

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) RIZZO	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) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) GILIBERTI

Seduta del 07/05/2026

FATTO

Parte ricorrente, nel proprio ricorso, afferma che:

- si è verificato un utilizzo fraudolento dei propri strumenti di pagamento;
- non ha mai effettuato i bonifici disconosciuti.

Pertanto, chiede il rimborso di € 6.223,00 oltre interessi.

L'intermediario resistente, nel respingere l'avversa pretesa, sostiene che:

- il ricorso è inammissibile per genericità e indeterminatezza, mancando qualsiasi informazione utile alla ricostruzione dell'accaduto;
- nel ricorso la cliente disconosce operazioni di bonifico per un totale di € 6.223,10, senza specificare a quali disposizioni faccia riferimento;
- il ricorso deve consentire una chiara individuazione del *petitum* e della *causa petendi*, non potendo l'ABF essere chiamato a svolgere un'attività di ricostruzione e integrazione delle allegazioni di parte;

- dall'esame della denuncia è dato supporre che l'odierna controversia abbia ad oggetto il disconoscimento di 8 operazioni di bonifico istantaneo addebitate sul conto corrente della cliente n. 808;
- in particolare,
 - 1) 6 operazioni sono state eseguite in data 28/08/2025, di cui:
 - a) 4 tramite app (tutte a favore di G*B* iban *900);
 - b) 2 tramite contatto al banking center (una a favore di G*B* iban *900, l'altra a favore di A*E*C* iban *454);
 - 2) 2 operazioni sono state eseguite in data 02/09/2025 tramite app (una a favore di F*C* iban *687, l'altra a favore di M*G*M* iban *884);
- per quanto riguarda le operazioni di bonifico istantaneo eseguite tramite home banking, la cliente ha fatto accesso all'app mediante inserimento di codice cliente e primo codice segreto; il codice bmed veniva generato in modo silente dal mobile token e il login di terzo livello (codice OTP/notifica push) veniva convalidato mediante access token; le operazioni venivano autorizzate mediante codice segreto e codice bmed generato dal mobile token;
- gli ordini di bonifico sono stati inseriti con il *device* ordinariamente utilizzato dalla cliente, certificato ben due anni prima, in data 05/07/2023;
- ha fornito tempestiva conferma dell'esecuzione delle operazioni mediante sms alert;
- in occasione della navigazione del 28/08/2025 sono presenti 2 tentativi di disposizione di bonifici (una a favore di G*B* iban *900, l'altra a favore di A*E*C* iban *454) non andate a buon fine, in quanto bloccati dal proprio motore antifrode e successivamente eseguiti telefonicamente;
- la cliente, in ragione dell'impossibilità di disporre tali operazioni in autonomia in ragione del blocco apposto, ha contattato il banking center per procedere telefonicamente;
- con riferimento a tali due operazioni, il contatto telefonico proveniva dal recapito riferibile alla ricorrente n. *988 e censito nella propria anagrafica; le operazioni sono state autorizzate previa verifica del numero telefonico censito e certificato del chiamante e mediante inserimento di due cifre del primo codice segreto e due cifre del secondo codice segreto;
- gli ordini di bonifico disposti, come nel caso in esame, via telefono tramite soluzioni di *Interactive Voice Response (IVR)* non rientrano nell'ambito di applicazione degli obblighi di SCA di cui alla PSD2 (come chiarito nel considerando 95);
- cita la decisione del Collegio di Milano n. 436 del 20/01/2026;
- la cliente non ha fornito, sia in sede di ricorso che di denuncia, informazioni idonee alla ricostruzione dell'accaduto;
- la volontà della cliente di disporre taluni dei bonifici contestati è stata dalla stessa espressamente dichiarata anche in occasione dei contatti telefonici intervenuti con un operatore del proprio ufficio sicurezza, che ha provveduto a contattarla direttamente;
- riporta alcuni stralci delle telefonate intercorse con la ricorrente;
- nel corso di tali contatti telefonici gli operatori hanno richiesto più volte alla ricorrente se fosse stata indotta da terzi ad effettuare le operazioni contestate o avesse ricevuto telefonate da terzi e la stessa ha confermato in modo inequivocabile la propria volontà di disporre i bonifici;

- dall'ascolto delle registrazioni delle chiamate la voce della cliente risulterebbe essere sempre la medesima, anche in confronto con la telefonata in occasione della quale la stessa ha formalizzato il disconoscimento;
- nelle medesime date delle telefonate sopra richiamate, si riscontrano ulteriori contatti telefonici, in occasione dei quali sono state richieste informazioni e disposizioni da parte della cliente, riguardanti differenti operazioni non disconosciute dalla stessa;
- in occasione del contatto telefonico del 03/09/2025, durante il quale la cliente ha disconosciuto i bonifici oggetto del presente ricorso, la stessa ha dichiarato di riconoscere e ritenere valido un bonifico di € 12,00 del 02/09/2025 eseguito dal medesimo *device* dal quale sono state effettuate le operazioni disconosciute;
- a differenza di quanto dichiarato dalla cliente nella denuncia, il contatto per il disconoscimento è avvenuto il 03/09/2025 e non il 02/09/2025;
- alcuna omissione o negligenza può essere imputabile allo stesso, non sussistendo elementi tali da far generare dubbi sulla genuinità delle operazioni contestate.

Nelle repliche la ricorrente chiarisce quanto di seguito:

- non conosce i destinatari dei bonifici e non ha effettuato alcuna chiamata per effettuare i bonifici;
- il 02/09/2025 ha terminato il turno lavorativo notturno alle 6:00 di mattina e ha dormito tutto il giorno;
- il giorno successivo, 03/09/2025, ha sporto denuncia e presentato il disconoscimento.

L'intermediario controreplica che:

- la ricorrente afferma di non aver effettuato alcuna chiamata in data 02/09/2025, avendo dormito tutto il giorno dopo un turno di lavoro notturno durato sino alle 6:00 del mattino, ma l'affermazione non coglie nel segno, in quanto i contatti telefonici in occasione dei quali sono stati disposti i bonifici sono stati effettuati in data 28/08/2025;
- la cliente non ha mai segnalato o denunciato lo smarrimento del proprio *device* o la sottrazione dei propri codici.

DIRITTO

In via preliminare, sulla contestata inammissibilità del ricorso per genericità, il Collegio osserva che benché la parte ricorrente non circostanzi in alcun modo la dinamica della truffa (limitandosi ad affermare che ignoti hanno indebitamente eseguito dal proprio conto corrente bonifici per complessivi € 6.223,10), il ricorso consente di individuare chiaramente sia *petitum* che *causa petendi*.

In particolare, con il ricorso si chiede il rimborso delle operazioni fraudolente e contestate, per complessivi € 6.223,10, oltre interessi, si allega la denuncia, e vengono dettagliate le date e gli importi dei bonifici fraudolenti, con relativo disconoscimento di tali operazioni.

Nel merito, dunque, si osserva che il ricorso ha ad oggetto n. 8 operazioni contestate, e nel dettaglio di bonifici istantanei, per un importo complessivo di € 6.223,10, di cui n. 6 eseguite il giorno 28.08.2025 e n. 2 il giorno 2.9.2025.

Nella denuncia la cliente non descrive lo svolgimento della truffa, limitandosi ad affermare quanto segue:

- ignoti hanno indebitamente fatto accesso al proprio conto corrente disponendo numerosi bonifici;
- in data 02/09/2025 ha fatto accesso al proprio conto corrente, in quanto doveva pagare l'affitto di casa, e si è avveduta che non vi era più disponibilità;
- ha immediatamente contattato il servizio clienti dell'intermediario e ha accertato che i truffatori avevano eseguito dal proprio conto corrente bonifici per complessivi € 6.223,10 (in particolare in data 28/08/2025 sei bonifici di importo rispettivamente pari a € 10,00; 54,50; 133,50; 287,60; 689,60 e 1.459,90 e in data 02/09/2025 due bonifici di importo rispettivamente pari a € 1.524,00 e € 2.064,00);
- precedentemente, aveva fatto accesso al proprio conto corrente in data 27/08/2025 per verificare l'accredito dello stipendio;
- non ha mai richiesto né autorizzato i bonifici sconosciuti, né ha mai ceduto a terzi le password di sicurezza o il proprio cellulare, su cui è installata l'app dell'intermediario;
- in data 02/09/2025 ha segnalato la frode all'intermediario e bloccato l'operatività online del conto.

Dalle dichiarazioni rese nella denuncia e nel ricorso, risulta che la cliente si sia avveduta delle operazioni fraudolente solo dopo l'esecuzione delle stesse, facendo accesso al proprio conto tramite home banking. La cliente non fornisce alcun elemento utile a ricostruire la dinamica della truffa, limitandosi ad affermare di non aver eseguito i bonifici e di non aver condiviso le proprie password né consegnato il proprio smartphone ad alcuno.

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 dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Sul punto, l'intermediario premette che gli ordini di bonifico disposti tramite app sono stati inseriti con il *device* certificato della cliente in data 05/07/2023 (due anni prima delle disposizioni sconosciute) ed abitualmente utilizzato dalla stessa, identificato con codice univoco 70f86**.

In riferimento alla fase di accesso all'APP eseguita i giorni in cui sono state eseguite le operazioni contestate, il Collegio rileva che, sulla base delle evidenze prodotte dall'intermediario, risulterebbero quali fattori di autenticazione della fase di login: codice (elemento di conoscenza); OTP/notifiche push (elemento di possesso).

In particolare, in data 28.8.2025, l'autenticazione parrebbe avvenuta tramite l'applicazione di mobile token del PSP sullo smartphone, sbloccata con codice, che genera un codice che ha il valore dei due fattori della SCA congiunti ("conoscenza" del codice e "possesso" dello smartphone).

In un caso analogo, alla luce dei due fattori sopra indicati, il presente Collegio ha ritenuto provata la SCA (decisione n. 8724/25 del 01/10/2025).

Al contempo, in data 2.9.2025 (data in cui sono stati eseguiti 2 bonifici), l'intermediario produce evidenze dalle cui emerge che l'accesso all'app sarebbe stata eseguita tramite : "login primo livello"; "login secondo livello codice corretto"; "login terzo livello codice corretto".

Specificando, inoltre, che l'operazione di bonifico risulta, alle ore 15:10, 15:12 e 15:14, bloccata per frode (BLOCCO FRAUD-OPERAZIONE FRAUDOLENTA) e successivamente eseguita alle ore 15:15, nell'ambito della medesima sessione di accesso dei precedenti tentativi bloccati per frode.

Orbene, in generale, riguardo alle operazioni contestate è possibile concludere che, sulla base delle evidenze prodotte dall'intermediario risulta che le operazioni sono state autenticata tramite: codice segreto (elemento di conoscenza); OTP/notifica push (elemento di possesso).

Più nello specifico, inoltre, per quanto concerne i bonifici eseguiti dopo il contatto telefonico intercorso tra un operatore dell'intermediario e la cliente, si premette che i pagamenti M.O.T.O. ("*mail order/telephone order*") sono transazioni in cui i clienti forniscono i dati della propria carta di pagamento al telefono o per posta.

Con riguardo alle conseguenze del disconoscimento di un'operazione M.O.T.O., si è ritenuto pertanto che il regime di responsabilità tra le parti è regolato dalle norme di diritto comune, per cui l'intermediario è tenuto a dimostrare di aver verificato la provenienza dell'ordine dal pagatore con la diligenza professionale qualificata di cui all'art. 1176 comma 2 c.c.; in caso contrario, risponde per intero dell'operazione fraudolenta (Collegio di Milano, decisione n. 7847 del 20 agosto 2025).

Quanto alle operazioni disposte telefonicamente, l'intermediario afferma che:

- in occasione della navigazione del 28/08/2025 sono presenti diversi tentativi di disposizione dei bonifici di € 689,60 a favore di G*B* (IBAN *0900) e di € 1.459,90 a favore di A*E*C* (IBAN *0454) non andati a buon fine in quanto bloccate dai propri motori antifrode;
- tali operazioni sono state successivamente eseguite telefonicamente, a seguito di un processo di identificazione della cliente da parte dell'operatore del contact center in aggiunta all'inserimento di codici segreti;
- in particolare, le operazioni hanno avuto inizio mediante interazione con il canale self-service, basato sulle tecnologie IVR (*Interactive Voice Recognition*);
- il contatto proveniva dal numero della cliente, censito e certificato, e pertanto non è stato necessario inserire il codice cliente, essendo attiva la funzione di identificazione del numero;
- l'interazione con l'IVR è proseguita con la richiesta di inserimento di due cifre del primo codice segreto e il successivo passaggio della telefonata a un operatore;
- ai fini della conferma delle disposizioni di bonifico, l'addetto al contact center ha chiesto alla cliente di validare le stesse mediante inserimento di due cifre del secondo codice segreto (rimanda all'allegato 8);

- conclusivamente, le operazioni di bonifico sono state autorizzate – previa verifica del numero telefonico censito e certificato chiamante – mediante inserimento di due cifre del primo codice segreto e due cifre del secondo codice segreto, per ciascuna disposizione;
- come confermato anche dalle Q&A dell'EBA in relazione alla risposta alla domanda ID 2018_4058, gli ordini di bonifico disposti, come nel caso in esame, via telefono tramite soluzioni di Interactive Voice Response (IVR) non rientrano nell'ambito di applicazione degli obblighi di SCA di cui alla PSD2 (come chiarito nel considerando 95).

Anche in questo caso, dalle evidenze prodotte in atti dall'intermediario, emerge che la chiamata è stata eseguita dal numero certificato della cliente e che la relativa validazione è stata eseguita con un codice di esclusiva conoscenza della medesima.

Quanto ad eventuali profili di colpa, la cliente non ha riferito nulla in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento. Nella denuncia e/o nel ricorso rappresenta solo di essersi accorta degli utilizzi fraudolenti consultando l'estratto conto per cui, in aderenza al dato normativo (art. 10 del D.Lgs. 11/20105), il Collegio può valutare la mancata allegazione dei fatti, tra i vari elementi, per formare il proprio convincimento circa la colpa grave del ricorrente solo una volta verificata la sussistenza della SCA.

Anche in riferimento ad eventuali profili di colpa grave, il Collegio non rinviene in atti elementi utili ad ascrivere tale responsabilità all'intermediario resistente.

Assume rilievo, difatti, quanto dimostrato dall'intermediario resistente circa la volontà di disposizione di taluni bonifici contestati, espressamente dichiarata dalla cliente, oltre che con i contatti al numero verde, anche in occasione dei contatti telefonici intervenuti con un operatore dell'ufficio sicurezza.

Le due operazioni di bonifico di € 689,60 e € 1.459,90 del 28/08/2025 venivano eseguite telefonicamente in quanto non andavano a buon fine tramite app perché bloccate dal motore antifrode e tale circostanza si è realizzata anche per la successiva operazione del 02/09/2025 di € 1.524,00 inserita tramite app, per la quale, all'esito delle risultanze emerse dal motore antifrode in fase di disposizione, l'ufficio sicurezza ha provveduto al temporaneo blocco dell'esecuzione e a contattare la ricorrente per accertarsi dell'effettiva volontà di disporre il pagamento.

In tutte tali occasioni, rileva che la cliente ha confermato la propria volontà di procedere con i bonifici e di conoscere l'identità dei beneficiari.

Da ultimo il Collegio non rileva indici di anomalia applicabili al caso di specie e valuta la correttezza delle notifiche push e degli sms alert inviati alla ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE