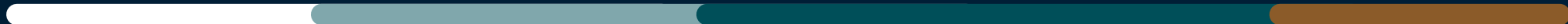


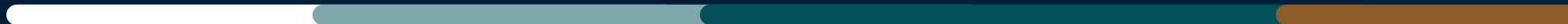
Banca Finint S.p.A.

GUIDA AI DISCONOSCIMENTI DELLE OPERAZIONI DI PAGAMENTO

Vers. 0.1 – Giugno 2025



Come mi devo comportare nel caso di un addebito avvenuto senza la mia autorizzazione e che voglio disconoscere?



Premessa

Capita a volte di trovare sul proprio estratto conto movimenti che non si riconoscono. Che si tratti di un acquisto mai effettuato, un abbonamento non richiesto o una transazione fraudolenta, è fondamentale sapere come **disconoscere un'operazione di pagamento** per tutelare i propri diritti e il proprio denaro. Questa guida è pensata per i clienti della nostra Banca e ti spiegherà passo dopo passo cosa fare.

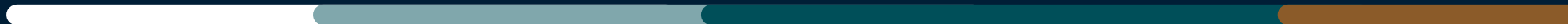
Disconoscere un'operazione di pagamento può sembrare complesso, ma seguendo questi passaggi e agendo prontamente, potrai tutelare i tuoi interessi. La nostra Banca è al tuo fianco per assisterti in ogni fase di questo processo.

Ricorda che quando utilizzi uno strumento di pagamento hai l'obbligo di:

1. utilizzarlo in conformità con quanto disposto dal contratto;
2. comunicare immediatamente alla Banca o a Nexi per le carte di pagamento lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento, secondo le modalità previste nel contratto o in questa Guida.

Non appena ricevi uno strumento di pagamento, devi adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate. Custodisci con cura la carta, il PIN e tutti i codici d'accesso ai servizi di pagamento. Solo tu li conosci: non comunicarli mai a terzi, non riportarli sulla carta e non conservarli insieme.

Ricorda che la Banca non ti chiederà mai password dispositive o di accesso ai servizi di “Multicanalità”, né il numero, il PIN o il codice di sicurezza a tre cifre riportato sul retro della stessa. Inoltre, non ti sarà mai chiesto di seguire istruzioni per risolvere una situazione "critica", bonificare un conto provvisorio, mettere in salvo somme di denaro o eseguire uno storno. Tutela la riservatezza dei dati bancari e personali e diffida da qualsiasi contatto telefonico che abbia queste caratteristiche.



Basi legali e normative: La PSD2 e i tuoi diritti

Il disconoscimento di un'operazione di pagamento è un diritto tutelato da specifiche normative, in particolare dalla **Direttiva Europea sui Servizi di Pagamento (PSD2 - Payment Services Directive 2)**, recepita in Italia con il Decreto Legislativo n. 218/2017. Questa direttiva rafforza la protezione dei consumatori nel settore dei pagamenti elettronici.

Queste disposizioni sottolineano l'importanza della tempestività nella segnalazione e la protezione offerta al correntista.

Cos'è il disconoscimento di un'operazione?

Il disconoscimento di un'operazione di pagamento è la procedura formale con cui un titolare di conto corrente o di carta di pagamento dichiara di non riconoscere una transazione addebitata sul proprio conto. Questo avvia un'indagine da parte della Banca per verificare la legittimità dell'operazione e, se fondato, portare al rimborso delle somme.

Nel caso di un'operazione di pagamento non autorizzata o non correttamente eseguita, hai il diritto di ottenerne il rimborso o la rettifica solo se comunichi senza indugio tale circostanza al Prestatore di Servizi di Pagamento (PSP) ossia, nei rispettivi casi, alla Banca o a Nexi per le carte di pagamento.

Approfondimento sulle tipologie di disconoscimento

1. Operazioni non autorizzate (Frodi):

- **Furto/Clonazione carta:** Addebiti derivanti dall'uso illecito di una carta fisica o dei suoi dati dopo furto o clonazione. In questo caso, è fondamentale il **blocco immediato della carta** e la **denuncia alle Forze dell'Ordine**.
- **Phishing/Smishing/Vishing:** Addebiti conseguenti alla divulgazione involontaria delle proprie credenziali (PIN, OTP, password) a malintenzionati tramite email (phishing), SMS (smishing) o telefonate (vishing) fraudolente. La denuncia è cruciale per dimostrare la frode.
- **Acquisti online fraudolenti:** Transazioni su siti web non sicuri o fasulli che hanno carpito i tuoi dati.

2. Operazioni non corrette (Errori o disaccordi contrattuali):

- **Doppio addebito:** Accade che la stessa transazione venga processata due volte per errore tecnico del POS o del sistema del commerciante.
- **Importo errato:** L'addebito non corrisponde a quanto pattuito o visualizzato al momento dell'acquisto (es. prezzo esposto era X, addebitato Y).
- **Mancata o parziale fornitura del bene/servizio:** Hai pagato ma non hai ricevuto nulla, oppure quanto ricevuto è palesemente non conforme a quanto ordinato.
- **Abbonamenti/Servizi a rinnovo automatico non desiderati:** Abbonamenti attivati in modo non chiaro, difficili da disdire o che si sono rinnovati nonostante la tua disdetta.
- **Mancato storno:** Hai effettuato un reso o una cancellazione di un servizio, e il venditore ti ha confermato il rimborso, ma questo non è mai arrivato sul tuo conto.

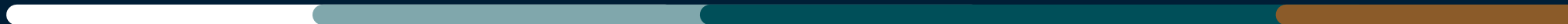
In caso di **errori o disaccordi contrattuali**, prima di rivolgerti alla Banca, è spesso consigliabile **tentare di risolvere la questione direttamente con il commerciante o il fornitore**. Conserva tutta la corrispondenza (email, messaggi, chat) relativa a questi tentativi. Se la risoluzione diretta non va a buon fine, allora procedi con il disconoscimento bancario.

ATTENZIONE: la Banca è estranea ai rapporti che intercorrono tra te e l'esercente.

Passi da seguire per disconoscere un'operazione

È importante agire tempestivamente quando noti un'operazione sospetta.

Di seguito i **4 step** da seguire



1. Verifica l'operazione

Prima di procedere, assicurati che l'operazione non sia legittima. Controlla i tuoi acquisti recenti, gli abbonamenti attivi e verifica con i membri della tua famiglia. A volte, un nome diverso del beneficiario sull'estratto conto può generare confusione.

Venuto a conoscenza di una “operazione di pagamento non autorizzata” o “non correttamente eseguita”, devi inviare una comunicazione alla Banca senza indugio e comunque entro 13 mesi dalla data di addebito o di accredito dell'operazione; il termine di 13 mesi non si applica qualora la Banca non abbia fornito le informazioni relative all'operazione, secondo quanto previsto dalle Disposizioni di Trasparenza.

Nel caso di operazioni di pagamento preventivamente autorizzate e disposte su iniziativa del beneficiario o per il suo tramite (es: Sepa Direct Debit o domiciliazioni su conto) e già eseguite, puoi richiederne il rimborso dell'addebito se:

- l'autorizzazione all'addebito da te rilasciata non specificava l'importo dell'operazione, e
- l'importo della operazione supera l'importo che avresti potuto ragionevolmente aspettarti, prendendo in considerazione ogni tua precedente spesa, le condizioni del tuo contratto e altre circostanze specifiche e concrete. In questo caso, devi effettuare la richiesta di rimborso entro 8 settimane dall'addebito, fornendo su richiesta della Banca documenti e ogni altro elemento utile a supporto della sussistenza delle circostanze che giustificano il rimborso. Entro 10 giornate lavorative dalla ricezione della richiesta la Banca provvede al rimborso oppure può declinare la richiesta, fornendoti la relativa motivazione. Il diritto al rimborso è precluso se hai dato l'autorizzazione di pagamento direttamente alla Banca e le informazioni sulla futura operazione di pagamento sono state fornite da te stesso o messe a tua disposizione da parte della Banca o del beneficiario, almeno 4 settimane prima dell'esecuzione di pagamento stessa.

2. Blocca la carta, l'internet banking o l'app

In caso di transazioni fraudolente la tempestività è fondamentale.

- **Blocca la carta:** se ti accorgi di un'operazione avvenuta con una carta che ti è stata rubata o hai smarrito, oppure se hai subito un furto di dati della carta
- **Blocca l'internet banking o l'app:** se ti accorgi di non aver autorizzato tu un'operazione come ad esempio un bonifico

In caso di furto, smarrimento o contraffazione, puoi bloccare lo strumento di pagamento attraverso i seguenti canali:

Conti Correnti / Online Banking – contatta la Banca per segnalare la possibilità di una frode al numero **+39 0438 360 350** (lun-ven 8.30-13.00 | 14.00–15.30) o al numero **800 080 640** (lun-ven 9.30-12.30 | 14.30-16.30)

Carte di Pagamento: contatta immediatamente Nexi ai seguenti numeri dedicati al blocco delle carte e al disconoscimento delle operazioni non autorizzate (servizio attivo 24 ore su 24 e 365 giorni l'anno):

- dall'Italia 800 15 16 16
- dall'estero:
 - +39 02 3498 00201 (si accettano chiamate a carico Nexi)
 - Dagli USA: 1 800 473 68962

3. Raccogli le prove

Prepara tutta la documentazione utile a supportare la tua richiesta:

- **Estratto conto** dove compare l'operazione da disconoscere.
- **Ricevute, fatture o email di conferma** relative all'acquisto (se ne hai).
- **Comunicazioni** con il commerciante o il fornitore del servizio (se hai già tentato di risolvere la questione direttamente).
- **Denuncia alle Forze dell'Ordine** (Polizia Postale o Carabinieri): in caso di furto, frode o utilizzo non autorizzato della tua carta/dati bancari, la denuncia è un passo fondamentale e spesso richiesto dalla Banca.

3. Raccogli le prove

La qualità delle prove che fornisci può fare la differenza nell'esito della tua pratica sia essa gestita.

- **Denuncia alle Forze dell'Ordine:** Per le frodi (furto, clonazione, truffe online, phishing), la denuncia è quasi sempre un requisito fondamentale. Rivolgiti alla Polizia Postale (per reati informatici) o ai Carabinieri. Assicurati che la denuncia contenga tutti i dettagli rilevanti: data e ora dell'operazione, importo, beneficiario (se conosciuto) e le circostanze in cui è avvenuta la frode.
- **Estratto conto/Lista movimenti:** Evidenzia chiaramente l'operazione contestata. Ti aiuteremo a reperire i dettagli se non li hai a portata di mano.
- **Comunicazioni con il commerciante:** Se hai tentato di risolvere direttamente, allega screenshot di chat, email scambiate, conferme d'ordine, tracking di spedizioni (se non consegnate). Questo dimostra che hai esaurito le altre vie.
- **Altre prove:** Qualsiasi elemento che possa corroborare la tua versione dei fatti. Ad esempio, se hai un abbonamento non riconosciuto, potresti allegare screenshot che mostrano l'assenza di un account attivo o la mancata corrispondenza tra il servizio offerto e quanto ti viene addebitato.

Attenzione: Queste prove potrebbero essere richieste anche da Nexi per i disconoscimenti relativi alle transazioni su carta di pagamento.

4. Disconoscimenti per tipo di transazione

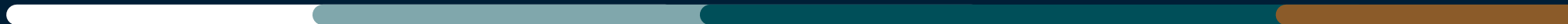
Per comunicare il disconoscimento di una operazione non autorizzata utilizzando i canali messi a disposizione dalla Banca a tale scopo:

Per operazioni con le carte di pagamento: il disconoscimento di operazioni effettuate tramite carte di pagamento (debito, credito e prepagato) avviene contattando immediatamente Nexi ai seguenti numeri dedicati al blocco delle carte e al disconoscimento delle operazioni non autorizzate (servizio attivo 24 ore su 24 e 365 giorni l'anno):

- dall'Italia 800 15 16 16
- dall'estero
 - +39 02 3498 00201 (si accettano chiamate a carico Nexi)
 - Dagli USA: 1 800 473 68962

Per operazioni sui conti correnti: Il disconoscimento di operazioni disposte su conti correnti (incluso il servizio di Corporate Banking Interbancario Passivo) avviene con l'invio del modulo "Disconoscimento operazioni di pagamento" inviato senza indugio all'attenzione della Banca al seguente indirizzo email: disconoscimenti@bancafinint.com.

Il processo di gestione della pratica in Banca



Il processo di gestione della pratica in Banca

Una volta che hai presentato il modulo di disconoscimento e la documentazione necessaria:

1. Presa in carico: La Banca prenderà in carico la tua richiesta e aprirà una pratica. La Banca si impegna ad effettuare il rimborso e/o la rettifica dell'operazione di sconosciuta immediatamente o al più tardi entro la fine della giornata operativa successiva alla contestazione ricevuta. In particolare, 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, assicurando che la data valuta dell'operazione di rettifica non sia successiva a quella dell'operazione contestata.

2. Verifica interna (Istruttoria): La Banca esaminerà i dati della transazione e le prove fornite. La Banca potrà richiederti documenti e informazioni aggiuntive, ma non subordinerà la presa in carico della pratica alla richiesta dei dati integrativi e garantirà la gestione dell'eventuale rimborso nei tempi previsti dalla normativa vigente. Se la Banca ritiene che l'operazione di pagamento contestata sia stata correttamente autorizzata, su richiesta ti fornirà la prova della corretta autorizzazione dell'operazione di pagamento contestata. Nel caso in cui la Banca abbia il motivato sospetto che tu abbia agito fraudolentemente, può sospendere le operazioni di rimborso descritte, dandone immediata comunicazione alla Banca d'Italia.*

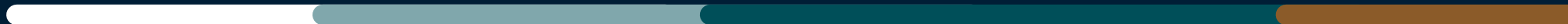
*ATTENZIONE: un'eccezione all'obbligo di rimborso opera nel caso di motivato sospetto che l'operazione non autorizzata derivi da un comportamento fraudolento posto in essere dal Cliente; in tal caso - come indicato dalla direttiva 2015/2366/UE - PSD2 (art. 11, comma 2, del D. Lgs. n. 11/2010 e successive modifiche) - la Banca provvederà a effettuare l'opportuna segnalazione alla Banca d'Italia.

Il processo di gestione della pratica in Banca

3. Riaccredito provvisorio: Il rimborso delle operazioni disconosciute e da intendersi salvo buon fine (SBF); tale condizione implica che la disponibilità delle somme accreditate non sia definitiva, in quanto soggetta alla positiva conclusione dell'eventuale attività istruttoria della Banca. Il PSP, infatti, anche in un momento successivo al rimborso, può dimostrare che, in realtà, l'operazione di pagamento era stata correttamente autorizzata oppure è conseguente ad una tua azione colposa o dolosa; in tal caso, ha diritto di richiedere ed ottenere la restituzione dell'importo rimborsato. La Banca addebiterà quindi autonomamente il tuo conto corrente, stornando il precedente accredito anticipato.

4. Comunicazione dell'esito: La Banca ti informerà sull'esito della tua richiesta, sia che si tratti di un rimborso (totale o parziale) sia di un rifiuto, spiegandoti le motivazioni. L'istruttoria per disconoscimenti potrà avere una durata massima di 120 giorni. Oltre tale termine, l'istruttoria si considera conclusa.

Responsabilità del cliente



Responsabilità del cliente

La normativa esonera la Banca dal rimborso se il cliente ha agito con "negligenza grave" o dolo. Ma cosa si intende per negligenza grave? Non esiste una definizione tassativa, ma la giurisprudenza ha individuato alcuni comportamenti che rientrano in questa categoria:

- Annotare il PIN sulla carta o in un luogo facilmente accessibile in caso di furto della carta stessa.
- Comunicare il PIN o altri dati sensibili (es. codici OTP) a terzi, anche se si spacciano per operatori bancari o di forze dell'ordine.
- Non segnalare tempestivamente il furto o lo smarrimento dello strumento di pagamento.
- Utilizzare software pirata o navigare su siti non sicuri senza protezioni, esponendosi a rischi noti di frode informatica.

È importante agire con la diligenza del "buon padre di famiglia" nella custodia dei propri strumenti di pagamento e delle proprie credenziali.

Ricorsi e Strumenti di Tutela: ABF

Se la Banca rifiuta il disconoscimento o non sei soddisfatto della gestione della tua pratica, oltre al reclamo interno, hai la possibilità di interpellare l'Arbitro Bancario Finanziario (ABF).

L'ABF è un organismo indipendente e imparziale che decide in tempi brevi (solitamente entro 90 giorni) e senza formalità complesse le controversie tra clienti e intermediari bancari e finanziari.

Il ricorso è relativamente economico e non richiede l'assistenza legale (anche se è consigliata per casi complessi).

Le decisioni dell'ABF non sono vincolanti in senso stretto, ma le banche tendono a rispettarle per non incorrere in sanzioni o pregiudizi reputazionali.

Prevenzione è la migliore difesa

Per ridurre il rischio di dover disconoscere operazioni:

- **Controlla regolarmente i movimenti** del tuo conto e delle tue carte, anche tramite app mobile banking.
- **Attiva i servizi di notifica SMS/email** per ogni operazione effettuata con la tua carta o sul tuo conto.
- **Proteggi i tuoi dati:** Non comunicare mai PIN, codici OTP o password a nessuno. La Banca non ti chiederà mai questi dati via email, SMS o telefono.
- **Sii cauto con le email e i messaggi sospetti:** Non cliccare su link di dubbia provenienza e non scaricare allegati da mittenti sconosciuti.
- **Utilizza siti web sicuri (HTTPS)** per gli acquisti online e verifica sempre l'affidabilità del venditore.
- **Aggiorna antivirus e sistemi operativi** sui tuoi dispositivi.
- **Conserva le ricevute** degli acquisti.

Comprendere a fondo questi aspetti ti permetterà di agire con maggiore sicurezza e consapevolezza qualora ti trovassi di fronte a un'operazione di pagamento da disconoscere. La nostra Banca è sempre a tua disposizione per supportarti e fornirti la consulenza necessaria.



“

La Prevenzione è la migliore difesa