8201 Schaffhausen
Telefon +41 52 635 22 22
www.shkb.ch

Schaffhauser Kantonalbank

Bedingungen der Schaffhauser Kantonalbank zur Nutzung der «one» App

Ausgabe März 2026

A ALLGEMEINER TEIL

1. Einleitung

1.1 Geltungsbereich dieser Bedingungen und weitere relevante Geschäftsbedingungen

Die vorliegenden Bedingungen gelten für die von Viseca Payment Solutions (nachfolgend Servicebetreiberin genannt) im Auftrag der Schaffhauser Kantonalbank (nachfolgend Bank genannt) an Inhaberinnen und Inhaber einer Visa Debit-Karte (nachfolgend Karte(n) genannt) unter der Bezeichnung «one» zur Verfügung gestellten Online-Services (nachfolgend Services genannt).

Die «one» App ist verfügbar über:
- die «one» Website (nachfolgend Website genannt) und
- die SHKB «one» App (nachfolgend App genannt).

Zu beachten sind die weiteren Informationen zu «one» – insbesondere zur Bearbeitung von Daten und zur Datensicherheit – in der Datenschutzerklärung der Bank sowie den Datenschutzbestimmungen für «one» der Servicebetreiberin unter https://card-terms.ch/de/viseca/bestimmungen-one.

Die vorliegenden Bedingungen gelten zusätzlich zu den jeweils anwendbaren Allgemeinen Geschäftsbedingungen der Bank sowie den «Bedingungen für die Nutzung der Visa Debit-Karten» (nachfolgend Nutzungsbedingungen Debit-Karten genannt). Im Fall abweichender Regelungen gehen die vorliegenden Bedingungen den Nutzungsbedingungen Debit-Karten vor.

1.2 Was ist «one» und wie wird es weiterentwickelt?

«one» umfasst Services, die durch die Servicebetreiberin erbracht werden. Die Nutzung von «one» setzt eine Registrierung voraus. Der registrierten Inhaberin/dem registrierten Inhaber werden neu eingeführte Services durch Aktualisierungen (Updates) zur Verfügung gestellt. Die Servicebetreiberin informiert die Inhaberin/den Inhaber auf angemessene Weise über die Weiterentwicklungen und gegebenenfalls die damit zusammenhängenden Änderungen der vorliegenden Bestimmungen.

1.3 Welche Funktionen bietet die «one» App?

«one» kann insbesondere folgende Funktionen umfassen:
- Benutzerkonto zur Verwaltung persönlicher Daten;
- Kontrolle und Bestätigung von Zahlungen z.B. mittels 3-D Secure (Visa Secure) in der App oder durch Eingabe eines SMS-Code (vgl. Ziff. 5);
- Kontrolle und Bestätigung bestimmter Handlungen (z.B. Logins, Kontakte mit der Servicebetreiberin) in der App oder durch Eingabe eines SMS-Code;
- Aktivierung von Karten zur Nutzung von Zahlmöglichkeiten (vgl. Ziff. 6);
- Austausch von Mitteilungen und Benachrichtigungen aller Art zwischen der Inhaberin/dem Inhaber und der Servicebetreiberin (auch z.B. die Mitteilung einer Änderung von Bestimmungen), sofern nicht eine besondere Form der Mitteilung bzw. Benachrichtigung vorbehalten wird;
- Übersicht über Transaktionen und Karten;
- Informationen im Zusammenhang mit der Verwendung der Karte.

2. Nutzung der «one» App

2.1 Nutzungsberechtigung

Die Inhaberin/der Inhaber ist nur unter folgenden Voraussetzungen berechtigt, «one» zu nutzen:
- Sie/er ist in der Lage, die vorliegenden Bestimmungen und die damit verbundenen Anforderungen umzusetzen (insbesondere Ziff. 3.2) und
- sie/er ist zur Nutzung einer Karte der Bank berechtigt.

2.2 Einwilligungen bei der Registrierung und im Rahmen der Weiterentwicklung von «one»

Die Inhaberin/der Inhaber erteilt der Bank durch die Verwendung von «one» hiermit ausdrücklich folgende Einwilligungen:
- Einwilligung in die Bearbeitung von Daten, die bei der Nutzung von «one» erhoben wurden oder werden. Dies umfasst insbesondere auch die Einwilligung in deren Verbindung mit bei der Bank bereits bestehenden Daten und die Erstellung von Profilen, jeweils zu Zwecken des Risikomanagements und zu Marketingzwecken der Bank oder im Auftrag der Bank oder der Servicebetreiberin und Dritter gemäss Datenschutzbestimmungen «one».
- Einwilligung in den Empfang von Mitteilungen und Informationen zu Produkten und Dienstleistungen der Bank und Dritter zu Marketingzwecken (Werbung). Diese können von der Bank per E-Mail, direkt in der App oder auf der Website zugestellt werden.
- Einwilligung in die Verwendung der bei der Registrierung angegebenen E-Mail-Adresse sowie der Website und der App zur gegenseitigen elektronischen Kommunikation mit der Bank (z.B. Mitteilungen von Adressänderungen, Mitteilung der Änderung von Bedingungen (AGB) oder Mitteilungen im Zusammenhang mit der Bekämpfung von Kartenmissbrauch).

Die Einwilligung in den Empfang von Mitteilungen zu Produkten und Dienstleistungen und/oder in die Datenbearbeitung zu Marketingzwecken kann jederzeit durch Mitteilung an die Bank mit Wirkung für die Zukunft widerrufen werden (opt-out-

Recht). Die entsprechenden Kontaktangaben finden sich in der Datenschutzerklärung der Bank.

2.3 Ablehnung von Einwilligungen im Rahmen der Weiterentwicklung von «one»

Lehnt die Inhaberin/der Inhaber die Erteilung einer Einwilligung in Bestimmungen im Rahmen der Weiterentwicklung von «one» (z.B. bei Updates) ab, können die App oder die Website oder einzelne Services davon unter Umständen nicht oder nicht mehr genutzt werden.

2.4 Wirkung der Vornahme von Bestätigungen

Jede Bestätigung, die über die App oder durch die Eingabe eines SMS-Code vorgenommen wird, gilt als Handlung der Inhaberin/des Inhabers. Sie/er hat das Recht, den Beweis des Gegenteils zu erbringen. Die Inhaberin/der Inhaber verpflichtet sich, für aus Bestätigungen resultierende Belastungen ihrer/seiner Karte einzustehen und ermächtigt die Bank zur Ausführung entsprechender Aufträge und zur Vornahme entsprechender Handlungen.

2.5 Verfügbarkeit / Sperrung / Änderungen

Die Bank kann die Möglichkeit zur Nutzung von «one» aus zureichenden Gründen jederzeit ganz oder teilweise auch ohne vorgängige Mitteilung unterbrechen, einschränken, einstellen oder durch eine andere Leistung ersetzen. Die Bank hat insbesondere das Recht, den Zugang der Inhaberin/des Inhabers zu «one» vorübergehend oder definitiv zu sperren (z.B. bei Verdacht auf Missbrauch).

2.6 Immaterialgüterrechte und Lizenz

Sämtliche Rechte (insbesondere Urheber- und Markenrechte) an Software, Texten, Bildern, Videos, Namen, Logos und anderen Daten und Informationen, die über «one» zugänglich sind oder im Lauf der Zeit zugänglich werden, stehen ausschliesslich der Bank oder den entsprechenden Partnern und Dritten (z.B. Mastercard, Visa) zu, sofern in diesen Bedingungen nichts Anderes vorgesehen ist. Die auf «one» sichtbaren Namen und Logos sind geschützte Marken.

Für die Nutzung der App gewährt die Bank der Inhaberin/dem Inhaber eine nicht ausschliessliche, nicht übertragbare, unbefristete, widerrufliche und unentgeltliche Lizenz, um die App herunterzuladen, auf einem im dauerhaften Besitz der Inhaberin/des Inhabers befindlichen Gerät zu installieren und sie im Rahmen der vorgesehenen Funktionen zu nutzen.

3. Risiken, Gewährleistungsausschluss und allgemeine Sorgfalts- und Meldepflichten

3.1 Risiken bei der Nutzung von «one»

Die Inhaberin/der Inhaber nimmt zur Kenntnis und akzeptiert, dass die Nutzung von «one» Risiken mit sich bringt.

Es ist insbesondere möglich, dass mit der Nutzung von «one» Karten, Benutzername und Passwort, verwendete Geräte oder persönliche Daten der Inhaberin/des Inhabers durch unberechtigte Dritte missbraucht werden. Dadurch kann die Inhaberin/der Inhaber finanziell (durch Belastung ihrer/seiner Karte) geschädigt und in ihrer/seiner Persönlichkeit (durch Missbrauch persönlicher Daten) verletzt werden. Weiter besteht das Risiko, dass «one» oder einer der auf «one» angebotenen Services nicht genutzt werden kann (z.B. kein Login auf «one» möglich).

Missbräuche werden ermöglicht oder begünstigt insbesondere durch:

- die Verletzung von Sorgfalts- oder Meldepflichten durch die Inhaberin/den Inhaber (z.B. durch unsorgfältigen Umgang mit Benutzername / Passwort oder Nichtmelden von Kartenverlust);
- die von der Inhaberin/dem Inhaber gewählten Einstellungen oder mangelhaften Unterhalt der für die Nutzung von «one» verwendeten Geräte und Systeme (z.B. Computer, Mobiltelefon, Tablet und weitere EDV-Infrastruktur), z.B. durch fehlende Bildschirm-Sperre, durch fehlende oder ungenügende Firewall bzw. Virenschutz oder durch veraltete Software;
- Eingriffe Dritter oder Fehler bei der Datenübermittlung über das Internet (z.B. Hacking, Phishing oder Datenverlust);
- fehlerhafte Bestätigungen in der App oder durch Eingabe eines SMS-Code (z.B. bei mangelhafter Kontrolle einer Bestätigungsanfrage);
- von der Inhaberin/dem Inhaber für «one» – insbesondere für die App – gewählte schwächere Sicherheitseinstellungen (z.B. Speicherung des Logins).

Hält die Inhaberin/der Inhaber die folgenden Sorgfalts- und Meldepflichten im Umgang mit den mobilen Geräten und dem Passwort sowie die Pflichten zur Kontrolle der Bestätigungsanfragen ein, kann sie/er diese Risiken eines Missbrauchs vermindern. Weitere Informationen zur Verminderung der Risiken bei der Nutzung von «one» werden unter www.one-digitalservice.ch zur Verfügung gestellt.

Die Bank sichert nicht zu und leistet keine Gewähr, dass die Website und die App dauerhaft zugänglich sind oder störungsfrei funktionieren oder dass Missbräuche erkannt und mit Sicherheit verhindert werden können.

3.2 Sorgfaltspflichten der Inhaberin/des Inhabers

3.2.1 Sorgfaltspflichten für verwendete Geräte und Systeme, insbesondere mobile Geräte

«one» verwendet zur Authentifizierung u.a. mobile Geräte (z.B. Mobiltelefon, Tablet; jeweils „mobiles Gerät" genannt) der Inhaberin/des Inhabers. Der jederzeitige Gewahrsam dieser mobilen Geräte ist deshalb ein wesentlicher Sicherheitsfaktor. Sie/er hat mobile Geräte mit angemessener Sorgfalt zu behandeln und für deren angemessenen Schutz zu sorgen.

Die Inhaberin/der Inhaber hat daher insbesondere folgende allgemeine Sorgfaltspflichten im Zusammenhang mit den verwendeten Geräten und Systemen, insbesondere den mobilen Geräten, einzuhalten:

- für mobile Geräte ist eine Bildschirm-Sperre zu aktivieren und es sind weitere Sicherheitsmassnahmen zu ergreifen, um die Entsperrung durch Unberechtigte zu verhindern;
- mobile Geräte müssen geschützt vor einem Zugriff Dritter an einem sicheren Ort aufbewahrt werden, und sie dürfen nicht an Dritte zum dauernden oder zum unbeaufsichtigten Gebrauch weitergegeben werden;
- Software (z.B. Betriebssysteme und Internet-Browser) muss regelmässig aktualisiert werden;
- Eingriffe in die Betriebssysteme (z.B. „Jailbreaking" oder „Rooting") sind zu unterlassen;
- auf dem Laptop/Computer sind Virenschutz- und Internet-Security-Programme zu installieren und aktuell zu halten;

- die App darf ausschliesslich aus den offiziellen Stores (z.B. Apple Store und Google Play Store) heruntergeladen werden;
- Aktualisierungen (Updates) der App sind umgehend zu installieren;
- im Fall eines Verlusts eines mobilen Gerätes ist das Mögliche zu unternehmen, um den Zugriff Unberechtigter auf die von der Bank an das mobile Gerät übermittelten Daten zu verhindern (z.B. durch Sperren der SIM-Karte, Sperren des Gerätes, Löschen der Daten beispielsweise über „mein iPhone suchen" bzw. „Android Geräte Manager", Zurücksetzen oder Zurücksetzenlassen des Benutzerkontos). Der Verlust ist der Bank zu melden (vgl. Ziff. 3.3);
- die App muss vor einem Verkauf oder einer sonstigen dauerhaften Weitergabe des mobilen Gerätes an Dritte gelöscht werden.

3.2.2 Sorgfaltspflichten in Bezug auf das Passwort

Neben dem Besitz des mobilen Gerätes dienen Benutzername und Passwort als weitere Faktoren für die Authentifizierung der Inhaberin/des Inhabers. Sie/er hat im Zusammenhang mit dem Passwort insbesondere folgende allgemeine Sorgfaltspflichten einzuhalten:

- die Inhaberin/der Inhaber muss ein Passwort festlegen, das sie/er nicht bereits für andere Dienste verwendet hat und das nicht aus leicht ermittelbaren Kombinationen besteht (z.B. Telefonnummer, Geburtsdatum, Autokennzeichen, Namen der Inhaberin/des Inhabers oder ihr/ihm nahestehender Personen, wiederholte oder direkt anschliessende Zahlen- oder Buchstabenfolgen wie "123456" oder „aabbcc");
- das Passwort muss geheim gehalten werden. Es darf Dritten nicht bekanntgegeben oder zugänglich gemacht werden. Die Inhaberin/der Inhaber nimmt zur Kenntnis, dass die Bank sie/ihn nie zur Bekanntgabe des Passwortes auffordern wird;
- das Passwort darf weder notiert noch ungesichert gespeichert werden;
- die Inhaberin/der Inhaber muss das Passwort ändern oder das Benutzerkonto zurücksetzen oder durch die Bank zurücksetzen lassen, wenn Verdacht besteht, dass Dritte in den Besitz des Passwortes oder weiterer Daten gelangt sind;
- die Eingabe des Passwortes darf nur so erfolgen, dass sie von Dritten nicht eingesehen werden kann.

3.2.3 Sorgfaltspflichten bei Bestätigungsanfragen, insbesondere Kontrolle

Bestätigungen verpflichten die Inhaberin/den Inhaber verbindlich. Sie/er hat daher folgende allgemeinen Sorgfaltspflichten im Zusammenhang mit Bestätigungen und Kontrollen in der App oder durch die Eingabe eines SMS-Code einzuhalten:

- die Inhaberin/der Inhaber darf nur dann bestätigen, wenn die Bestätigungsanfrage mit einer bestimmten Handlung oder einem bestimmten Vorgang (z.B. Zahlung, Login, Kontakt mit der Bank) der Inhaberin/des Inhabers in unmittelbarem Zusammenhang steht;
- die Inhaberin/der Inhaber muss vor der Bestätigung kontrollieren, ob der Gegenstand der Bestätigungsanfrage mit dem betreffenden Vorgang übereinstimmt. Insbesondere sind bei Bestätigungsanfragen im Zusammenhang mit 3-D Secure die angezeigten Zahlungsdetails zu kontrollieren. Bei Verdacht auf missbräuchliche Transaktionen durch Dritte kann Viseca betroffene Nutzerinnen/Nutzer über die «one» App kontaktieren und auffordern, die verdächtigen Transaktionen zu prüfen und zu bestätigen.

3.3 Meldepflichten der Inhaberin/des Inhabers

Folgende Ereignisse sind der Bank umgehend zu melden:

- Verlust eines mobilen Gerätes, nicht hingegen ein nur kurzzeitiges Nichtauffinden;
- Bestätigungsanfragen, die nicht mit einer Online-Zahlung, einem Login durch die Inhaberin/den Inhaber, einem Kontakt mit der Bank oder ähnlichen Vorgängen in Zusammenhang stehen (Missbrauchsverdacht);
- anderweitiger Verdacht, dass Bestätigungsanfragen in der App oder der SMS-Code nicht von der Servicebetreiberin stammen;
- Verdacht auf Missbrauch von Benutzername, Passwort, mobilen Geräten, der Website, der App etc. oder Verdacht, dass unberechtigte Dritte in den Besitz derselben gelangt sind;
- Änderungen der Telefonnummer und anderer relevanter persönlicher Daten;
- Wechsel des mobilen Gerätes, das für «one» verwendet wird (erfordert eine Neuregistrierung der App).

Mögliche Missbräuche oder der Verlust eines mobilen Gerätes sind umgehend telefonisch dem Contact Center der Bank zu melden: Tel. +41 52 635 22 22 oder +41 58 958 69 50 (24h Sperrzentrale).

4. Haftung

4.1 Haftung bei Schäden im Allgemeinen

Unter Vorbehalt von Ziff. 4.2 ersetzt die Bank Schäden (ohne Selbstbehalt), die nicht durch eine Versicherung übernommen werden,

- wenn die betreffenden Schäden:
  - entstanden sind infolge eines nachweislich rechtswidrigen Eingriffs in Einrichtungen von Netzwerk- und/oder Telekommunikationsbetreibern oder in die von der Inhaberin/dem Inhaber genutzten Geräte und/oder Systeme (z.B. Computer, mobile Geräte und weitere EDV-Infrastruktur) und
  - die Inhaberin/der Inhaber die vorstehend in Ziff. 3.2 und 3.3 statuierten allgemeinen und besonderen Sorgfalts- und Meldepflichten, insbesondere die Pflichten zur Kontrolle von Bestätigungsanfragen und die in den Nutzungsbedingungen Debitkarten statuierte Pflicht zur Prüfung des Kontoauszugs (Debitkarte) bzw. der Monatsrechnung (Kreditkarte) sowie die rechtzeitige Beanstandung missbräuchlicher Transaktionen, eingehalten hat und
  - die Inhaberin/den Inhaber auch sonst in keiner Weise ein Verschulden an der Entstehung der Schäden trifft.
- wenn die betreffenden Schäden ausschliesslich durch eine Verletzung der geschäftsüblichen Sorgfalt der Bank entstanden sind.

Die Haftung für allfällige indirekte Schäden oder Folgeschäden der Inhaberin/des Inhabers irgendwelcher Art wird von der Bank unter Vorbehalt von Vorsatz oder Grobfahrlässigkeit nicht übernommen.

4.2 Ausnahmen

Die Inhaberin/der Inhaber trägt das Risiko für Schäden in den folgenden Fällen selbst und die Bank schliesst insoweit die Haftung aus:

- wenn die betreffenden Schäden nicht nach Ziff. 4.1 von der Bank getragen werden (somit insbesondere bei einer Verletzung von Sorgfalts- und Meldepflichten durch die Inhaberin/den Inhaber), oder
- wenn die Inhaberin/der Inhaber, deren/dessen Ehe- bzw. eingetragene Partner, direkt verwandte Familienmitglieder (insbesondere Kinder und Eltern) oder andere der Inhaberin/dem Inhaber nahestehende Personen, Bevollmächtigte, Inhaberinnen/Inhaber von Zusatzkarten und/ oder im gleichen Haushalt lebende sowie sich dort regelmässig aufhaltende Personen eine Handlung (z.B. Bestätigung in der App oder per SMS-Code) vorgenommen haben.

B BESONDERER TEIL

5. 3-D Secure

5.1 Was ist 3-D Secure?

3-D Secure ist ein international anerkannter Sicherheitsstandard für Kartenzahlungen im Internet. Er wird bei Mastercard „SecureCode", bei VISA „Visa Secure" genannt. Die Inhaberin/der Inhaber ist aufgrund der Nutzungsbedingungen Debit-Karten verpflichtet, diesen Sicherheitsstandard bei Zahlungen zu verwenden, sofern er von der Akzeptanzstelle (dem Händler) angeboten wird. Die Verwendung von 3-D Secure ist nur nach einer Registrierung bei «one» möglich.

5.2 Wie funktioniert 3-D Secure?

Zahlungen mit 3-D Secure können auf zwei Arten bestätigt (autorisiert) werden:

- in der App oder
- durch Eingabe eines SMS-Codes im Browserfenster, während des Bezahlvorgangs. Der Code wird der Inhaberin/dem Inhaber durch die Servicebetreiberin per Kurzmitteilung (SMS) gesendet.

Gemäss den Nutzungsbedingungen Debit-Karten gilt jeder autorisierte Einsatz der Karte mit 3-D Secure als durch die Inhaberin/den Inhaber erfolgt.

5.3 Aktivierung von Karten für 3-D Secure

3-D Secure wird für alle Karten, die auf den Namen der Inhaberin/des Inhabers lauten und mit ihrer/seiner registrierten Geschäftsbeziehung zur Bank zusammenhängen, durch die Registrierung auf «one» aktiviert.

5.4 Deaktivierung von Karten für 3-D Secure

3-D Secure kann aus Sicherheitsgründen nach erfolgter Aktivierung nicht mehr deaktiviert werden.

6. Mobile Payment

6.1 Was ist Mobile Payment?

Mit Mobile Payment werden Lösungen für den Einsatz von Karten über ein mobiles Gerät bezeichnet. Mobile Payment ermöglicht der Inhaberin/dem Inhaber, die/der über ein kompatibles mobiles Gerät verfügt, berechtigte Karten über eine mobile Applikation (App) der Bank (dazu Ziff. 6.8) oder eines Drittanbieters für kontaktloses Bezahlen wie auch das Bezahlen in Online-Shops und in Apps zu nutzen. Dabei wird aus Sicherheitsgründen anstelle der Kartennummer jeweils eine andere Nummer (Token) generiert und als „virtuelle Karte" hinterlegt. Virtuelle Karten können über Mobile Payment wie eine physische Karte eingesetzt werden. Bei der Bezahlung mit einer virtuellen Karte wird nicht die Kartennummer, sondern lediglich die generierte Nummer (Token) an den Händler weitergegeben. Nutzerinnen/Nutzer finden in der «one» App eine Übersicht aller aktiven Token und können diese dort verwalten.

6.2 Click to Pay

Click to Pay von Mastercard und Visa vereinfacht das Bezahlen bei Online-Einkäufen, indem E-Mail- und Lieferadresse bei der Kartenorganisation registriert werden. Danach können Nutzer überall, wo das Click to Pay Symbol abgebildet ist, mit ihrer E-Mail-Adresse online einkaufen, ohne Kartendetails eingeben zu müssen.
Karteninhaberinnen und -inhaber, welche die Nutzungsbestimmungen der Kartenorganisation akzeptieren und deren Datenschutzbestimmungen zur Kenntnis nehmen, können die Karte für Click to Pay in der «one» App hinterlegen. Nach Hinterlegung der Karte werden mit Zustimmung der Nutzerin oder des Nutzers Informationen zur Karte, E-Mail-Adresse sowie zur Lieferadresse an die Kartenorganisation übermittelt. Im Benutzerkonto von Click to Pay können die für die Zahlung hinterlegten Information zu Karten, E-Mail-Adresse sowie Lieferadresse jederzeit bearbeitet und gelöscht werden.

Die Nutzung von Click to Pay kann jederzeit beendet werden, indem die hinterlegte Karte bei den Kartenorganisationen entfernt wird.

Mastercard oder Visa können Click to Pay jederzeit weiterentwickeln oder sperren, insbesondere, wenn Grund zur Annahme besteht, dass Click to Pay missbräuchlich verwendet wird.

6.3 Alias-Verzeichnisdienst

Mit dem Alias-Verzeichnisdienst, der von Visa angeboten wird, können Nutzerinnen/Nutzer einen «Alias» wie z. B. E-Mail-Adresse oder Telefonnummer mit ihrer Karte verknüpfen. Damit werden die Überweisung und der Empfang von Geldern über die Zahlungssysteminfrastruktur vereinfacht und sensible Zahlungsinformationen geschützt. Die Nutzerin/der Nutzer akzeptiert, dass die Servicebetreiberin bei Hinterlegung des Alias Informationen zur Karte, zum Namen und zur Telefonnummer der Nutzer an Visa übermittelt. Die Nutzer sind dafür verantwortlich, ihre Alias-Daten im Rahmen des Alias-Verzeichnisdienstes korrekt einzugeben und jederzeit aktuell zu halten.

Weder die Bank noch die Servicebetreiberin haften für Schäden aus der Verwendung des Alias-Verzeichnisdienstes.

Visa kann den Alias-Verzeichnisdienst jederzeit weiterentwickeln oder sperren, insbesondere, wenn Grund zur Annahme besteht, dass der Dienst missbräuchlich verwendet wird.

6.4 Welche mobilen Geräte sind kompatibel, und welche Karten sind zugelassen?

Kompatibel sind mobile Geräte wie z.B. Computer, Mobiltelefone, Smartwatches und Fitnesstracker, soweit sie die Verwendung virtueller Karten unterstützen und von der Servicebetreiberin zugelassen sind. Die Servicebetreiberin entscheidet, welche Karten für welche Anbieter zugelassen sind. Weitere Informationen zu kompatiblen Geräten und zu den berechtigten Karten finden Sie auf der Website der Bank oder auf der

Schaffhauser Kantonalbank

Website des Herstellers Ihres mobilen Gerätes. Diese Informationen sind nicht verbindlich und können jederzeit geändert werden.

6.5 Aktivierung und Deaktivierung

Aus Sicherheitsgründen setzt die Aktivierung einer Karte voraus, dass die Inhaberin/der Inhaber die Nutzungsbedingungen des jeweiligen Anbieters (z.B. Apple, Google oder Samsung) akzeptiert und dessen Datenschutzbestimmungen zur Kenntnis nimmt. Die Inhaberin/der Inhaber ist der Bank für Schäden infolge einer Verletzung dieser Bedingungen ersatzpflichtig.

Virtuelle Karten können bis zu einer Sperrung oder Deaktivierung der Karte über die App durch die Inhaberin/den Inhaber eingesetzt werden. Vorbehalten bleiben Einschränkungen des Karteneinsatzes nach den Bestimmungen der jeweils anwendbaren Nutzungsbedingungen Debit-Karten. Die Inhaberin/der Inhaber kann die Nutzung von Mobile Payment jederzeit beenden, indem sie/er die virtuelle(n) Karte(n) beim jeweiligen Anbieter entfernt.

Kosten in Zusammenhang mit der Aktivierung und dem Einsatz virtueller Karten (z.B. Kosten für eine mobile Internetnutzung im Ausland) gehen zu Lasten der Inhaberin/des Inhabers.

6.6 Einsatz der virtuellen Karte (Autorisierung)

Der Einsatz einer virtuellen Karte entspricht einer üblichen Kartentransaktion. Jeder Einsatz einer virtuellen Karte gilt als durch die Inhaberin/den Inhaber autorisiert. Sie/er hat das Recht, den Beweis des Gegenteils zu erbringen.

Der Einsatz virtueller Karten ist entsprechend der vom Anbieter oder Händler vorgesehenen Weise zu autorisieren, z.B. durch Eingabe einer Geräte-PIN oder durch Fingerabdruck- oder Gesichtserkennung. Die Inhaberin/der Inhaber nimmt zur Kenntnis, dass sich dadurch das Risiko erhöht, dass virtuelle Karten durch Unberechtigte eingesetzt werden können, wenn das allenfalls vom Anbieter oder Händler zusätzlich geforderte Autorisierungsmittel (Geräte-PIN oder Karten-PIN) aus leicht zu ermittelnden Kombinationen („1234") besteht. Sie/er nimmt weiter zur Kenntnis, dass je nach Anbieter oder Händler bis zu einem von diesem zu bestimmenden Betrag, keine Autorisierung verlangt wird. Im Übrigen richtet sich die Haftung nach Ziffer 4 dieser Bedingungen.

6.7 Risiken und Sorgfaltspflichten

Die Inhaberin/der Inhaber nimmt nur Kenntnis und akzeptiert, dass die Nutzung von Mobile Payment trotz aller Sicherheitsmassnahmen Risiken mit sich bringt. Es ist insbesondere möglich, dass virtuelle Karte(n) und persönliche Daten von Unberechtigten missbraucht oder eingesehen werden. Dadurch kann sie/er finanziell geschädigt (durch missbräuchliche Belastungen einer Karte) und in ihrer/seiner Persönlichkeit verletzt werden (durch Missbrauch von persönlichen Daten).

Die Inhaberin/der Inhaber hat daher die verwendeten Geräte und virtuellen Karten mit Sorgfalt zu behandeln und für ihren Schutz zu sorgen. Sie/er hat – zusätzlich zu den Sorgfaltspflichten gemäss den jeweils anwendbaren Nutzungsbedingungen Debit-Karten und den Sorgfalts- und Meldepflichten nach Ziff. 3.2.1 und Ziff. 3.3 – insbesondere folgende besondere Sorgfaltspflichten einzuhalten:

- Die verwendeten Geräte müssen bestimmungsgemäss verwendet und geschützt vor einem Zugriff Dritter sicher aufbewahrt werden;
- virtuelle Karten sind wie physische Karten persönlich und nicht übertragbar. Sie dürfen nicht an Dritte zum Gebrauch weitergegeben werden (z.B. durch Hinterlegung von Fingerprints bzw. durch Scannen des Gesichts Dritter zur Entsperrung des verwendeten Geräts);
- bei einem Wechsel oder einer Weitergabe eines mobilen Geräts (z.B. im Fall eines Verkaufs) muss jede virtuelle Karte in der App des Anbieters und im mobilen Gerät gelöscht werden;
- ein Verdacht auf Missbrauch einer virtuellen Karte oder eines dafür verwendeten Geräts ist der Bank umgehend zu melden, damit die betroffene virtuelle Karte gesperrt werden kann.

6.8 Gewährleistungsausschluss

Es besteht kein Anspruch auf die Nutzung von Mobile Payment. Die Bank kann die Nutzung – d.h. die Möglichkeit, virtuelle Karten einzusetzen – jederzeit unterbrechen oder beenden, insbesondere aus Sicherheitsgründen oder bei Änderungen des Mobile Payment-Angebotes oder einer Beschränkung der berechtigten Karten oder kompatiblen Geräte. Die Bank ist ferner nicht für Handlungen und Angebote der Servicebetreiberin oder anderer Dritter wie z.B. Internet- und Telefonieanbieter verantwortlich.

6.9 Karteneinsatz über die «one» App

Verfügt die Inhaberin/der Inhaber über ein kompatibles Gerät, kann sie/er die Karte(n) in der «one» App der Bank als virtuelle Karte aktivieren. Zur Gewährleistung der Sicherheit bei Mobile Payment muss die Inhaberin/der Inhaber bei der Aktivierung eine Geheimzahl festlegen. Die Bank kann diesen Dienst jederzeit anpassen. Im Übrigen gelten die vorliegenden Bestimmungen für Mobile Payment, insbesondere die Sorgfaltspflichten gemäss Ziff. 6.5.

6.10 Datenschutz Mobile Payment

Der Drittanbieter und die Bank sind für ihre jeweilige Bearbeitung von Personendaten unabhängig verantwortlich. Die Inhaberin/der Inhaber nimmt zur Kenntnis, dass Personendaten im Zusammenhang mit dem Angebot und dem Einsatz von Mobile Payment (insbesondere Angaben über Inhaberin/Inhaber und aktivierte Karten und Transaktionsdaten aus dem Einsatz virtueller Karten) vom Drittanbieter erhoben und in der Schweiz oder im Ausland gespeichert und weiterbearbeitet werden. Die Bearbeitung von Personendaten durch den Drittanbieter im Zusammenhang mit Mobile Payment und der Verwendung von Angeboten und Leistungen des Drittanbieters einschliesslich dessen Geräte und Software richtet sich nach dessen Nutzungs- und Datenschutzbestimmungen.

Die Inhaberin/der Inhaber bestätigt daher durch jede Aktivierung einer Karte, dass sie/er die einschlägigen Datenschutzbestimmungen des jeweiligen Drittanbieters gelesen und verstanden hat und dass sie/er mit der entsprechenden Datenbearbeitung des Drittanbieters ausdrücklich einverstanden ist. Wünscht sie/er die entsprechende Bearbeitung nicht, liegt es in ihrer/seiner Verantwortung, auf die Aktivierung einer Karte zu verzichten oder der Bearbeitung gegenüber dem Drittanbieter zu widersprechen. Für die Bearbeitung von Personendaten durch die Bank sowie der Servicebetreiberin gelten die Datenschutzbestimmung «one» unter https://card-terms.ch/de/viseca/bestimmungen-one sowie die Datenschutzerklärung der Bank.