

## Disposizioni per l'utilizzo di funzionalità elettroniche

### 1. Funzionalità disponibili

La Cornèr Banca SA (di seguito denominata «Banca») mette a disposizione del titolare di carte di credito e carte prepagate personali (di seguito denominato «titolare») funzionalità elettroniche che possono variare a seconda della tipologia di carta e di titolare. Le funzionalità sono compatibili con tutti i terminali della Banca che stabiliscono un collegamento verso reti elettroniche (Internet, SMS ecc.), telefonia mobile e altri canali d'accesso elettronici. In primo luogo, queste funzionalità permettono al titolare di consultare gli utilizzi della sua carta e i relativi addebiti oppure di ricevere dei messaggi in merito. Tramite queste funzionalità, il titolare può inoltre far uso degli standard di sicurezza Verified by Visa e MasterCard SecureCode concepiti da Visa e MasterCard per le transazioni effettuate in Internet. Le informazioni e le transazioni disponibili risalgono a quelle registrate dalla Banca fino al giorno lavorativo precedente la consultazione. In caso di discrepanze tra le informazioni consultate elettronicamente e i dati contabili interni alla Banca fanno stato quest'ultimi. La Banca si riserva il diritto di ampliare, ridurre, modificare e/o interrompere l'offerta riguardante le funzionalità elettroniche secondo il suo giudizio in qualsiasi momento. La Banca declina ogni responsabilità per danni derivanti da blocchi o interruzioni di questo tipo.

### 2. Comunicazione elettronica

La Banca è autorizzata a indirizzare ai dati di contatto (numero di cellulare, indirizzo e-mail ecc.) forniti dal titolare comunicazioni e offerte di ogni genere nonché informazioni specifiche legate alla carta e alle transazioni effettuate. Il titolare non deve in alcun caso inviare tramite una normale e-mail informazioni personali relative alla carta o comunque confidenziali. Salvo indicazioni contrarie esplicite, la Banca non accetta nessun incarico o ordine sopraggiunto per e-mail o trasmesso da altri sistemi elettronici. Allo stesso modo, **messaggi inviati dal titolare o da terzi tramite canali elettronici non implicano nessun obbligo da parte della Banca.**

### 3. Dispositivi di sicurezza e di identificazione

L'accesso alle funzionalità elettroniche avviene tramite la combinazione di diversi dispositivi di sicurezza (autenticazione tramite SMS, generazione di codici tramite strumenti di identificazione particolari, password ecc.) definiti dalla Banca e di cui il titolare è informato in modo adeguato. L'identificazione può avvenire secondo livelli di sicurezza singoli o combinati. La Banca si riserva il diritto di modificare il procedimento e le misure di identificazione per l'accesso e l'utilizzo di singole funzionalità elettroniche.

### 4. Legittimazione

Per la Banca è autorizzato ad accedere e a utilizzare le funzionalità elettroniche colui che al momento dell'utilizzo ha legittimato la sua identità tramite i dispositivi di sicurezza valevoli, conformemente al punto 3 delle presenti disposizioni (**autolegittimazione**). La Banca è pertanto espressamente svincolata da ogni altro obbligo di controllo, indipendentemente dai rapporti interni tra la Banca e i titolari e dal dover tener conto di eventuali disposizioni modificate all'interno dei formulari della Banca (richiesta di carta ecc.). Tuttavia, la Banca si riserva il diritto di rifiutare in qualsiasi momento l'accesso alle funzionalità elettroniche senza doverne indicare il motivo. **Tutte le transazioni e gli addebiti registrati sulla carta che saranno effettuati in seguito alla legittimazione/all'identificazione saranno attribuiti al titolare della carta, nel caso di una carta partner emessa senza un limite di spesa e un conteggio mensile propri anche al titolare della carta principale, che le accetta senza alcuna riserva come legalmente vincolanti. La Banca declina ogni responsabilità in caso di utilizzi abusivi da parte di terzi.**

### 5. Sicurezza; obblighi di diligenza

Data la configurazione pubblica dei canali elettronici, il titolare dichiara di essere a conoscenza del fatto che terzi non autorizzati potrebbero avere accesso alla connessione stabilita tra il terminale del titolare e il sistema informatico della Banca. Conformemente al punto 3, è raccomandata una particolare attenzione alla cura dei dispositivi di sicurezza e dei terminali utilizzati per l'identificazione. Il titolare si impegna in particolare a:

- non annotare in nessun luogo i dispositivi di sicurezza comunicati dalla Banca conformemente al punto 3 e a non divulgarli né a renderli accessibili a terzi o a chiunque sostenga di essere un collaboratore della Banca;
- comunicare tempestivamente i cambiamenti degli indirizzi elettronici registrati dalla Banca (numero di cellulare, indirizzo e-mail ecc.);
- comunicare immediatamente alla Banca l'eventuale smarrimento o furto della carta di credito o della carta prepagata, del terminale elettronico (ovvero del cellulare o di un altro terminale mobile), della scheda SIM ecc. o il sospetto di utilizzo abusivo;
- controllare regolarmente i terminali utilizzati per l'impiego di funzionalità elettroniche al fine di intervenire in caso di virus, software danneggiati o casi simili. La Banca raccomanda inoltre di utilizzare la versione più recente dell'applicazione e il sistema operativo presente sul terminale nonché, se possibile, di attivare un codice di blocco su ogni terminale (ad esempio una password per il salvaschermo).

Modificando le impostazioni del terminale al fine di ottenere un accesso illimitato alle funzionalità fornite (ad esempio jailbreak sui dispositivi iOS o root sui dispositivi Android), il titolare rinuncia ai sistemi di sicurezza installati dal produttore. Nei confronti della Banca, il titolare è quindi responsabile di tutte le conseguenze risultanti da tali modifiche. Per questo motivo, la Banca sconsiglia vivamente di apportare modifiche al terminale e, in questo caso, si riserva il diritto di bloccare l'accesso alle proprie funzionalità elettroniche.

L'utilizzo di link che dai siti web o dalle applicazioni della Banca conducono a siti web di terzi avviene a proprio rischio e pericolo. La Banca declina espressamente ogni responsabilità per i contenuti dei siti web menzionati così come dei prodotti, servizi ecc. ivi offerti.

**La Banca declina ogni responsabilità per le conseguenze risultanti dal mancato rispetto degli obblighi di diligenza, dallo smarrimento o dall'utilizzo abusivo dei terminali, degli indirizzi elettronici del titolare o degli strumenti di identificazione comunicati al titolare dalla Banca.**

### 6. Responsabilità

Partendo dal presupposto che il titolare rispetti senza riserve i suoi obblighi di diligenza conformemente al punto 5 e che non possa essere accusato di nulla (indipendentemente dal titolo giuridico), la Banca è responsabile dei danni diretti causati dall'utilizzo delle funzionalità elettroniche se quest'ultime sono esclusivamente imputabili a un errore o a una mancanza della Banca o attribuibili in qualche altra maniera alla sfera di rischio della Banca. Non possono essere fatti risalire alla sfera di rischio della Banca i danni sopraggiunti in seguito a errori, interruzioni, malfunzionamenti, mancanze o intercettazioni da parte di terzi nel corso di una trasmissione o di un'elaborazione di dati su installazioni di telecomunicazione o reti pubbliche. La Banca declina ogni responsabilità per danni indiretti di qualsiasi entità. La Banca declina ogni responsabilità anche per danni diretti che fanno capo a una copertura assicurativa specifica. Ogni danno deve essere comunicato tempestivamente alla Banca.

### 7. Tasse

Le tasse applicate per l'utilizzo delle funzionalità elettroniche in Svizzera e all'estero sono consultabili sul sito web [cornercard.ch/ig](http://cornercard.ch/ig)

### 8. Modifiche delle disposizioni per l'utilizzo

La Banca si riserva il diritto di modificare in qualsiasi momento le presenti condizioni di utilizzo. Le modifiche vengono comunicate al titolare tramite circolare o secondo un'altra modalità appropriata e sono considerate come approvate in assenza di una contestazione scritta entro 30 giorni dal giorno della notifica. In caso di obiezioni, la Banca si riserva il diritto di bloccare o revocare l'accesso del titolare alle funzionalità elettroniche.

### 9. Attivazione, durata e altre disposizioni

Le funzionalità elettroniche possono essere richieste e attivate, ma anche revocate in ogni momento (anche da parte della Banca). Se non previsto diversamente dalle presenti disposizioni, le funzionalità elettroniche rimangono attive fino alla scadenza della carta del titolare. Il titolare prende atto che non è più possibile accedere a Onlineaccess e alle sue funzionalità una volta disdetto o risolto il contratto della carta. Le disposizioni presenti sostituiscono la versione precedente delle disposizioni per l'utilizzo aventi il medesimo oggetto. Per tutte le trattande non regolamentate in questa sede fanno stato le **Condizioni Generali per le carte Visa e MasterCard della Cornèr Banca SA** applicabili ai prodotti in questione.

Versione P/R-B00Q-1