Commerz Real Investmentgesellschaft mbH Online Banking Bedingungen (Stand 01.04.2015)

1. Leistungsangebot

(1) Der Kontoinhaber kann Bankgeschäfte mittels Online Banking in dem von der CRI angebotenen Umfang abwickeln. Für die Abwicklung gelten die Bedingungen für die jeweiligen Bankgeschäfte (z.B. Sonderbedingungen für CRI Online Banking-Geschäfte über hausInvest Anteile). Zudem kann er Informationen der CRI mittels Online Banking abrufen. Die CRI ist berechtigt, dem Kontoinhaber die Änderung ihrer Geschäftsbedingungen auf elektronischem Weg anzuzeigen und zum Abruf bereitzustellen. Wegen des Wirksamwerdens der Änderungen verbleibt es bei der Regelung in Nummer 1 Abs. 2 der Bedingungen für *hausInvest*-Bausteinkonten oder den mit den Bausteinkontoinhabern vereinbarten abweichenden Regelungen.

(2) Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet.

2. Voraussetzungen zur Nutzung des Online Banking

Der Kontoinhaber benötigt für die Abwicklung von Bankgeschäften mittels Online Banking die mit der CRI vereinbarten personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der CRI als berechtigter Kontoinhaber auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- die persönliche Identifikationsnummer (PIN),
- einmal verwendbare Transaktionsnummern (TAN),

2.2 Authentifizierungsinstrumente

Die TAN wird dem Kontoinhaber durch Versand einer SMS an ein mobiles Endgerät (z.B. Mobiltelefon) zur Verfügung gestellt.

3. Zugang zum Online Banking

Der Teilnehmer erhält Zugang zum Online Banking, wenn

- dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN übermittelt hat,
- die Prüfung dieser Daten bei der CRI eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 9.1 und 10) vorliegt.

Nach Gewährung des Zugangs zum Online Banking kann der Kontoinhaber Informationen abrufen oder Aufträge erteilen.

4. Auftragsabwicklung im Rahmen des Online Bankings

4.1 Auftragserteilung und Autorisierung

Der Kontoinhaber muss einen im Rahmen des Online Bankings erteilten Auftrag zu dessen Wirksamkeit mit dem vereinbarten personalisierten Sicherheitsmerkmal autorisieren und der CRI mittels Online Banking übermitteln. Die CRI bestätigt mittels Online Banking den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Online Bankings erfolgen, es sei denn, die CRI sieht eine Widerrufmöglichkeit im Online Banking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die CRI

(1) Die Bearbeitung der im Rahmen des Online Bankings erteilten Aufträge erfolgt nach den für die Abwicklung der jeweiligen Auftragsart geltenden Regelungen.

(2) Für Zahlungsaufträge (Überweisung, Lastschrift) gelten folgende Sonderregelungen:

Die CRI wird den Zahlungsauftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Kontoinhaber hat sich mit seinem personalisierten Sicherheitsmerkmal legitimiert
- Die Berechtigung des Kontoinhabers für die jeweilige Auftragsart liegt vor
- Das Online Banking Datenformat ist eingehalten
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen liegen vor

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die CRI den Auftrag aus. Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstoßen.

(3) Liegen die Ausführungsbedingungen nach Absatz (2) Satz 1 1.– 4. Spiegelstrich nicht vor, wird die CRI den Auftrag nicht ausführen.

Führt sie den Auftrag nicht aus, wird sie den Kontoinhaber über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, eine Information zur Verfügung stellen. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstößt.

6. Information des Kontoinhabers über mittels Online Banking erteilte Verfügungen

Die CRI unterrichtet den Kontoinhaber über die mittels Online Banking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg und gemäß den für den Auftrag geltenden Bedingungen.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum Online Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online Banking nur über die von der CRI gesondert mitgeteilten Online Banking Zugangskanäle (z.B. Internetadresse) herzustellen.

7.2 Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

(1) Der Teilnehmer hat

- seine personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der CRI gesondert mitgeteilten Online Banking Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmal das Online Banking Verfahren missbräuchlich nutzen.

(2) Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Die personalisierten Sicherheitsmerkmale PIN und TAN dürfen nicht elektronisch gespeichert werden
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z.B. nicht auf Online-Händlerseiten)
- Die personalisierten Sicherheitsmerkmale dürfen nicht außerhalb des Online Banking Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail
- Der Teilnehmerdarf zur Autorisierung eines Auftrags nicht mehr als eine TAN verwenden.
- Wird ein mobiles Endgerät zum Empfang einer TAN mittels SMS eingesetzt, darf diese TAN nicht auf dem selben Gerät für das Online Banking verwendet werden

7.3 Kontrolle der Auftragsdaten mit von der CRI angezeigten Daten

Soweit die CRI dem Teilnehmer Daten aus seinem Online Banking Auftrag (z.B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z.B. Mobiltelefon) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Ein- und Ausfuhr von Software im Ausland

In Ländern, in denen Nutzungs- oder Einfuhr- und Ausfuhrbeschränkungen für Verschlüsselungstechniken bestehen, darf eine von der CRI zur Verfügung gestellte Software nicht verwendet werden.

Commerz Real Investmentgesellschaft mbH Online Banking Bedingungen (Stand 01.04.2015)

9. Anzeige- und Unterrichtungspflichten

9.1 Sperranzeige

(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl des Authentifizierungsinstruments,
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines persönlichen Sicherheitsmerkmals

fest, muss der Teilnehmer die CRI hierüber unverzüglich unterrichten (Sperranzeige). Der Kontoinhaber kann der CRI eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

9.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kontoinhaber hat die CRI unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

10. Nutzungssperre

10.1 Sperre auf Veranlassung des Teilnehmers

Die CRI sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 9.1,
- den Online Banking Zugang für ihn oder alle Teilnehmer oder
- sein Authentifizierungsinstrument.

10.2 Sperre auf Veranlassung der CRI

(1) Die CRI darf den Online Banking Zugang für einen Teilnehmersperren, wenn
- sie berechtigt ist, den Online Banking Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

(2) Die CRI wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

10.3 Aufhebung der Sperre

Die CRI wird eine Sperre aufheben, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

10.4 Automatische Sperre eines Online Banking Zugang über das Portal mittels PIN und TAN

Die dreimalige Falscheingabe des PIN führt zu einer Sperre des Online Banking Zugangs über das Portal.

11. Haftung

11.1 Haftung der CRI bei einer nicht autorisierten Online Banking Verfügung und einer nicht oder fehlerhaft ausgeführten Online Banking Verfügung

Die Haftung der CRI bei einer nicht autorisierten Online Banking Verfügung und einer nicht oder fehlerhaft ausgeführten Online Banking Verfügung richtet sich vorrangig nach Ziffer 11.2 und nachrangig nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen.

11.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verloren gegangenen, gestohlenen oder sonst abhandengekommenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der CRI hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Kontoinhaber an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Authentifizierungsinstruments ein Verschulden trifft.

(2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verloren gegangen, gestohlen oder sonst abhandengekommen ist, haftet der Kontoinhaber für den der CRI hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Kontoinhaber seine Pflicht zur sicheren Aufbewahrung der personalisierten Sicherheitsmerkmale schuldhaft verletzt hat.

(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absatz 1 und 2 hinaus bis zu einem Höchstbetrag von der Hälfte des verfügten Betrages, wenn der Kontoinhaber fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.

(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 9.1 nicht abgeben konnte, weil die CRI nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(5) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er
- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des personalisierten Sicherheitsmerkmals der CRI nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 9.1 Absatz 1),
- das personalisierte Sicherheitsmerkmal gespeichert hat (siehe Nummer 7.2 Absatz 2 1. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt oder das Autorisierungsinstrument einem Dritten zugänglich macht und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1 2. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2 3. Spiegelstrich),
- das personalisierte Sicherheitsmerkmal außerhalb des Online Banking Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2 4. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet hat (siehe Nummer 7.2 Absatz 2 5. Spiegelstrich),
- wenn der Teilnehmer die mittels SMS empfangene TAN auf demselben Empfangsgerät für das Online Banking einsetzt. (siehe Nummer 7.2 Absatz 2 7.Spiegelstrich) oder
- die auf seinem Authentifizierungsinstrument angezeigten Auftragsdaten nicht prüft.

11.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verloren gegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung und ist der CRI hierdurch ein Schaden entstanden, haften der Kontoinhaber und die CRI nach den gesetzlichen Grundsätzen des Mitverschuldens.

11.2.3 Haftung der CRI ab der Sperranzeige

Sobald die CRI eine Sperranzeige eines Kontoinhabers erhalten hat, übernimmt sie alle danach über das Online Banking durch nicht autorisierte Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

12. Datenschutz

Alle im Rahmen von Commerz Real Investmentgesellschaft mbH Online Banking entstehenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der CRI nur innerhalb der Europäischen Union erhoben und verarbeitet.

Commerz Real Investmentgesellschaft mbH