

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) PERON

Seduta del 06/05/2026

FATTO

Parte ricorrente espone al Collegio che in data 03/09/2025 riceveva un SMS apparentemente proveniente dall'intermediario, recante la sua intestazione, che segnalava un pagamento anomalo di € 1.490,99 effettuato con carta di credito. Seguendo le istruzioni, contattava il numero verde indicato chiedendo di parlare esclusivamente con un operatore certificato; poco dopo, riceveva una chiamata dal numero telefonico dell'ufficio dell'intermediario, già memorizzato nella propria rubrica. Un sedicente operatore, con il pretesto di dover sbloccare il conto corrente, induceva la parte ricorrente a comunicare il codice del token e i codici temporanei via via generati. Convinta dell'autenticità dell'interlocutore, seguiva le istruzioni e concordava un appuntamento per il giorno successivo. Tuttavia, in data 04/09/2025, recandosi presso l'istituto, apprendeva dell'inesistenza dell'appuntamento e della sottrazione illegittima di € 4.080,00 a favore di M*** s.r.l. Sporta immediata denuncia e inviate diverse comunicazioni, in data 07/11/2025 presentava reclamo ufficiale, riscontrato negativamente dall'intermediario.

Per queste ragioni parte ricorrente chiede che l'ABF disponga a suo favore il rimborso di € 4.080,00, oltre al rimborso delle spese legali e di € 20,00 per la presentazione del ricorso.

L'intermediario, ricostruiti i fatti, chiede il rigetto del ricorso sostenendo che la parte ricorrente sia stata vittima di spoofing. L'operazione risulta regolarmente autorizzata, registrata e contabilizzata, senza che siano state riscontrate anomalie, malfunzionamenti o intrusioni nei sistemi informatici. L'intermediario evidenzia che l'SMS civetta non conteneva riferimenti a conti o carte della parte ricorrente e utilizzava toni vaghi e allarmistici, estranei alle normali comunicazioni istituzionali,

precisando di non aver mai inviato tali messaggi e che non è prassi richiedere codici telefonicamente per risolvere emergenze. Viene dunque ravvisata la colpa grave della parte ricorrente, poiché la frode si è perfezionata solo grazie alla sua collaborazione attiva nel seguire le indicazioni del finto operatore, comunicando codici riservati e inserendo l'IBAN del beneficiario. Infine, l'intermediario dichiara di aver tentato senza successo il recall del bonifico di € 4.080,00.

Per questi motivi l'intermediario chiede il rigetto del ricorso in quanto infondato in fatto ed in diritto.

Parte ricorrente, replica lamentando di non essere stata sufficientemente tutelata dal raggiro, poiché la chiamata truffaldina proveniva dall'utenza telefonica dell'intermediario a lei nota e utilizzata abitualmente per contattare la filiale. Insiste sull'apparente veridicità del messaggio e sul fatto di aver espressamente richiesto, durante il primo contatto, di essere richiamata dal proprio istituto. Pertanto, l'utilizzo del numero ufficiale da parte dei truffatori è stata l'unica circostanza che l'ha indotta ad abbassare le difese e ad accettare assistenza, motivo per cui insiste nell'accoglimento del ricorso.

L'intermediario insiste nel rigetto del ricorso.

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente del complessivo importo di € 4.080,00 sottratto a seguito di un'operazione di pagamento fraudolenta eseguita tramite bonifico ordinario in data 03/09/2025 alle ore 18:18.

L'operazione contestata è disciplinata dal D.lgs. 27/01/2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 05.07.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di strong customer authentication (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori: a) è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / enrollment dell'applicazione / registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni; inoltre la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse; b) è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di alert. Peraltro 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. 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.

Ciò posto dalle dichiarazioni di parte ricorrente emerge che vi è stato un suo parziale concorso causale nella fase dispositiva/ autorizzativa. Secondo l'orientamento dei Collegi, se il concorso causale della parte ricorrente in fase dispositiva o autorizzativa è parziale, ad esempio tramite l'inserimento di uno solo dei fattori di autenticazione, la transazione non si intende automaticamente autorizzata. La normativa speciale, come la PSD2 e le relative disposizioni di recepimento, prescinde dalla nozione civilistica di "consenso" e stabilisce che quest'ultimo debba essere prestato esclusivamente nella forma convenuta tra il pagatore e l'intermediario. Rimane ferma la possibilità di valutare se la parte ricorrente abbia agito con dolo, frode o colpa grave nel mancato adempimento degli obblighi di custodia, ai sensi degli articoli 7 e 12 del D.Lgs. 11/2010.

Il Collegio procede dunque ad esaminare la prova dell'autenticazione forte dell'intermediario in tutte le fasi in cui si è realizzata l'operazione contestata.

L'operazione contestata è un bonifico ordinario effettuato da Browser e autorizzato tramite controllo Mapellum (inserimento Codice PIN + Token VASCO + Captcha).

Con riguardo al sistema di autenticazione forte dell'intermediario per le fasi antecedenti all'esecuzione dell'operazione, il Collegio constata che dalle evidenze in atti l'accesso all'Home Banking è avvenuto tramite inserimento del Codice PIN (fattore di conoscenza) e inserimento codice prodotto dal Token VASCO (fattore di possesso). Il Collegio in proposito sottolinea che la stessa parte ricorrente ha dichiarato, con valore confessorio, di aver comunicato al truffatore i codici vi via generati dal token fisico.

Quanto alla fase dispositiva dell'operazione risulta in atti che l'operazione è stata autenticata tramite l'inserimento del Codice PIN (fattore di conoscenza) e l'inserimento del Codice Token VASCO (fattore di possesso). Il sistema ha poi effettuato un ulteriore duplice controllo che, secondo l'intermediario, rientra nel sistema Mapellum (sistema Captcha MAPELLUMCHECKIMAGE e MAPELLUMCHECKAUTOCODE).

Il Collegio, ritenuta provata la SCA, in relazione a tutti i singoli passaggi esaminati, procede a verificare se parte ricorrente abbia agito con colpa grave e se vi sia stato un concorso di colpa da parte dell'intermediario.

In proposito il Collegio osserva che parte ricorrente riferisce di aver ricevuto un messaggio relativo a un'operazione anomala di € 1.490,99, con l'indicazione di contattare un numero per bloccare il pagamento, istruzione che ha prontamente eseguito. Dall'evidenza prodotta emerge che la denominazione della chat non è riferibile all'intermediario, sebbene l'SMS riporti il suo nome in apertura, e neppure è riferibile il numero mittente (**922), il quale online è segnalato come truffaldino. Non si rileva la presenza di messaggi genuini antecedenti o successivi a quello civetta, né di ulteriori messaggi fraudolenti o "parlanti" relativi alle operazioni contestate. Il testo contiene un numero di

telefono (**407) per il blocco del pagamento e presenta errori di punteggiatura, come l'uso della virgola dopo il simbolo € e la conseguente mancata maiuscola. Si osserva infine che il messaggio è stato ricevuto alle ore 16:38 del 03/09/2025, circa un'ora e quaranta minuti prima dell'operazione delle ore 18:18.

Per tutti questi motivi il Collegio ritiene che la condotta di parte ricorrente sia connotata da colpa grave e non rinvenendo una responsabilità concorrente da parte dell'intermediario, reputa il ricorso non meritevole di accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE