

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 EMANUELE BILOTTI

Seduta del 09/01/2026

FATTO

1. – Con ricorso del 6 giugno 2025, previo reclamo del 6 febbraio 2025, la parte ricorrente chiede il rimborso di Euro 17.451,00 corrispondente ad un bonifico sconosciuto disposto da ignoti truffatori. Nel ricorso la parte ricorrente riferisce che il 14 novembre 2024 riceveva sul proprio dispositivo mobile un messaggio di testo nel quale le veniva comunicato l'inserimento di un bonifico di Euro 4.900,00 con addebito sul proprio conto. Facevano seguito numerosi contatti telefonici con numeri riferibili all'intermediario. L'interlocutore telefonico si qualificava come operatore dell'intermediario ed invitava la parte ricorrente a porre in essere delle operazioni per bloccare l'addebito e per evitare ogni forma di truffa. La parte ricorrente riteneva così di aver messo in sicurezza il proprio conto. Successivamente però, a seguito di una telefonata al numero verde dell'intermediario, si rendeva conto di essere rimasta vittima di una truffa, constatando l'addebito di un bonifico di Euro 17.451,00. Chiedeva quindi di bloccare l'operazione, ma le veniva comunicato che non era più possibile.

2. – Nelle controdeduzioni del 28 luglio 2025 l'intermediario resistente fa valere anzitutto la "inefficacia" del ricorso per mancanza di denuncia. Rileva quindi che il numero telefonico contattato dalla parte ricorrente non è a sé riferibile e così pure il link riportato sul messaggio di testo depositato. Fa valere che l'operazione contestata è stata autorizzata con sistema a doppio fattore e così pure l'attivazione del token mobile. Rileva infine la grave negligenza della parte ricorrente. Conclude per il rigetto del ricorso.

DIRITTO

La parte ricorrente disconosce un bonifico di Euro 17.451,00 disposto, a suo dire, il 14 novembre 2024 da ignoti truffatori. Chiede quindi che l'intermediario resistente ne rimborsi l'intero importo.

L'intermediario resistente fa valere anzitutto l'inefficacia del ricorso per mancanza di denuncia. A suo dire, infatti, la denuncia costituirebbe una condizione di procedibilità del ricorso all'Arbitro.

In realtà, nessuna delle disposizioni vigenti di Banca d'Italia che regolano il procedimento dinanzi all'Arbitro riconosce alla denuncia la rilevanza di condizione di procedibilità del ricorso che le viene invece attribuita dall'intermediario resistente. Il ricorso può dunque essere deciso nel merito.

In atti non è presente la documentazione contabile dell'operazione contestata. La sua esistenza è tuttavia pacifica tra le parti. Si tratta di un'operazione che non risulta disposta direttamente dalla parte ricorrente e, dunque, di un'operazione che può dirsi non autorizzata dall'utente. Deve perciò trovare applicazione lo speciale regime di responsabilità di cui all'art. 10 ss. del d. lgs. n. 11 del 2010, come modificato dal d. lgs. n. 218 del 2018, che ha dato attuazione nell'ordinamento italiano alla direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).

In particolare, viene in considerazione anzitutto la regola dell'art. 10, co. 1, d. lgs. n. 11 cit., in forza della quale, in caso di disconoscimento di operazioni di pagamento da parte dell'utilizzatore dei servizi di pagamento, il prestatore degli stessi servizi ha l'onere di provare che l'operazione in questione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri malfunzionamenti.

L'art. 10, co. 2, d. lgs. n. 11 cit., dispone poi che, quando l'utente di servizi di pagamento neghi di aver autorizzato una determinata operazione di pagamento, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è sufficiente a dimostrare che quell'operazione è stata autorizzata dall'utilizzatore medesimo né che questi abbia agito in modo fraudolento o non abbia adempiuto correttamente all'obbligo di utilizzare lo strumento di pagamento in conformità con i termini contrattuali che ne regolano l'emissione e l'uso, segnatamente all'obbligo di custodia dello strumento di pagamento e dei relativi codici di autenticazione e all'obbligo di sollecita comunicazione al prestatore dei servizi di pagamento del furto o dello smarrimento dello strumento di pagamento. Sempre l'art. 10, co. 2, cit., dispone poi che è onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente.

Al riguardo il Collegio di coordinamento, nella decisione n. 22745 del 2019, ha chiarito che la previsione appena indicata dell'art. 10, co. 2, sull'onere posto a carico del prestatore di servizi di pagamento della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretata nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa di per sé l'onere probatorio. Si ritiene dunque necessario che l'intermediario proceda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utilizzatore.

Secondo l'orientamento consolidato dei Collegi territoriali, in aderenza al dato normativo e ai chiarimenti interpretativi offerti dal Collegio di coordinamento, la prova di autenticazione rappresenta un prius logico rispetto alla prova della colpa grave dell'utente. Ne consegue che, solo qualora sia stato soddisfatto tale onere probatorio, il Collegio può valutare eventuali profili di responsabilità ascrivibili al cliente.

Ciò posto, nell'ordine indicato, il Collegio deve anzitutto verificare la corretta autenticazione dell'operazione contestata con sistema conforme alle discipline tecniche vigenti (c.d. Strong Customer Authentication). Si tratta in particolare di verificare se in atti risulti documentazione attestante che l'operazione contestata è stata autorizzata attraverso una procedura caratterizzata dall'impiego di due fattori distinti tra i seguenti: possesso (qualcosa che possiede solo l'utilizzatore, come un dispositivo mobile); inerenza (qualcosa che è inerente alla persona dell'utilizzatore, come l'impronta digitale o il riconoscimento facciale); conoscenza (qualcosa che solo l'utilizzatore conosce, come un codice segreto o una password).

Nel caso in esame, attraverso la produzione di opportuna documentazione informatica, l'intermediario resistente ha anzitutto provato che l'accesso al conto è avvenuto con inserimento di un codice segreto e con l'utilizzo del token mobile per la generazione di una password dinamica monouso. L'intermediario resistente ha quindi provato che anche l'operazione dispositiva è stata autorizzata attraverso l'inserimento di un codice segreto e la generazione silente di una password dinamica monouso attraverso il token mobile. In entrambi i casi, dunque, sono stati utilizzati un fattore di conoscenza e un fattore di possesso. Si tratta perciò di un sistema autorizzativo del tutto conforme alle regole della c.d. Strong Customer Authentication. Del resto, già in altre occasioni questo Collegio territoriale ha avuto modo di considerare il sistema autorizzativo in questione conforme alle regole indicate (v. Coll. Roma, dec. n. 19821 del 2021).

Quanto poi alla possibilità di riconoscere elementi di grave colpevolezza nella condotta dell'utilizzatore, nel ricorso la parte ricorrente riferisce di aver ricevuto sul proprio dispositivo mobile un messaggio di testo apparentemente proveniente dall'intermediario. In realtà, lo screenshot prodotto in atti non consente di ricavare informazioni di alcun tipo né con riferimento al mittente del messaggio né con riferimento alla data in cui è stato ricevuto. Il messaggio di testo in questione reca poi un recapito telefonico, al quale, come risulta dal registro delle chiamate prodotto, la parte ricorrente ha chiamato. Non si tratta comunque di un recapito telefonico riferibile all'intermediario.

Sulla base dei dati indicati il Collegio non ritiene che la truffa realizzata ai danni della parte ricorrente sia riconducibile a una tipologia particolarmente insidiosa, tale da far escludere la colpa grave della stessa parte ricorrente. In particolare, la documentazione relativa al messaggio di testo dal quale la truffa ha preso avvio non consente di ricondurla alla tipologia del c.d. SMS spoofing, nella quale i malviventi riescono ad alterare il mittente di un messaggio di testo, facendolo apparire come l'intermediario. Si deve dunque ritenere che la parte ricorrente sia rimasta vittima di una truffa ordinaria che ha potuto avere successo unicamente in virtù della sua condotta gravemente negligente. La domanda risarcitoria non può pertanto trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso

IL PRESIDENTE