

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 06/03/2026

FATTO

Il ricorrente espone quanto segue:

- si accorgeva che dal conto acceso presso l'intermediario resistente venivano effettuati tra il 23 aprile e il 30 maggio 2025, 38 bonifici non autorizzati verso un Iban collegato a un conto acceso presso l'Intermediario B;
- non ha fornito le sue credenziali a nessuno per eseguire i bonifici e il device è sempre rimasto in suo possesso;
- non ha mai ricevuto sms alert;
- l'intermediario avrebbe dovuto rilevare l'anomalia di tali operazioni;
- l'app potrebbe aver generato per errore i bonifici in esame.

Chiede:

1. il rimborso della somma di € 5.550, corrispondente ai 37 bonifici disconosciuti;
2. il rimborso della somma di € 300,00, a fronte del bonifico fatto il 30 maggio 2025 per errore a favore dell'iban verso cui sono stati effettuati gli altri bonifici disconosciuti.

L'intermediario resiste al ricorso ed eccepisce quanto segue:

- il 05/06/2025, il ricorrente sporgeva denuncia per i bonifici eseguiti dal 23/04/2025 al 30/05/2025, senza esporre, però, elementi utili a ricostruire una (eventuale) frode;
- le operazioni risultano correttamente autenticate e autorizzate; inoltre, nelle giornate dei bonifici disconosciuti sono stati eseguiti ben tre (3) bonifici - due dei quali per un importo di € 9.900,00 ciascuno - non contestati, ma che sono stati eseguiti con le medesime modalità dei bonifici oggetto di ricorso;
- per l'esecuzione dei bonifici sono necessari i seguenti passaggi:
 - accesso all'area riservata tramite sito web o app, inserendo le credenziali statiche (username e password - fattore conoscenza) scelte dal cliente. È possibile eseguire l'accesso tramite l'app con i dati biometrici del dispositivo, che dovrà essere attivato previo accesso all'area riservata, con le modalità di cui sopra, inserendo la OTP ricevuta;
 - per eseguire un bonifico dal conto è necessario:

1. inserire l'ordine di bonifico all'interno dell'area riservata (dopo aver fatto accesso); 2. confermare il bonifico mediante l'OTP ricevuta sul numero di cellulare associato al conto, oppure 3. tramite Conferma con Token attivato sull'app dello smartphone del cliente.

La "Conferma con Token" può essere attivata: 1. "Con un SMS e un selfie", attraverso l'inserimento di una OTP ricevuta tramite SMS sul numero di cellulare e l'acquisizione di un selfie "live"; 2. "Con la tua carta di debito", attraverso l'avvicinamento del chip della carta di debito del cliente con la tecnologia NFC dello smartphone.

L'accesso all'area riservata rappresenta il primo fattore (fattore di conoscenza o di inerENZA) mentre la OTP o la Conferma con Token rappresenta il secondo fattore (fattore di possesso) ai fini dell'autenticazione forte a doppio fattore (SCA);

- in data 15/09/2023 sono stati attivati il Riconoscimento Biometrico nonché la Conferma con Token sull'abituale dispositivo del Cliente usato anche nelle giornate in esame;
- pertanto, dal 23/04/2025 al 30/05/2025 vi sono stati solo accessi con Riconoscimento Biometrico nonché bonifici ordinari e istantanei autenticati con Conferma Token;
- tutto quanto sopra dimostra non solo che tutte le operazioni sono state eseguite dal ricorrente, ma, soprattutto, che sono state eseguite con autenticazione forte a due fattori;
- anche ove il cliente riuscisse a dimostrare di non aver operato lui all'interno della propria area riservata dal proprio dispositivo, non ha mai denunciato il furto o lo smarrimento dello smartphone, ma ha anzi dichiarato nel ricorso che: "I codici di accesso al conto e il mio cellulare sono in mio esclusivo possesso";
- il cliente avrebbe potuto accorgersi molto prima delle operazioni anomale nel proprio conto e avrebbe potuto bloccare quanto meno i bonifici successivi, se avesse precedentemente contattato il Servizio Clienti.

Chiede di respingere il ricorso.

Con le repliche la parte ricorrente rileva quanto segue:

- la banca non fornisce tramite i log elementi che consentano di provare che il dispositivo utilizzato dai frodatori sia quello del ricorrente;
- il report dell'home banking non consente di individuare l'IBAN del beneficiario dei bonifici e questo impedisce al cliente di controllare l'effettivo beneficiario;
- ha riscontrato la presenza dei bonifici sconosciuti solo il 4 giugno 2025, quando ha tentato di ripetere un bonifico da € 300 verso il conto detenuto presso l'Intermediario B, scoprendo poi che tale conto recava un IBAN diverso dal suo.

Chiede che la banca fornisca documentazione integrativa ai log e sia condannata al risarcimento del danno per le violazioni delle norme della PSD 2 sui sistemi di monitoraggio.

Nelle controrepliche la parte resistente rileva quanto segue:

- i log forniti sono esaustivi e confermano la corretta autenticazione delle operazioni;
- sono state fornite al cliente notifiche in merito ai bonifici contestati;
- ha immediatamente attuato ogni opportuna iniziativa, ivi incluso i tentativi di recall, per il recupero delle somme, ma non è stata ricevuta alcuna risposta dal beneficiario.

DIRITTO

1.- Il ricorrente, titolare di un conto presso la resistente, lamenta l'esecuzione di 38 bonifici non autorizzati verso un conto acceso presso un altro intermediario. Chiede la restituzione dell'importo di 5.850,00 euro.

Più precisamente il ricorrente rappresenta di aver sconosciuto 38 operazioni (di cui 37 da 150,00 euro e una da 300,00 euro, evidenziate in verde) eseguite tra il 23.04.2025 e il 30.05.2025 per un totale di 5.550,00 euro.

2.- Nel reclamo specifica che il bonifico da 300,00 euro del 30.05.2025 è stato disposto dallo stesso mediante la funzione ripeti bonifico pensando di effettuarlo a favore del suo conto acceso con

l'Intermediario B; si accorgeva poi che tale conto presentava un IBAN diverso dal suo (ossia l'IBAN del beneficiario dei bonifici contestati).

Rispetto a tale bonifico deve quindi applicarsi il principio secondo cui il prestatore dei servizi di pagamento non è tenuto ad alcun controllo sulla conformità tra IBAN e beneficiario indicato, essendo sufficiente che la disposizione di pagamento sia eseguita in conformità con l'identificativo unico fornito dal pagatore. In tali casi il Collegio è solito respingere il ricorso in applicazione dell'art 24 del D.lgs. 11/2010 (Coll. Roma, dec. n. 2661/2025).

3.- Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).

L'intermediario rappresenta che le operazioni sono state eseguite da app con il device del ricorrente tramite accesso con "Riconoscimento Biometrico" (codice 106) nonché autorizzazione con "Conferma con Token" (codice 132).

Le operazioni risultano effettuate con lo stesso device utilizzato per operazioni precedenti a quelle in contestazione (cfr colonna=user agent).

In base ai Log l'attivazione del "conferma con token" e della "biometria" sono avvenuti mediante username, password (fattori di conoscenza) e OTP (fattore di possesso), (cfr. codici 02, 05 e 259) utilizzando sempre lo stesso device.

Il Collegio ritiene il sistema di autenticazione sopra descritto conforme a SCA (Collegio di Roma, decisione n. 9180/24).

4.- La parte ricorrente si limita a disconoscere i bonifici, ma non fornisce alcun elemento idoneo a descrivere la possibile truffa in suo danno.

Si osserva poi che in caso di operazioni disconosciute intervallate da operazioni autorizzate (come nel caso in esame), questo Collegio ha rilevato come la prospettazione del ricorrente, che impugni selettivamente solo alcune operazioni – implicitamente riconoscendo la legittimità delle altre – fornisca un quadro presuntivo, incerto e contraddittorio incompatibile con una presunta frode (Collegio di Roma, decisione n. 5208 2023).

Peraltro, ai fini della valutazione della colpa grave del ricorrente rientra anche l'omesso controllo, per un periodo di tempo significativo, della movimentazione del conto corrente in relazione al quale risultano compiute le operazioni di pagamento disconosciute (Collegio di Roma, decisione n. 1849 del 2025).

Al riguardo il ricorrente afferma di essersi accorto della operatività anomala soltanto il 4 giugno 2025, quando ha tentato di ripetere un bonifico da € 300 (eseguita invero il 30.5.2025) verso il conto detenuto presso l'Intermediario B scoprendo che, a suo nome, risultava il conto in contestazione che recava un IBAN diverso dal suo.

Il ricorrente lamenta di non aver ricevuto alcun alert in occasione delle operazioni in contestazione.

L'intermediario con le controrepliche afferma di aver inviato notifiche al ricorrente. Nel periodo considerato (23 aprile – 30 maggio) il 10 e 18 maggio risultano inviate sia push che email. Le altre notifiche risultano inviate da portale web.

5.- All'esito dell'esame istruttorio è emerso che manca qualsiasi descrizione della presunta truffa, le operazioni sono state disposte dal device del ricorrente (già utilizzato in precedenza e durante lo stesso periodo per altre operazioni non contestate), vi è la SCA con accesso mediante riconoscimento biometrico, vi sono operazioni non contestate nel periodo in cui vi è stata la presunta truffa, vi è un omesso controllo per un periodo lungo, l'intermediario ha inviato notifiche push e email ed altre da portale web.

Invero, ferma restando l'allocazione dell'onere della prova a carico dell'intermediario, questo Collegio ritiene che sussista in capo al ricorrente un onere di allegazione delle circostanze che possano, al minimo, offrire una attendibile ipotesi alternativa rispetto a quella, altrimenti residuale (ed anzi unica), dell'utilizzo imputabile (direttamente o per colpa grave) al titolare (Coll. Roma, dec. n. 10723/19).

6.- Per cui il Collegio osserva che, ai sensi dell'art. 10 del D. Lgs. 27 gennaio 2010, n. 11, come in vigore dal 13 gennaio 2018, grava sul prestatore di servizi l'onere di dimostrare che l'operazione di pagamento sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Nel caso di specie, l'intermediario ha prodotto evidenza della corretta autorizzazione delle operazioni contestate con rispetto degli standard di sicurezza (SCA) indicati dalla PSD2.

Come già ritenuto in diverse occasioni da questo Collegio, il ricorso ad un sistema di autenticazione a doppio fattore, in assenza di malfunzionamento del sistema, consente di ritenere che l'intermediario abbia assolto all'onere della prova che la legge gli impone in caso di disconoscimento di una operazione di pagamento.

Infatti, a fronte di una allegazione generica di disconoscimento delle operazioni della parte ricorrente, non si ravvisano, d'altro canto, elementi idonei ad imputare una qualche responsabilità in capo all'intermediario resistente.

Alla luce di quanto esposto, il Collegio ritiene che la domanda non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE