

VADEMECUM PER I CLIENTI DI SOLUTION BANK

Frodi e operazioni non autorizzate: come difendersi e cosa fare

Premessa

In un mondo sempre più digitale, può accadere di notare sul proprio conto corrente o sulla carta di pagamento movimenti che **non si riconoscono**. Questo vademecum ha lo scopo di informarti sui comportamenti da adottare, le misure di sicurezza richieste, le modalità per segnalare anomalie e le tutele previste dalla normativa.

1. Misure di sicurezza da adottare

Per prevenire usi non autorizzati degli strumenti di pagamento, è importante:

- non comunicare mai a terzi PIN, OTP, password, dati della carta o credenziali di accesso;
- non cliccare su link sospetti ricevuti via SMS, e-mail o social network;
- accedere all'Home Banking solo da dispositivi sicuri e aggiornati;
- monitorare costantemente saldo e movimenti del conto;
- attivare le notifiche push/SMS per ogni operazione.

2. Cosa si intende per operazione non autorizzata?

Un'operazione non autorizzata è un pagamento eseguito **senza il tuo consenso**, ad esempio:

- un addebito su carta per un acquisto che non hai effettuato;
- un bonifico disposto dal tuo Home Banking che non hai mai autorizzato;
- un prelievo da ATM mai eseguito da te.

Attenzione: se non riconosci un'operazione, controlla le notifiche ricevute (app, SMS, e-mail) e l'estratto conto.

3. Cosa fare in caso di movimenti sospetti, uso indebito o smarrimento

Appena ti accorgi di un movimento sospetto:

a. Blocca la carta (se coinvolta)

- Direttamente dall'app Inbank o chiamando il numero verde del circuito (es. Nexi, Amex).

b. Contatta la Banca

- Recati in Filiale o invia una e-mail (disconoscimenti@solution.bank) con la richiesta e la documentazione allegata.

c. Compila i moduli

- **Modulo disconoscimento operazioni di pagamento** o specifico modulo **disconoscimento carta BCC** (se trattasi di questa casistica);
- **Questionario Frodi HB** (per operazioni via app o web banking);
- **Denuncia all'Autorità Giudiziaria** (Carabinieri, Polizia);

Esempio: hai ricevuto un SMS con un codice OTP che non hai richiesto, seguito da un bonifico di 950 € → segnala subito l'operazione.

4. Entro quanto tempo va fatta la richiesta?

Hai **13 mesi** di tempo dalla data dell'addebito per fare richiesta di disconoscimento.

Nel caso di **addebiti SDD (domiciliazioni bancarie)**:

- puoi chiedere il rimborso entro **8 settimane** se l'importo è anomalo o inatteso;
- la Banca risponderà entro 10 giorni lavorativi.

Ricorda: prima lo fai meglio è! Effettuare la richiesta il prima possibile agevola l'istruttoria e il blocco di ulteriori operazioni.

5. Cosa succede dopo la richiesta?

- La Banca prende in carico la tua richiesta **entro un giorno lavorativo**.
- Riceverai un'**e-mail o lettera di conferma** dell'avvio dell'istruttoria.
- In assenza di sospetti di frode, la Banca **ti rimborsa l'importo contestato**.
- In caso di dubbi o elementi sospetti (uso OTP, accessi da tuoi dispositivi), la richiesta può essere **sospesa o rifiutata**.

Esempio: la Banca scopre che l'operazione è stata eseguita con la tua password e il tuo smartphone → può respingere la richiesta.

6. E se il rimborso viene negato?

- Riceverai una comunicazione formale con le motivazioni.
- Potrai presentare un **reclamo scritto** alla Banca o un ricorso all'**Arbitro Bancario Finanziario (ABF)**.

Nota Bene:

- Successivamente al rimborso, se la Banca verifica che l'operazione era stata in realtà correttamente autorizzata dal cliente, la stessa ha diritto, procedendo autonomamente, in base alla normativa in vigore¹ sui servizi di pagamento, di chiedere direttamente e di ottenere da te la restituzione dell'importo rimborsato.
- Ferme le responsabilità collegate agli obblighi di custodia e di protezione dei tuoi strumenti di pagamento e delle tue credenziali personalizzate, non sopporterai alcuna perdita:
 - derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente, intervenuto dopo aver effettuato le dovute comunicazioni o disconoscimenti alla Banca;

¹ La normativa non prevede un esplicito limite temporale massimo per porre in essere questa azione. Sulla base delle migliori prassi di mercato la banca ha individuato quale soglia ragionevole il limite di 13 mesi dalla data operazione.

- derivante dall'utilizzo della Carta smarrita, sottratta o utilizzata indebitamente quando la Banca non ha assicurato la disponibilità degli strumenti per consentire la comunicazione di richiesta di blocco;
- se lo smarrimento, la sottrazione o l'appropriazione indebita dello strumento di pagamento non potevano essere da te notati prima di un pagamento, o se la perdita è stata causata da atti o omissioni di dipendenti, agenti o succursali della Banca o dell'Ente cui sono state esternalizzate le attività;
- se la Banca non esige l'autenticazione forte per l'autorizzazione all'operazione di pagamento.

7. Blocchi e limitazioni dello strumento

La Banca si riserva il diritto di bloccare lo strumento di pagamento nei seguenti casi:

- fondato sospetto di uso fraudolento;
- uso non conforme alle condizioni contrattuali;
- ordine dell'Autorità giudiziaria o di vigilanza;
- segnalazioni di smarrimento/sottrazione.

Il blocco verrà tempestivamente comunicato tramite canali sicuri (e-mail, telefono, posta).

8. Come proteggerti dalle frodi?

- **Non condividere mai OTP o codici di sicurezza**, nemmeno con chi si presenta come operatore della Banca.
- Diffida da:
 - SMS o e-mail con link sospetti (phishing);
 - chiamate da falsi operatori (vishing);
 - messaggi che ti chiedono urgenze o verifiche anomale (smishing).
- Usa solo canali ufficiali per accedere al tuo Home Banking.

Attenzione: in nessun caso la Banca richiede comunicazione di credenziali, codici OTP o password tramite telefono, SMS o e-mail.

9. Reclami e ricorsi

In caso di disaccordo con l'esito della pratica:

- è possibile presentare **reclamo scritto** alla Banca;
- oppure ricorso all'**Arbitro Bancario Finanziario (ABF)** entro i termini previsti.

Questo documento ha finalità informativa e sintetica. Per maggiori dettagli ti aspettiamo in Filiale.