

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) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore STEFANO DEPLANO

Seduta del 09/01/2026

FATTO

Parte ricorrente rappresenta che: i.) in data 25 gennaio 2025 è stato effettuato un pagamento *online* su una piattaforma di compravendita di criptovalute tramite la carta di debito associata al suo conto corrente; ii.) mentre si perfezionava il pagamento *online*, si è accorta che il proprio *smartphone* non era accessibile in quanto compromesso da un attacco informatico e controllato esclusivamente da remoto da un *hacker*; iii.) è stato aggirato il codice PIN e gli estremi della carta di debito sono stati ottenuti in maniera impropria; iv.) a séguito del ripristino delle normali funzionalità dello *smartphone* ha potuto ricostruire la presenza di un SMS proveniente dalla Banca resistente con indicazione del codice OTP da utilizzare per il completamento del pagamento fraudolento ed il corrispettivo SMS *alert* con la comunicazione di “esito autorizzato”; v.) è presente altresì un precedente SMS delle ore 01:26 da parte della Banca nel quale veniva richiesta la conferma dell’operazione fraudolenta con 4 SMS di risposta affermativa; vi.) i sistemi di sicurezza della Banca non sono risultati idonei.

Parte resistente riferisce che: i.) per l’autorizzazione dell’operazione è stato adottato un sistema di “autenticazione forte” a due fattori ossia il codice PIN (fattore di conoscenza) e il codice OTP inviato tramite SMS all’utenza cellulare del ricorrente (fattore di possesso); ii.) risulta inviato un SMS al ricorrente per avvisarlo dell’avvenuta autorizzazione del pagamento; iii.) i sistemi di monitoraggio adottati hanno rilevato come potenzialmente sospetta l’operazione oggetto di controversia sì che è stato inviato apposito SMS con l’intento di allertare il ricorrente e impedire l’operazione; iv.) il ricorrente ha fornito una risposta affermativa e ha permesso il buon esito dell’operazione contestata; v.) non emergono elementi tecnici né indizi concreti che possano far pensare che una persona terza, come un *hacker*, sia riuscita ad alterare il processo rappresentato; vi.) il ricorrente ha riferito al servizio clienti: «[...]loro hanno praticamente installato questa app binance sul mio telefono e hanno creato un account e hanno utilizzato i

miei soldi per comprare criptovalute»; vii.) il ricorrente non ha fornito alcun elemento specifico utile all'accertamento dei fatti, in particolare difetta qualsiasi prova concreta che certifichi l'impossibilità per il titolare di accedere al proprio dispositivo; viii.) per poter disporre un pagamento a distanza, è necessario inserire sul sito *e-commerce*: PAN, CVV e data scadenza della carta mentre per autorizzare il pagamento occorrono il PIN di accesso all'*home banking* e la OTP inviata tramite SMS; ix.) in ogni caso, laddove i dati della carta fossero stati recepiti dall'*Internet banking* della Banca, per accedere era necessario conoscere il PIN collegato al codice cliente, un'informazione in possesso soltanto del ricorrente.

Parte ricorrente chiede il rimborso della somma di 1.850,00 (milleottocentocinquanta/zero) euro, corrispondente all'importo di un'operazione disconosciuta eseguita fraudolentemente da terzi non autorizzati.

Parte resistente insiste per il rigetto del ricorso.

DIRITTO

1. – La controversia ha ad oggetto il disconoscimento di un'operazione di pagamento *online* eseguita in data 25 gennaio 2025 per la somma di 1.850,00 euro.

2. – L'operazione contestata è stata effettuata 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 disconosciute 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, l'operazione disconosciuta è stata autorizzata mediante inserimento del codice OTP, inviato tramite SMS al numero di telefono del ricorrente (fattore di possesso) ed inserimento del codice PIN/Password (fattore di conoscenza) correlato alle credenziali di accesso ai servizi *online*. L'operazione appare conforme a SCA.

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

4. – Con riferimento al secondo profilo innanzi richiamato e in base a quanto emerge dalla denuncia, in data 25 gennaio 2025, tra le ore 01:00 e le ore 02:00, il ricorrente si è accorto che il suo cellulare vibrava ripetutamente e non rispondeva ai comandi. Ricevuta una notifica

dall'APP bancaria presente sul suo computer e visionata la lista-movimenti ha appurato la presenza di un'operazione non autorizzata su un sito per la vendita di criptovalute.

4.1. – Alle ore 01:53 il ricorrente ha ricevuto un SMS genuino dalla Banca resistente recante il codice OTP per confermare l'operazione di pagamento presso il sito di criptovalute per la somma di 1.850,00 euro. Dai *log* prodotti emerge che la carta di pagamento è stata bloccata alle ore 03:16, circa un'ora dopo la frode.

5. – Alla luce di quanto premesso il ricorrente non fornisce elementi utili alla ricostruzione della frode, in particolare alla sua genesi. Egli, nel dettaglio, si limita a riferire che il telefono ha iniziato a vibrare ma non chiarisce se abbia concesso ai frodatori il controllo da remoto oppure abbia installato un'APP di terze parti.

6. – Codesto Collegio riconosce, 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 del 2019). Si vuol dire che, in caso di disconoscimento dell'operazione, è onere del ricorrente fornire «elementi utili a provare che l'operazione sia stata realmente fraudolenta» (Coll. Roma, dec. n. 299 del 2020).

7. – Qualora, come accaduto nel caso di specie, l'Intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento circa la colpa grave del ricorrente medesimo (Coll. Roma, dec. n. 8058 del 2022).

8. – Tanto premesso, il ricorso non è fondato e non merita di essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE