

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 22/12/2025

FATTO

Il ricorrente espone quanto segue:

In data 28/5/2025 accedeva alla propria app per effettuare un'operazione dispositiva e si avvedeva che dal suo conto corrente, alle ore 11,35 del medesimo giorno, era stato disposto un bonifico di € 1.125,00 a favore di un terzo.

Afferma di non aver mai autorizzato il bonifico in questione e di non aver mai fornito i propri codici autorizzativi, conscio degli schemi di truffa in quanto lavoratore dipendente della banca resistente.

Chiede il rimborso delle somme sottratte.

L'intermediario resiste al ricorso ed eccepisce che le operazioni sono state eseguite previa autenticazione SCA compliant, correttamente contabilizzate senza alcuna anomalia. In particolare, le operazioni sono state eseguite dal dispositivo in uso al ricorrente e non vi è stato enrollment di nuovi dispositivi.

E' presumibile che i bonifici siano stati disposti nell'ambito di una truffa che prevede la collaborazione attiva del soggetto passivo, indotto tramite artifici e raggiri a disporre personalmente le operazioni sconosciute.

L'autorizzazione delle operazioni dispositive è avvenuta in tre fasi:

- enrollment della carta di pagamento, avvenuta molto tempo prima della truffa, che ha richiesto ricezione del codice OTP al numero di cellulare in uso al ricorrente, corrispondente a quello indicato nella denuncia in atti e nel modulo di ricorso;
- log-in nella propria internet banking, che ha richiesto inserimento dell'user ID e della password (fattore di conoscenza) seguita da codice segreto (fattore di possesso), con specifico risalto della fase dispositiva a mezzo della stessa chiave cifrata P***ID del ricorrente;
- fase dispositiva delle operazioni, avvenuta tramite inserimento della password (fattore di conoscenza) seguita da codice segreto (fattore di possesso), "con specifico risalto della fase dispositiva a mezzo della stessa chiave cifrata P***ID della ricorrente".

Le operazioni disconosciute, tenuto conto della modalità con cui sono state autorizzate, potevano essere eseguite soltanto dal titolare dello strumento di pagamento, che è in possesso del device su cui è inviata la notifica in APP per l'inserimento del codice di sicurezza "P***ID".

Eccepisce la colpa grave del ricorrente, che non specifica le circostanze della frode subita.

In sede di repliche, pate ricorrente contesta le deduzioni dell'intermediario affermando che grava su quest'ultimo l'onere di provare la colpa del cliente e che nel caso di specie non può essergli attribuita alcuna responsabilità. Aggiunge che in data 15/5/2025 (tredici giorni prima dell'operazione oggetto di ricorso) aveva subito il furto del portafogli e della carta di debito associata al conto corrente in essere presso l'intermediario. Ritiene possibile che in detta occasione i frodatori abbiano potuto carpire le proprie credenziali.

In sede di controrepliche l'intermediario si riporta alle controdeduzioni.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita il 28 maggio 2025. Risulta pertanto effettuata dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tale operazione è altresì successiva alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-bis, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-bis), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che

sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione”.

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che *“a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)”*.

4.- La controversia ha ad oggetto un bonifico istantaneo di € 1.125,00 eseguito il 28/5/2025 alle ore 11:35.

L'intermediario afferma che l'operazione di pagamento risulta correttamente autenticata, registrata e contabilizzata e che non è emerso alcun malfunzionamento o compromissione dei sistemi.

L'intermediario afferma in particolare che l'operazione è stata eseguita attraverso l'App dell'intermediario (fattore di possesso) e mediante utilizzo del codice P****ID (fattore di conoscenza).

L'intermediario deduce che, il giorno della truffa, la procedura di Log In app è stata validata attraverso autenticazione SCA compliant, previo inserimento del codice P***ID.

L'intermediario chiarisce che il device da cui è stato effettuato l'accesso e l'operazione contestata risulta essere il medesimo utilizzato dal ricorrente per precedenti operazioni dispositive non disconosciute.

Dopo l'accesso all'app dell'intermediario, è stata effettuata l'operazione dispositiva di cui l'intermediario allega la seguente evidenza informatica, evidenziando che la medesima è stata autorizzata attraverso il medesimo sistema P***ID.

Il sistema autorizzativo basato sul c.d. codice P****ID prevede la possibilità, per l'utente, di scegliere, in fase di configurazione dell'app, un codice statico da utilizzare per l'esecuzione delle singole operazioni dispositive. Tale sistema autorizzativo è stato considerato conforme alla SCA (Collegio di Roma, decisione n. 318/2021).

5.- Le allegazioni del ricorrente in ordine alla modalità della frode sono le seguenti:

- in sede di denuncia querela, sporta il 28/5/2025 (medesimo giorno in cui è stato disposto il bonifico disconosciuto), dichiara di essersi avveduto per caso dell'operazione contestata;
- in sede di repliche, rappresenta di aver subito il furto del portafogli contenente, tra l'altro, anche la carta di debito associata al conto corrente, il giorno 15/5/2025 (otto giorni prima) e che con detta carta erano state effettuate operazioni non autorizzate (non oggetto di ricorso e rispetto alle quali non chiarisce se sia stato presentato disconoscimento all'intermediario);

L'intermediario contesta che il ricorrente non abbia contestualizzato efficacemente la dinamica della frode, incorrendo in colpa grave.

6.- 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).

Il Collegio ritiene dunque che, in caso di disconoscimento dell'operazione, è onere del ricorrente fornire “elementi utili a provare che l'operazione sia stata realmente fraudolenta” (Collegio di Roma, decisione n. 299/2020).

Secondo l'orientamento condiviso dei Collegi, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo, qualora l'Intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute (Collegio di Roma, decisione n. 8058/2022).

7.- 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 dell'operazione della parte ricorrente, l'intermediario ha documentato che l'operazione contestata è stata correttamente autenticata, registrata e contabilizzata.

Non si ravvisano, d'altro canto, elementi idonei ad imputare una qualche responsabilità in capo all'intermediario resistente.

8.- 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