NORME PER LA TRASPARENZA DELLE OPERAZIONI E DEI SERVIZI BANCARI

(D.LGS 385 DEL 01/09/1993 e successivi aggiornamenti)

INFORMAZIONI SULLA BANCA

LA CASSA DI RAVENNA S.p.A. – GRUPPO BANCARIO LA CASSA DI RAVENNA
Sede Sociale e Direzione Generale: Piazza G.Garibaldi, 6 - 48121 Ravenna
Tel. 0544/480111 - Fax 0544/480535 - www.lacassa.com - E-mail: lacassa@lacassa.com
Cod. Fisc. / Partita IVA / numero di iscrizione al Registro Imprese di Ravenna 01188860397 - Codice ABI 6270.3
Aderente al Fondo Interbancario di Tutela dei Depositi e al Fondo Nazionale di Garanzia,
iscrizione all'albo delle Aziende di Credito presso Banca d'Italia n. 5096

In caso di offerta "Fuori Sede" compilare i riferimenti del soggetto che entra in contatto con il Cliente:

Soggetto:_____ Società:_____ Qualifica:_____

Indirizzo: _____ Numero di telefono:_____ e-mail:_____

Il sottoscritto dichiara di aver ricevuto copia del presente documento dal soggetto sopra indicato:

Nome del Cliente:_____ Data e Firma del Cliente_____

La Banca non commercializza questo prodotto attraverso tecniche di comunicazione a distanza.

Se quanto illustrato in questo foglio informativo non è chiaro o se si necessita di ulteriori informazioni, è opportuno chiedere chiarimenti al personale prima della firma.

CHE COS'É IL CORPORATE BANKING

Il Corporate Banking è un servizio attraverso il quale una banca detta "Proponente", a seguito della stipula di uno specifico contratto, è in grado di offrire alla propria clientela la possibilità di scambiare, mediante collegamento telematico, flussi elettronici contenenti disposizioni e/o informazioni con la stessa banca e con tutte le altre banche, dette "Passive", con cui la clientela intrattiene rapporti tramite il Corporate Banking Interbancario (CBI).

Per le sue caratteristiche, il servizio è particolarmente indirizzato a risolvere le esigenze delle imprese che operano con una pluralità di banche e che eseguono un numero rilevante di operazioni bancarie. Infatti gli operatori sono in grado di conoscere costantemente l'andamento dei flussi finanziari dei conti accesi presso le varie banche e di controllare l'andamento dei rapporti commerciali con la propria clientela grazie, ad esempio, alla informativa sull'esito degli incassi. La trasmissione telematica delle disposizioni di pagamento e incasso realizza economie in termini di tempi e costi, consente alle aziende di operare con le banche senza limiti di orario, garantendo un'efficace gestione amministrativa e finanziaria.

Il servizio è proposto in modalità internet (Comodo Banking): che consiste nell'utilizzo di una procedura completamente accessibile online tramite un comune browser di navigazione internet previo inserimento delle chiavi di accesso (user e password).). In caso di necessità di supporto tecnico e funzionale, il Cliente può contattare la struttura di Help Desk dedicata per l'assistenza ai riferimenti (numero verde / email) presenti nella pagina di accesso al servizio.

ACCESSO AL SERVIZIO e AUTORIZZAZIONE DELLE DISPOSIZIONI E SISTEMI DI SICUREZZA

L'accesso al servizio e la fase dispositiva sono soggette dal mese di settembre 2019 all'autenticazione forte come da indicazione della Direttiva Europea 2015/2366 (PSD2).

Per accedere al servizio di **Corporate Banking in modalità internet**, è necessario – oltre alla digitazione delle credenziali personali (user e password) un ulteriore codice generato tramite i seguenti sistemi alternativi scelti dal Cliente in base alle proprie necessità:

- entità di sicurezza **"Secure Call**", attivata all'atto della sottoscrizione del contratto, subordinatamente al possesso di un numero cellulare italiano, che consente di accedere al servizio tramite una telefonata dal cellulare del Cliente ad un numero verde gratuito visualizzato nella schermata di conferma sul proprio dispositivo (PC/ tablet/ smartphone). Dopo che il Cliente ha chiamato il numero verde, una voce registrata chiede di inserire, come conferma, il codice di 4 cifre visualizzato sempre sulla schermata del proprio dispositivo (PC/ tablet/ smartphone). Se il Cliente opera dall'estero per concludere l'operazione deve prima spuntare il messaggio *"Sono all'estero e voglio procedere alla conferma dell'operazione attraverso cellulare*"; in tal caso il Cliente riceve una telefonata al suo numero abilitato al servizio Secure Call che gli fornisce le indicazioni per dare la conferma. Il costo della chiamata dal confine italiano al paese estero è a carico del Cliente, in linea con la tariffa internazionale contrattualizzata con la propria compagnia telefonica;
- entità di sicurezza **"Digipass**" "time based", consegnato e attivato al momento della sottoscrizione del contratto, che

consente al Cliente di accedere al servizio inserendo il codice numerico di 6 cifre generato con casualità dallo stesso strumento
- entità di sicurezza **"Digipass**" "transaction based" con tastierino numerico, consegnato e attivato al momento della sottoscrizione del contratto, che consente al Cliente di accedere al servizio inserendo il codice numerico di 6 cifre generato con casualità dallo stesso strumento tramite il tasto 1 del tastierino.

Per concludere le transazioni dispositive tramite il servizio di **Corporate Banking in modalità internet**, è necessario inserire uno o più codici generati dai seguenti sistemi alternativi scelti dal Cliente in base alle proprie necessità:
- entità di sicurezza **"Secure Call**", attivata all'atto della sottoscrizione del contratto, subordinatamente al possesso di un numero cellulare italiano, che consente di autorizzare le operazioni tramite una telefonata dal cellulare del Cliente ad un numero verde gratuito visualizzato nella schermata di conferma sul proprio dispositivo (PC/ tablet/ smartphone). Per autorizzare le operazioni dopo che il Cliente ha chiamato il numero verde, una voce registrata:
  - chiede di inserire, come conferma, il codice di 4 cifre (PIN1) visualizzato sulla schermata del proprio dispositivo (PC/ tablet/ smartphone)
  - richiede di seguito l'inserimento di un successivo codice (PIN2) visualizzato sullo schermo (questo codice è collegato dinamicamente all'operazione disposta).

  Se il Cliente opera dall'estero per concludere l'operazione deve prima spuntare il messaggio *"Sono all'estero e voglio procedere alla conferma dell'operazione attraverso cellulare*"; in tal caso il Cliente riceve una telefonata al suo numero abilitato al servizio Secure Call che gli fornisce le indicazioni per dare la conferma. Il costo della chiamata dal confine italiano al paese estero è a carico del Cliente, in linea con la tariffa internazionale contrattualizzata con la propria compagnia telefonica;
- entità di sicurezza **"Digipass**" "time based", consegnato e attivato al momento della sottoscrizione del contratto, che consente al Cliente di autorizzare le operazioni:
  - inserendo a video un codice numerico di 8 caratteri (collegato dinamicamente all'operazione) ricevuto via SMS su un dispositivo mobile precedentemente comunicato alla Banca
  - digitando, sempre sulla schermata del prodotto, il codice numerico di 6 cifre generato con casualità dal Digipass;
- entità di sicurezza **"Digipass**" "transaction based" con tastierino numerico, consegnato e attivato al momento della sottoscrizione del contratto, che consente al Cliente di autorizzare le operazioni:
  - inserendo sul digipass il numero di 8 cifre esposto a video (tasto 3 del tastierino) collegato dinamicamente all'operazione
  - confermando con il tasto ok il numero inserito (viene generato un nuovo codice)
  - digitando il nuovo codice riportato sul digipass sul prodotto di Corporate banking

I PRINCIPALI RISCHI (GENERICI E SPECIFICI)

Tra i principali rischi, vanno tenuti presente:
- ❑ variazione in senso sfavorevole delle condizioni economiche (commissioni e spese del servizio) ove contrattualmente previsto;
- ❑ modifiche/ aggiornamenti applicativi per esigenze di carattere tecnico oppure per migliorare l'efficienza e/o la sicurezza del servizio offerto che comportano la necessità da parte del Cliente di adeguare i propri dispositivi hardware e relativi software per salvaguardare la continuità del servizio. Il Cliente è responsabile della idoneità e affidabilità delle apparecchiature, dei collegamenti e dei programmi utilizzati per il colloquio telematico con la Banca, nonché del mantenimento dei citati requisiti nel tempo;
- ❑ il Cliente deve garantire il rispetto delle indicazioni fornite dalla Banca relativamente alle procedure ed agli strumenti necessari per le operazioni di identificazione, bilateralmente efficaci, dell'identità del Cliente e della Banca, da eseguire all'atto del collegamento e durante i successivi scambi di flussi. Il Cliente è responsabile dell'esattezza e della autenticità delle istruzioni date nonché della correttezza dei flussi inviati;
- ❑ sospensione o rifiuto dell'esecuzione di un pagamento se non sono soddisfatte le condizioni previste dall'"Accordo quadro dei servizi di pagamento" o per altro giustificato motivo. In caso di sospensione o rifiuto, la Banca comunica tramite canale telefonico o comunicazione elettronica le informazioni sulla mancata esecuzione e le relative motivazioni, riservandosi di addebitare al Cliente le spese della comunicazione. In caso di sospensione, l'ordine si intende ricevuto dalla Banca quando vengono meno le ragioni della sospensione stessa;
- ❑ rischio informatico, furto dell'identità (cattura della password). Il Cliente è responsabile in caso di indebito uso dei codici, comunque avvenuto, anche se causato da smarrimento o furto;
- ❑ il Cliente deve rispettare scrupolosamente le raccomandazioni per un corretto uso dei servizi di pagamento on line messe a disposizione dalla Banca (si rinvia, per maggiori dettagli, all'Informativa Antitruffa e al Manuale operativo utente pubblicati anche sul sito internet istituzionale della Banca);
- ❑ il Cliente è responsabile della custodia e del corretto utilizzo delle chiavi di accesso fornite dalla Banca si impegna a custodirli ed utilizzarli con la massima diligenza. In caso di sottrazione o smarrimento di tutti o di alcuni codici, il Cliente deve darne tempestiva comunicazione alla Filiale che ha aperto il servizio, personalmente oppure a mezzo di lettera. La Filiale che riceve la comunicazione può richiedere al Cliente di denunciare i fatti all'Autorità competente. Ricevuta la relativa comunicazione, la Banca provvede a bloccare l'utenza interessata;
- ❑ il Cliente è responsabile della custodia e conservazione del dispositivo Digipass. In caso di furto o smarrimento, il Cliente deve effettuare regolare denuncia alla Pubblica Sicurezza inoltrandone apposita copia alla filiale di riferimento della Banca. La filiale provvede al blocco immediato dell'operatività effettuando la relativa sostituzione se richiesta addebitando al Cliente i costi indicati nel presente Prospetto Informativo.
- ❑ sospensione del servizio anche senza preavviso nei seguenti casi: interventi di aggiornamento tecnico, sicurezza del servizio, utilizzo improprio o difforme dalle norme indicate nel contratto da parte del Cliente.

CORPORATE BANKING AZIENDE – COMODO BANKING

CARATTERISTICHE
Il prodotto Comodo Banking è disponibile in **modalità internet** e consente di visualizzare dati informativi relativi ai servizi attivati oltre a permettere l'invio di disposizioni (bonifici, riba, ecc.) sia relativi alla Banca "Proponente" (cioè colei che offre il servizio al Cliente) che relativi alle banche "passive" (cioè le banche terze presso le quali possono essere eventualmente accesi ulteriori rapporti del Cliente).

Le voci di spesa riportate nel prospetto che segue rappresentano, con buona approssimazione, la gran parte dei costi complessivi sostenuti per un contratto di Corporate Banking Comodo Banking.

Questo vuol dire che il prospetto non include tutte le voci di costo. Alcune delle voci escluse potrebbero essere importanti in relazione sia al singolo deposito sia all'operatività del singolo Cliente.

Prima di scegliere e firmare il contratto è necessario leggere attentamente anche la sezione "altre condizioni economiche".

Tutte le voci di costo sono esposte al valore massimo applicabile (ad esclusione di quelle con una diversa e specifica indicazione).

PRINCIPALI CONDIZIONI ECONOMICHE

V O C I D I C O S T O	
Canone annuo Comodo Banking (WEB)	€ 180,00 canone annuo + € 39,60 iva = € 219,60 (canone mensile € 15,00 + € 3,30 iva = € 18,30)
Canone annuo per sub-holding Comodo Banking (WEB)	€ 120,00 canone annuo + € 26,40 iva = € 146,40 (canone mensile € 10,00 + € 2,20 iva = € 12,20)
Spese invio documento di sintesi	Le spese relative all'invio del documento di sintesi sono applicate per l'importo convenuto sul conto corrente di regolamento

ALTRE CONDIZIONI ECONOMICHE

Costo avviamento servizio	€ 0,00 + iva
Costo rilascio nuova busta PIN	€ 0,00 + iva
Costo rilascio dispositivo DIGIPASS (accessorio per One Time Password per i profili dispositivi)	€ 20,00 + € 4,40 iva = € 24,40
Generazione fattura	A richiesta del Cliente
Periodicità di addebito del canone al Cliente	Trimestrale posticipato

RECESSO E RECLAMI

Recesso dal contratto

La Banca e l'Utente possono recedere dall'accordo, con un preavviso di 90 giorni lavorativi rispetto alla data di efficacia del recesso, dandone comunicazione mediante raccomandata a/r.

La Banca avrà la facoltà di risolvere l'accordo con effetto immediato e conseguente interruzione del servizio nei seguenti casi:

a) inosservanza da parte dell'utente degli obblighi posti da norme di legge o di regolamento vigenti in materia;
b) inadempimento da parte dell'utente delle norme contrattuali;
c) cause di forza maggiore o impossibilità da parte della Banca di erogare il servizio con condizioni simili a quelle pre-esistenti.

Tempi massimi di chiusura del rapporto

Il recesso provoca la chiusura del contratto immediatamente.

Reclami e procedure di risoluzione stragiudiziale delle controversie

I reclami vanno inviati all'Ufficio Reclami della banca, che risponde entro 60 giorni dal ricevimento, per posta ordinaria all'indirizzo "La Cassa di Ravenna S.p.A. – Ufficio Reclami – Piazza G. Garibaldi 6 – 48121 Ravenna", o per posta elettronica a reclami@lacassa.com o tramite pec a reclami@pec.lacassa.com ovvero consegnata allo sportello dove è intrattenuto il rapporto.
In relazione ai servizi di pagamento i tempi massimi di risposta non sono superiori a 15 giornate lavorative dal ricevimento del reclamo. Se il cliente non è soddisfatto della risposta o non ha ricevuto risposta entro i termini previsti, prima di ricorrere al giudice può rivolgersi a:

- *Arbitro Bancario Finanziario* (ABF); per sapere come rivolgersi all'Arbitro e l'ambito della sua competenza si può consultare il sito *www.arbitrobancariofinanziario.it*, chiedere presso le filiali della Banca d'Italia, oppure chiedere alla Banca. Resta fermo diritto del Cliente di presentare esposti alla Banca d'Italia.

Se il Cliente intenta il procedimento presso l'ABF si intende assolta la condizione di procedibilità prevista dalla normativa. La decisione dell'Arbitro non pregiudica la possibilità per il Cliente di ricorrere all'autorità giudiziaria ordinaria.
Ai fini del rispetto degli obblighi di mediazione obbligatoria previsti dal decreto legislativo 4 marzo 2010 n. 28, prima di fare ricorso all'autorità giudiziaria, quale condizione di procedibilità, il Cliente e la Banca devono tentare il procedimento di mediazione, ricorrendo:

- all'*Organismo di Conciliazione Bancaria* costituito dal Conciliatore BancarioFinanziario - Associazione per la soluzione delle controversie bancarie, finanziarie e societarie – ADR (*www.conciliatorebancario.it*, dove è consultabile anche il relativo regolamento) oppure
- ad uno degli altri organismi di mediazione, specializzati in materia bancaria e finanziaria, iscritti nell'apposito registro tenuto dal Ministero della Giustizia.

LEGENDA

Canone	E' il corrispettivo che il Cliente paga periodicamente alla Banca per l'utilizzo dello specifico servizio. Viene di regola addebitato sul conto corrente del Cliente. La periodicità del versamento può essere variabile.
Busta PIN	Busta che contiene la password per il primo accesso (che dovrà essere immediatamente modificata dal Cliente).
Digipass	E' un dispositivo di sicurezza che permette di generare delle password utilizzabili una sola volta per la conferma di disposizioni (bonifici, ordini titoli).
Firma digitale	La firma digitale consente di firmare digitalmente documenti e transazioni (in caso di utilizzo all'interno del servizio Corporate Banking) in formato elettronico assumendo lo stesso valore legale di una tradizionale firma autografa apposta su carta.
Funzioni di ricerca	Funzionalità di estrazione dei documenti informatici in relazione ai criteri previsti dalla Legge (cognome, nome, denominazione, codice fiscale, partita IVA, data o associazioni logiche fra essi).
Marca temporale	La Marca temporale è un certificato che viene associato a un determinato documento contenente l'indicazione di una data e un orario certi col quale si firma il documento stesso.
Responsabile della Conservazione	E' la figura responsabile del processo di conservazione sostitutiva. Nel caso specifico, il Cliente conferisce l'incarico a ICBPI S.p.A.
Sub-holding	Si tratta di contratti relativi a società che per vincoli di controllo e/o di firma vengono ricondotti e fruiti tramite il contratto dalla società capofila.
Secure Call	Servizio subordinato al possesso di un numero cellulare italiano, che permette, tramite una telefonata ad un numero verde, la digitazione di un codice generato in maniera casuale dalla procedura; per la conferma delle disposizioni inserire.

RACCOMANDAZIONI PER UN CORRETTO UTILIZZO DEI SERVIZI DI PAGAMENTO ONLINE

- ❑ Custodire con cura i propri dati di accesso, non salvandoli sul proprio computer, mantenendo separati username e password, e modificando periodicamente quest'ultima.
- ❑ Scegliere una password di accesso sicura utilizzando numeri, lettere e simboli e non parole che derivino da informazioni personali facilmente ottenibili da malintenzionati. Solo in questo caso ha efficacia il doppio livello di sicurezza utilizzato per l'operatività online.
- ❑ Non fornire MAI le proprie password ad alcuno. Si precisa che nessun dipendente è autorizzato a richiederle, pertanto è opportuno diffidare di qualsiasi richiesta in tal senso, sia essa effettuata di persona oppure tramite telefono, posta, e-mail o altro mezzo.
- ❑ Accedere sempre ai servizi online digitando www.lacassa.com, evitando di "cliccare" su eventuali collegamenti presenti nelle e-mail e di dare adito ad eventuali richieste in esse contenute. La Cassa di Ravenna S.p.A. e tutte le Banche del Gruppo Bancario non richiedono MAI di accedere via email ai servizi online e neppure di fornire le credenziali di accesso ai servizi medesimi per eventuali controlli.
- ❑ Assicurarsi che la pagina web in cui si inseriscono dati personali sia protetta, diffidando dei "*pop-up*". Per verificare che la pagina web sia protetta, controllare che l'indirizzo sia preceduto da "https" e che sul browser sia presente l'icona che attesta il collegamento ad un sito protetto, solitamente posizionata in basso a destra.
- ❑ Controllare regolarmente gli estratti conto dei propri conti e depositi, per assicurarsi che le transazioni riportate siano quelle realmente effettuate.
- ❑ Installare e mantenere costantemente aggiornato il software dedicato alla sicurezza del proprio dispositivo, in particolare: Sistema Operativo, Personal Firewall, Antivirus ed Anti-*spyware*.
- ❑ Contattare immediatamente la propria Filiale / l'Help Desk nei seguenti casi:
  - sono stati forniti a terzi i propri codici di accesso
  - è stata dimenticata la propria password o persa la busta PIN per il primo accesso (prima di essersi collegati per la prima volta)
  - si sono ricevute e-mail "sospette"
  - si notano transazioni sospette ed inattese nell'estratto conto
  - si notano sequenze operative diverse da quelle abituali con richiesta del codice di autorizzazione prima della conferma dei dati inseriti o prima dell'inserimento dei dati della disposizione.
  - si individua in elenco un indirizzo IP sconosciuto dalla videata di sfondo dell'applicazione "Riepilogo dei dati recenti collegamenti".