Banca del Piemonte

DISCONOSCERE LE OPERAZIONI NON AUTORIZZATE

Cosa sono le operazioni non autorizzate

Un'operazione di pagamento si intende "**non autorizzata**" quando viene effettuata senza il consenso del titolare.

Ad esempio, se qualcuno effettua un pagamento utilizzando la carta di un altro soggetto senza la sua approvazione, quella transazione è considerata "non autorizzata".

Si definisce, invece, non correttamente eseguita quando l'esecuzione non è conforme all'ordine o alle istruzioni impartite (ad esempio quando l'importo dell'operazione non è corretto).

È importante difendersi dalle frodi e poterle riconoscere in tempo. Per ogni informazione al riguardo è possibile consultare la sezione "Sicurezza" presente sul sito della Banca all'indirizzo www.bancadelpiemonte.it.

Cos'è il disconoscimento

È l'azione che permette al titolare di un conto corrente, di una carta di pagamento (es. carta di credito, carta di debito, carta prepagata) o di un servizio internet di richiedere il rimborso e/o la rettifica di una operazione che non ha autorizzato.
Esistono strumenti o tecniche che permettono di individuare più agevolmente un'operazione non autorizzata quali:

- ✓ Attivare le notifiche sullo smartphone tramite l'app Nexi;
- ✓ Verificare i movimenti o consultare l'estratto conto all'interno dell'app o del sito web della Banca/Nexi;
- ✓ Attivare ove possibile il Servizio tramite SMS.

In caso di furto, smarrimento o pagamenti non autorizzati, è possibile bloccare rapidamente lo strumento di pagamento contattando i numeri specifici riportati sul sito della Banca nella sezione "Sicurezza" oppure rivolgersi alla filiale/gestore di riferimento. Nel caso di carte Nexi il Cliente dovrà rivolgersi direttamente a Nexi consultando sul sito www.nexi.it la sezione sicurezza.

È importante custodire con cura la carta, il PIN e i codici d'accesso ai servizi accessori, e non condividerli con altri. Nessuna Banca chiederà mai al titolare di condividere o confermare notifiche o codici per autorizzare pagamenti.

Si ricorda al tal fine che, fatte salve le responsabilità collegate agli obblighi di custodia e di protezione degli strumenti di pagamento e delle credenziali personalizzate, il Cliente non sopporterà alcuna perdita nei casi di:

- utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente, intervenuto dopo aver effettuato le dovute comunicazioni o disconoscimenti alla Banca;
- 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;

- smarrimento, sottrazione o appropriazione indebita dello strumento di pagamento che non potevano essere 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;
- mancanza dell'autenticazione forte per l'autorizzazione all'operazione di pagamento (vedasi definizione di autenticazione forte sotto riportata).

Qualora il Cliente abbia agito in modo fraudolento, ovvero non abbia adempiuto ad uno o più obblighi contrattualmente previsti per l'utilizzo di uno Strumento di Pagamento e per la Comunicazione di furto, smarrimento e appropriazione indebita come sopra riportati o abbia agito con dolo o colpa grave, lo stesso sopporta tutte le perdite derivanti da Operazioni di Pagamento non autorizzate e non si applica il limite di euro 50,00 (franchigia).

Alla sezione "Sicurezza" del sito della Banca è possibile trovare tutte le informazioni relative ai potenziali rischi di truffe, raggiri per sottrarre denaro o dati personali, nonché le relative modalità per riconoscerli, oltre agli strumenti per proteggersi da questi.

Cos'è un'operazione fraudolenta

Una transazione fraudolenta è un'azione illegale o non autorizzata che coinvolge l'utilizzo di strumenti di pagamento o sistemi finanziari, in genere con l'obiettivo di ottenere denaro, beni o servizi senza il consenso o l'autorizzazione dell'intestatario del conto o del titolare dello strumento di pagamento/servizio internet.
Si parla di operazione fraudolenta, ad esempio, nei casi di utilizzo fraudolento di carte di credito, bonifici non autorizzati, furto di identità online.

Tempi per comunicare il disconoscimento

Qualora il Cliente disconosca un'operazione di pagamento non autorizzata, quindi eseguita senza il suo consenso, deve comunicarlo alla Banca non appena venutone a conoscenza, e, in ogni caso, **entro il termine di 13 mesi decorrenti dalla data di addebito o accredito**. In mancanza di tale comunicazione il Cliente non ha diritto di ottenere il rimborso di un'operazione non autorizzata.
Il Cliente può effettuare tale comunicazione anche oltre il termine di 13 mesi, nel caso in cui la Banca non gli abbia messo a disposizione le informazioni relative all'Operazione di Pagamento contestata.

Modalità di comunicazione del disconoscimento

La comunicazione alla Banca deve essere effettuata compilando l'apposito modulo reperibile sul sito della Banca all'indirizzo www.bancadelpiemonte.it - Sezione Sicurezza o presso la propria filiale/gestore di riferimento ed inviando tale modulo all'indirizzo disconoscimenti@bancadelpiemonte.it. È possibile anche inviare alla Banca il modulo di disconoscimento tramite raccomandata o con consegna a mani presso la filiale/gestore di riferimento. Nel modulo dovranno essere riportate le informazioni delle operazioni oggetto di disconoscimento, i dettagli dell'evento e occorrerà rispondere ad alcune domande necessarie alla Banca per effettuare la propria istruttoria.

Modalità e tempistiche di rimborso dell'operazione disconosciuta

L'operazione disconosciuta dal Cliente viene rettificata, o rimborsata dalla Banca immediatamente o al massimo, entro la fine della giornata operativa successiva a quella in cui la Banca viene a conoscenza dell'operazione non autorizzata, mediante ricezione della comunicazione da parte del Cliente.

La procedura di rimborso può essere sospesa dalla Banca nel caso di motivato sospetto di frode; in tal caso, la Banca darà tempestiva comunicazione al Cliente interessato.
Successivamente al rimborso, se la Banca verifica che l'operazione era stata in realtà correttamente autorizzata dal Cliente, ha diritto in base alla normativa in vigore sui servizi di pagamento, di chiedere direttamente al Cliente ed ottenere da quest'ultimo i fondi originariamente trasferiti al Cliente, ripristinando la situazione come se il rimborso non avesse avuto luogo. Il Cliente dovrà, pertanto, mettere a disposizione i fondi originariamente trasferiti dalla Banca al Cliente, per il rimborso dell'operazione stessa. Il riaddebito dell'operazione di pagamento avverrà entro 45 (quarantacinque) giorni successivi all'accredito dell'operazione al fine di completare le proprie verifiche e approfondimenti.

Valute e costi applicati alle operazioni di disconoscimento

L'importo dell'operazione di pagamento non autorizzata viene riaccreditata sul conto del Cliente assicurando che la data valuta dell'accredito non **sia successiva a quella dell'addebito dell'importo, senza spese, oneri o interessi aggiuntivi a carico del Cliente**.

Pertanto, la Banca riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo.
La stessa valuta viene applicata al Cliente nel caso di diniego riportando il conto nello stato in cui l'operazione fosse stata effettivamente autorizzata dal Cliente.

Motivo del diniego

Il Cliente non ha diritto di ottenere dalla Banca il rimborso dell'operazione nel caso in cui:

- abbia agito fraudolentemente;
- non abbia adempiuto, con dolo o colpa grave, agli obblighi previsti contrattualmente;
- non abbia adottato le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate;
- in caso di furto, smarrimento, appropriazione indebita o uso non autorizzato di uno Strumento di Pagamento il Cliente non abbia notificato tali eventi non appena ne sia venuto a conoscenza.

È onere della Banca e/o, se del caso, del Prestatore di Servizi di disposizione di Ordine di Pagamento fornire la prova della frode, del dolo o della colpa grave del Cliente.
Il Cliente, in questi casi, sopporta tutte le perdite derivanti da Operazioni di Pagamento non autorizzate (ivi compreso il caso di furto, smarrimento e/o appropriazione indebita) e non ha diritto di ottenere dalla Banca e se del caso dal Prestatore di Servizi di disposizione di Ordini di Pagamento la rettifica e l'eventuale rimborso dell'importo di Operazioni di Pagamento.

Che cos'è l'autenticazione forte (SCA – Strong Customer Authentication)

L'autenticazione forte del Cliente è una procedura per convalidare l'identificazione di un utente basata sull'uso di due o più elementi di autenticazione (cd. "autenticazione a due fattori"), appartenenti ad almeno due categorie tra le seguenti:

- **conoscenza** (qualcosa che solo l'utente conosce, come una password o un PIN);
- **possesso** (qualcosa che solo l'utente possiede, come un token/chiavetta, o uno smartphone);
- **inerenza** (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale).

Questi elementi (o credenziali di autenticazione) devono essere indipendenti tra loro, in modo che un'eventuale violazione di uno di essi non comprometta l'affidabilità degli altri. La procedura di autenticazione del Cliente tramite SCA è necessaria per l'autorizzazione di un pagamento on line.

Diritti del Cliente

- laddove non risultino comportamenti fraudolenti del Cliente, andrà garantito a quest'ultimo il diritto al rimborso nei casi in cui la Banca non richieda un'autenticazione forte (strong customer authentication - SCA) ovvero non riesca a dimostrare che l'operazione è stata autorizzata con SCA;
- il Cliente ha diritto di far valere la responsabilità della Banca, anche oltre il termine di 13 mesi, se la Banca non ha messo a disposizione del Cliente le informazioni relative all'Operazione di Pagamento contestata;
- il Cliente non sopporta alcuna perdita se lo smarrimento, la sottrazione o l'appropriazione indebita dello Strumento di Pagamento non potevano essere notati dallo stesso prima di un pagamento, salvo il caso in cui abbia agito in modo fraudolento 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;

negli altri casi, salvo che abbia agito in modo fraudolento o che non abbia adempiuto a uno o più degli obblighi contrattuali previsti per utilizzo di uno Strumento di Pagamento, per la Comunicazione di furto, smarrimento e appropriazione indebita o che abbia agito con dolo o colpa grave, il Cliente può sopportare la perdita, per un importo comunque non superiore a euro 50,00 (franchigia).

Doveri del Cliente

- adempiere agli obblighi contrattualmente pattuiti con la Banca in termini di utilizzo degli strumenti di pagamento e di comunicazione di furto, smarrimento e appropriazione indebita;
- adottare le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate come il PIN della carta e non condividere queste informazioni con terzi non autorizzati;
- il titolare deve fornire informazioni corrette ed accurate in fase di registrazione e per le operazioni di pagamento;
- il titolare dovrebbe monitorare regolarmente le operazioni effettuate con lo strumento di pagamento per identificare eventuali operazioni sospette o non autorizzate;
- in caso di errori nell'esecuzione di operazioni di pagamento, il titolare deve comunicare immediatamente all'intermediario l'errore per permetterne la rettifica.

il Cliente ha l'obbligo di restituire alla Banca qualsiasi importo rimborsato in relazione all'Operazione di Pagamento contestata nel caso in cui la Banca stessa possa provare, anche in un momento successivo - che l'Operazione di Pagamento contestata era stata debitamente autorizzata dal Cliente. In tal caso la Banca avrà diritto di chiedere direttamente al Cliente ed ottenere da quest'ultimo i fondi originariamente trasferiti allo stesso, ripristinando la situazione come se il rimborso non avesse avuto luogo entro un termine massimo di 45 giorni.

Canali di contatto e assistenza

Per ogni informazione o assistenza è possibile contattare il proprio Gestore/Filiale di riferimento o consultare nell'area Sicurezza il "Numeri Utili" dove è possibile trovare, in base al tipo di strumento, il numero più idoneo da contattare, ad esempio:

- **Servizio Clienti:** il Cliente può contattare il servizio clienti al numero 011.2345679 o via mail (servizioclienti@bancadelpiemonte.it) attivo dal lunedì al giovedì 8:30 – 13:40, 14:40 - 16:55, venerdì 8:30-13:40, 14:40-16,20 - prefestivi 8:30-13:25;
- **Assistenza internet banking:** Il Cliente può contattare il contact center C-Global al numero verde di assistenza 800998050 attivo dal lunedì al venerdì 8:00-22:00, sabato 8:00-14:00, festività Borsa 9:00-18:00. Dall'estero: + 39 0131.1923198.
- **Contatto con il Punto Operativo:** il Cliente può contattare il P.O. secondo i consueti canali.
- **Sito Banca:** il Cliente accedendo al sito della Banca, invia in autonomia la segnalazione al Gruppo Disconoscimenti (disconoscimenti@bancadelpiemonte.it) unitamente alla documentazione in suo possesso.

Nel caso in cui l'operazione disconosciuta sia relativa ad una carta Nexi, il Cliente dovrà contattare direttamente l'assistenza Nexi per segnalare l'operazione non autorizzata. Per ulteriori informazioni si rimanda al sito www.nexi.it.

La Banca effettua una **costante campagna di comunicazione** sul sito (pagina dedicata alla sicurezza), sui social e tramite newsletter, **con l'obiettivo di mantenere elevata l'attenzione da parte della clientela sui tentativi di frode**. Vengono inoltre costantemente pubblicati messaggi di notifica nell'area riservata dell'internet banking per allertare, aggiornare e sensibilizzare il Cliente sul tema.