

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) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore STEFANO DEPLANO

Seduta del 04/12/2025

FATTO

Parte ricorrente rappresenta che: i.) in data 7 giugno 2025 ha pubblicato su una nota piattaforma *online* un annuncio di vendita di un bene ad un prezzo di 450,00 euro; ii.) è stata contattata da un sedicente acquirente che le ha proposto di utilizzare una piattaforma di pagamento e spedizioni per effettuare il pagamento e consegna; iii.) a tal fine ha trasmesso un *link* che reindirizzava verso un sito-clone; iv.) ha inserito i dati personali e i dati della carta n. *549 emessa dal resistente e si è vista addebitare due operazioni da 270,04 euro ciascuna.

Parte resistente riferisce che: i.) le operazioni fraudolente sono state eseguite in data 7 giugno 2025, rispettivamente alle ore 17:57 e 17:58; ii.) esse risultano autorizzate tramite l'APP bancaria in possesso al cliente, il quale ha ricevuto due distinte notifiche riepilogative delle transazioni e le ha approvate con riconoscimento biometrico; iii.) le notifiche di autorizzazione riportano in maniera schematica e precisa i dati relativi a ciascuna operazione di pagamento; iv.) controparte versa in atti la conversazione intrattenuta con il frodatore dalla quale si evince che l'operazione si è interamente svolta su una piattaforma estranea a quella della Banca.

In sede di repliche si rileva che, in considerazione della natura degli addebiti autorizzati – relativi ad un sito di *gaming* con sede estera – la Banca si sarebbe dovuta accorgere dell'anomalia delle operazioni. Si esclude, inoltre, che sia stata dimostrata la colpa grave del ricorrente.

In sede di controrepliche si evidenzia che non risultano integrati i cd. indici di anomalia di cui all'art. 8, comma 1, lett. a) n. 2, d.m. 30 aprile 2007, n. 112.

Parte ricorrente chiede la restituzione della somma di 540,08 euro, pari all'importo di due operazioni sconosciute a séguito di *phishing*.

Parte resistente insiste per il rigetto del ricorso.

DIRITTO

1. – La controversia ha ad oggetto operazioni di pagamento eseguite in data 7 giugno 2025, in particolare due pagamenti *online* effettuati tra le ore 18:57 e 18:58.

2. – Le operazioni contestate sono state poste in essere sotto la vigenza del d.lgs. n. 11 del 2010, così come modificato dal d.lgs. n. 218 del 2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). In base a tali disposizioni, come applicate da questo Arbitro (cfr. Coll. Coord., dec. n. 22745 del 2019), occorre volgere l'attenzione a due dirimenti profili disciplinari.

2.1 – In primo luogo, è l'Intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza che le operazioni sconosciute siano state autenticate con un c.d. "Sistema di autenticazione forte" (SCA), posto che ai sensi del comma 2 *bis*, art. 12, d.lgs. n. 11 del 2010, come inserito dal d.lgs. n. 218 del 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 accertano l'autenticazione forte del cliente». In secondo luogo, è sempre l'Intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.

3. – Con riferimento al primo profilo, visto quanto versato in atti, emerge che le operazioni di pagamento sono state autenticate mediante ricezione della notifica *push* ricevuta sullo *smartphone* tramite l'APP *mobile banking* che costituisce fattore di possesso e inserimento del fattore biometrico. Il Collegio di Roma ha già ritenuto *compliant* alla SCA tale modalità autorizzativa (Coll. Roma, dec. n. 6187 del 2022).

4. – L'Intermediario ha quindi dato prova di essersi dotato di un sistema di autenticazione forte in linea con la normativa di settore.

5. – Con riferimento al secondo profilo innanzi richiamato, in data 7 giugno 2025, il ricorrente ha pubblicato su un sito un annuncio di vendita di un bene al prezzo di 450,00 euro ed è stato contattato da un potenziale acquirente. Quest'ultimo gli ha proposto di effettuare il pagamento tramite una piattaforma che offre servizi di pagamento e di spedizione ed ha richiesto a tal fine *e-mail* e numero di telefono. Forniti i dati, il ricorrente ha ricevuto un *link* che lo ha reindirizzato su un sito-clone della piattaforma prescelta dove ha visualizzato la foto del bene messo in vendita e il prezzo richiesto. A quel punto ha inserito i dati dello strumento di pagamento e ha ricevuto le notifiche di conferma dei due pagamenti.

6. – La questione della mancata attivazione del servizio di *alert* non viene in rilievo dal momento che il ricorrente ha ricevuto le notifiche *push* autorizzative dei pagamenti, come ammesso in denuncia.

7. – La condotta posta in essere dal ricorrente appare gravemente colposa. Egli, per un verso, ha fornito i dati della propria carta ad un sito-clone non riconducibile a quello dell'Intermediario. Pur avvertito dalla ricezione delle notifiche *push*, in secondo luogo, non si è avveduto di autorizzare due pagamenti nonostante fosse la parte venditrice del bene.

8. – Il ricorso, in definitiva, non appare fondato e non merita di essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE