

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

Relatore DOMENICO BONACCORSI DI PATTI

Seduta del 17/04/2026

FATTO

Il ricorrente riferisce di aver ricevuto - in data 27.01.2025 - un sms apparentemente proveniente dalla banca resistente, con il quale veniva invitato a contattare il servizio clienti per comunicazioni urgenti. Entrava in contatto con un sedicente operatore della banca, il quale riferiva la necessità di effettuare operazioni di manutenzione sui conti online per ragioni di sicurezza. Su indicazione del truffatore, il ricorrente scaricava dal play store una app apparentemente riconducibile alla banca convenuta, che consentiva a terzi di controllare da remoto il dispositivo. Venivano effettuate ad insaputa del cliente 5 operazioni di bonifico per complessivi 71.190,00 euro. Due di esse sono state stornate. Apprendeva successivamente che sul telefono era stato installato un malware del tipo "remote access trojan" in grado di controllare da remoto l'operatività dei dispositivi android. Il cliente nega di aver comunicato al truffatore le proprie credenziali.

Il ricorrente chiede il ristoro dell'importo di euro 41.640,00.

La banca nelle proprie controdeduzioni premette che delle 5 operazioni originariamente disconosciute, 2 sono state stornate. Afferma che per accedere all'home banking occorre inserire il numero cliente, il pin e il codice OTP generato da mobile token. Riferisce che le operazioni sono state correttamente autorizzate, registrate e contabilizzate, senza anomalie con le modalità sopra indicate. L'intermediario sostiene che le operazioni sono imputabili alla negligente custodia dello strumento di pagamento e delle relative credenziali da parte del cliente. La banca ha tentato il recall delle operazioni, senza successo. L'intermediario chiede pertanto il rigetto del ricorso.

DIRITTO

La controversia ha ad oggetto 3 bonifici online: i) Bonifico di euro 29.650,00 del 28.01.2025; ii) Bonifico di euro 6.000,75 del 30.01.2025; iii) Bonifico di euro 5.990,75 del 30.01.2025. Altri due bonifici (di euro 19.200,75 e 29.650,75) sono stati riaccreditati/stornati e non costituiscono oggetto del contendere. La somma richiesta dal ricorrente è dunque di euro 41.640,00.

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).

Il Collegio preliminarmente rileva che nel modulo di ricorso parte ricorrente si qualifica “consumatore”. Dall’esame degli estratti conto in atti emergono però movimentazioni di importo elevato che vengono quindi ricondotte anche ad una attività professionale, dovendo ricondurre la qualifica dell’odierno ricorrente in non consumatore.

L’intermediario afferma che le operazioni di pagamento risultano correttamente autenticate, registrate e contabilizzate e che non è emerso alcun malfunzionamento o compromissione dei sistemi. L’intermediario afferma in particolare che le operazioni sono state effettuate in essere con il dispositivo del cliente (sottoposto al controllo da remoto da parte del truffatore) ed autenticate attraverso un sistema a doppio fattore. L’accesso al conto è avvenuto con inserimento del PIN [fattore di conoscenza] e l’utilizzo del mobile token per la generazione dell’OTP [fattore di possesso]. Le operazioni dispositive sono state autorizzate con PIN [fattore di conoscenza] e OTP generata in maniera silente dal Mobile token [fattore di possesso].

Il ricorrente rileva di aver ricevuto un sms civetta, con il quale veniva invitato a mettersi in contatto con gli operatori dell’intermediario contattando un numero di cellulare. Dalla documentazione versata in atti: i) l’sms civetta è privo di intestazione; ii) il numero non è riferibile all’intermediario. Parte ricorrente riferisce che tale operatore lo convinceva a scaricare dal play store una app che consentiva il controllo da remoto del dispositivo. Sostiene che a tale app era abbinato il logo della banca resistente, ma non produce documentazione al riguardo.

I Collegi ABF riconoscono la colpa grave dell’utente che, su indicazione del frodatore, installi anche inconsapevolmente un’applicazione “la cui funzionalità risiede (...) nel permettere l’accesso ed il controllo di pc e smartphone da remoto”, consentendo in tal modo al frodatore di agire indisturbato e disporre i pagamenti (Collegio di Roma, decisione n. 4317/2024). Il Collegio pertanto ravvisa una colpa grave nei confronti dell’odierno ricorrente, la cui condotta risulta connotata anche da negligenza grave avendo agevolato il compimento della truffa. Alla luce di quanto sopra il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE