

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore COSIMO DAMIANO FABIO MASTROROSA

Seduta del 18/02/2026

FATTO

Parte ricorrente domanda la condanna dell'intermediario al rimborso di due operazioni di pagamento disconosciute da 400,05 € ciascuna, eseguite il 21/08/2025 a valere sul suo conto corrente, sostenendo di non aver comunicato ad alcuno le proprie credenziali di home banking.

Nelle controdeduzioni l'intermediario afferma quanto segue.

- Il 21/08/2025, alle 16:05 e alle 16:35, sono state eseguite due operazioni di pagamento online tramite le due carte di debito della ricorrente.
 - La disposizione delle operazioni è stata preceduta dall'installazione dell'app bancaria su un nuovo dispositivo, utilizzando le credenziali statiche di accesso all'home banking (elemento di conoscenza) e un OTP trasmesso via SMS al numero di cellulare della ricorrente (elemento di possesso).
 - Dopodiché, le due operazioni sono state avviate online e autenticate tramite il dispositivo appena configurato, digitando il PIN (elemento di conoscenza) all'interno dell'app bancaria (elemento di possesso), a seguito della ricezione di una notifica push.
 - Quanto alla colpa grave dell'utente, la ricorrente non ha fornito alcun elemento relativo alla dinamica della frode. Pertanto, deve ritenersi che abbia negligenemente comunicato le proprie credenziali al frodatore, consentendo l'esecuzione delle operazioni.
- Di conseguenza, l'intermediario domanda il rigetto del ricorso.

Nell'istruttoria è stato accertato che 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). Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Quanto all'autenticazione, l'intermediario resistente precisa che in una prima fase il 21/08/2025 è stata installata l'app bancaria su un nuovo dispositivo, utilizzando le credenziali statiche di accesso all'home banking (elemento di conoscenza) e un codice dinamico trasmesso via SMS al numero di cellulare della ricorrente (elemento di possesso).

Produce a riprova il relativo log, da cui risulta l'invio dell'SMS contenente il codice dinamico al numero di telefono della ricorrente (riportato anche nel ricorso).

Produce, altresì, il link da cui emerge l'impiego delle credenziali statiche.

A seguire, sempre in base alla ricostruzione dell'intermediario, le due operazioni di e-commerce sono state avviate da browser e autenticate tramite lo smartphone probabilmente di altro soggetto, digitando il PIN (elemento di conoscenza) all'interno dell'app bancaria appena configurata (elemento di possesso), a seguito della ricezione di una notifica push.

Produce l'intermediario il log, da cui sembra risultare per entrambe le operazioni la validazione tramite token app bancaria (cfr. "esitoVerificaOTP"), a seguito della ricezione di una notifica push.

E' importante evidenziare che nella denuncia alle forze dell'ordine, così come nel ricorso, parte ricorrente non ha ricostruito le modalità della assunta truffa, limitandosi ad affermare di aver constatato l'effettuazione il 21/08/2025 di n. 2 addebiti fraudolenti dell'importo di 400,50 € ciascuno a valere sul suo conto corrente.

Nega di aver comunicato ad alcuni le proprie credenziali.

La ricorrente fa riferimento alla ricezione di "messaggi strani" riguardanti il suo conto corrente. A questo riguardo, unitamente al ricorso, produce alcune e-mail genuine di alert trasmesse dall'intermediario in occasione della configurazione dell'app bancaria su un nuovo dispositivo il 21/08/2025, giorno in cui sono state effettuate le operazioni.

DIRITTO

Considerato che in base al recente orientamento condiviso tra i Collegi territoriali, in aderenza al dato normativo (art. 10 del D.Lgs. 11/2010), ai fini dell'applicazione della PSD2 è necessario e sufficiente che il cliente neghi di aver autorizzato la transazione; e che tuttavia, il Collegio può valutare la mancata allegazione dei fatti, tra i vari elementi, per formare il proprio convincimento circa la colpa grave del ricorrente, una volta verificata la sussistenza della SCA (cfr. ex multis Collegio di Roma, decisione n. 8058/2022), visto anche il precedente di questo stesso Collegio (Collegio di Roma, decisione n. 13177 del 20/12/2024) in cui si è statuito che " Nella denuncia alle forze dell'ordine, come nel ricorso, la parte ricorrente non ha ricostruito le modalità della truffa, limitandosi ad affermare di aver constatato solo il 19/12/2023 l'effettuazione, tra il 16/12/2023 e il 19/12/2023, di n. 22 utilizzi fraudolenti della propria carta di debito, per l'importo complessivo di € 5.454,99.

In base al recente orientamento condiviso tra i Collegi territoriali, in aderenza al dato normativo (art. 10 del D.Lgs. 11/2010), è necessario e sufficiente ai fini dell'applicazione della PSD2 che il cliente neghi di aver autorizzato la transazione: il Collegio può valutare la mancata allegazione dei fatti, tra i vari elementi, per formare il proprio convincimento circa la colpa grave del ricorrente solo una volta verificata la sussistenza della SCA."

A mente anche della decisione di questo Collegio di Roma, n. 8058/2022 " "Il sistema descritto dall'intermediario è conforme a SCA, e così l'operazione controversa risulta effettuata attraverso i passaggi previsti da questo sistema, senza anomalie. Un sistema che procede solo se vengono inserite correttamente le credenziali statiche e dinamiche di cui sopra. Il ricorrente nega di averle fornite a terzi, ma né in sede di querela, né nel ricorso offre elementi idonei a contestualizzare l'evento truffaldino,

che renderebbe possibile una ricostruzione alternativa rispetto all'ipotesi di una sua comunicazione delle credenziali ai truffatori. Posto che le regole che impongono agli operatori stringenti requisiti di sicurezza sull'autenticazione e sull'autorizzazione dei pagamenti, come risulta essere quello adottato dall'intermediario resistente (anche) per l'operazione qui contestata, hanno la funzione di offrire la massima sicurezza possibile per le operazioni di pagamento, è evidentemente onere di chi allega un'anomalia nel funzionamento provarla. Tuttavia, in assenza di elementi idonei a contestualizzare l'evento truffaldino, questo Collegio ritiene di respingere la richiesta restitutoria del ricorrente, desumendone la colpa grave (così già con la decisione n. 23474/2021, per cui «[l']assoluta carenza di allegazione da parte del cliente rende eccessivamente generica la rappresentazione del fatto costitutivo della pretesa restitutoria, che legittima la veridicità dell'ipotesi dell'utilizzo dello strumento di pagamento imputabile per colpa grave al titolare»).

Considerata l'assenza di elementi utili a ricostruire la truffa,

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE