

FOGLIO INFORMATIVO SULLE OPERAZIONI E SERVIZI OFFERTI ALLA CLIENTELA

INTERNET BANKING/CORPORATE BANKING

Data pubblicazione: 22/04/2020

INFORMAZIONI SULLA BANCA

Denominazione e forma giuridica BANCA POPOLARE VALCONCA SOCIETA' PER AZIONI
Sede Legale e Amministrativa: VIA R. BUCCI, 61 - MORCIANO DI ROMAGNA – RN
Indirizzo Telematico: info@bancavalconca.it
Sito Internet: www.bancavalconca.it
Numero di Iscrizione all'Albo delle Banche presso Banca d'Italia n 627.00
Codice ABI n. 05792
Codice Fiscale: 00125680405 P.IVA.: 00125680405 Iscrizione al Registro delle Imprese di Rimini - n.16601
Aderente al Fondo Interbancario di Tutela dei Depositi ed al Fondo Nazionale di Garanzia

CHE COS'E' L'INTERNET BANKING E IL CORPORATE BANKING

Il Servizio di **Internet Banking** permette al Cliente, attraverso il collegamento Internet attivo 24 ore su 24, di effettuare, nei giorni, orari e secondo le modalità tecniche ed operative indicate, interrogazioni sul proprio conto corrente (saldo, lista movimenti, ecc..) e disporre, nei limiti di saldo disponibili, bonifici e giroconti. Il Servizio consente inoltre, previa sottoscrizione degli appositi contratti, l'esecuzione di operazioni di acquisto e vendita di strumenti finanziari (trading online) a valere su un deposito a custodia ed amministrazione intestato al Cliente stesso.

Il Servizio di Corporate Banking Interbancario è un servizio bancario che consente ad un'azienda di operare con più banche delle quali è cliente, tramite un unico collegamento telematico, utilizzando così una piattaforma comune per l'inoltro dei flussi telematici relativi alla propria operatività finanziaria e commerciale (verifica saldi e movimentazione dei conti, disposizione in merito a pagamenti e gestione degli incassi).

La Banca Popolare Valconca che presta il Servizio e con la quale il Cliente stipula uno specifico contratto di Corporate Banking Interbancario, è detta banca attiva; le altre banche collegate sono dette banche passive. Il servizio di Corporate Banking Interbancario presuppone che il Cliente sia titolare di conto corrente.

Il Cliente è tenuto ad indicare ad ognuna delle banche passive con cui intrattiene rapporto di conto le funzioni per la cui esecuzione intende utilizzare il Servizio, nonché a concordare le funzioni facoltative, e ad autorizzare le medesime banche passive ad eseguire tutte le istruzioni contenute nei flussi inviati, assumendosi la responsabilità della legittimità, liceità, autenticità, esattezza e completezza delle medesime istruzioni. Ai fini di cui sopra, il Cliente deve concludere con le sue banche passive un apposito contratto e, dopo aver ottenuto la disponibilità ad eseguire il Servizio da parte della singola banca passiva, può avviare lo scambio dei flussi elettronici con la medesima banca.

RISCHI TIPICI

Tra i principali rischi, vanno tenuti presenti:

- variazione in senso sfavorevole delle condizioni economiche (commissioni e spese del servizio) ove contrattualmente previsto;
- utilizzo indebito o improprio dei codici personali di accesso e di disposizione (codice utente e password) in conseguenza a smarrimento o furto;

- utilizzo indebito da parte di terzi dell'apparecchio cellulare e del numero di utenza telefonica associata;
- sospensione del funzionamento del servizio in relazione ad esigenze connesse all'efficienza e alla sicurezza dello stesso, ritardo o mancata esecuzione delle operazioni per motivi tecnici o di forza maggiore;
- messa a disposizione e trasmissione dei dati sul circuito Internet;
- ai sensi della comunicazione Consob n. DI/30396 del 21 aprile 2000 si informa che l'utilizzo dei servizi di trading on line può indurre il cliente a moltiplicare le transazioni, operando in una prospettiva intraday, con conseguente aumento del rischio relativo. L'eventuale incremento della frequenza operativa potrà inoltre comportare dei riflessi in termini di costo complessivo sostenuto per la negoziazione degli strumenti finanziari.

Obblighi del Cliente

Ai fini del contenimento dei rischi operativi elencati, il Cliente è tenuto a custodire con la massima cura i codici di Accesso al Servizio, evitandone la conservazione insieme al dispositivo "Token", ed evitando di cederli in uso a terzi.

Qualunque uso improprio dei codici di Accesso, del dispositivo "Token", del telefono cellulare associato al Servizio, da chiunque e in qualsiasi modo effettuato, rimane ad esclusivo rischio del Cliente.

In caso di furto o smarrimento (dei Codici di Accesso, del Token o del telefono cellulare associato al Servizio) il Cliente deve chiedere immediatamente il blocco del Servizio, informando tempestivamente la Banca e denunciare l'accaduto all'Autorità Giudiziaria o di Polizia.

Al fine di mitigare i rischi connessi al servizio in argomento, si raccomanda la lettura dei documenti "Guida all'accesso all'Internet Banking / Corporate Banking", disponibili sul sito internet www.bancavalconca.it nell'Area Clienti.

NOVITA' IN MATERIA DI AUTENTICAZIONE FORTE E PSD2

Dal **14 Settembre 2019** si applicherà il nuovo Regolamento delegato (UE) 2018/389, integrante la direttiva (UE) 2015/2366 (PSD2), nato per promuovere l'innovazione e lo sviluppo dei digital payment, aumentare la protezione e la sicurezza degli utenti nei servizi di pagamento online e favorire più alti livelli di concorrenza all'interno del mercato dei pagamenti.

La richiamata normativa impone criteri di sicurezza molto più efficaci rispetto agli attuali (Autenticazione forte del Cliente o Strong Customer Authentication – SCA) ed interesserà sia la fase di collegamento al servizio, che l'autorizzazione di eventuali operazioni dispositive.

La procedura di login sarà resa ancora più sicura tramite due passaggi autorizzativi, e grazie alla S.C.A., il nuovo Sistema di Autenticazione Sicura prevede:

- in fase di accesso ai conti, in aggiunta alle User ID e Password già in possesso del Cliente, l'inserimento di una ulteriore password usa e getta (OTP);
- in fase dispositiva l'inserimento di una password, sempre del tipo usa e getta, generata tenendo conto degli estremi del pagamento (Importo, IBAN del beneficiario, ecc.).

1) CLIENTI CON INTERNET BANKING INFORMATIVO

Per continuare ad operare attraverso il canale Web il Cliente dovrà recarsi presso la propria Filiale di riferimento, per sostituire il contratto di IB informativo, avente come credenziali di accesso la User-Id, la password e il Secure Call. In fase di sottoscrizione della nuova contrattualistica, verrà richiesto il recapito telefonico da associare al servizio.

2) CLIENTI CON INTERNET BANKING CON "TOKEN"

Per continuare ad operare attraverso il canale Web, il Cliente dovrà:

1. Recarsi presso la propria Filiale di riferimento, per certificare il numero di cellulare sul quale sarà inviato un sms con il Codice necessario per disporre le operazioni di pagamento (Bonifici, Ricariche Telefoniche, Pagamento Bollette, etc.).
2. Una volta completato quanto sopra descritto, per l'accesso al servizio Online Banking sarà necessario inserire la User ID, Password e il codice OTP generato dal Token in uso (Digipass).

Per le operazioni dispositive, dopo aver effettuato l'autorizzazione con le modalità già in uso, sarà necessario inserire un secondo codice specifico per beneficiario ed importo della singola operazione che Le verrà inviato tramite SMS sul numero di cellulare certificato presso la sua Filiale; quest'ultimo insieme al codice OTP generato dal Digipass dovrà essere inserito negli appositi campi che compariranno a schermo.

3) CLIENTI CON INTERNET BANKING CON "SECURE CALL"

Per l'accesso al servizio Online Banking sarà necessario:

1. Inserire la User ID, Password
2. Chiamare il numero verde 800.24.23.14 inserendo il Codice usa e getta mostrato a video.

Per le operazioni dispositive, compariranno a schermo due diversi codici numerici, tali codici, alla stregua di quanto effettuato in fase di accesso, dovranno essere digitati al risponditore vocale contattabile previa chiamata al numero verde 800.24.23.14. Una volta digitati entrambi i codici il risponditore vocale riepilogherà gli estremi dell'operazione da validare.

4) CLIENTI CON CORPORATE BANKING CON "TOKEN"

Per continuare ad operare attraverso il canale Web, il Cliente dovrà:

1. Recarsi presso la propria Filiale di riferimento, per certificare il numero di cellulare sul quale sarà inviato il Codice necessario per l'accesso al servizio Online Banking e ritirare il suo nuovo Dispositivo Token.
2. Una volta completato quanto sopra descritto, per l'accesso al servizio Online Banking sarà necessario inserire la User ID, Password e il primo codice OTP generato dal Nuovo Token.

Per le operazioni dispositive, dopo aver effettuato l'autorizzazione con le modalità già in uso, sarà necessario inserire un secondo codice Dynamic Linking specifico per beneficiario ed importo della singola operazione che verrà generato sempre tramite il suo Nuovo Token Transaction Based; quest'ultimo insieme al codice OTP dovrà essere inserito negli appositi campi che compariranno a schermo.

INTERNET BANKING – PROFILI OPERATIVI

Il Servizio di Internet Banking è disponibile nei seguenti profili operativi, caratterizzati da specifiche funzionalità e attivati dal Cliente al momento della sottoscrizione del Contratto o con successiva comunicazione inviata per iscritto alla Banca:

a) profilo informativo: consente al Cliente di consultare i saldi e i movimenti dei propri conti correnti, la situazione assegni, la posizione del deposito titoli e dell'esito degli ordini e di ricevere le comunicazioni online;

b) profilo dispositivo, in aggiunta alle funzionalità del profilo informativo, permette di:

- effettuare operazioni di giroconto e bonifico.
Per le relative condizioni economiche, si rimanda al Foglio Informativo n. 13 "Bonifici"
- prenotazione e pagamento effetti, ricariche telefoniche, pagamento di bollettino bancario, pagamento MAV e RAV e le eventuali ulteriori operazioni che la Banca dovesse, nel tempo, rendere eseguibili tramite il Servizio.
Per le relative condizioni economiche, si rimanda al Foglio Informativo n. 12 "Incassi"

c) profilo trading online: in aggiunta alle funzionalità del profilo dispositivo, consente al Cliente di ricevere l'informativa finanziaria aggiornata in tempo reale nonché di effettuare operazioni su strumenti finanziari.

Il profilo trading online può essere attivato solo se il Cliente sottoscrive presso la Banca il contratto per la negoziazione, la ricezione e la trasmissione di ordini su strumenti finanziari. Il Cliente può disporre ordini di vendita di strumenti finanziari di cui ha la piena disponibilità nel deposito titoli in custodia e amministrazione. Per le relative condizioni economiche, si rimanda al Foglio Informativo n. 11 "Deposito titoli".

CONDIZIONI ECONOMICHE

Servizio di Internet Banking	
Costo per prodotto di Banca Virtuale	€ 0,00
Costo per chiamata Call Center	€ 0,00

Costo per chiamata Call Center operatore	€ 0,00
Costo per operazione (Call Center)	€ 0,00
Costo per fax prodotti (Call Center)	€ 0,00
Costo per rilascio nuove buste PIN	€ 0,00
Canone mensile Secure Call	€ 0,75
Spese per comunicazioni ai sensi della normativa sulla Trasparenza bancaria	
Spese produzione "Documento di Sintesi"	
Formato cartaceo	€ 0,00
Formato elettronico	€ 0,00
Servizio di Corporate Banking	
Spesa una tantum del dispositivo (Token)	€ 20,00
Sostituzione dispositivo (Token) per smarrimento	€ 20,00
Sostituzione dispositivo (Token) per guasto	Gratuita

LIMITI OPERATIVI

Limite giornaliero bonifici "Electronic Banking"	€ 500,00
Limite mensile bonifici "Electronic Banking"	€ 500,00

RECESSO E RECLAMI

Recesso dal contratto

Il cliente ha diritto di recedere in ogni momento, dandone comunicazione scritta alla banca, senza alcun preavviso, senza penalità e senza spese di chiusura. La banca ha diritto di recedere in ogni momento, dandone comunicazione scritta al cliente con 30 giorni di preavviso (60 giorni se il cliente è un Consumatore o una Microimpresa) e senza alcun onere per il cliente. Il recesso senza preavviso è ammesso in presenza di giusta causa o giustificato motivo, dandone immediata comunicazione.

Tempi massimi di chiusura del rapporto

N° 15 giorni dal ricevimento della richiesta del cliente.

Reclami

I reclami vanno inviati all'Ufficio Reclami della banca (via Bucci, 61 - 47833 Morciano di Romagna). È consentito l'inoltro a mezzo:

1. Posta ordinaria o raccomandata all'indirizzo: Via Bucci, 61 - 47833 Morciano di Romagna (RN);
2. Email ordinaria: Legale@bancavalconca.it;
3. Posta Elettronica Certificata (PEC): Legalepec@bancavalconca.com;
4. Fax: 0541/859236.

La struttura organizzativa responsabile della trattazione del reclamo è l'Ufficio Legale.

L'Ufficio Reclami risponde entro 30 giorni dal ricevimento.

Tuttavia, in relazione ai servizi di pagamento la Banca è tenuta a fornire una risposta entro il termine di quindici (15) giorni operativi.

In situazioni eccezionali, se la Banca non può rispondere entro quindici (15) giornate operative per motivi indipendenti dalla sua volontà, è tenuta a inviare una risposta interlocutoria, indicando chiaramente le ragioni del ritardo nella risposta al reclamo e specificando il termine entro il quale il cliente otterrà una risposta definitiva. In ogni caso il termine per la ricezione della risposta definitiva non supera le trentacinque (35) giornate operative.

Se il cliente non è soddisfatto o non ha ricevuto risposta entro i 30 giorni, prima di ricorrere al giudice può rivolgersi a:

- Arbitro Bancario Finanziario (ABF). Per sapere come rivolgersi all'Arbitro si può consultare il sito www.arbitrobancariofinanziario.it, chiedere presso le Filiali della Banca d'Italia, oppure chiedere alla Banca;

- Conciliatore Bancario Finanziario. Qualunque sia il valore della controversia, prima di ricorrere all'autorità giudiziaria, il cliente può - singolarmente o in forma congiunta con la banca - attivare una procedura di conciliazione al fine di trovare un accordo con la banca per la soluzione delle controversie relative al rapporto presso il Conciliatore Bancario Finanziario con sede legale in Via delle Botteghe Oscure, 54 Roma 00186, Tel. 06/674.821, sito internet www.conciliatorebancario.it.

Resta impregiudicata la facoltà di ricorrere all'autorità giudiziaria nel caso in cui la conciliazione si dovesse concludere senza il raggiungimento di un accordo.

- Il cliente unitamente alla banca, può infine attivare (anche presso il Conciliatore Bancario Finanziario) una procedura arbitrale (ai sensi degli art. 806 e ss. del c.p.c.).

LEGENDA

Autenticazione	Il processo volto a verificare e a comprovare l'autenticità di un messaggio o di un'operazione dispositiva e/o informativa o il processo che identifica il soggetto legittimato ad operare mediante l'utilizzo del PIN, della Password, o di altri dispositivi di sicurezza.
Codice utente (User-id)	Il codice numerico che identifica univocamente il Cliente, immutabile e predeterminato dalla Banca;
Password di accesso	Codice numerico consegnato all'utente dalla Banca per consentire il primo collegamento: tale codice dovrà necessariamente essere modificato in occasione del primo collegamento al Servizio mediante indicazione di un nuovo codice alfanumerico - formato da almeno otto caratteri - liberamente scelto dall'utente in fase di attivazione del Servizio e successivamente modificabile, attraverso cui l'utente viene riconosciuto in maniera univoca; è idoneo ad autenticare l'operazione. La Password serve per entrare nel servizio di Internet Banking e poter disporre dei dati a livello informativo.
Token	Supporto generatore di password (ogni 60 secondi) che consente al cliente l'accesso al proprio Internet/Corporate Banking in maniera del tutto protetta.
Secure Call	Servizio che prevede l'autenticazione tramite il cellulare del Cliente collegato al contratto di Internet banking. Il Cliente ha a disposizione circa 60 secondi dalla conferma dell'operazione eseguita per la digitazione del corretto codice numerico monouso (di seguito OTP, ovvero One Time Password), sul dispositivo cellulare di cui si avvale
Strong Customer Authentication (SCA)	La Strong Customer Authentication (SCA) è una forma di autenticazione forte, che si basa sulla verifica di almeno due elementi di diversa natura per accertare l'identità di un utente al momento dell'accesso online a un conto di pagamento e la riconducibilità allo stesso utente delle operazioni di pagamento.