

# Kommunikation über die Webseite in Zusammenhang mit Kundensicherheit und Betrugserkennung

## Unser Sicherheitsansatz

Wenn es um Ihre Finanzdaten geht, legen wir höchsten Wert auf Ihre Sicherheit. Deshalb ist es wichtig, dass wir wissen, dass wirklich Sie es sind, wenn auf Ihr elektronisches Geldkonto zugegriffen wird. Dafür sorgen wir beispielsweise so:

**Login-Daten** – Beim Aktivieren Ihrer Karte haben Sie eindeutige Login-Daten für den Online-Zugang erstellt. Für Ihre eigene Sicherheit raten wir dazu, diese Daten geheim zu halten und Ihr Passwort regelmäßig zu ändern.

**Fragen zu personenbezogenen Daten** – Wenn Sie unseren Kundendienst kontaktieren, bitten wir Sie möglicherweise darum, Ihre Identität dadurch zu bestätigen, dass Sie Fragen zu den bei der Erstellung Ihres E-Geldkontos gemachten personenbezogenen Daten beantworten.

**Bereitstellen von Informationen** – Wir bitten Sie unter keinen Umständen darum, uns Ihr Online-Passwort, Ihre PIN oder Ihre vollständige 16-stellige Kartenummer mitzuteilen. Vor jeder Kontaktaufnahme erhalten Sie von uns grundsätzlich eine E-Mail. In dringenderen Fällen rufen wir Sie daraufhin möglicherweise auch an.

## Wie Sie einen Betrug melden können

Falls Sie etwas Verdächtiges bemerken und vermuten, es könnte sich dabei um eine betrügerische Aktivität handeln, sollten Sie uns schnellstmöglich telefonisch oder per E-Mail kontaktieren.

**Betrug melden:** Kontaktaufnahme per E-Mail an [support@cardcompact.co.uk](mailto:support@cardcompact.co.uk) oder telefonisch unter +49 (0) 1807 667766 \* = die ersten 30 Sekunden frei, danach 14 cent pro Minute aus dem deutschen Festnetz, Mobilfunk ggf. teurer, first 30 seconds for free, afterwards 14 cent per minute from the German landline. Prices for mobile phones may differ.

**Verlorene oder gestohlene Karten:** +49 (0)1805 666026 (rund um die Uhr erreichbar)

**Verdächtige E-Mails:** Kontaktaufnahme per E-Mail an [support@cardcompact.co.uk](mailto:support@cardcompact.co.uk) oder telefonisch unter +49 (0) 1807 667766 \* = die ersten 30 Sekunden frei, danach 14 cent pro Minute aus dem deutschen Festnetz, Mobilfunk ggf. teurer, first 30 seconds for free, afterwards 14 cent per minute from the German landline. Prices for mobile phones may differ.

### So schützen Sie sich vor Betrug

Indem Sie die Ratschläge unten befolgen, können Sie dazu beitragen, sich vor Betrügern zu schützen. Denken Sie immer daran: Handeln Sie nicht, wenn Sie sich unsicher fühlen! Aufrichtige Unternehmen werden Sie nie zum Handeln drängen.

Sorgen Sie dafür, dass Ihre bei uns hinterlegte Telefonnummer und E-Mail-Adresse stets aktuell sind, da wir über diese Kontakt zu Ihnen aufnehmen, wenn wir ungewöhnliche Aktivitäten auf Ihrem E-Geldkonto feststellen.

### Einige Tipps zur sicheren Nutzung Ihres E-Geldkontos und Ihrer Prepaid-Karte:

Wenn Sie über das Internet auf Ihr E-Geldkonto zugreifen:

- Machen Sie Gebrauch von Antiviren-Software und Firewalls.
- Sorgen Sie dafür, dass Ihr Computer und Ihr Browser stets auf dem aktuellen Stand sind.
- Nutzen Sie sichere Netzwerke.
- Verwenden Sie sichere Passwörter.
- Halten Sie alle Passwörter geheim – auch solche, die Ihnen zur einmaligen Verwendung übermittelt werden.

Wenn Sie Handy-Apps nutzen:

- Installieren Sie grundsätzlich nur Apps, die Sie über einen anerkannten App-Store beziehen können.
- Achten Sie auf die Bewertungen, die eine App erhalten hat.

- Achten Sie auch auf die Berechtigungen, die Sie erteilen.
- Behandeln Sie Ihr Handy so, wie Sie Ihr Portemonnaie behandeln würden.

Wenn Sie im Internet oder einem Laden einkaufen:

- Wenn Sie zum ersten Mal bei einem Internethändler einkaufen, recherchieren Sie ein wenig über das entsprechende Unternehmen, um sich zu vergewissern, dass es sich dabei um eine redliche Firma handelt.
- Antworten Sie nicht auf E-Mails, die Sie unaufgefordert von Ihnen unbekanntem Unternehmen erhalten.
- Vergewissern Sie sich, dass ein Link sicher ist, ehe Sie Prepaid-Karten-Daten eingeben. Beim Einloggen oder Registrieren sollte im Browserframe-Fenster ein Schlosssymbol angezeigt werden – erscheint dieses stattdessen auf der entsprechenden Seite selbst, handelt es sich dabei möglicherweise um eine betrügerische Webseite. Die URL sollte mit „<https://>“ beginnen, wobei das ‚s‘ für „sicher“ steht.
- Loggen Sie sich grundsätzlich aus, wenn Sie Ihren Besuch auf einer Webseite beenden. Wenn Sie einfach nur Ihren Browser schließen, ist die Sicherheit Ihrer Daten nicht gewährleistet.
- Verwahren Sie Ihre PIN sicher und halten Sie diese geheim.
- Achten Sie beim Eingeben Ihrer PIN auf in Ihrer Umgebung befindliche Personen und sorgen Sie dafür, dass diese die PIN nicht einsehen können.
- Überprüfen Sie grundsätzlich Ihre Kontoauszüge.

**Denken Sie bitte daran:** Wenn Sie alte Mobiltelefone, Computer, Laptops oder Tablet PCs verschenken, verkaufen oder der Wiederverwertung zuführen, löschen Sie vorher unbedingt alle Daten und Apps. Andernfalls kann möglicherweise jeder, an den Ihr Gerät in der Folge weitergegeben wird, darauf zugreifen.