dem anwendbaren europäischen Recht dürfte dies ebenfalls der Fall sein, denn die EU kennt striktere Regeln als die Schweiz.[14]

Simon Schlauri

12 Derartige Sensoren sind regelmässig leicht zu überlisten, und Fingerabdrücke sind – anders als ein Passwort – nicht geheim, sondern finden sich im Umfeld jeder Person massenhaft; vgl. statt vieler Tobias Bühlmann, iPhone lässt sich mit Knetmasse entsperren, NZZ Online 3. März 2016, tinyurl.com/zn76wcb; vgl. auch Schlauri (FN 3), N 305.

13 Vgl. auch Artikel 63 der zweiten EU-Zahlungsdiensterichtlinie 2015/2366 (PSD2).

14 Hinzuweisen ist erneut auf die EU-Zahlungsdiensterichtlinie 2015/2366 (PSD2) sowie auf Richtlinien der EZB (tinyurl.com/zagcgh2) und Leitlinien der EBA (tinyurl.com/z9rjwjv).