Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore COSIMO DAMIANO FABIO MASTROROSA

Seduta del 18/02/2026

FATTO

Parte ricorrente ha adito questo Arbitro al fine di chiedere la condanna dell'intermediario al pagamento della somma di euro 1490,00 corrispondente all'importo di un bonifico on line disconosciuto.

All'uopo parte ricorrente espone di essere stata vittima di una truffa in data 8 ottobre 2025. Riferisce di aver ricevuto un SMS da un numero di cellulare, non riconducibile all'intermediario, che segnalava operazioni in corso su un conto presso altro istituto e la invitava a contattare un numero di telefono. Seguendo le indicazioni, la ricorrente chiamava il numero e veniva istruita da un sedicente operatore del servizio antifrode, il quale le rappresentava la necessità di autorizzare alcune operazioni di pagamento per sventare una truffa in atto. In buona fede, la ricorrente accedeva alla propria area riservata e disponeva un bonifico istantaneo di € 1.490,00 in favore di un terzo, nonché una ricarica sulla propria carta prepagata e poi un bonifico a favore di un terzo. Successivamente, avvedutasi dell'inganno, sporgeva denuncia e chiedeva il rimborso all'intermediario.

L'intermediario resistente, nelle controdeduzioni, eccepisce la colpa grave della cliente. Sostiene che:

- le operazioni contestate sono state regolarmente autenticate mediante un sistema di autenticazione forte (SCA) conforme alla normativa PSD2, che prevede l'inserimento delle credenziali

statiche (fattore di conoscenza) e la validazione tramite notifica push sull'app installata sul dispositivo della cliente (fattore di possesso), previa attivazione del codice P***ID;

- la ricorrente ha volontariamente fornito le proprie credenziali e ha autorizzato le operazioni, come emerge dalla documentazione tecnica (log informatici) prodotta;
- la condotta della ricorrente integra gli estremi della colpa grave, in quanto ha prestato fede a un messaggio proveniente da un numero non collegato all'intermediario di cui è cliente, ha compiuto operazioni dispositive dietro istruzione di un terzo e, soprattutto, ha autorizzato l'accesso da remoto al proprio dispositivo, consentendo ai truffatori di agire indisturbati;
- la ricorrente non ha prodotto il messaggio SMS ricevuto, né ha fornito elementi idonei a ricostruire la dinamica della frode in modo da escludere la propria negligenza.

Tanto premesso, l'intermediario chiede il rigetto del ricorso.

Nelle repliche, parte ricorrente ribadisce la propria buona fede e lamenta la mancanza di adeguate informative da parte dell'intermediario sui rischi di frode.

Nelle controrepliche, l'intermediario insiste per il rigetto, richiamando i propri precedenti argomenti e la giurisprudenza dell'ABF in materia di frodi informatiche.

DIRITTO

La controversia concerne il disconoscimento di un'operazione di pagamento online (bonifico istantaneo) e di due ricariche di carta prepagata, per un importo complessivo di € 1.490,00, asseritamente eseguite in conseguenza di una truffa (c.d. smishing).

L'art. 10, comma 1, del d.lgs. n. 11/2010 pone a carico del prestatore di servizi di pagamento l'onere di provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze di malfunzionamenti tecnici. L'art. 10, comma 2, stabilisce che l'utilizzo di uno strumento di pagamento registrato non è di per sé sufficiente a dimostrare che l'operazione sia stata autorizzata, né che l'utilizzatore abbia agito in modo fraudolento o con dolo o colpa grave.

Nel caso di specie, l'intermediario ha prodotto la documentazione tecnica (log informatici) attestante che:

- l'operazione di bonifico istantaneo è stata preceduta dall'accesso all'home banking mediante credenziali statiche (user ID e password) e dalla validazione tramite notifica push sull'app installata sul dispositivo della ricorrente, previa generazione di un codice OTP trasmesso via SMS al numero di cellulare della stessa;
- le operazioni di ricarica sono state autorizzate mediante il medesimo sistema P***ID, che integra un fattore di conoscenza (codice statico scelto dall'utente) e un fattore di possesso (il dispositivo previamente tokenizzato);
- non risultano anomalie nei sistemi informatici dell'intermediario.

Tali evidenze sono state ritenute conformi ai requisiti di autenticazione forte dalla giurisprudenza di questo Arbitro (cfr. Collegio di Roma, decisioni nn. 318/2021, 2299/2021, 12449/2023). L'intermediario ha quindi assolto all'onere probatorio su di esso gravante, dimostrando la regolare autenticazione delle operazioni.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Ciò posto, occorre valutare la condotta della ricorrente al fine di stabilire se la stessa abbia agito con dolo o colpa grave, circostanza che, ai sensi dell'art. 12, comma 3, del d.lgs. n. 11/2010, esclude il diritto al rimborso.

Dalla denuncia prodotta in atti e dalle dichiarazioni della ricorrente emerge che:

- la stessa ha ricevuto un SMS da un numero di cellulare (quindi non riconducibile all'intermediario) che la invitava a contattare un numero per sventare una presunta frode;
- ha chiamato tale numero e si è lasciata istruire da un finto operatore;
- su indicazione del truffatore, ha autorizzato l'accesso da remoto al proprio dispositivo (come si evince dal riferimento all'installazione di un'app o alla concessione del controllo);
- ha quindi disposto le operazioni contestate, nonostante queste riguardassero un bonifico verso un terzo sconosciuto e ricariche della propria carta, in un contesto del tutto anomalo.

La giurisprudenza di questo Arbitro è costante nel ritenere gravemente colposa la condotta dell'utente che, su indicazione di un sedicente operatore, autorizzi l'accesso da remoto al proprio dispositivo e compia operazioni di pagamento, in quanto tale comportamento vanifica i presidi di sicurezza adottati dall'intermediario e costituisce violazione degli obblighi di diligenza nella custodia delle credenziali e nella gestione dello strumento di pagamento (cfr. Collegio di Roma, decisioni nn. 4317/2024, 7806/2023). In tali ipotesi, l'utente non può addossare all'intermediario le conseguenze di una frode resa possibile dalla propria ingenuità o negligenza.

Ulteriore elemento rilevante è la mancata produzione del messaggio SMS ricevuto. Secondo il consolidato orientamento dell'ABF, l'omessa produzione del messaggio "esca" costituisce un indice di colpa grave, in quanto impedisce di valutare l'affidamento che l'utente avrebbe potuto riporni e la sussistenza di eventuali elementi che avrebbero dovuto insospettirlo (cfr. Collegio di Roma, decisione n. 3032/2023). La ricorrente non ha fornito alcuna giustificazione per tale omissione, limitandosi a descrivere il contenuto del messaggio.

Alla luce di quanto precede, deve ritenersi che la ricorrente abbia tenuto una condotta gravemente colposa, che ha consentito ai truffatori di eseguire le operazioni contestate. Non sussistono, pertanto, i presupposti per la condanna richiesta.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE