FOGLIO INFORMATIVO

CARTA DI DEBITO RAIFFEISEN

INFORMAZIONI SULLA BANCA

CASSA RAIFFEISEN BASSA ATESINA SOC. COOPERATIVA
VIA B. FRANKLIN 6 - 39055 - LAIVES / ZONA INDUSTRIALE
Tel: 0471/592500
Fax: 0471/592520
E-mail: cra.bassa-atesina@raiffeisen.it
PEC: pec08114@raiffeisen-legalmail.it
Sito internet: http://www.raiffeisen.it/unterland.html

Numero di iscrizione all'albo delle banche: 4577.3.0
aderente al Fondo di Garanzia dei Depositanti del Credito Coop. e al Fondo Nazionale di Garanzia di cui all'art. 62 del d.lgs. n. 415/96

CHE COSA È LA CARTA DI DEBITO RAIFFEISEN

La Carta di debito Raiffeisen (di seguito anche carta) consente al Cliente, a seconda dei Servizi rispettivamente sistemi attivati sulla stessa, di effettuare pagamenti senza contanti o ritirare denaro contante presso le apposite apparecchiature. I relativi importi vengono addebitati direttamente sul conto corrente.
Inoltre il Cliente può effettuare versamenti di denaro contante presso le apposite apparecchiature (ATM) della Banca a ciò abilitate. Le somme versate saranno accreditate sul conto corrente collegato alla carta di debito. È necessaria la digitazione del Codice Personale Segreto (PIN).
Le operazioni si svolgono tramite diversi operatori rispettivamente sistemi:

Prelievo e versamento di contante: ritiro e versamento di denaro contante - entro i limiti contrattualmente convenuti - presso qualunque apparecchiatura (ATM e/o macchina self-service) contraddistinta dal marchio BANCOMAT®, Maestro o dagli altri marchi comunicati dalla Banca. È necessaria la digitazione del Codice Personale Segreto (PIN).
Servizio di pagamento: compimento di acquisti di beni e Servizi - entro i limiti contrattualmente convenuti - presso esercizi convenzionati mediante qualunque apparecchiatura contrassegnata con il Marchio PagoBANCOMAT®, Maestro o degli altri circuiti comunicati dalla Banca. È necessaria la digitazione del Codice Personale Segreto (PIN).
Fastpay: pagamento dei pedaggi autostradali presso le barriere autostradali dotate di apposite apparecchiature e contraddistinte dal marchio FASTpay, relativi a percorsi su tratti gestiti da Società od Enti convenzionati. La contabilizzazione dell'importo dei pedaggi avverrà con un unico addebito mensile comprensivo dei pagamenti effettuati nel mese antecedente a quello di addebito, con valuta media ponderata.
Il Servizio Fastpay può essere attivato anche per l'acquisto di titoli di viaggio per autobus e treno presso le biglietterie automatiche gestite dalla SAD Trasporto Locale spa, per il pagamento del parcheggio, etc.
Selfservice: ricarica telefoni cellulari mediante utilizzo congiunto della Carta di debito Raiffeisen e del P.I.N., stampa dell'estratto conto e di altri documenti, nonché svolgimento di eventuali altri Servizi.
Pagamenti su Internet: pagamenti elettronici in negozi online tramite la funzione Maestro con utilizzo di due codici personali.
PayPass: pagamento POS in Italia e all'estero per gli importi massimi convenuti, senza inserimento Carta e senza digitazione del codice P.I.N.

I principali rischi della Carta di debito Raiffeisen consistono nell'abuso rispettivamente uso illecito della stessa da parte di terzi. Pertanto va osservata la massima attenzione nella custodia della Carta e del PIN; quest'ultimo, in particolare, deve restare segreto. Nel caso di smarrimento o sottrazione il Cliente è tenuto a richiedere immediatamente il blocco della Carta, secondo le modalità contrattualmente previste (Numero Verde per il blocco della Carta). Per prevenire questi rischi, sulla Carta possono essere attivate le seguenti misure di sicurezza:

SMS-Alert: Messaggi SMS sul numero telefonico convenuto nei casi in cui vengono effettuati con la Carta prelievi o pagamenti che superano l'importo convenuto.
Blocco nei Paesi fuori Europa: La Carta di debito Raiffeisen viene attivata solo su espressa richiesta da parte del Cliente e per un periodo limitato nei paesi fuori Europa.

Conseguenze negative risultano, infine, dalla revoca, da parte della Banca, dell'autorizzazione ad utilizzare la carta (blocco) nel caso di utilizzo fraudolento o non autorizzato della Carta da parte del Cliente.

Informazione ai sensi del Regolamento (UE) 2015/751

Circuiti disponibili: BANCOMAT® e PagoBancomat, FastPay, MAESTRO

Tecnologia e funzionalità:

	BANCOMAT® e PagoBancomat	**FastPay**	**MAESTRO**
Tecnologia	banda magnetica, chip e C-less	banda magnetica	banda magnetica, chip e C-less
Funzionalità	prelievo ATM e pagamento POS fisico in Italia		prelievo ATM e pagamento POS fisico e virtuale in Italia, UE e extra UE

Costi fissi: vedasi singole voci di cui sotto (Condizioni economiche)

Costi variabili: vedasi singole voci (prelievo, pagamento POS, ecc.) nel foglio informativo relativo al contratto di conto corrente, al quale si rinvia.

Caratteristiche di sicurezza:

Sono garantite:

- certificazioni/omologazioni Mastercard e Consorzio BANCOMAT® su tutti i prodotti;
- conformità a standard EMV/ISO;
- conformità agli standard Mastercard per antenna RFID e chip per pagamenti anche "contact-less";
- richiesta di autorizzazione online per le transazioni chip.

Il sistema autorizzativo rappresenta il primo livello di controllo delle transazioni, come per esempio:

- validazione del PIN;
- disponibilità del plafond abbinato alla carta;
- stato della carta (bloccata, non bloccata);
- validazione elementi di sicurezza della carta (CVV2, CVC2, 3DSecure);
- limite utilizzo per tipo spesa.

Tutti i disconoscimenti per frode sono segnalati giornalmente affinché sia predisposto il flusso informativo verso l'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP) previsto dal SIPAF (Sistema di prevenzione delle frodi sulle carte di pagamento).

Il titolare può richiedere l'estensione o la riduzione della spendibilità della carta a valere su singole aree geografiche predefinite o in tutto il mondo. Tramite il servizio Online Banking, sono messe a disposizione del Cliente:

- funzionalità abilita l'utilizzo della carta: disabilitare/abilitare la possibilità di effettuare prelevamenti/pagamenti con la carta su ATM/POS fuori Europa;
- 3D Secure: sistema di protezione identificato con "Mastercard SecureCode" che permette di acquistare sui siti internet convenzionati al servizio tramite l'inserimento di una password; inoltre al Cliente viene associata una frase identificativa visualizzabile al momento dell'inserimento del codice per permettere di riconoscere un sito sicuro;
- avvisi e-mail/SMS: impostati per essere ricevuti a ogni utilizzo.

Lo scambio di informazioni tra terminale, centri applicativi e Banca è eseguito nel rispetto di tutti gli standard di sicurezza.
Qualora si verifichino delle situazioni in cui un'operazione, nonostante la possibilità, non viene eseguita utilizzando il microchip, si crea una situazione definita fallback. Al fine di aumentare il grado di sicurezza delle carte, non è consentito il funzionamento della carta in fallback.

CONDIZIONI ECONOMICHE

	VOCI	COSTI
SPESE	Spese di rilascio di una carta di debito (BANCOMAT®, PagoBANCOMAT®, Mastercard) - comprende emissione e gestione della carta	0,00 euro (emissione) 15,00 euro annualmente (gestione)
	Spese di rinnovo della carta di debito	5,00 euro
	Spese per la sostituzione della carta di debito	5,00 euro
	Spese di blocco tramite la Banca	0,00 euro
	Spese di blocco tramite numero telefonico di blocco	0,00 euro
	Spese di blocco su iniziativa della Banca	0,00 euro
MASSIMALI D'UTILIZZO	BANCOMAT®: importo giornaliero	1.500,00 euro
	BANCOMAT®: importo mensile	3.000,00 euro
	PagoBANCOMAT®: importo giornaliero	3.000,00 euro
	PagoBANCOMAT®: importo mensile	3.000,00 euro
	Prelievo di contante con Maestro all'ATM: importo giornaliero	2.500,00 euro
	Prelievo di contante con Maestro all'ATM: importo mensile	3.000,00 euro
	Pagamento con Maestro al POS: importo giornaliero	3.000,00 euro
	Pagamento con Maestro al POS: importo mensile	3.000,00 euro
	Importo totale (ATM + POS nazionale e estero) giornaliero	3.000,00 euro
	Importo totale (ATM + POS nazionale e estero) mensile	3.000,00 euro
	FASTpay: importo massimo per singolo pedaggio importo per altri Servizi giornaliero importo massimo per singolo pedaggio Autostrada del Brennero SpA	 100,00 euro 100,00 euro 113,62 euro
	NFC - pagamenti contactless : importo massimo per singolo pagamento senza digitazione del PIN	 25,00 euro
CAMBIO	Agli addebiti di norma viene applicato il cambio del giorno operativo bancario successivo al giorno in cui avviene l'operazione.	
VALUTA	giorno del prelievo di contante Pagamento tramite POS: giorno dell'operazione Fastpay: valuta media ponderata di tutti i pagamenti del mese precedente Versamento di contante presso un ATM e/o una macchina self-service: giorno del versamento se il cliente è un consumatore, entro il prossimo giorno lavorativo bancario se il cliente non è un consumatore	

RECESSO E RECLAMI

Recesso dal contratto

Il Cliente ha facoltà di recedere dal presente contratto in qualunque momento, dandone comunicazione scritta alla Banca e restituendo la Carta, nonché ogni altro materiale in precedenza consegnato.
La Banca può recedere dal presente contratto o dai singoli Servizi in qualsiasi momento con preavviso di 2 mesi. Qualora ricorra un giustificato motivo ai sensi del Codice del Consumo d.lgs. n. 206/2005, art. 33, comma 3, ovvero sia necessario tutelare l'efficienza e la sicurezza dei Servizi, la Banca ha anche facoltà di recedere dal contratto senza preavviso, dandone immediata comunicazione al Cliente.
Il Cliente resta responsabile di ogni conseguenza dannosa che possa derivare dalla prosecuzione dell'uso dei Servizi successivamente al recesso della Banca o nel periodo in cui abbia ricevuto dalla Banca medesima eventuale comunicazione dell'esistenza di un temporaneo divieto di utilizzazione della Carta.

Tempi massimi di chiusura del rapporto contrattuale

Il rapporto contrattuale termina con la restituzione della Carta, nonché di ogni altro materiale consegnato.

Reclami

Il Cliente può presentare un reclamo all'intermediario, anche per lettera raccomandata A/R o per via telematica (CASSA RAIFFEISEN BASSA ATESINA SOC. COOPERATIVA, VIA B. FRANKLIN 6, 39055 LAIVES / ZONA INDUSTRIALE, PEC08114@RAIFFEISEN-LEGALMAIL.IT, CRA.BASSA-ATESINA@RAIFFEISEN.IT, fax: 0471/592520).
Il Cliente rimasto insoddisfatto o il cui reclamo non abbia avuto esito nel termine di 60 giorni dalla sua ricezione ovvero, in caso di servizi di pagamento, entro 15 giorni lavorativi, può presentare ricorso all'Arbitro Bancario Finanziario (ABF) entro 12 mesi dalla presentazione del reclamo. Per ulteriori informazioni si consulti il sito www.arbitrobancariofinanziario.it, oppure si contatti una Filiale della Banca d'Italia o la Banca.
Il Cliente può - singolarmente o in forma congiunta con la Banca - attivare una procedura di conciliazione finalizzata al tentativo di trovare un accordo. Detto tentativo sarà esperito dall'Organismo di conciliazione bancaria costituito dal

Conciliatore BancarioFinanziario - Associazione per la soluzione delle controversie bancarie, finanziarie e societarie - ADR (www.conciliatorebancario.it).
Qualora il Cliente intenda, per una controversia relativa all'interpretazione ed applicazione del contratto, rivolgersi all'autorità giudiziaria, deve preventivamente, pena l'improcedibilità della relativa domanda, avvalersi di uno dei procedimenti per la risoluzione stragiudiziale delle controversie (mediazione presso soggetto autorizzato, mediazione presso soggetto autorizzato e designato in contratto o citato procedimento presso l'Arbitro Bancario Finanziario-ABF); ciò ai sensi dell'art. 5 comma 1-bis del d.lgs. 28/2010. La procedura di mediazione si svolge davanti all'organismo territorialmente competente e con l'assistenza di un avvocato.

LEGENDA

Prelievo di contante	Operazione con la quale il cliente ritira contante dal proprio conto. La Carta di debito Raiffeisen consente il prelievo di contante, in presenza di fondi disponibili sul conto corrente, presso sportelli automatici (ATM - Automated Teller Machine e/o macchina self-service), sul circuito domestico.
Pagamento	La Carta di debito Raiffeisen consente l'acquisto di beni e Servizi, in presenza di fondi disponibili sul conto corrente, presso gli esercizi convenzionati, sul circuito domestico.
ATM (Automated Teller Machine)	Postazioni automatiche per l'utilizzo delle Carte nelle funzioni previste (p.e. prelievo di contante, versamento di contante, self service, ricariche).
POS	Postazioni automatiche (POS - Point of Sale) per l'utilizzo delle carte per l'acquisto di beni e Servizi.
Blocco della Carta di debito	Blocco dell'utilizzo della Carta per smarrimento o furto.
BANCOMAT® **PagoBANCOMAT®** **Maestro**	Marchi dei circuiti italiani ed esteri che offrono diversi servizi (pagamenti e prelievi) che il Cliente può utilizzare tramite la Carta di debito Raiffeisen. BANCOMAT®: pagamenti e prelievi di contante presso ATM in Italia. PagoBANCOMAT®: pagamenti senza contante presso postazioni automatiche POS in Italia. Maestro: pagamenti senza contante presso postazioni automatiche POS in Italia e all'estero.

Raiffeisen

Guida
Per un utilizzo sicuro della Carta di debito Raiffeisen in caso di pagamenti via internet

Il presente documento costituisce parte integrante del contratto relativo alla Carta di debito Raiffeisen

La Banca, nell'offrire i servizi che permettono di effettuare pagamenti via internet, adotta i migliori accorgimenti dell'attuale tecnologia.. Ciò nonostante permane la possibilità che il Cliente possa subire una frode informatica. Pertanto, oltre alle misure di sicurezza adottate dalla Banca, è necessario che il Cliente abbia delle conoscenze sufficienti per gestire in modo sicuro i pagamenti via internet.

I principali rischi della Carta di debito Raiffeisen consistono nell'abuso rispettivamente uso illecito della stessa da parte di terzi. Pertanto va osservata la massima attenzione nella custodia della Carta e della password; quest'ultima, in particolare, deve restare segreta. Nel caso di smarrimento o sottrazione della Carta o della password, il Cliente è tenuto a richiedere immediatamente il blocco della Carta, secondo le modalità contrattualmente previste (Numero Verde per il blocco della Carta).
Conseguenze negative risultano, inoltre, dalla revoca da parte della Banca dell'autorizzazione ad utilizzare la carta (blocco) nel caso di utilizzo fraudolento o non autorizzato della Carta da parte del Cliente.
Infine, il Cliente può essere vittima di un attacco informatico realizzato verso il dispositivo utilizzato dal Cliente stesso che provochi p.es. il furto delle credenziali, la cattura di schermate del PC, la modifica di pagine web per l'acquisizione fraudolenta della password ed il controllo remoto del computer.
Può, infatti, succedere che il Cliente riceva un messaggio di posta elettronica che imiti la grafica di un sito. Questa e-mail, che ha come unico scopo quello di ottenere i dati del Cliente con i quali autorizza i pagamenti, invita il destinatario a seguire un link, presente nel messaggio. Tale link però porta ad un sito fittizio, simile al sito ufficiale e situato sul server controllato da un altro soggetto. Tale tipo di truffa via internet, detta "phishing", può essere realizzata anche mediante l'invio di SMS.

Vi sono, inoltre, diverse forme di attacco che mirano a fare entrare un malware (c.d. Banking Trojan) nel computer. Ciò può avvenire attraverso le più svariate vie, come p.es. tramite una e-mail con allegati, un link contenuto in una e-mail diretto ad un sito web infettante ovvero semplicemente consultando dei siti web infetti (c.d. drive-by-download). Di solito il Banking Trojan viene installato definitivamente sul disco rigido del computer. Vi sono però anche altre varianti del malware che si trovano nella memoria operativa del computer e che, pertanto, non lasciano tracce rivelatrici sul disco rigido. Una volta che il malware è divenuto attivo sul PC, l'organizzazione criminale può ricorrere a diverse tecniche per raccogliere illecitamente dati, tra cui p.es. l'intercettazione dei campi di inserimento (p.es. della password o dei dati della carta di credito), la rappresentazione di siti web falsificati, il blocco dell'accesso al Servizio, la modifica degli abbinamenti tra il dominio e l'indirizzo IP, la disattivazione di antivirus installati, la modifica dei dati inseriti (p.es. nel corso di un bonifico) e addirittura l'accesso in remoto al computer.

Per tali motivi è necessario adottare tutte le misure precauzionali che permettono di evitare l'effettuazione di operazioni in un ambiente infetto ove vi sia il potenziale pericolo di presenza di malware. Si sconsiglia di compiere pagamenti via internet con un dispositivo non conosciuto (p.es. utilizzo di un PC in un internet café). Qualora l'ordine di pagamento avviene da un proprio dispositivo elettronico, prima di effettuare l'operazione online, bisogna verificare che il dispositivo abbia un sistema operativo aggiornato con tutte le patch di sicurezza, le ultime versioni di software utente (p.es. Acrobat Reader) e un antivirus costantemente aggiornato.

I requisiti citati costituiscono precauzioni e strumenti di minima, irrinunciabili per un'efficace difesa contro possibili attacchi informatici. Inoltre è importante che il Cliente fornisca la massima collaborazione alla propria Banca ed aiuti, soprattutto nel proprio interesse, a prevenire gli attacchi suddetti, **rispettando le seguenti regole di comportamento**.

In generale, occorre,
- dotarsi di un antivirus attivo e costantemente aggiornato e di appositi firewall;
- effettuare pagamenti via internet da postazioni proprie e periodicamente controllate;
- proteggere la propria postazione con una password di almeno 8 caratteri, non agevolmente riconducibili alla persona e sostituire la stessa almeno ogni 6 mesi;
- controllare regolarmente gli estratti conto e le operazioni eseguite tramite i servizi internet.

Con riguardo all'utilizzo del servizio, è necessario:
- custodire e utilizzare con la massima accuratezza la Carta di debito, la password e gli elementi di sicurezza;
- non conservare insieme la Carta di debito, la password e gli elementi di sicurezza;
- non cedere la Carta di debito, la password e gli elementi di sicurezza a terzi;
- denunciare tempestivamente il furto, lo smarrimento, la distruzione o un qualsiasi altro uso non autorizzato della Carta e/o della password;
- prestare massima attenzione ai diversi metodi di potenziale attacco informatico tra cui le cosiddette e-mail

civetta, le false comunicazioni di scadenza, l'invito a seguire un certo link;
- procedere agli acquisti solo in negozi virtuali affidabili e prestare attenzione al marchio di qualità (p.es. Trusted Shop) nonché alla presenza del colofone e delle condizioni generali di contratto e al loro contenuto;

Si raccomanda la verifica degli accessi e delle operazioni tramite il servizio SMS-Alert e/o e-mail-Alert.

Al momento del pagamento via internet è necessario:
- verificare costantemente la presenza dell'acronimo di protocollo "https" e il simbolo della chiavetta nella stringa operativa, che sono quelli di una pagina web protetta e che si distinguono dall'acronimo di protocollo "http";
- verificare che sul sito internet, tramite il quale viene effettuato il pagamento, siano presenti i loghi Verified by Visa e MasterCard® SecureCode™;
- verificare che il sito del venditore, sul quale Lei effettua acquisti/pagamenti, La identifica come proprietario della Carta, chiedendo la password personale (3D Secure);
- verificare che durante la procedura di pagamento appare la frase di riconoscimento e se essa corrisponde a quella da Lei generata al momento della registrazione (appare solo se il venditore supporta 3D Secure);
- evitare pagamenti su siti che non supportano il predetto sistema di sicurezza ovvero procedere con ulteriore attenzione e prudenza in caso di pagamento;
- informarsi circa le altre possibilità di impartire l'ordine (p.es. attraverso telefono o fax), se la pagine web non è protetta;
- astenersi dal pagamento o interrompere lo stesso e darne immediata comunicazione alla Banca - anche attraverso il numero verde pubblicato sul sito - se si notano irregolarità o malfunzionamenti del sistema;
- chiudere l'applicazione dopo aver effettuato il pagamento.

In caso di smarrimento o furto della Carta è necessario:
- richiedere immediatamente il blocco della Carta tramite il Numero Verde e fare denuncia all'Autorità Giudiziaria o di Polizia;
- fornire alla Banca copia della denuncia presentata all'Autorità Giudiziaria o di Polizia, affinché possa essere ordinata una carta sostitutiva.