

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 società cliente afferma quanto segue:

- in data 21/08/2025 ha disposto, tramite *home banking*, un bonifico di importo pari a € 22.854,13 a favore di beneficiario con IBAN estero, in adempimento ad una fattura ricevuta via e-mail da un fornitore abituale;
- successivamente è emerso che l'IBAN era stato sostituito mediante frode informatica del tipo *man in the middle/business e-mail compromise*;
- ha tempestivamente informato la banca e presentato denuncia;
- contesta la responsabilità dell'intermediario in quanto, a fronte di un'operazione anomala per importo elevato e beneficiario estero mai utilizzato in precedenza, non sono stati attivati efficaci sistemi antifrode;
- l'intermediario aveva garantito un sistema di controllo dei bonifici inseriti tramite home banking, attraverso verifica telefonica dei bonifici disposti;

- ha beneficiato di tale servizio solo inizialmente e, successivamente, non è più stata contattata da alcun operatore;
- solo a seguito dell'accaduto sono stati attivati messaggi di alert per i bonifici inseriti in *home banking* a favore di nuovi beneficiari.

Il ricorrente chiede un rimborso parziale per corresponsabilità dell'intermediario convenuto per € 11.427,00.

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

- la società cliente è titolare di conto corrente presso lo stesso;
- la cliente è rimasta vittima di una truffa di tipo *business e-mail compromise*;
- è inapplicabile al caso di specie la disciplina di cui al d.lgs. n. 11/2010, in quanto il bonifico è stato disposto ed autorizzato personalmente dalla ricorrente, seppur sulla base di un consenso viziato dal raggiro subito;
- l'operazione è stata correttamente autenticata, registrata e contabilizzata, in assenza di malfunzionamenti o altre anomalie;
- da quanto dichiarato in denuncia, emerge una condotta gravemente negligente e colposa della ricorrente e in particolare:
 1. è la cliente a riconoscere che il frodatore si è introdotto nella catena di comunicazioni intercorse tra la stessa e il fornitore M* e che, mediante tale intrusione nel proprio sistema di comunicazione/informatico, ha ricevuto la comunicazione (solo apparentemente inviata dal fornitore M*) contenente il codice IBAN utilizzato per effettuare il pagamento;
 2. la documentazione acquisita dimostra che la cliente aveva già segnalato il 07/08/2025 al proprio *provider* un hackeraggio delle caselle di posta elettronica, confermato a seguito di verifica tecnica;
 3. nonostante fosse già a conoscenza della compromissione delle proprie caselle di posta, il 21/08/2025 ha disposto un bonifico verso un nuovo IBAN comunicato via e-mail, senza effettuare alcuna verifica diretta con il fornitore o con la banca;
 4. solo il 27/08/2025, una volta accertato che l'IBAN non apparteneva al fornitore abituale, la cliente ha modificato la password dell'account e-mail e contattato lo stesso per richiedere il recall del bonifico;
- in data 27/08/2025, appena venuta a conoscenza della truffa, ha immediatamente provveduto ad inserire richiesta di *recall* che, tuttavia, ha avuto esito negativo;

- il proprio sistema informatico ha notificato alla cliente la presenza di un nuovo beneficiario prima della conferma dell'operazione: alle ore 11:17:58 del 21/08/2025 - al momento del salvataggio del bonifico, ossia prima della firma e della conferma definitiva dell'operazione di pagamento - il proprio sistema ha inviato all'indirizzo e-mail della cliente (r**.com) una e-mail di sicurezza automatica avente ad oggetto "*Avviso nuovo beneficiario IBAN: SCT 21.08.2025*" (cfr. doc. 7, pag. 11); la conferma del bonifico è avvenuta solo successivamente (alle ore 11:19:02);
 - contestata l'ulteriore affermazione avversaria secondo cui la banca in precedenza avrebbe contattato la cliente per chiedere informazioni/conferma telefonica in merito a bonifici disposti;
 - alcuna norma prevede un obbligo automatico di blocco o allerta per i bonifici di importo elevato o verso nuovi beneficiari, in assenza di specifici indicatori di rischio o sospetto di frode; l'obbligo di intervento nasce soltanto in presenza di comportamenti effettivamente anomali (es. accessi da aree geografiche insolite o utilizzo di dispositivi non riconosciuti);
 - l'analisi del log dei bonifici eseguiti dalla cliente tra il 27/02/2025 e il 01/10/2025 (doc. 8) dimostra che la società dispone con regolarità pagamenti di importi anche rilevanti verso diversi fornitori, con valori compresi tra € 47,00 ed € 142.828,25 e una media di € 14.408,17 per singola operazione;
 - l'operazione è stata correttamente inoltrata alla banca di accredito in conformità con l'identificativo unico (IBAN) inserito dalla cliente (ex art. 24 d.lgs. n. 11/2010);
 - non era tenuto a verificare l'incongruenza tra l'IBAN e la ragione sociale del beneficiario.
- L'intermediario chiede il rigetto del ricorso.

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

- la mail menzionata dall'intermediario del 21/08/2025 non le risulta ricevuta;
- dal mese di marzo 2025, pur inserendo nuovi beneficiari, il sistema non le ha più inviato tali e-mail di alert.

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

- diversamente da quanto sostenuto da controparte, il proprio sistema informatico ha correttamente notificato alla cliente la presenza di un nuovo beneficiario prima che questa confermasse l'operazione.

DIRITTO

In data 21/08/2025 la ricorrente ha disposto, tramite *home banking*, un bonifico di importo pari a € 22.854,13 a favore di beneficiario con IBAN estero, in adempimento ad una fattura ricevuta via e-mail da un fornitore abituale subendo una truffa. Preliminarmente si rileva che la società cliente chiede - oltre all'accertamento della corresponsabilità dell'intermediario e il rimborso parziale della somma di cui al bonifico contestato - anche di "*ordinare alla banca di fornire informazioni circa i protocolli antifrode adottati per le operazioni di pagamento estere di importi rilevanti*". Sul punto, si rappresenta che risulta preclusa all'ABF la possibilità di esaminare richieste finalizzate a ottenere pronunce di carattere costitutivo o di condanna, e, dall'altro lato, che, come confermato dal pacifico orientamento dei Collegi, non possono essere proposte innanzi all'ABF domande aventi ad oggetto un *facere* infungibile. Inammissibile dunque tale seconda domanda, si prosegue nell'analisi del ricorso.

Orbene, è pacifico che l'operazione oggetto del ricorso sia stata eseguita direttamente dalla società cliente, che – cadendo vittima di un raggio – ha personalmente disposto il pagamento, a favore dell'IBAN indicato nella fattura inviata tramite mail. Secondo l'orientamento dei Collegi, quando l'operazione è eseguita per intero dal pagatore, l'operazione stessa deve considerarsi autorizzata; pertanto, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al D. Lgs n. 11/2010. Rientrano in questa fattispecie, in particolare, le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura"). Nella fattispecie in esame, il Collegio non procede dunque alla verifica della corretta esecuzione e autenticazione delle operazioni contestate ai sensi degli artt. 10 ss. del decreto citato.

Nel caso di specie occorre poi osservare che:

- nonostante parte ricorrente fosse già a conoscenza - dal 07/08/2025 - della compromissione delle proprie caselle di posta, il 21/08/2025 ha disposto un bonifico verso un nuovo IBAN comunicato via e-mail, senza effettuare alcuna verifica diretta con il fornitore o con la banca;
- il ricorrente ha inserito la richiesta di *recall* diversi giorni dopo aver posto in essere l'operazione: in data 27/08/2025 (medesimo giorno in cui la cliente, come dichiarato in denuncia, si è resa conto della truffa e ha contattato l'intermediario) a fronte di una operazione compiuta il 21 dello stesso mese;
- l'indirizzo da cui la ricorrente ha ricevuto la mail con l'IBAN modificato era diverso, ancorché simile, a quello con cui abitualmente comunica con il proprio fornitore M* (con una lettera modificata: "*meaat*" al posto di "*meatt*");

- alla data dell'operazione (21/08/2025) non era ancora in vigore l'obbligatoria verifica di corrispondenza tra nome e IBAN del beneficiario (di cui all'art. 5 *quater* nel Regolamento UE n. 2012/260). L'intermediario pertanto non era tenuto a verificare l'incongruenza tra l'IBAN e la ragione sociale del beneficiario;
 - l'operazione oggetto di truffa non appare anomala per ammontare rispetto all'operatività della ricorrente: l'analisi del log dei bonifici eseguiti dalla cliente tra il 27/02/2025 e il 01/10/2025 dimostra che la società dispone con regolarità pagamenti di importi anche rilevanti verso diversi fornitori, con valori compresi tra € 47,00 ed € 142.828,25 e una media di € 14.408,17 per singola operazione.
- Orbene, alla luce di quanto precede non si rinvergono elementi sufficienti a considerare l'intermediario corresponsabile della truffa e del danno patiti dalla ricorrente.

PER QUESTI MOTIVI

Il Collegio dichiara il ricorso in parte inammissibile e in parte infondato.

IL PRESIDENTE