

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 05/02/2026

FATTO

La ricorrente, in qualità di delegata ad operare sui conti correnti n. *283 e n. *278, intestati rispettivamente ai suoi genitori, ha presentato ricorso a questo Arbitro per ottenere il rimborso di due operazioni di bonifico istantaneo, per un importo complessivo di € 4.000,00, da lei disposte in data 21.03.2025 a seguito di una complessa frode informatica riconducibile a tecniche di “vishing” e “smishing/spoofing”. La ricorrente espone di aver ricevuto una telefonata apparentemente proveniente dall'intermediario, che la induceva in errore e la portava a eseguire le operazioni contestate, credendo di agire per bloccare tentativi di frode sulla propria carta di credito. Sostiene di aver agito in buona fede, facendo affidamento sulla provenienza della chiamata e degli SMS dai canali ufficiali della banca, e che pertanto nessuna colpa grave possa esserle imputata. Tutto ciò premesso, la ricorrente chiede che l'intermediario sia dichiarato tenuto a corrisponderle l'importo di € 4.000,00.

L'intermediario si è costituito in giudizio con controdeduzioni, rilevando che la somma oggetto di disconoscimento ammonta a € 4.420,00 (due bonifici istantanei) e non all'importo indicato dalla ricorrente. Nel merito, l'intermediario ha sostenuto che il perfezionamento della truffa è stato reso possibile unicamente dalla "colpevole collaborazione" della ricorrente, la quale ha personalmente eseguito le operazioni. Secondo la ricostruzione dell'intermediario, la frode si è svolta secondo una precisa dinamica: un sedicente operatore bancario avrebbe contattato la ricorrente informandola di un presunto movimento fraudolento sulla sua carta di credito personale (*650); a seguito di ciò, la

ricorrente, anziché contattare i canali ufficiali della banca, avrebbe proseguito la conversazione, cliccato su un link ricevuto via SMS e inserito le proprie credenziali di internet banking in una pagina contraffatta. A quel punto, senza porsi alcun dubbio circa l'inverosimiglianza della procedura richiesta rispetto alla finalità antifrode dichiarata, avrebbe disposto personalmente i due bonifici istantanei oggi contestati. L'intermediario sottolinea che le operazioni sono state autorizzate con tutti i fattori di autenticazione forte (SCA) e che la ricorrente non ha prodotto alcuna evidenza documentale né della chiamata telefonica ricevuta né della conversazione SMS integrale, in particolare del messaggio contenente il link malevolo. Evidenzia inoltre plurimi indici di anomalia che avrebbero dovuto allertare la cliente, quali il fatto che il numero chiamante fosse quello predisposto per le chiamate dall'estero e che i bonifici fossero diretti verso IBAN palesemente non italiani. Solo dopo aver eseguito le disposizioni ed essere stata rassicurata dal truffatore, la ricorrente avrebbe contattato il servizio antifrode della banca, che ha provveduto al blocco dei servizi. Tutto ciò premesso, l'intermediario chiede che il ricorso sia rigettato, in quanto infondato.

Nelle proprie repliche, la ricorrente ha ribadito la propria versione dei fatti, precisando che l'importo sottratto sarebbe di € 2.100,00 da ciascun conto, per un totale di € 4.200,00. Ha inoltre introdotto nuovi elementi, sostenendo che la telefonata e gli SMS provenivano dal canale internet della banca, che, a dire del direttore della filiale, sarebbe stato oggetto di un "bypass" mediante sistemi di frode informatica. A riprova di una presunta falla nei sistemi dell'intermediario, ha evidenziato che il sedicente operatore era a conoscenza del suo codice cliente e delle lettere iniziale e finale della sua password, prefigurando una violazione della privacy. La ricorrente insiste quindi per l'accoglimento del ricorso, elevando la propria domanda risarcitoria a € 4.200,00.

L'intermediario, in sede di controrepliche, ha contestato l'ammissibilità delle nuove allegazioni relative alla violazione della privacy e in materia di cybersicurezza, qualificandole come domanda nuova. Ha negato recisamente che il direttore di filiale abbia mai ammesso un "bypass" dei sistemi informatici e ha evidenziato l'incompletezza degli screenshot prodotti dalla ricorrente, dai quali mancherebbe proprio il messaggio contenente il link malevolo. Ha ribadito la mancanza di prova della chiamata telefonica e la presenza di anomalie evidenti anche nei pochi SMS prodotti, confermando che le operazioni sono state eseguite integralmente dalla cliente, seppur tratta in inganno. L'intermediario insiste quindi per il rigetto del ricorso.

Dalla documentazione in atti, nonché dalle stesse dichiarazioni rese dalla ricorrente nel reclamo, nel ricorso e nelle repliche, emerge che le operazioni contestate sono state disposte mediante accesso al servizio di internet banking a lei intestato e associate ai conti sui quali era delegata, con inserimento delle credenziali di accesso e successiva autorizzazione dei bonifici istantanei attraverso i presidi di sicurezza previsti dall'intermediario.

In simili ipotesi, secondo l'orientamento consolidato dei Collegi, quando l'operazione è eseguita per intero dal cliente – anche se indotto in errore da artifici e raggiri di terzi – essa deve qualificarsi come autorizzata ai sensi dell'art. 5 del d.lgs. n. 11/2010. Ne consegue che non trova applicazione la disciplina speciale prevista dalla direttiva (UE) 2015/2366 (PSD2) e dagli artt. 10 e ss. del d.lgs. n. 11/2010 in materia di operazioni non autorizzate, con esclusione del regime di responsabilità oggettiva dell'intermediario.

Neppure risultano nel caso di specie elementi idonei a configurare una responsabilità concorrente dell'intermediario ai sensi delle regole di diritto comune, le quali impongono all'intermediario un obbligo di diligenza professionale nella prestazione dei propri servizi bancari. Non emerge, infatti, alcuna prova di malfunzionamenti dei sistemi, di indisponibilità dei canali ufficiali o di omissioni nella gestione della segnalazione. Le allegazioni relative a un presunto “bypass” dei sistemi informatici non risultano supportate da evidenze documentali e appaiono, peraltro, introdotte solo in sede di repliche. Parimenti, la ricorrente non ha prodotto la conversazione SMS integrale né prova della chiamata asseritamente ricevuta, sicché non è possibile verificare la concreta idoneità delle comunicazioni a generare un legittimo affidamento. Infine, le operazioni si presentavano, sotto il profilo tecnico, formalmente regolari e correttamente autenticate, senza indici macroscopici di anomalia tali da imporre all'intermediario un blocco preventivo delle disposizioni.

Alla luce di tutte le considerazioni che precedono, il ricorso deve essere respinto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE