NORME PER LA TRASPARENZA DELLE OPERAZIONI E DEI SERVIZI BANCARI
(D.LGS 385 DEL 01/09/1993 e successivi aggiornamenti)

HAPPY BANKING

INFORMAZIONI SULLA BANCA

BANCO DI LUCCA E DEL TIRRENO S.p.A. - GRUPPO BANCARIO LA CASSA DI RAVENNA
Sede Sociale: Viale Marti, 443 -55100 - Lucca - Iscr. Albo Aziende di Credito n. 5564 - R.E.A. - Lucca n. 181609
Codice Banca n.3242 – Cod. Fisc. e Partita IVA n. 01880620461 - Tel. 0583 43271 - Fax 0583 491255 – www.bancodilucca.it
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. 5564

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 di questo 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 L'INTERNET BANKING

L'Internet Banking consente di accedere alle funzioni informative e dispositive - se previste - ai rapporti di conto corrente, dossier titoli, finanziamenti e agli altri rapporti accesi con la Banca, via Internet 24 ore su 24.

Accesso al servizio, autorizzazione delle disposizioni e sistemi di sicurezza
Per accedere al servizio, oltre alla digitazione delle credenziali personali (user e password), è necessario confermare la propria identità attraverso la Strong Customer Autentication (cd. SCA) ovvero un ulteriore codice casualmente monouso (One Time Password cd.OTP) generato da uno dei seguenti dispositivi definiti in fase di sottoscrizione contrattuale:

- dispositivo **"Secure Call**", strettamente collegato ad un numero di cellulare italiano, consente di confermare la propria identità tramite una telefonata effettuata dal cellulare del Cliente ad un numero verde gratuito e la successiva digitazione del PIN casuale generato dal sistema, attraverso la tastiera del proprio telefono.
In caso di operatività dall'estero, il Cliente - sul telefono abilitato - riceverà una telefonata dove la voce guida indicherà le istruzioni da seguire per l'autenticazione SCA. Il costo della chiamata internazionale è a carico del Cliente e dipendente dalle condizioni contrattualizzate con la propria compagnia telefonica;

- dispositivo di sicurezza **"Digipass**" (cd. time based), consente al Cliente di accedere al servizio inserendo il codice numerico casuale generato dallo strumento. Tale strumento è in disuso per obsolescenza.

- dispositivo di sicurezza "**Digipass**" (cd. transaction based) con tastierino numerico, consente al Cliente di accedere al servizio inserendo il codice numerico di 6 cifre casuale generato dallo strumento.

- dispositivo di sicurezza "**Mobile Token"** integrato nell'APP Happy Banking installata nello smartphone, consente al Cliente di accedere al servizio confermando le notifiche ricevute nell'APP attraverso l'autorizzazione biometrica o il codice PIN rigorosamente personale. Il funzionamento è garantito anche in assenza di copertura rete dati sullo smartphone attraverso l'uso della fotocamera dello stesso e il QRCode pubblicato nell'Internet Banking web.

In fase dispositiva (es autorizzare bonifici, effettuare pagamenti, ordini titoli etc etc) i dispositivi sopra descritti generano la password OTP necessaria a concludere l'operazione.

La password OTP – come le altre credenziali – sono strettamente personali e non devono essere comunicate a terzi.

Il Cliente può attivare anche il servizio aggiuntivo "email/SMS alert" che consente la ricezione di email e/o SMS di notifica al verificarsi di determinati eventi o disposizioni effettuate sull'Internet Banking.

I profili operativi
Sono disponibili vari profili operativi:

- **Documentale**: consente la sola visualizzazione dei documenti inviati dalla Banca (es. estratto conto, ecc.);

- **<u>Informativo</u>**: consente la visualizzazione dei saldi e dei movimenti dei conti correnti e dei depositi titoli; oltre alla visualizzazione di documenti (es. estratto conto, ecc.);
- **<u>Base</u>**: oltre alle funzioni previste dal profilo informativo, consente di effettuare disposizioni bancarie. In via esemplificativa ma non esaustiva, tale profilo può effettuare disposizioni di bonifico o giroconto, F24, prenotazioni effetti, ricariche telefoniche, MAV/RAV, bollettini postali, bancari e CBILL, bollo ACI auto e moto, ricariche Nexi Ricaricassa;
- **<u>Trading</u>**: oltre alle funzioni previste dal profilo Base, il profilo fornisce informazioni e quotazioni (sia mercato diurno che *After Hours*) relative ai titoli Azionari quotati sulla Borsa Italiana, Mercato Telematico Azionario (MTA), ETF e Fondi Chiusi, Titoli di Stato, Obbligazioni, Obbligazioni Convertibili, Mercato EuroTLX, Diritti, Indici, Cambi. Sono disponibili la Watch List, Grafici e Cambi Valutari, informazioni relative ai Fondi e la consultazione delle Gestioni Patrimoniali. Sono inoltre disponibili le informazioni sulla situazione degli ordini.
- <u>Il profilo Trading</u> consente di effettuare:
  - operazioni di compravendita di titoli azionari e warrant e di titoli obbligazionari italiani, quotati sulla Borsa Valori di Milano, titoli quotati su EuroTLX e ETF e Fondi Chiusi;
  - operazioni di compravendita di titoli azionari quotati sui mercati europei SBR-VIR-XET-AEX-MAD, sul mercato LSE (London Stock Ex) e sui mercati americani NAS (NASDAQ), NYS (NYSE) e AMEX.

  L’inoltro degli ordini sul mercato sarà vincolato agli orari di operatività del mercato stesso. **I prezzi dei titoli quotati su mercati esteri non sono in tempo reale, ma sono aggiornati con un ritardo fino a 20 minuti**.

SmartCash

Con i profili BASE E TRADING, il Cliente Consumatore può attivare il servizio SMARTCASH ATM che consente di prelevare contante da ATM convenzionati, tramite l’utilizzo di dispositivi smartphone e con l’ausilio della relativa APP disponibile negli store digitali.

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 messe a disposizione dalla Banca anche sul suo sito internet;
- ❑ 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. La Filiale che riceve la comunicazione richiede 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 messo a disposizione dalla Banca. 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.;
- ❑ 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;
- ❑ per quanto riguarda il Profilo Trading, si evidenzia come il suo utilizzo può indurre ad aumentare il numero delle proprie transazioni operando in una prospettiva *intraday*.

INTERNET BANKING – HAPPY BANKING

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

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

PRINCIPALI CONDIZIONI ECONOMICHE

VOCI DI COSTO	
Canone annuo	(applicato in quote trimestrali posticipate)
profilo informativo	€ 60,00 canone annuo + € 13,20 iva = € 73,20 (€ 5,00 canone mensile + € 1,10 iva = € 6,10)
profilo base	€ 108,00 canone annuo + € 23,76 iva = € 131,76 (€ 9,00 canone mensile + € 1,98 iva = € 10,98)
profilo trading	€ 168,00 canone annuo + € 36,96 iva = € 204,96 (€ 14,00 canone mensile + € 3,08 iva = € 17,08)
profilo documentale	€ 0,00 canone annuo +€ 0,00 iva = € 0,00
Canone annuo servizio MOBILE TOKEN (5) profilo base/profilo trading (si aggiunge al canone annuo)	€ 3,00 canone annuo + € 0,66 iva = € 3,66 (€0,25 canone mensile + € 0,055 iva = € 0,305)
Spese sospensione contratto, su iniziativa della banca, per inutilizzo per un periodo superiore a 180 giorni	€ 10,00 + iva
Importo massimo giornaliero / mensile bonifici	Pattuito in base alle necessità del Cliente
Importo massimo giornaliero / mensile bonifici effettuati con il servizio My Bank	Pattuito in base alle necessità del Cliente
Importo massimo singola ricarica telefonica	Pattuito in base alle necessità del Cliente
Importo massimo giornaliero per ricariche telefoniche	Pattuito in base alle necessità del Cliente
Generazione fattura	A richiesta del Cliente
Periodicità di fatturazione	Trimestrale posticipato
Costo rilascio dispositivo DIGIPASS (1) successivo al primo (richiesto a seguito rottura, smarrimento, ecc…) (accessorio per One Time Password per i profili dispositivi "Base e Trading")	€ 15,00 + € 3,30 iva = € 18,30
Costo **unitario** per avvisi informativi tramite SMS sui servizi bancari e finanziari	€ 0,25 + iva
Costo **unitario per** avvisi tramite SMS per operazioni disposte da Internet Banking/Corporate Banking (2) (l'invio degli avvisi tramite email, dove previsto, è sempre gratuito).	€ 0,15 + iva
Costo **unitario per** avvisi tramite SMS per operazioni con carta di debito (3)	€ 0,12 + iva
Commissioni relative ad operazioni di pagamento con addebito in conto corrente	Indicate nel Foglio Informativo "Servizi Incassi/Pagamenti e Servizi Vari

(1) E' prevista la fornitura gratuita del primo dispositivo "Digipass", per i profili dispositivi "Base" e "Trading" non attivi con il Servizio Secure Call.

(2) Viene inviato un SMS di avvertimento a fronte di predeterminate operazioni disposte tramite il prodotto di "Happy Banking". Per le operazioni di Bonifico il messaggio sms viene inviato per operazioni di importo non inferiore a € 50,00.

(3) Viene inviato un SMS di avvertimento a fronte di operazioni effettuate con carta di debito BANCOMAT®/ PagoBANCOMAT® di importo pari o superiore all'importo pattuito. In ogni caso il suddetto importo pattuito non può essere inferiore a € 120,00.

(4) **Nuovo sistema di autenticazione delle operazioni bancarie che sostituisce il "Token fisico" o "Secure Call". Attivabile in autonomia dal cliente, intestatario di un rapporto di internet banking base/trading.**

CONDIZIONI ECONOMICHE SERVIZIO SMARTCASH ATM

VOCI DI COSTO	
Canone annuo	€ 0,00
Massimale giornaliero operazioni di prelievo presso sportelli ATM	€ 500,00
Massimale mensile operazioni di prelievo presso sportelli ATM	€ 1.500,00

RECESSO E RECLAMI

Recesso dal contratto
Si può recedere dal contratto in qualsiasi momento, senza penalità e senza spese di chiusura del conto.

Tempi massimi di chiusura del rapporto
Il recesso provoca la chiusura del contratto immediatamente. Il tempo massimo di chiusura del rapporto è pari a 5 giorni lavorativi.

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 "Banco di Lucca e del Tirreno S.p.a. – Ufficio Reclami c/o La Cassa di Ravenna S.p.A. Piazza Giuseppe Garibaldi 6 48121 Ravenna RA", o per posta elettronica alla casella reclami@bancodilucca.it o tramite pec a reclami@pec.bancodilucca.it 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

Autenticazione forte del Cliente	Autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.
Canone	È 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.
Bonifico istantaneo	Bonifico SEPA che consente di trasferire, 24 ore su 24, 7 giorni su 7, entro pochi secondi dal ricevimento della relativa richiesta, importi in euro da un Conto ad altro Conto aperto presso banche che si trovino in Italia o in un altro paese SEPA ed aderiscano allo schema SEPA Instant Credit Transfer (SCT Inst) definito dall'EPC - European Payments Council e che siano raggiungibili mediante il canale TIPS (TARGET Instant Payment Settlement).
Busta PIN	Busta che contiene la password per il primo accesso (che dovrà essere immediatamente modificata dal Cliente).
Digipass	Dispositivo di sicurezza SCA che permette di generare codici casuali monouso per l'accesso e/o la conferma di disposizioni (es bonifici, ordini titoli).
MyBank	È un servizio europeo di pagamento per e-commerce, promosso dall'Autorità Bancaria Europea (EBA), che permette di effettuare pagamenti elettronici utilizzando direttamente il proprio Internet Banking "Happy Banking" senza alcun scambio di dati riservati in rete, effettuando un bonifico SEPA.
SmartCash	APP (Applicazione Mobile) che consente di prelevare contante da ATM convenzionati, tramite l'utilizzo di dispositivi smartphone. Alcune funzionalità richiedono la registrazione dell'utente.
Secure Call	Dispositivo di sicurezza SCA, collegato ad un numero di cellulare italiano, consente di confermare la propria identità tramite una telefonata sul cellulare del Cliente in Italia o all'estero.

SCA	Strong Customer Autentication procedura per convalidare l'identificazione di un utente basata sull'uso di due o più elementi di autenticazione (cd. "autenticazione a due fattori").

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 e che rispettino i requisiti minimi. Solo in questo caso ha efficacia il doppio livello di sicurezza utilizzato per l'operatività online.
- Non fornire MAI le proprie password a terzi. 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 https://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 e tutte le Banche del Gruppo Bancario La Cassa 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.