Anlage 1

Kundeninformation
mit Erläuterungen zu den Änderungen der Sonderbedingungen für das Online-Banking zum 14. September 2019

Sehr geehrte Kundin,
sehr geehrter Kunde,

am 14. September 2019 treten neue gesetzliche Bestimmungen für die Erbringung von Zahlungsdiensten in Kraft. Diese haben ihren Ursprung in europäischen Vorgaben der Zweiten EU-Zahlungsdiensterichtlinie. Sie dienen vor allem der Gewährleistung der Sicherheit im Online-Banking. Deshalb ändern wir mit Wirkung zum 14. September 2019 die Sonderbedingungen für das Online-Banking, die wir Ihnen als Anlage beifügen. Erläuterungen zu den wesentlichen Änderungen können Sie dieser Kundeninformation entnehmen.

I. Sicherheit durch Kundenauthentifizierung

Wenn Sie als Kunde eine Zahlung per Online-Banking auslösen, nutzen Sie die mit uns als Bank vereinbarten Authentifizierungselemente, wie z. B. Online-PIN und -TAN. So können wir feststellen, dass tatsächlich Sie als unser Kunde diese Vorgänge berechtigterweise veranlasst haben. Die Zweite EU-Zahlungsdiensterichtlinie erkennt diese Authentifizierungsverfahren an und regelt diese nunmehr gesetzlich:

- Grundsätzlich soll bei jeder Transaktion eine starke Kundenauthentifizierung erfolgen. Das erfordert, dass Authentifizierungselemente aus den Kategorien Wissen, Besitz und Sein (z. B. eine PIN als Wissenselement oder ein Mobiltelefon, an welches eine TAN übermittelt wird, als Besitzelement) einzusetzen sind. Das bedeutet für Sie konkret, dass Sie beispielsweise beim Zugriff auf Kontoinformationen in der Regel zwei Authentifizierungselemente – Online-PIN und -TAN – einsetzen müssen, wie Sie es bereits bisher gewohnt sind.

- Allerdings geben die gesetzlichen Vorschriften uns als Bank die Möglichkeit, in be-stimmten Fällen den Einsatz nur eines Authentifizierungselements anzufordern. So können wir z. B. beim wiederholten Abruf von Kontoinformationen innerhalb einer bestimmten Zeitspanne auch nur die Online-PIN verlangen. Weitere Ausnahmemöglichkeiten bestehen beispielsweise bei Überweisungen an vertrauenswürdige Empfänger, auf Eigenkonten und bei Kleinbetragszahlungen.

II. Einzelne Änderungen der Sonderbedingungen für das Online-Banking

1. Beschreibung des Einsatzes der Authentifizierungselemente

Die Regelungen über Authentifizierungselemente sind neu gefasst worden, um einerseits den neuen gesetzlichen Vorgaben Rechnung zu tragen und andererseits die Vielfalt an möglichen Authentifizierungsverfahren technikneutral zu erfassen. Das bedeutet im Einzelnen:

- In Nummer 2 der Bedingungen wird der neue Begriff „Authentifizierung" eingeführt. Dabei handelt es sich um das Verfahren, mit dessen Hilfe die Bank Ihre Identität oder die berechtigte Verwendung eines vereinbarten Zahlungsinstrumentes überprüfen kann (Nummer 2 Absatz 2). Ihre Authentifizierung ist die Voraussetzung für die Nutzung des Online-Banking (Nummer 2 Absatz 1). Sie erfolgt anhand der zwischen Ihnen und der Bank vereinbarten Authentifizierungselemente (Nummer 2 Absatz 2 und Absatz 4).
- In Nummer 2 Absatz 3 wird der neue Begriff „Authentifizierungselemente" eingeführt. Dies sind:
  - Wissenselemente, also etwas, das nur Sie wissen (z. B. eine PIN),
  - Besitzelemente, also etwas, das nur Sie besitzen (z. B. Ihre girocard mit TAN-Generator oder ein Mobiltelefon, an welches eine TAN übermittelt wird), oder
  - Seinselemente, also etwas, das nur Sie sind (z. B. Ihr Fingerabdruck als biometrisches Merkmal).

- Mit Authentifizierungselementen können Sie sich im Online-Banking als berechtigter Teilnehmer ausweisen, auf Informationen (z. B. Kontostand und Umsätze) zugreifen sowie Aufträge (z. B. Überweisungen) erteilen (Nummer 2 Absatz 4). Welche Authentifizierungselemente Sie im Online-Banking einsetzen müssen, richtet sich nach der Vereinbarung zwischen Ihnen und Ihrer Bank und der jeweiligen Anforderung durch die Bank.

- In Nummern 3 und 4 wird der Einsatz der Authentifizierungselemente beschrieben, um Zugang zum Online-Banking und Zugriff auf Informationen (z. B. Kontodaten) zu erhalten und Aufträge zu erteilen. Wichtig ist, dass wir als Bank von Ihnen die jeweils erforderlichen Authentifizierungselemente anfordern (z. B. bei Erteilung eines Zahlungsauftrags Online-PIN und -TAN), damit wir prüfen können, wer handelt.

- Aufgrund der Einführung des Begriffs „Authentifizierungselemente" haben sich auch weitere Regelungen geändert. So sind die Authentifizierungselemente nunmehr der Bezugspunkt für die Sorgfaltspflichten (Nummer 7.1), der Pflicht zur Sperranzeige (Nummer 8.1), der Nutzungssperre (Nummer 9) und der Regelungen zu Haftung (Nummer 10).

2. Sorgfaltspflichten zum Schutz der Sicherheit des Online-Banking

Aufgrund der neuen gesetzlichen Bestimmungen und der damit einhergehenden technischen Anpassungen an die neuen Sicherheitsanforderungen haben sich auch Ihre Sorgfaltspflichten als Teilnehmer im Online-Banking geändert (Nummer 7.1). Zum Schutz Ihrer Authentifizierungselemente vor unbefugtem Zugriff müssen Sie alle zumutbaren Vorkehrungen treffen. Anderenfalls besteht die Gefahr, dass das Online-Banking nicht autorisiert oder missbräuchlich genutzt wird. So müssen Sie nach Nummer 7.1 Absatz 2 insbesondere

- Ihre Wissenselemente (z. B. Ihre PIN) geheim halten,
- Ihre Besitzelemente (z. B. Ihre girocard mit TAN-Generator oder Ihr Mobiltelefon, an welches eine TAN übermittelt wird) vor Missbrauch schützen und
- bei der Verwendung von Seinselementen (z. B. Ihr Fingerabdruck als biometrisches Merkmal) beachten, dass auf Ihrem mobilen Endgerät (z. B. Mobiltelefon mit Finger-abdrucksensor) keine anderen Seinselemente anderer Personen gespeichert sind.

Wir bitten Sie, die Sorgfaltspflichten sorgfältig zu lesen. Indem Sie die Sorgfaltspflichten be-achten, schützen Sie Ihr Online-Banking und reduzieren die Betrugsrisiken. Bei vorsätzlicher oder grob fahrlässiger Verletzung der Sorgfaltspflichten könnten Sie für den hieraus entstandenen Schaden haften.

3. Nutzung des Online-Banking mittels Kontoinformationsdiensten, Zahlungsauslösediensten und sonstigen Drittdiensten

Sie können das Online-Banking auch mittels Kontoinformationsdiensten, Zahlungsauslöse-diensten und von Ihnen ausgewählten, sonstigen Drittdiensten nutzen (Nummer 1 Absatz 1). Ihre Authentifizierungselemente dürfen Sie gegenüber einem von ihnen ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst sowie einem sonstigen Drittdienst ver-wenden. Sofern Sie sonstige Drittdienste nutzen, müssen Sie diese sorgfältig auswählen (Nummer 7.1 Absatz 5).

Den gesetzlichen Regelungen entsprechend kann die Bank nach Nummer 9.5 Kontoinforma-tions- und Zahlungsauslösedienstleistern den Zugang zu einem Zahlungskonto verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Kontoinformations- oder des Zahlungsauslö-sedienstleisters zum Zahlungskonto es rechtfertigen. Über die Sperre sowie ggf. über die Aufhebung der Sperre wird der Kontoinhaber informiert.