CONDIZIONI SPECIALI PER L'ELECTRONIC BANKING CON WESTERN UNION DIGITAL BANKING APP

Per comodità di lettura, le presenti Condizioni Speciali per l'electronic banking con Western Union Digital Banking App non sono formulate in modo specifico per genere e si applicano ugualmente a tutti i generi.

Ai fini delle presenti Condizioni Speciali, con il termine "Documenti del Conto" si intendono tutti i documenti relativi al processo di onboarding del cliente nell'ambito della Western Union Digital Banking App, inclusi, a titolo esemplificativo, il Foglio Informativo fornito da Western Union International Bank GmbH, i Termini e Condizioni Generali di Western Union International Bank GmbH, le Condizioni Speciali per la carta di debito e la carta di debito virtuale, le presenti Condizioni Speciali, le Condizioni Speciali per i pagamenti istantanei SEPA e relativi listini prezzi, in quanto applicabili caso per caso, a seconda dei servizi che la Banca deve prestare al cliente, insieme a qualsiasi altra documentazione accessoria necessaria per la finalizzazione o attuazione del processo di onboarding nell'ambito della Western Union Digital Banking App, come espressamente e individualmente accettata dal cliente e come di volta in volta modificata.

1. Disposizioni generali
1.1. Utilizzo dell'electronic bankingcon Western Union Digital Banking App (di seguito denominata "e-banking")
(1) Le presenti Condizioni Speciali disciplinano l'utilizzo dell'e-banking di Western Union International Bank GmbH che agisce attraverso la sua sede secondaria italiana (di seguito denominata "Banca") da parte del cliente.

(2) La Western Union Digital Banking App (di seguito denominata “App”) è un'applicazione della Banca che consente al cliente, nel rispetto dei requisiti concordati nelle presenti Condizioni Speciali, di utilizzare un terminale mobile (ad esempio uno smartphone) per effettuare ricerche (ad esempio saldo del conto, fatturato) e impartire ordini (ad esempio ordini di pagamento), nonché per rilasciare dichiarazioni d'intenti giuridicamente vincolanti e altre dichiarazioni.

(3) L'e-banking è una forma di internet banking come definito nell'Allegato al Decreto sui Servizi di Conto di Pagamento per Consumatori (BGBl II n. 60/2018).

1.2. Condizioni per l'utilizzo dell'App
La possibilità di utilizzare l'App richiede l'esistenza di una relazione d'affari tra la Banca e il cliente, e un contratto per l'e-banking tra il cliente e la Banca. La relazione d'affari in sé è disciplinata dai Documenti del Conto e dai termini e condizioni in essi contenuti; in particolare, le presenti condizioni speciali regolano l'uso dell'e-banking con l'App da parte del cliente.

1.3. Registrazione nell'App
La registrazione nell'App avviene seguendo i passaggi previsti dall'App. Uno dei passaggi del processo di registrazione è l'inserimento dell'indirizzo e-mail e della Password che viene (i) utilizzata dal cliente per accedere al proprio profilo wu.com o (ii) creata dal cliente al momento della registrazione nell'App. Dopo aver impostato lo Username e la Password, il cliente ha la possibilità di attivare i dati biometrici o un Passcode.

1.4. Firma elettronica nell'App
Per concludere il contratto con la Banca e utilizzare l'App, il cliente dovrà attivare e utilizzare una firma elettronica avanzata o una firma elettronica qualificata come indicato nei Termini e Condizioni della Banca sull'utilizzo della firma elettronica avanzata o della firma elettronica qualificata.

1.5 Definizioni
Password
La password è la parola segreta (combinazione di 8-16 caratteri con almeno 1 maiuscola, 1 minuscola e 1 numero o carattere speciale) che viene (i) utilizzata dal cliente per accedere al proprio profilo wu.com o (ii) specificata dal cliente al momento della registrazione nell'App. La password è un elemento di identificazione personale del cliente, che serve a identificarlo nell'e-banking se viene specificato anche l'indirizzo e-mail. La password può essere modificata dal cliente nell'App.

Passcode
Il Passcode è un numero di sei cifre che può essere creato dal cliente e utilizzato per l'accesso al posto della password. Inserendo il codice di accesso si possono piazzare ordini ed effettuare dichiarazioni d'intenti giuridicamente vincolanti o altre dichiarazioni. Ai fini del controllo da parte del cliente, vengono visualizzati i dati relativi all'ordine da autorizzare (ad es. l'IBAN del destinatario e l'importo dell’operazione di pagamento) o alla dichiarazione d'intenti o altra dichiarazione giuridicamente vincolante.
L'inserimento del Passcode è necessario altresì per accedere all'App se è richiesta un'autenticazione forte del cliente ai sensi della Legge Austriaca sui Servizi di Pagamento del 2018 o del Regolamento Delegato (UE) 2018/389. Il Passcode può essere modificato dal cliente nell'App.

Touch ID
Il Touch ID è una funzione di identificazione personale del cliente che consente l'identificazione nell'e-banking per mezzo di un'impronta digitale e deve essere attivata dal cliente nell'App. Il Touch ID è un'opzione alternativa per identificare il cliente tramite indirizzo e-mail e Password. Inserendo il Touch ID si possono piazzare ordini ed effettuare dichiarazioni d'intenti giuridicamente vincolanti o altre dichiarazioni. Ai fini del controllo da parte del cliente, vengono visualizzati i dati relativi all'ordine da autorizzare (ad es. l'IBAN del destinatario e l'importo dell’operazione di pagamento) o alla dichiarazione d'intenti o altra dichiarazione giuridicamente vincolante. Per utilizzare Touch ID, il cliente deve disporre di un dispositivo mobile abilitato al Touch ID (ad es. uno smartphone) e deve avere Touch ID abilitato.

Face ID
Face ID è una funzione di identificazione personale del cliente che consente l'identificazione nell'e-banking per mezzo del riconoscimento facciale e deve essere abilitata dal cliente nell'App. Il Face ID è un'opzione alternativa per identificare il cliente tramite indirizzo e-mail e Password. Inserendo il Face ID si possono piazzare ordini ed effettuare dichiarazioni d'intenti giuridicamente vincolanti o altre dichiarazioni. Ai fini del controllo da parte del cliente, vengono visualizzati i dati relativi all'ordine da autorizzare (ad es. l'IBAN del destinatario e l'importo dell’operazione di pagamento) o alla dichiarazione d'intenti o altra dichiarazione giuridicamente vincolante. Per utilizzare il Face ID, il cliente deve disporre di un dispositivo mobile abilitato al Face ID (ad es. smartphone) e deve avere Face ID abilitato.

e-Postbox
La e-Postbox è la casella di posta elettronica a disposizione del cliente per inviare notifiche alla Banca in caso di domande o se il cliente ha bisogno di assistenza e per ricevere notifiche dalla Banca.

Codice di autenticazione
Il codice di autenticazione è un codice che viene generato durante l'autenticazione forte del cliente, come definita nella Legge Austriaca sui Servizi di Pagamento del 2018 e nel Regolamento Delegato (UE) 2018/389 ed è dinamicamente collegato alla fase da autorizzare (ad esempio, l'ordine da autorizzare o la dichiarazione di intenti del cliente da presentare). Ogni volta che viene inserito il Passcode, viene generato un codice di autenticazione unico.

Autenticazione Forte del Cliente
L'autenticazione forte del cliente è la procedura di autenticazione forte del cliente regolamentata dalla Legge Austriaca sui Servizi di Pagamento del 2018 e dal Regolamento Delegato (UE) 2018/389.

2. Accesso - Ordini e dichiarazioni
(1) L'accesso all'e-banking è consentito solo ai clienti che si sono legittimati inserendo il proprio indirizzo e-mail e Password o tramite Touch ID o Face ID o Passcode. L'ulteriore inserimento del Passcode per l'accesso all'App è richiesto se sono trascorsi più di 30 giorni dall'ultima autenticazione forte del cliente o se il cliente accede per la prima volta al suo conto di pagamento.

(2) L'inoltro di ordini e la presentazione di dichiarazioni d'intenti giuridicamente vincolanti o altre dichiarazioni da parte del cliente dovrà avvenire tramite inserimento del Passcode, del Touch ID o del Face ID.

(3) Dichiarazioni di intenti giuridicamente vincolanti da parte del cliente possono essere fatte anche dal cliente che accetta un'offerta espressamente fattagli dalla Banca nell'e-banking dichiarando l'accettazione (ad esempio cliccando su una casella contenente la sua dichiarazione di consenso) e confermando successivamente la sua accettazione (ad esempio premendo un pulsante); il cliente può anche effettuare altre dichiarazioni in questo modo.

(4) La Banca ha il diritto, ma non l'obbligo, di eseguire i bonifici del cliente alle condizioni di cui agli Articoli da 10 a 21 del Regolamento Delegato (UE) 2018/389 anche senza l'autorizzazione del Passcode, Touch ID o Face ID.

(5) L'accettazione degli ordini da parte della Banca non sarà considerata una conferma dell'esecuzione.

3. Due Diligence e misure di sicurezza raccomandate
3.1. Obbligo di conformità
Ogni cliente è tenuto a rispettare gli obblighi di diligenza concordati alla sezione 3.2. I clienti che sono imprenditori sono inoltre tenuti a rispettare le misure di sicurezza raccomandate ai sensi della Sezione 3.3. Per i clienti consumatori, la Banca raccomanda l'osservanza delle misure di sicurezza raccomandate, senza che i consumatori siano obbligati a rispettarle. Una violazione di questi obblighi può comportare, ai sensi della Sezione 7 (per i consumatori) o della Sezione 8 (per gli imprenditori), la responsabilità del cliente per danni o l'eliminazione o riduzione delle sue richieste di risarcimento nei confronti della Banca.

3.2. Obblighi di Due Diligence
3.2.1. Obbligo di riservatezza e di blocco
(1) Il cliente dovrà mantenere la sua Password e il suo Passcode segreti; non potrà rivelarli a terzi o trasmetterli a terzi in alcun altro modo. Tuttavia, la divulgazione ai fornitori di servizi di avvio pagamenti e ai fornitori di servizi di informazione sui conti è consentita nella misura in cui sia necessaria per consentire loro di fornire i propri servizi al cliente.

(2) Il cliente è tenuto a prestare la massima attenzione nel conservare e utilizzare la sua Password e il suo Passcode, al fine di evitare usi impropri. In particolare, il cliente dovrà assicurarsi che la sua Password e il suo Passcode non vengano spiati durante il loro utilizzo; il cliente non dovrà inoltre memorizzarli nel suo dispositivo mobile su cui ha installato l'App o annotarli elettronicamente, ad esempio in un'app per appunti, a meno che tale memorizzazione o app non sia protetta dall'accesso di terzi.

(3) In caso di smarrimento della Password e/o Passcode, nonché nel caso in cui il cliente sia venuto a conoscenza di un uso improprio o altro utilizzo non autorizzato dell'e-banking, il cliente dovrà provvedere immediatamente a bloccare l'accesso al proprio e-banking.

(4) In caso di smarrimento o furto del dispositivo mobile del cliente su cui è installata l'App, il cliente dovrà provvedere immediatamente al blocco del suo accesso all'e-banking; ciò varrà anche se il cliente ha installato l'App su più dispositivi mobili e uno di essi viene rubato o smarrito.

3.2.2. Due Diligence per il blocco del dispositivo mobile e durante l'installazione
(1) Il cliente è tenuto a bloccare l'accesso all'uso del dispositivo mobile su cui è installata l'App o l'accesso ai dati ivi memorizzati a persone non autorizzate se il cliente non utilizza il dispositivo.

(2) Il cliente può installare l'App esclusivamente dall'App Store di Apple o dal Google Play Store.

3.2.3. Due Diligence per ordini e dichiarazioni
La correttezza dei dati visualizzati nell'App dopo l'inserimento da parte del cliente deve essere verificata dal cliente stesso prima di utilizzare il Passcode, Touch ID o Face ID. Il Passcode, Touch ID o Face ID possono essere utilizzati per piazzare ordini o effettuare dichiarazioni solo se i dati visualizzati nell'App corrispondono all'ordine desiderato o alla dichiarazione d'intenti o altra dichiarazione giuridicamente vincolante.

3.3. Misure di sicurezza raccomandate nell'utilizzo dell'e-banking
(1) Si raccomanda al cliente di modificare autonomamente la Password e il Passcode con regolarità, almeno ogni due mesi.

(2) Si consiglia al cliente di bloccare immediatamente l'accesso all'e-banking se si ha motivo di temere che terzi non autorizzati siano venuti a conoscenza della Password e/o del Passcode, o se vi sono altre circostanze che potrebbero consentire a terzi non autorizzati di utilizzare in modo improprio la Password e/o il Passcode.

(3) Si raccomanda al cliente di proteggere il proprio dispositivo mobile, su cui è installata l'App, dai rischi provenienti da Internet, in particolare di mantenerlo aggiornato, nonché di eseguire gli aggiornamenti di sicurezza del sistema operativo del dispositivo mobile e di utilizzare una protezione antivirus aggiornata.

4. Blocco
4.1. Blocco automatizzato
(1) L'accesso all'e-banking viene automaticamente bloccato temporaneamente se la Password viene inserita in modo errato per tre volte di seguito durante un accesso. Dopo la rimozione automatica del primo blocco temporaneo e se la Password viene inserita in modo errato per due volte di seguito, si verificherà un secondo blocco temporaneo. Dopo la rimozione del secondo blocco temporaneo, ogni ulteriore inserimento errato della Password comporterà un nuovo blocco temporaneo. Il numero massimo di immissioni errate della Password che possono causare un blocco temporaneo è nove. Dopo il decimo inserimento di una Password errata, l'accesso all'e-banking sarà automaticamente bloccato in modo permanente. La Banca comunicherà immediatamente al cliente la durata del rispettivo blocco temporaneo.

(2) L'accesso all'e-banking viene automaticamente bloccato in modo permanente se il Passcode è stato inserito in modo errato per cinque volte di seguito.

4.2. Blocco da parte del cliente
Il cliente può bloccare l'accesso all'e-banking inserendo il Passcode in modo errato per cinque volte di seguito, oppure telefonando al numero +390685960176.

4.3. Blocco da parte della Banca
(1) La Banca ha il diritto di bloccare l'e-banking di un cliente se ragioni oggettive di sicurezza lo giustificano o se vi è il sospetto di un uso non autorizzato o fraudolento.

(2) La Banca informerà il cliente dell'eventuale blocco dell'e-banking e delle relative motivazioni per quanto possibile prima, ma al più tardi senza ritardi ingiustificati dopo il blocco, a condizione che la divulgazione del blocco o delle relative motivazioni non violi un'ordinanza giudiziaria o un ordine di un'autorità amministrativa o sia contraria al diritto nazionale o europeo o a considerazioni oggettive di sicurezza.

4.4. Annuncio e revoca del blocco
(1) Prima che un blocco diventi permanente, il cliente riceverà un avviso.

(2) La Banca revocherà il blocco di cui alla sezione 4.3. non appena non sussistono più i motivi del blocco. La Banca informerà il cliente della revoca del blocco senza ritardi ingiustificati.

(3) Il cliente può richiedere la revoca di un blocco in qualsiasi momento telefonando al numero +390685960176.

5. Ordini e dichiarazioni giuridicamente vincolanti del cliente
(1) Gli ordini e le dichiarazioni d'intenti giuridicamente vincolanti, nonché le altre dichiarazioni effettuate dal cliente nell'e-banking , si considerano emessi o effettuati dal cliente se quest'ultimo li ha rilasciati tramite Passcode, Touch ID o Face ID. Il Cliente può anche rilasciare dichiarazioni d'intenti secondo le modalità di cui alla Sezione 2 (3).

(2) La Banca non è tenuta ad ottenere una conferma dell'ordine o della dichiarazione d'intenti giuridicamente vincolante o di qualsiasi altra dichiarazione. Il diritto della Banca di ottenere una conferma d'ordine come concordato nella Sezione 4 dei "Termini e Condizioni generali di Western Union International Bank GmbH" (di seguito denominati "TCG"), rimane inalterato.

(3) Gli ordini e le dichiarazioni d'intenti giuridicamente vincolanti, nonché altre dichiarazioni del cliente, possono essere emessi o effettuati utilizzando l'App solo nella misura in cui siano coperti da un'autorizzazione alla disposizione ai sensi della Sezione 32 dei TCG.

6. Ora di ricezione/Esecuzione degli ordini di pagamento

(1) Ora di ricezione degli ordini di pagamento: L'ora in cui un ordine di pagamento viene ricevuto dalla Banca attraverso e-banking sarà considerata l'ora della ricezione. Se l'ordine di pagamento viene ricevuto in un giorno lavorativo dopo l'orario limite o non in un giorno lavorativo della Banca, l'ordine sarà trattato come se fosse stato ricevuto dalla Banca il giorno lavorativo successivo.

(2) L'orario limite per gli ordini di pagamento in un giorno lavorativo è specificato nella sezione 3.2 del "Foglio informativo WUIB".

(3) Ordini di pagamento: Se il cliente non indica una data di esecuzione futura, l'ordine di pagamento sarà eseguito nello stesso giorno se i dati dell'operazione di pagamento sono disponibili per l'elaborazione al più tardi entro il termine di accettazione della Banca. In caso contrario, l'esecuzione avverrà al più tardi nel giorno lavorativo successivo a quello della trasmissione dei dati da parte dell'ordinante. Il presupposto per l'esecuzione è una sufficiente copertura del conto (saldo attivo o fido).

(4) Inoltre, le Sezioni 36 e 36a dei TCG si applicheranno quando gli ordini di trasferimento sono regolamentati.

7. Responsabilità del cliente in quanto consumatore

(1) Il cliente che è un consumatore sarà responsabile dell'intera perdita di un'operazione di pagamento non autorizzata causata alla Banca (i) dalla violazione intenzionale o per grave negligenza da parte del cliente degli obblighi di diligenza di cui alla Sezione 3.2 o (ii) con intento fraudolento.

(2) Se la violazione degli obblighi di diligenza di cui alla Sezione 3.2 è dovuta a una negligenza lieve da parte del cliente, la responsabilità di quest'ultimo sarà limitata a un massimo di 50 EUR. Se il cliente non ha violato gli obblighi di diligenza di cui alla Sezione 3.2 né in modo fraudolento né intenzionale, nella ripartizione dei danni tra il cliente e la Banca si terrà conto del tipo di funzioni di sicurezza personalizzate e delle circostanze particolari in cui si è verificato l'uso improprio dell'e-banking.

(3) Se lo smarrimento o il furto del terminale mobile su cui è installata l'App o l'uso improprio dell'e-banking non poteva essere notato dal cliente prima del pagamento, il cliente non sarà responsabile in caso di violazione lievemente colposa degli obblighi di diligenza di cui alla Sezione 3.2. Il cliente non sarà inoltre responsabile in caso di violazione lievemente colposa degli obblighi di diligenza ai sensi della Sezione 3.2 se la perdita delle funzioni di identificazione personale è stata causata da atti o omissioni della Banca (compresi i suoi dipendenti e agenti e altre entità a cui tali servizi sono stati esternalizzati).

(4) Nonostante la Sezione 7 (2), il cliente non sarà responsabile se la Banca non ha richiesto l'autenticazione forte del cliente in caso di uso improprio dell'e-banking o in caso di pagamento non autorizzato tramite e-banking. Se un'operazione di pagamento non autorizzata è stata agevolata in modo fraudolento dal cliente, quest'ultimo sarà responsabile indipendentemente dal fatto che la Banca abbia richiesto o meno l'autenticazione forte del cliente.

(5) Il cliente non sarà responsabile se i danni derivano da un uso non autorizzato dell'e-banking dopo che il cliente ha informato la Banca di una perdita, furto o uso improprio in conformità alla sezione 3.2.1(3) o alla sezione 4, a meno che il cliente non abbia agito con intento fraudolento.

8. Responsabilità verso imprenditori/Responsabilità del cliente in quanto imprenditore

In relazione agli imprenditori, la sezione 68 della Legge Austriaca sui Servizi di Pagamento del 2018 è interamente derogata; la responsabilità della Banca per danni causati da negligenza lieve sarà esclusa. La Banca non sarà responsabile, indipendentemente dal grado di colpa, per i danni causati in relazione all'hardware o al software del cliente o causati dalla mancata creazione di un collegamento con il centro di elaborazione dati della Banca o causati da un guasto temporaneo delle strutture della Banca per il funzionamento dell'e-banking, o se l'imprenditore ha violato gli obblighi di diligenza di cui alla Sezione 3 o se l'imprenditore non ha rispettato le misure di sicurezza raccomandate di cui alla Sezione 3. Se l'imprenditore ha violato gli obblighi di diligenza di cui alla Sezione 3 o non ha rispettato le misure di sicurezza raccomandate nella Sezione 3, l'imprenditore sarà responsabile nei confronti della Banca per i danni che ne derivano.

9. Dichiarazioni e comunicazioni

(1) Il cliente riceverà dichiarazioni legali, notifiche e informazioni dalla Banca (di seguito congiuntamente definite "Dichiarazioni") in una forma di comunicazione concordata con il cliente. Le forme di comunicazione concordate sono l'e-mail, gli SMS, le notifiche push e la trasmissione alla e-Postbox del cliente con notifica al cliente stesso. Se il cliente e la Banca stipulano accordi su altre forme di comunicazione, la loro efficacia non sarà pregiudicata dalla presente disposizione; ciò varrà anche per la comunicazione con l'App. Anche l'efficacia delle dichiarazioni scritte (comprese quelle inviate per posta) rimane inalterata.

(2) La Banca può trasmettere dichiarazioni al cliente all'indirizzo e-mail fornito dal cliente alla Banca. Le dichiarazioni fatte dalla Banca al cliente via e-mail a questo indirizzo di posta elettronica saranno pertanto efficaci. Il cliente può inoltre comunicare con la Banca via e-mail ed effettuare dichiarazioni efficaci via e-mail e tramite la e-Postbox nell'App.
Il cliente non può comunicare con la Banca ed effettuare dichiarazioni efficaci se viene informato in un messaggio di posta elettronica che non è possibile rispondere a questo indirizzo di posta elettronica ("indirizzi no-reply").

(3) In caso di modifica del proprio indirizzo di posta elettronica, il cliente dovrà comunicare senza indebito ritardo alla Banca il nuovo indirizzo di posta elettronica; ciò sarà possibile per telefono al numero +390685960176 o nell'App. Se il cliente non ha comunicato alla Banca il suo nuovo indirizzo di posta elettronica e se la Banca riceve l'informazione che l'indirizzo di posta elettronica non è più attuale, le dichiarazioni della Banca si considereranno ricevute dal cliente se la Banca le ha sia inviate all'ultimo indirizzo di posta elettronica comunicato dal cliente sia trasmesse alla e-Postbox del cliente con notifica al cliente; se la Banca non ha ricevuto tale informazione, le dichiarazioni della Banca si considereranno ricevute dal cliente se la Banca le ha inviate all'ultimo indirizzo di posta elettronica comunicato dal cliente.

10. Modifica delle Condizioni Speciali per l'e-banking con Western Union Digital Banking App

(1) La Banca proporrà al cliente modifiche alle presenti Condizioni Speciali, a condizione che vi sia un motivo oggettivamente giustificato, al più tardi due mesi prima della data di entrata in vigore proposta; le disposizioni interessate dalla proposta di modifica e le modifiche proposte alle presenti Condizioni Speciali saranno presentate in un confronto (di seguito "Confronto") allegato alla proposta di modifica. La proposta di modifica sarà comunicata al cliente mediante l'invio di un avviso, intitolato *"Proposta di modifica unilaterale del contratto"*, che descriva il contenuto della/e modifica/e proposta/e tramite e-mail o altro mezzo durevole precedentemente concordato dal cliente ai sensi della Sezione 27 dei TCG. Si riterrà che il cliente abbia acconsentito alle modifiche se la Banca non riceverà un'obiezione da parte del cliente prima della data di entrata in vigore proposta tramite e-mail, posta o altro mezzo durevole concordato dal cliente ai sensi della Sezione 27 dei TCG. Nella proposta di modifica la Banca richiamerà l'attenzione del cliente sul fatto che il silenzio del cliente, in assenza di obiezioni in forma scritta o per via elettronica [ad es. via e-mail o l'App], a seconda dei casi, sarà considerato un consenso alle modifiche e che il cliente, che è un consumatore, avrà il diritto di recedere dal contratto di e-banking con Western Union Digital Banking App e dai Documenti del Conto per i quali è stato concordato l'e-banking con Western Union Digital Banking App, senza preavviso e senza spese prima dell'entrata in vigore delle modifiche. Inoltre, la Banca pubblicherà sul proprio sito web il Confronto e la versione completa delle nuove condizioni speciali per e-banking con Western Union Digital Banking App e invierà al cliente via e-mail la versione completa delle nuove condizioni speciali; quanto precede sarà inoltre menzionato dalla Banca nell'offerta di modifica.

(2) La notifica e proposta di modifica in conformità al paragrafo (1) della Sezione 11 saranno fornite al cliente mediante la trasmissione della proposta di modifica insieme al Confronto via e-mail o altri mezzi durevoli precedentemente concordati dal cliente ai sensi della Sezione 27 dei TCG. La notifica dovrà essere effettuata in modo tale per cui la Banca non possa più modificare unilateralmente la proposta di modifica e il cliente abbia la possibilità di memorizzare e stampare ulteriormente la notifica per sé. La proposta di modifica si considererà ricevuta dal cliente nel momento in cui il cliente riceve la notifica ed è in grado di recuperare tali informazioni in circostanze ordinarie.

(3) La variazione dei servizi della Banca mediante una modifica alle presenti Condizioni Speciali ai sensi del paragrafo (1) della Sezione 11 sarà limitata a casi oggettivamente giustificati; si riterrà che esista una giustificazione oggettiva,

(i) se la modifica è richiesta da un cambiamento delle disposizioni di legge che disciplinano i servizi di pagamento e il loro regolamento o da requisiti dell'Autorità per i Mercati Finanziari, dell'Autorità Bancaria Europea, della Banca Centrale Europea, della Banca Nazionale Austriaca o di qualsiasi altra autorità competente,

(ii) se la modifica è resa necessaria dall'evoluzione della giurisprudenza relativa ai servizi di pagamento e al loro regolamento,

(iii) se la modifica promuove la sicurezza delle operazioni bancarie o il trattamento del rapporto commerciale con il cliente per l'e-banking,

(iv) se la modifica è necessaria per implementare sviluppi tecnici o per adattarsi a nuovi programmi di utilizzo dei dispositivi mobili o dell'App,

(v) se la modifica è resa necessaria da un cambiamento dei requisiti legali per l'inoltro di ordini e il rilascio di dichiarazioni nell'App,

(vi) se la modifica è resa necessaria da un cambiamento delle disposizioni di legge per le operazioni bancarie che il cliente può effettuare nell'App.

L'introduzione di commissioni e la modifica delle commissioni concordate a causa di una modifica delle presenti Condizioni Speciali sono escluse.