

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) ABATE	Membro di designazione rappresentativa dei clienti

Relatore (MI) ABATE

Seduta del 29/01/2026

FATTO

La cliente afferma quanto segue:

- dal 19/09/2018 è titolare del conto corrente n. *599 acceso presso l'intermediario convenuto, con operatività di home banking;
- in data 14/04/2025, alle ore 19:49, il legale rappresentante della società ricorrente riceveva un sms apparentemente proveniente dall'intermediario, che avvisava di un movimento sospetto in c/c, comunicando un numero da contattare;
- contattato il numero indicato, l'interlocutore (qualificatosi come sig. SB, operatore dell'intermediario) informava della presenza di 3 bonifici sospetti in uscita, ciascuno di importo pari a 4.900,00 €;

- per bloccare tali movimenti il cliente seguiva le istruzioni del sedicente operatore, eseguendo un accesso “urgente” al proprio conto, digitando nel browser l'indirizzo al portale di home banking e inserendo le credenziali di accesso,
- si trovava così davanti alla schermata dei movimenti del conto, in cui apparivano i movimenti comunicati dal sedicente operatore;
- continuando a seguire le istruzioni dettate dall'operatore, il cliente tentava di cancellare le disposizioni sospette senza successo;
- l'operatore comunicava quindi che avrebbe riferito l'accaduto al suo superiore, che lo avrebbe richiamato per fornire assistenza e risolvere il problema;
- entro breve tempo il cliente riceveva effettivamente una seconda chiamata da un sedicente operatore dell'ufficio antifrode dell'intermediario, tale sig. GD il quale lo induceva con l'inganno a eseguire un bonifico di importo di 28.900,00 €, previa concessione di controllo remoto del pc;
- il messaggio civetta e il numero telefonico di provenienza della chiamata apparivano come genuini;
- in data 15 aprile 2025, intorno alle ore 15:00 prima del cd. cutoff, insospettitosi, il cliente si recava fisicamente presso l'intermediario, appurando la truffa e richiamando il bonifico con successo;
- il direttore di filiale confermava che il bonifico era stato segnalato come potenzialmente truffaldino dal sistema e di essere in contatto con l'ufficio antifrode del PSP ricevente;
- al momento della segnalazione il bonifico si trovava nella disponibilità della banca;
- in seguito, il cliente veniva invitato ad attendere il buon esito della procedura di richiamo del bonifico e a sporgere denuncia del fatto;
- con mail del 30 aprile 2025 l'intermediario comunicava che, dall'importo del bonifico, 14.000,00 € risultano bloccati temporaneamente sul conto di destinazione a seguito di un sequestro giudiziario, circostanza del tutto inattesa;
- in data 14 maggio 2025 è stato presentato reclamo, respinto adducendo un comportamento inerte del cliente il quale, al contrario, si è dimostrato tempestivo nell'attivarsi prontamente con la richiesta di recall;
- l'intermediario avrebbe dovuto bloccare il bonifico;
- non è chiaro il motivo per cui l'intermediario ricevente abbia bloccato solamente una parte dell'importo del bonifico;

- la banca ha omesso di attivare tempestivamente le misure tecniche di sicurezza necessarie e si è rifiutata di intervenire successivamente, pure avendo il tempo tecnico per farlo, aggirando il blocco automatico del bonifico;
- come confermato da una perizia eseguita per incarico del cliente, questo è stato oggetto di un sofisticato attacco complesso di smishing, vishing spoofing e di Man in the browser;
- dalla perizia sono emersi accessi abusivi al conto del cliente, ad opera dei terzi truffaldini e l'esecuzione di un ulteriore bonifico non autentico, oltre alla presenza di malware;
- il cliente è stato dunque vittima di una truffa sofisticata, nessun profilo di dolo o colpa grave è in alcun modo riconducibile alla condotta del cliente;
- il bonifico presentava caratteristiche di anomalia, rispetto allo storico del cliente per importo, per la causale e il destinatario non usuale;
- secondo l'ABF è dovuto il risarcimento per truffe come quella in esame, eseguite senza colpa del cliente tramite insidiosi programmi silenti di tipo malware;
- il risarcimento è dovuto anche ai sensi della normativa di riferimento, D.lgs. n. 11/2010, tenuto conto della condotta dell'intermediario;
- il mancato rimborso integra responsabilità contrattuale in capo all'intermediario, con un danno pari a 28.900,00 e danno non patrimoniale ex art. 2059 c.c. da liquidare in via equitativa (cfr. ABF, Bari 27/2025) ex art. 1224 cod. civ. o anche in via presuntiva, cfr. Cass. n.19499/2008.

La ricorrente chiede di accertare la responsabilità dell'intermediario e di condannare il medesimo al rimborso di euro 28.900 oltre interessi oltre al risarcimento di danni non patrimoniali e al pagamento delle spese legali.

L'intermediario, riportato il fatto, afferma quanto segue:

- Il ricorrente richiede alla banca il rimborso di 28.900,00 € relativi a un bonifico ordinario disposto il 14.4.2025, autorizzato dal cliente con autenticazione forte, revocabile ma non revocato entro le ore 20.00 dello stesso giorno;
- la domanda è infondata e carente di una chiara esposizione dei fatti;
- la denuncia è stata presentata solo il 29.4.2025, oltre dieci giorni dopo l'evento;
- il cliente ha parlato genericamente di un accesso abusivo al sistema informatico della società, versione non coerente con quanto riferito successivamente al call center della banca;

- il 14.4.2025 alle ore 16.59 il cliente ha ricevuto un SMS phishing, non riconducibile alla banca, con testo sgrammaticato e privo di indicazioni specifiche sull'operazione sospetta, quindi con evidenti elementi di inattendibilità facilmente riconoscibili con l'ordinaria diligenza;
- il cliente, invece di contattare il numero verde della banca o verificare l'operatività tramite app, ha chiamato il numero indicato nel messaggio fraudolento e, su indicazione del truffatore, comunicato codici riservati e disposto il bonifico;
- il cliente si era già collegato all'home banking tra le ore 17.06 e le 17.40, per verificare l'assenza di movimenti sospetti, disponendo comunque il bonifico alle 19.48 (previo accesso alle 19.44) verso un IBAN sconosciuto con autenticazione forte;
- non sono state riscontrate violazioni dei sistemi della banca e l'operazione risulta eseguita dal cliente tramite un dispositivo abituale;
- la banca ha inviato notifica dell'esecuzione del bonifico all'utenza cellulare del cliente;
- il cliente non ha revocato il bonifico entro il cut off e ha contattato l'intermediario solo il 15.4.2025 alle ore 15.37, quando il bonifico era ormai irrevocabile;
- la banca si è attivata tempestivamente per il recall del bonifico e per fornire indicazioni al cliente sul recupero delle somme;
- la banca beneficiaria ha bloccato solo una parte dell'importo, pari a euro 13.995,94, in attesa di una denuncia formale con richiesta di sequestro;
- al cliente è stato più volte comunicato di presentare una denuncia completa di istanza di sequestro presso l'Autorità di P.S., ma ciò non è mai avvenuto compromettendo le possibilità di recupero delle somme eventualmente ancora disponibili;
- l'ABF esclude il rimborso quando le operazioni sono state autorizzate personalmente dal cliente, anche se indotto in errore da terzi;
- le richieste di risarcimento per danni non patrimoniali sono generiche e prive di prova;
- non sussistono i presupposti per la rifusione delle spese legali, non previste dalla normativa ABF e già escluse dalla giurisprudenza dell'Arbitro.

L'Intermediario chiede il rigetto del ricorso

Con le repliche il cliente ribadisce argomentazioni del ricorso e deduce inoltre che:

- il cliente è stato vittima di un attacco informatico sofisticato di tipo Man-in-the-Browser (MitB), combinato con tecniche di smishing, vishing e social engineering, confermato da perizia forense che ha

rilevato un file Trojan nel pc del cliente creato il giorno dell'evento, il quale ha permesso la manipolazione delle transazioni bancarie;

- l'operazione di € 28.900,00 è stata effettuata con consenso indotto tramite artifici e raggiri, facendo credere al cliente di bloccare un'operazione sospetta;
- l'autenticazione forte non ha impedito la frode, poiché il malware ha manipolato i dati della transazione in tempo reale;
- i log di navigazione evidenziano digitazioni assenti sulla tastiera del cliente e reindirizzamenti permanenti, segni di un attacco MitB;
- è stato disposto anche un ulteriore bonifico di € 14.900,00 verso la società O* S.r.l., sempre tramite manipolazione remota;
- l'autenticazione forte adottata dall'intermediario non garantisce sicurezza in caso di accesso abusivo alla pagina dispositiva, come avvenuto nella frode in esame;
- la banca ha ignorato un alert di sospetta frode e ha consentito l'operazione senza spiegazioni, violando protocolli di sicurezza e obblighi di diligenza;
- la segnalazione del cliente è stata tempestiva (15 aprile 2025), prima della valuta di accredito e ha tentato tempestivamente di presentare denuncia, bloccando il conto dal 15 aprile al 1° maggio per prevenire ulteriori frodi;
- la banca non ha attivato procedure di richiamo del bonifico nonostante la segnalazione di frode e ha fornito indicazioni errate sulla necessità di sequestro giudiziario;
- Il cliente ha successivamente integrato la querela e richiesto il sequestro preventivo alla Procura .

Il ricorrente insiste nelle richieste.

L'intermediario ribadisce argomentazioni delle controdeduzioni e deduce inoltre che:

- Il bonifico ordinario, che il cliente avrebbe potuto revocare entro le ore 20.00 del cut off serale, è stato pacificamente disposto personalmente dal titolare dell'azienda ricorrente;
- il contenuto della denuncia è confessorio della negligenza del cliente;
- i fatti si sono svolti come narrati al contact center dell'intermediario in data 15.4.2025: il cliente afferma di aver ricevuto un messaggio e di aver fornito i codici di accesso all'interlocutore (cfr. decisione n. 3569/25 del Collegio di Palermo);
- la perizia, inutile nel caso in esame, non evidenzia alcuna anomalia o intromissione nei sistemi della banca ma solo nel computer del ricorrente;

- Il servizio home banking messo a disposizione dalla Banca adotta un sistema di sicurezza rafforzato, finalizzato a rendere massima la protezione dell'utente, salva sua comunicazione a terzi dei codici di accesso;
- la rifusione delle spese legali non è dovuta.

L'intermediario insiste nella richiesta di rigetto.

DIRITTO

Il ricorrente richiede alla banca il rimborso di € 28.900 relativi a un bonifico ordinario disposto il 14.4.2025, autorizzato dal cliente in seguito ad una truffa subita da un soggetto terzo. Alla data delle operazioni trovava applicazione il d.lgs. 27 gennaio 2010, n. 11 come modificato dal d.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018. Pur essendo l'operazione posta in essere parzialmente dal cliente, si impone la verifica dell'autenticazione forte. Ebbene, sulla base delle evidenze in atti si osserva quanto segue: (i) è presente il riferimento al *token* Vasco, che secondo quanto sopra visto risulta essere un *token* fisico quale elemento di possesso; (ii) è presente un riferimento a "*controllopinmapellum*" che, come da legenda esplicativa in atti, implica l'inserimento del PIN. Ebbene, in linea con le pronunce del Collegio di Milano (decisione n. 7564/25 del 31/07/2025) e a Coll. Bologna n. 10226/2025, si ritiene provata l'autenticazione conforme a SCA, circostanza peraltro confermata anche da parte ricorrente in sede di replica.

Sulla base delle evidenze prodotte risulta provata la grave negligenza di parte ricorrente non consumatrice, nonché l'assenza di elementi idonei a riconoscere un concorso di colpa dell'intermediario nella truffa, tenuto conto che:

- la denominazione della *chat* in cui è inserito il messaggio ("verifica") è chiaramente non riferibile all'intermediario, la cui denominazione compare invece nel testo del messaggio stesso;
- nella medesima *chat* non sono presenti messaggi genuini dell'intermediario antecedenti o successivi a quello civetta;
- il messaggio contiene alcuni errori di punteggiatura;
- Il cliente dichiara di avere contattato un numero fisso che, dalle verifiche svolte, non corrisponde ad alcun contatto ufficiale dell'intermediario;

- Inoltre, nella denuncia, predisposta tardivamente, il cliente dichiara di avere consentito che il truffatore prendesse il controllo da remoto del pc, consentendogli così di eseguire le operazioni oggi contestate.

Ne consegue il rigetto di tutte le domande formulate da parte ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE