

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 MASSIMO CARATELLI

Seduta del 13/03/2026

FATTO

1. La controversia attiene alla contestazione di un addebito disposto su un rapporto di conto corrente intestato al ricorrente.
2. In particolare, in base alla dinamica riferita da parte attrice, l'istante – correntista della resistente e titolare di un altro conto corrente presso la banca Beta, estranea al presente ricorso –, in data 17 ottobre 2025 alle ore 16.00, riceveva una telefonata da un soggetto qualificatosi come operatore della medesima banca Beta. Costui rappresentava la necessità di aggiornare i dati personali al fine di continuare a utilizzare il servizio di home banking e, a tal fine, induceva il cliente a scaricare sul proprio dispositivo un'applicazione recante il logo ufficiale dell'istituto Beta. Il proponente inseriva quindi le proprie credenziali personali. Subito dopo, il dispositivo risultava bloccato e inutilizzabile per circa dieci minuti. Poco più tardi, accedendo da computer, l'istante riscontrava che – dal conto corrente intrattenuto presso la resistente – era stato disposto un bonifico di euro 1.000,00 in favore di una carta di pagamento a lui intestata, emessa dalla banca Beta. Con tale carta venivano successivamente eseguite due operazioni per l'acquisto di criptovalute, rispettivamente di euro 990,00 e di euro 90,00. Nel medesimo giorno, il proponente presentava querela-denuncia alle Autorità competenti e provvedeva al blocco delle carte e del conto corrente. In data 20 ottobre 2025 presentava, inoltre, reclamo alla resistente, riscontrato negativamente. Tanto premesso, parte attrice chiede all'ABF di accertare l'illegittimità dell'addebito relativo all'operazione non autorizzata del 17 ottobre 2025, per euro 1.000,00, nonché la responsabilità della convenuta per "omessa adozione di adeguate misure di sicurezza", ritenendo che la transazione avrebbe dovuto essere riconosciuta come fraudolenta. Per l'effetto, domanda il rimborso integrale della somma sottratta, assumendo di non aver autorizzato la disposizione, "eseguita dal truffatore che ha preso il controllo remoto del ... dispositivo telefonico tramite app malevola".
3. Con le controdeduzioni, parte convenuta riferisce che il ricorrente è titolare di un conto corrente presso l'intermediario, al quale è collegato il servizio di home banking. Ciò posto, la banca eccepisce, in via preliminare, il difetto di legittimazione passiva e, nel merito, l'infondatezza della domanda, evidenziando che il bonifico contestato costituisce una mera operazione di giroconto verso altro

rapporto, parimenti intestato al cliente, intrattenuto presso la banca Beta, ove si sarebbe verificata l'effettiva distrazione dei fondi a favore dei frodatori, poi perfezionatasi mediante l'acquisto di criptovalute. La resistente chiarisce, inoltre, che il bonifico oggetto di disputa è stato eseguito mediante un sistema di autenticazione conforme ai requisiti della strong customer authentication (SCA), con utilizzo di un doppio fattore di sicurezza, e che l'operazione non presentava alcun profilo di anomalia – né con riferimento all'importo né alla destinazione – sicché non può essere ascritta all'istituto di credito alcuna responsabilità per la mancata attivazione di misure di blocco preventivo. L'intermediario rileva, altresì, che la ricostruzione dei fatti prospettata dal ricorrente non è supportata da adeguati elementi probatori. In particolare, non risultano chiarite le modalità attraverso cui l'installazione di un'applicazione malevola riferibile alla banca Beta abbia consentito l'accesso anche al conto corrente intrattenuto presso la resistente; né l'istante non fornisce i dettagli del numero di telefono dal quale proveniva la telefonata "esca". La banca ritiene, pertanto, plausibile che il bonifico sia stato disposto dallo stesso proponente, indotto dal frodatore a eseguire l'operazione in favore del rapporto acceso presso la banca Beta, sul quale sarebbero poi state effettuate le operazioni di acquisto di criptovalute. Del resto, il cliente dichiara di aver installato l'applicazione malevola e di aver inserito le proprie credenziali relative all'home banking dell'istituto terzo, senza tuttavia chiarire in che modo i truffatori avrebbero acquisito anche i codici di accesso relativi al conto presso la resistente. Alla luce di quanto precede, la convenuta chiede – in via principale – di dichiarare l'inammissibilità del ricorso per difetto di legittimazione passiva in relazione alla truffa lamentata e – in via subordinata – il rigetto di "tutte le domande formulate", in quanto infondate in fatto e in diritto.

DIRITTO

1. L'intermediario eccepisce, in via preliminare, l'inammissibilità del ricorso per difetto di legittimazione passiva, sostenendo di non essere il soggetto responsabile dei fatti contestati e rappresentando che la frode, l'acquisizione delle credenziali e la successiva distrazione delle somme si sarebbero verificate presso un diverso intermediario. Tuttavia, sul punto, si osserva che – in coerenza con la prospettazione del ricorrente – anche l'operazione di c.d. "giroconto", dal rapporto intrattenuto presso la convenuta a quello acceso presso la banca Beta, risulta contestata in quanto non autorizzata, circostanza che radica la legittimazione passiva dell'odierna resistente. Ne consegue che l'eccezione sollevata dall'intermediario non è fondata e non può essere accolta.
2. Nel merito, ai fini della decisione, vanno anzitutto considerate quali siano le eventuali responsabilità ascrivibili alle parti, alla luce dei criteri indicati dal d.lgs. 27 gennaio 2010, n. 11, che regola la materia dei servizi di pagamento nel mercato interno, così come modificato dal d.lgs. 15 dicembre 2017, n. 218, che ha recepito la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. "PSD 2").
3. Ebbene, ad avviso di questo Arbitro il ricorrente non offre elementi utili a ricostruire la frode, limitandosi a riferire di essersi avveduto dell'operazione indebita soltanto a seguito dell'accesso al servizio di home banking tramite computer, dopo aver installato sul proprio dispositivo mobile un'applicazione contraddistinta dal logo ufficiale di un istituto terzo, su sollecitazione di un sedicente operatore dal quale veniva contattato telefonicamente per ripristinare "le autorizzazioni necessarie" sulla propria area riservata.
4. Sul punto si osserva che, secondo l'orientamento condiviso dai Collegi territoriali, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui l'Arbitro può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente (cfr. Collegio di Roma, decisione n. 11050/2024).
5. A quest'ultimo riguardo, si rileva che la banca ha offerto riscontro del procedimento seguito per autorizzare l'operazione disconosciuta, producendo i relativi log, con buon fine della digitazione dei

codici. Ne consegue il Collegio che il sistema di autenticazione adottato in fase dispositiva appare in grado di garantire un elevato livello di sicurezza.

6. Peraltro, non si rilevano nella documentazione prodotta dalle parti riscontri che lascino supporre qualche malfunzionamento del sistema di parte resistente durante il processo dispositivo.

7. Tanto premesso, in assenza di elementi idonei a contestualizzare l'evento truffaldino, questo Collegio ritiene di dover respingere la richiesta restitutoria del proponente, desumendone la colpa grave, in linea con quanto già espresso 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").

8. Rileva, altresì, il Collegio che, dalla ricostruzione dei fatti, emerge come l'istante abbia consentito – sia pure inconsapevolmente – il controllo da remoto del proprio servizio di home banking. In simili fattispecie, questo Arbitro riconosce la colpa grave dell'utente che, su indicazione del frodatore, installi 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 (cfr. Collegio di Roma, decisione n. 7806/2023).

9. In relazione a quanto precede, il ricorso non può, pertanto, essere accolto.

10. Sotto diverso profilo, il ricorrente sostiene che l'intermediario avrebbe dovuto bloccare preventivamente l'operazione perché di natura "fraudolenta". Le evidenze così come ricostruite dalle parti non consentono, tuttavia, di accertare anomalie nell'utilizzo contestato rispetto all'ordinaria operatività a valere del rapporto di conto corrente oggetto di disputa.

11. Sul punto va, peraltro, rilevato che secondo l'art. 2 del Regolamento (UE) n. 2018/389 gli intermediari devono predisporre meccanismi di monitoraggio in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. Peraltro, in base all'interpretazione fornita dall'EBA (cfr. EBA Q&A 4090/2018), non è necessario che questi meccanismi operino in tempo reale – vagliando le operazioni prima della loro esecuzione –, potendo limitarsi a un monitoraggio delle frodi ex post. Non può ritenersi, dunque, che la resistente avesse l'obbligo di negare l'autorizzazione delle operazioni contestate.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE