

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPAGNOL	Membro di designazione rappresentativa degli intermediari
(TO) COCCIA	Membro di designazione rappresentativa dei clienti

Relatore ALESSANDRA SPAGNOL

Seduta del 08/04/2026

FATTO

Dopo aver proposto reclamo in data 2.12.2025 (riscontrato negativamente in pari data dall'intermediario) la parte ricorrente proponeva ricorso all'ABF affermando che:

- in data 11/11/2025, accedendo all'home banking, riscontrava un pagamento POS non autorizzato di € 324,92, eseguito l'11/11/2025 alle ore 10:06, tramite carta di debito collegata al suo conto corrente;
- provvedeva immediatamente a contattare l'assistenza clienti al fine di bloccare il pagamento e il bancomat;
- disconosceva subito l'operazione;
- l'Intermediario, in un primo momento, stornava l'operazione riaccreditando la somma sul suo conto;
- con comunicazione del 02/12/2025, la banca revocava tuttavia la propria posizione, eccependo il regolare funzionamento delle infrastrutture tecnologiche e

contestandole una presunta negligenza nella conservazione dei codici di sicurezza.

Parte ricorrente, concludeva, quindi, chiedendo il rimborso dell'importo di € 324,92. Di contro, l'intermediario, nelle controdeduzioni, ha rappresentato: (i) che l'operazione oggetto di contestazione è stata disposta mediante la carta di pagamento n. *832, intestata alla ricorrente, attraverso il device usualmente utilizzato per l'operatività on line; (ii) che, per questo, deve qualificarsi come operazione autorizzata ai sensi dell'art. 5, commi 1 e 2, d.lgs. 11/2010; (iii) che l'avvenuta autorizzazione esclude il rimborso delle operazioni autorizzate, a prescindere da eventuali coartazioni della volontà del pagatore avvenute a monte del processo autorizzativo; (iv) che l'operazione è stata realizzata in modalità commercio elettronico sicuro, in completa assenza di anomalie; (v) che la cliente non ha effettuato alcun login alla propria utenza di Internet banking poiché, tramite l'app della banca, ha ricevuto solamente la notifica push contenente la descrizione del pagamento, che ha validato mediante l'inserimento del PIN; (vi) che la cliente non ha mai denunciato né lo smarrimento, né il furto della carta di pagamento (e del suo device/cellulare) tramite cui è stata effettuata l'operazione disconosciuta; (vii) che la ricorrente non ha fornito minimi elementi utili alla ricostruzione della vicenda, limitandosi a disconoscere genericamente l'operazione, e non indica quali siano i fatti che rendano plausibile la sussistenza dei presupposti per la responsabilità dell'intermediario; (viii) che la ricorrente ha agito in modo negligente, rendendo possibile l'esecuzione dell'operazione disconosciuta; (ix) che se la cliente avesse prestato la dovuta attenzione alla notifica push inviata sul suo device/cellulare certificato - che risulta regolarmente consegnata - avrebbe potuto evitare l'autorizzazione dell'operazione contestata. L'intermediario, di conseguenza, ha chiesto il rigetto del ricorso.

DIRITTO

L'utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. Secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento, essendo "ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi" (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare: A. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. In particolare, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente; B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni). Nel caso in esame, va evidenziato anzi tutto che l'intermediario ha eccepito che il ricorrente avrebbe eseguito personalmente le operazioni disconosciute, con conseguente inapplicabilità del regime di protezione previsto dal D.lgs. 11/2010.

L'eccezione non coglie nel segno in quanto, secondo l'orientamento condiviso dei Collegi, l'operazione può essere considerata autorizzata solo quando, diversamente dal caso in esame, la stessa è interamente eseguita dal pagatore.

L'operazione contestata consiste in n. 1 transazione e-commerce, eseguita in data 11/11/2025 alle ore 10:06, con la carta n.*832, dell'importo di € 324,92. L'intermediario ha riferito che l'operazione contestata è stata autenticata senza che parte ricorrente effettuasse alcun login alla propria utenza di Internet banking. Infatti, la cliente - tramite l'APP della banca - ha ricevuto solamente la notifica PUSH contenente la descrizione del pagamento, che ha confermato mediante l'inserimento del codice PIN. Ha inoltre precisato che l'operazione è stata disposta con il device usualmente utilizzato dalla ricorrente per l'operatività on line, avente chiave C***055. Dei sovrariportati assunti l'Intermediario ha prodotto prove documentali in linea con quanto richiesto dalla normativa e dall'orientamento compatto dei vari Collegi (elemento di conoscenza: codice PIN ed elemento di possesso: notifica PUSH inviata sul device della ricorrente) (cfr. Collegio di Palermo, decisione n. 6497/2025 "Con riferimento all'autorizzazione e all'esecuzione della transazione con SCA l'intermediario evidenzia che l'operazione in esame è stata autorizzata mediante invio della notifica push sul device registrato del ricorrente (bb029d51971eaf20) (fattore di possesso) e inserimento del PIN (fattore di conoscenza) fornendo i login dell'invio push e dell'inserimento pin. Il Collegio rappresenta che le evidenze prodotte sono ritenute idonee a dimostrare la SCA").

Si evidenzia che parte ricorrente non ha fornito elementi sufficienti utili alla ricostruzione dell'asserita frode subita, né in sede di denuncia né in quella di ricorso. Orbene, secondo l'orientamento condiviso dei Collegi, le mancate allegazioni del cliente sulle circostanze di fatto della frode subita rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo, qualora: a) l'intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute; b) il sistema di pagamento risulti conforme alla Strong Customer Authentication (SCA); 3) non risultino indizi di anomalia delle operazioni e/o ulteriori elementi.

Ricorrendo, nel caso di specie, tutte le richiamate circostanze, così come si evince dalle dichiarazioni rese e dalle allegazioni in atti, il Collegio conclude per il non accoglimento del ricorso, ritenendo il comportamento della ricorrente gravemente colposo.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE F.F.