BANCA PASSADORE & C.

Guida sui disconoscimenti di operazioni di pagamento non autorizzate

Giugno 2025

COSA SI INTENDE PER "DISCONOSCIMENTO DI UN'OPERAZIONE DI PAGAMENTO"?

Il "disconoscimento di un'operazione di pagamento" è **l'attività con cui un Cliente può comunicare alla Banca di non riconoscere un addebito o un accredito sul suo conto corrente o su una sua carta di pagamento** (carte di debito, credito, prepagate o carte con IBAN), in quanto operazione da lui stesso non preventivamente autorizzata o difforme rispetto alle istruzioni impartite.

📌 **Operazione di pagamento non autorizzata:** transazione eseguita senza il consenso del titolare intestatario del conto o della carta di pagamento.

📌 **Operazione non correttamente eseguita:** l'esecuzione della stessa non è conforme all'ordine o alle istruzioni impartite dal Cliente.

L'autorizzazione di un'operazione di pagamento mediante tecniche di "autenticazione forte[1]" del Cliente consente alla Banca di dimostrare che l'operazione è stata autenticata dal Cliente e, pertanto, di escludere il diritto del Cliente al rimborso.

Se il Cliente viene a conoscenza di un'operazione di pagamento non autorizzata o non correttamente eseguita e desidera ottenere il rimborso deve contattare la Banca o il soggetto *issuer* delle carte
non appena ne viene a conoscenza e senza indugio

[1] L'autenticazione forte, nota anche come *Strong Customer Authentication* (SCA), è una procedura di sicurezza che richiede l'utilizzo di almeno due elementi di autenticazione indipendenti per verificare l'identità di un utente.

COME EFFETTUARE LA RICHIESTA?

- 💳 **Operazioni effettuate con carte di pagamento**
  Se la transazione è avvenuta tramite carta di debito, carta di credito, carta prepagata senza IBAN o carta conto con IBAN (emessa a partire dal 24/02/2025), il Cliente deve inoltrare la richiesta direttamente al soggetto *issuer*.

- 🏦 **Tutti gli altri tipi di operazioni**
  Per operazioni diverse (es. operazioni tramite Internet *Banking*), il Cliente deve inoltrare la richiesta alla Banca utilizzando uno dei seguenti canali:
  - ✉️ contattando la propria filiale/agenzia[2]
  - 🏢 recandosi direttamente presso le dipendenze della Banca (sede, filiali e agenzie)
  - 📞 contattando il servizio *Help desk*, attivo tutti i giorni feriali, ai recapiti 800 893597 e 010 5393381

Il Cliente deve effettuare la comunicazione, in ogni caso, **entro e non oltre 13 (tredici) mesi dalla data nella quale l'operazione è stata addebitata[3]**, salvo che la Banca non abbia fornito le informazioni relative all'operazione, secondo quanto previsto dalle Disposizioni di Trasparenza di Banca d'Italia.

QUALE PUÒ ESSERE L'ESITO DELLA RICHIESTA?

L'esito delle verifiche condotte dalla Banca può essere positivo o negativo e il Cliente ne riceve comunicazione **entro 15 giorni lavorativi** dalla ricezione, da parte della Banca, della segnalazione del disconoscimento.

- **Esito positivo**: il rimborso avviene entro la fine della giornata lavorativa successiva alla richiesta, con accredito sul conto del Cliente dell'importo dell'operazione oggetto del disconoscimento.

[2] I recapiti telefonici delle filiali e delle agenzie sono riportati nell'apposita sezione del sito web della Banca.
[3] Nel caso di disconoscimento di operazioni di pagamento riguardanti addebiti diretti, il Cliente ha facoltà di richiedere il rimborso:
- fino a 8 settimane dopo la data di addebito, ancorché autorizzata (in caso di operazione contestata nell'ambito di un mandato valido);
- fino a 13 mesi dopo la data di addebito (in caso di mandato non valido o non esistente).

In particolare, se per l'esecuzione dell'operazione è stato addebitato il conto corrente o una carta di pagamento[4] del Cliente, **la Banca riporta il conto corrente o la carta di pagamento nello stato in cui si sarebbe trovato se l'operazione non avesse avuto luogo**. Il Cliente riceve una comunicazione di conferma del rimborso.

⚠️ Il rimborso non preclude la facoltà per la Banca di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata. In tal caso la Banca ha il diritto di addebitare al Cliente l'importo precedentemente rimborsato, inviando apposita comunicazione con le motivazioni dello storno.

- **Esito negativo**: in assenza di anomalie e/o in caso di dolo o colpa grave del Cliente per comportamenti, abitudini e/o azioni che, se non fossero state messe in atto, non avrebbero portato all'operazione non autorizzata, la Banca non procede con il rimborso. Il Cliente riceve una comunicazione con le motivazioni del rifiuto.

COSA SUCCEDE DOPO LA SEGNALAZIONE?

Il Cliente riceve riscontro da parte della Banca entro 15 giorni lavorativi dalla ricezione della segnalazione.

La Banca, nel corso dell'istruttoria, può richiedere al Cliente documenti e informazioni aggiuntivi.
L'istruttoria per disconoscimenti di operazioni non autorizzate potrà avere una durata massima di 120 giorni. Oltre tale termine, l'istruttoria si considera conclusa.

Nel caso in cui la Banca avesse il motivato sospetto che il Cliente abbia agito fraudolentemente, può sospendere le operazioni di rimborso descritte, dandone immediata comunicazione alla Banca d'Italia

[4] In caso di operazioni con carta di debito, carta di credito, carta prepagata senza IBAN o carta conto con IBAN (emessa a partire dal 24/02/2025) è il soggetto *issuer* a svolgere le verifiche necessarie e a disporre, per il tramite della Banca, il rimborso. In tal caso, il Cliente riceverà le comunicazioni direttamente dal soggetto *issuer.*

Nel dettaglio….
La Banca, salvo le eccezioni previste dalla legge, è tenuta a rimborsare al pagatore le operazioni di pagamento non autorizzate in quanto riconducibili a una delle seguenti categorie:

Operazioni effettuate senza il consenso del Cliente
Si tratta di tutte le operazioni di pagamento per le quali non sia possibile dimostrare che il consenso del cliente sia stato effettivamente prestato.

Operazioni eseguite con strumenti di pagamento smarriti, rubati o oggetto di appropriazione indebita
Se il cliente ha comunicato tempestivamente lo smarrimento o il furto dello strumento, l'operazione eventualmente eseguita dopo la comunicazione del cliente si considera non autorizzata.

Operazioni effettuate in violazione delle procedure di *Strong Customer Authentication* (SCA)
Qualora nei casi in cui tale tecnica di autenticazione è richiesta non siano rispettati i requisiti di autenticazione forte del cliente (es. quando difetti un secondo fattore di autenticazione), l'operazione può essere classificata come non autorizzata.

Operazioni fraudolente dovute a *phishing, smishing* o simili, se la Banca non dimostra l'inadempimento con dolo o colpa grave del cliente
Quando il Cliente è stato vittima di truffa, salvo che la Banca dimostri che il Cliente non ha adempiuto con dolo o colpa grave alle obbligazioni previste a suo carico.

Disconoscimenti motivati da malfunzionamenti degli strumenti messi a disposizione del Cliente
Include casi di bug, malfunzionamenti dei canali dispositivi o accessi non riconducibili al cliente.

Operazioni eseguite dopo la revoca dell'autorizzazione o la scadenza del mandato
Qualsiasi disposizione eseguita senza mandato valido al momento dell'operazione.

INFORMAZIONI UTILI

Furto/smarrimento dei dispositivi o delle Carte o in caso di pagamenti anomali
In caso di perdita o di sottrazione dei dispositivi personali o delle Carte, o in caso di abuso riscontrato o sospetto è importante agire tempestivamente. In questi casi, è necessario contattare immediatamente il Servizio Blocco Carta per bloccare immediatamente la Carta, le

credenziali di accesso all'Area Personale e verificare e, nel caso, contestare eventuali pagamenti non autorizzati.

I recapiti di riferimento dall'Italia sono[5]:

- **per le carte Nexi Banca Passadore, carte *PassadorePay* e nuove carte conto** (emessa a partire dal 24/02/2025): 800 151 616
- **per le carte conto:** 800 822 056
- **per le carte *American Express*:** 06 72900347

Pertanto, la Clientela è invitata a:

- **controllare spesso la lista dei movimenti** del conto e della carta per rilevare subito eventuali anomalie;
- **attivare i servizi di notifica** per ricevere un avviso ogni volta che viene effettuata un accesso o una transazione;
- consultare il vademecum ABI per agire in sicurezza dentro e fuori la filiale **"***Truffe, scippi e raggiri - Un vademecum ABI per agire in sicurezza dentro e fuori la filiale"* presente sul sito web della Banca alla sezione "Servizi *online*"/"Sicurezza".

Focus frodi digitali

Phishing

Il truffatore contatta l'utente tramite e-mail ingannevoli per indurre la vittima a fornire informazioni sensibili (credenziali, dati bancari, PIN, OTP).

- E-mail con urgenze o minacce (es. "il tuo conto sarà bloccato");
- Link a siti web falsi visivamente simili a quelli ufficiali;
- Allegati contenenti *malware*.

Smishing (SMS Phishing)

Variante del *phishing* veicolata tramite messaggi SMS che simulano comunicazioni ufficiali da parte della Banca.

- Inviti a cliccare su link per "verificare una transazione".

Vishing (Voice Phishing)

Il truffatore contatta telefonicamente l'utente fingendosi un operatore bancario per ottenere credenziali e/o convincere la vittima a compiere operazioni fraudolente.

- Falsi numeri identificativi;
- Richieste di OTP o accesso a *Internet banking.*

[5] I recapiti per le telefonate da paesi diversi dall'Italia sono consultabili direttamente sul sito web della Banca nella sezione "Assistenza Clienti".