

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) ABATE	Membro di designazione rappresentativa dei clienti

Relatore (MI) ABATE

Seduta del 08/09/2026

FATTO

La parte ricorrente afferma quanto segue:

- in data 24/10/2025 la Sig.ra S., impiegata presso la società ricorrente e correntista della Banca convenuta, riceveva un SMS sul proprio dispositivo personale apparentemente proveniente da un intermediario bancario, diverso dal convenuto;
- con il suddetto sms le veniva comunicato che sul suo conto corrente era stata eseguita un'operazione di € 256,00;
- allarmata dall'SMS, la signora chiamava il numero indicato nel messaggio stesso, per bloccare l'operazione, ma non otteneva risposta;
- veniva quindi immediatamente contattata, con un diverso numero, da un soggetto che si identificava come operatore "antifrode" della Banca convenuta e su indicazione del sedicente operatore, al fine di bloccare il pagamento sconosciuto, la signora procedeva a comunicare le credenziali di accesso al proprio conto corrente;
- successivamente, sempre su richiesta dell'operatore, la signora comunicava di avere accesso anche al conto bancario della società ricorrente;
- le veniva perciò intimato di comunicare i dati anche di questo conto corrente, per metterlo in sicurezza da eventuali attacchi informatici;

- vista la ritrosia della signora nel comunicare i dati, l'operatore la rassicurava, dicendole che sarebbe stata contattata dalla filiale per confermare la correttezza della procedura;
- subito dopo, la signora riceveva una chiamata dall'utenza fissa ***35, riconducibile all'intermediario e, rassicurata dalla provenienza apparentemente sicura dell'utenza, rispondeva;
- durante la chiamata un operatore della Banca la rassicurava sulla regolarità delle attività in svolgimento e di seguire le indicazioni fornitele per telefono;
- a questo punto, la signora si accorgeva della disposizione di n. 6 bonifici in uscita sul conto della società, ma l'operatore la rassicurava sul futuro riaccredito delle somme sottratte;
- si avvedeva quindi di essere stata vittima di una truffa e contattava il numero verde della Banca per bloccare il conto corrente;
- si recava immediatamente presso le Autorità competenti per sporgere denuncia, insieme con il Sig. S., rappresentante legale della società ricorrente;
- presentava reclamo all'intermediario in data 09/12/2025, che veniva riscontrato negativamente. Parte ricorrente chiede la restituzione di € 49.997,96 oltre interessi e spese legali.

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

- la Sig.ra S., dipendente della società ricorrente, è stata vittima di una truffa riconducibile alle tipologie note dello smishing/ vishing;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- sussiste la colpa grave della dipendente in quanto forniva, seppure inconsapevolmente, accesso a terzi sconosciuti al conto della società;
- in particolare, non solo forniva i dati di accesso al conto, ma consentiva al soggetto terzo il controllo da remoto del proprio dispositivo, tramite l'applicativo di "Assistenza Remota", garantendo così l'accesso ai sistemi della Banca tramite l'IP della società cliente;
- il soggetto terzo ha potuto quindi agire indisturbato, inserendo nella Rubrica i dati dei beneficiari, operazione necessaria per la disposizione dei bonifici, e inserire la richiesta di pagamento degli stessi;
- la ricostruzione dei fatti fornita da parte ricorrente è contraddittoria e non coerente nelle diverse fasi del procedimento, in quanto:
 - nella denuncia afferma che la truffa avrebbe avuto inizio da un sms riconducibile a un diverso intermediario e, comunque, il suddetto messaggio non è mai stato prodotto in atti;
 - in sede di reclamo ribadisce i fatti come riportati nella denuncia. Solo in fase di ricorso presso quest'Arbitro aggiunge un elemento fattuale, riferendo di una chiamata proveniente da un numero apparentemente riconducibile alla Banca, della durata di soli 11 secondi, allegando evidenze mai fornite prima;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici;
- la parte ricorrente, dopo aver commissionato un'analisi tecnica del PC aziendale, omette di produrre o anche solo menzionare tale elaborato tecnico, che esclude intrusioni da parte di terzi o anomalie informatiche dei software aziendali e che viene versato in atti da parte resistente;

- non sussistono, nel caso di specie, elementi sufficienti a integrare indici di anomalia/rischio tali da giustificare il blocco preventivo delle operazioni.

L'intermediario chiede il rigetto del ricorso.

La società cliente, richiamati i propri scritti, replica che:

- diversamente da quanto affermato dall'intermediario, la fattispecie in esame non può essere qualificata come semplice vishing, rientrando invece nella categoria dello spoofing ID caller;
- la dipendente, infatti, collaborava con i truffatori in quanto convinta di parlare con un operatore della Banca, ingannata dalla manipolazione dell'utenza telefonica comparsa sul dispositivo;
- la ricostruzione dei fatti non è affatto contraddittoria, in quanto l'sms iniziale è da considerarsi del tutto irrilevante ai fini del completamento della truffa, attuata con la successiva telefonata;
- la documentazione tecnica informatica richiamata dalla controparte dimostra che la sig.ra S. ha adottato tutte le misure di sicurezza esigibili, ma veniva tratta in inganno con azioni d'ingegneria sociale resa possibile dalla vulnerabilità dei canali comunicativi della Banca;
- in merito alla violazione degli obblighi di monitoraggio, le argomentazioni di controparte risultano deboli, in quanto l'esecuzione di sei operazioni in un tempo brevissimo (20 minuti) e per importi molto elevati, verso beneficiari persone fisiche mai censiti in precedenza, costituiscono anomalie tali per cui la Banca si sarebbe dovuta attivare a tutela della cliente.

L'intermediario, riportandosi alle conclusioni in atti, controreplica che:

- lo *screenshot* prodotto in atti da parte ricorrente dimostra unicamente la visualizzazione del numero sul *display*, senza la possibilità di attribuire la chiamata ai sistemi della Banca;
- la chiamata, di appena 11 secondi, non è idonea a giustificare la disposizione delle operazioni contestate, autorizzate nell'arco di circa 20 minuti;
- la dipendente, dopo aver sperimentato un'operatività anomala sul proprio conto personale, perseverava nella condotta imprudente, esponendo il conto della società all'uso fraudolento;
- i riferimenti agli obblighi antiriciclaggio e di segnalazione SOS risultano estranei alla materia del contendere, in quanto le operazioni venivano correttamente autorizzate tramite il dispositivo della dipendente e le richieste partivano da un indirizzo IP storicamente utilizzato dalla società.

DIRITTO

Oggetto di contestazione sono n. 6 operazioni da complessivi € 49.997,96 avvenute nell'arco di venti minuti. 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. Come evidenziato anche dall'intermediario nelle controdeduzioni, la denuncia presenta alcune differenze nella qualificazione dei fatti rispetto al ricorso, in particolare:

- non è menzionata la chiamata proveniente dal numero fisso ***35, riconducibile alla Banca, che avrebbe creato l'affidamento della cliente;

- la ricostruzione cronologica delle operazioni fraudolente non sembrerebbe corretta. Secondo la ricostruzione fornita nella denuncia, il pagamento effettuato dal conto della Sig.ra S veniva effettuato alle 17.44, mentre l'ultimo bonifico in uscita dal conto della società risulta effettuato alle 17.41. Da evidenze prodotte in atti la chiamata al numero verde sembrerebbe essere stata effettuata intorno alle 17:42.

Dalle dichiarazioni rese dalla cliente nel ricorso risulta che, nella convinzione di attuare operazioni volte al blocco di pagamenti fraudolenti, la stessa autorizzava da app i bonifici disposti dai truffatori tramite *homebanking*. Secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo debba essere prestato nella forma convenuta tra il pagatore stesso e il PSP. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.Lgs. 11/2010. Pertanto, si procederà di seguito ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010. In merito all'autenticazione forte, con riferimento alla fase di accesso all'*homebanking*, come affermato dall'intermediario e sulla base delle evidenze prodotte, risulta che i fattori di autenticazione siano:

- fattore di conoscenza: corretto inserimento del codice cliente e della password;
- fattore di possesso e conoscenza: ricezione di una notifica push sull'app, autorizzata mediante PIN.

Con riferimento alla prova della SCA relativamente alle operazioni di bonifico, sulla base delle evidenze prodotte e sopra riportate risulta che l'operazione è stata autenticata tramite:

- notifica push, inviata sull'app della cliente (fattore di possesso);
- inserimento del PIN di 6 cifre, scelto in fase di enrollment (fattore di conoscenza).

Risulta quindi provata la SCA sia con riferimento alla fase di accesso sia con riguardo all'inserimento delle operazioni di bonifico.

Sulla base delle evidenze prodotte risulta che:

- nessuno dei due numeri presenti nel messaggio è riconducibile all'intermediario convenuto, né tantomeno a quello individuato nel messaggio;
- il messaggio non si inserisce in nessuna conversazione tra la cliente e la Banca;
- il numero di carta su cui sarebbe stato addebitato il pagamento è interamente oscurato e non può, perciò, essere ricondotto ad alcuno strumento detenuto dalla dipendente;
- inserendo il numero su un motore di ricerca online, si trovano segnalazioni dello stesso come utenza telefonica usata per truffe, più nello specifico per frodi legate al sistema di pagamento, come nel caso di specie.

D'altro canto però, ferma la colpa grave della ricorrente, si rinvencono elementi di anomalia in quanto risultano effettuati, nell'arco di 21 minuti, n. 6 bonifici, per il considerevole importo complessivo di € 49.997,96, con beneficiari persone fisiche aggiunte alla rubrica dell'utente minuti prima di disporre il pagamento. Inoltre, Parte ricorrente insiste nell'evidenziare l'anomalia, per un conto societario usato per pagare i fornitori, di effettuare operazioni con questi importi nei confronti di persone fisiche. Alla

luce di quanto precede, si rinviene dunque un concorso colposo dell'intermediario che può essere quantificato in un un terzo rispetto alla somma complessiva oggetto di frode. Non si rinvencono invece i presupposti per accogliere la richiesta di restituzione delle spese legali.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 16.666,00, oltre interessi legali dal reclamo al saldo.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE