

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 di essere stata vittima di una frode sofisticata, orchestrata da truffatori qualificatisi come operatori del centro antifrode dell'intermediario. L'inganno è risultato estremamente credibile poiché i malfattori hanno inviato SMS tramite il numero ufficiale dell'intermediario e notifiche *push* sull'App, dimostrando di conoscere già i suoi dati personali e bancari. Parte ricorrente sostiene che la carta le sia stata sottratta mediante raggiro e di non aver autorizzato i prelievi eseguiti. Lamenta inoltre che l'intermediario, dopo un iniziale rimborso di € 4.000,00, ha provveduto allo storno della somma e che, nonostante le ripetute istanze in filiale e al *call center*, non le è stato consentito di contestare un ulteriore prelievo di € 5.000,00. Infine, evidenzia come le operazioni fraudolente fossero palesemente anomale rispetto al proprio profilo storico — per frequenza, importi elevati e vicinanza temporale — e che l'intermediario non abbia attivato alcun sistema di *alert* o blocco preventivo.

Per queste ragioni parte ricorrente chiede che il Collegio riconosca il rimborso a suo favore di complessivi € 9.000,00 e che ordini all'intermediario l'adozione di *“ogni misura necessaria alla tutela della ricorrente e degli altri clienti vittime di attacchi social engineering”*.

L'intermediario, ricostruiti i fatti, controdeduce che parte ricorrente è titolare del conto corrente n. *312, della carta di debito n. *120 e del servizio di banca multicanale n. *036. *Oggetto del ricorso*

sono tre prelievi effettuati in data 23/09/2025 presso la filiale di M (€ 5.000,00 alle ore 15:52, € 2.500,00 alle ore 15:54 e € 1.500,00 alle ore 15:55), risultati regolari poiché eseguiti con carta fisica e PIN corretto al primo tentativo. La prima operazione è stata inoltre autorizzata tramite un SMS OTP inviato al cellulare della parte ricorrente, la quale ha ricevuto notifiche *push* e SMS per ogni accesso e transazione.

L'intermediario rileva che la parte ricorrente ha dato credito a comunicazioni provenienti da utenze estranee (quali il cellulare *768 e il fisso *115) senza svolgere verifiche, nonostante una semplice ricerca *online* avrebbe segnalato il numero fisso come "chiamata truffa". I messaggi fraudolenti, peraltro, non erano accodati a quelli autentici, erano sgrammaticati, privi di intestazione ufficiale e inviati tramite WhatsApp, canale non utilizzato dall'intermediario. Sebbene la dinamica dell'inganno non sia del tutto documentata, è certo che la parte ricorrente abbia consegnato la carta integra a un falso corriere senza nemmeno tagliarla, assecondando la richiesta irrealistica di riconsegnare lo strumento asseritamente bloccato.

L'attività delittuosa non ha presentato particolari insidie tecniche; piuttosto, il malfattore ha operato grazie al possesso della tessera consegnata e alla conoscenza del PIN, presumibilmente carpito durante la telefonata. L'intermediario conclude ravvisando una grave negligenza nella condotta della parte ricorrente, la quale, ignorando evidenti segnali d'allarme, ha violato gli obblighi di custodia dello strumento e del codice segreto. Pertanto, essendo i prelievi avvenuti tramite tecnologia *chip* e PIN a causa della mancata diligenza del titolare, l'intermediario nega ogni responsabilità.

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

Nelle repliche la parte ricorrente insiste nella domanda, confermando quanto già rappresentato nel ricorso.

L'intermediario, riportandosi alle conclusioni in atti, controreplica evidenziando che la prima transazione delle ore 15:52 è stata autorizzata tramite un SMS OTP inviato sul cellulare della parte ricorrente, la quale avrebbe quindi potuto interrompere la truffa. Viene ribadito che la parte ricorrente ha consegnato lo strumento di pagamento a un falso corriere e ha comunicato il relativo codice segreto, permettendo così i prelievi fisici presso gli sportelli della filiale. Inoltre, l'intermediario osserva che la parte ricorrente ha consentito al truffatore l'accesso alla banca multicanale, seppur in modalità informativa, già nelle fasi iniziali, spiegando così come il malvivente conoscesse il saldo del conto. Infine, si precisa che diversi tentativi di accesso al conto e al PIN non sono andati a buon fine poiché la parte ricorrente non ha autorizzato le relative notifiche *push* ricevute sul cellulare).

DIRITTO

Il presente ricorso concerne la richiesta di parte ricorrente di ottenere il rimborso delle operazioni fraudolente contestate, pari a € 9.000,00. Parte ricorrente chiede altresì che il Collegio ordini all'intermediario l'adozione di "*ogni misura necessaria alla tutela della ricorrente e degli altri clienti vittime di attacchi social engineering*".

Con riferimento a tale ultima domanda, in via preliminare, il Collegio osserva che le “*Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*” circoscrivono la competenza dell’ABF alle questioni “*aventi ad oggetto l’accertamento di diritti, obblighi e facoltà*”, sicché risulta preclusa all’ABF la possibilità di esaminare richieste finalizzate a ottenere pronunce di carattere costitutivo, 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 (cfr. *ex multis*, Collegio di Milano, decisione n. 15195/2022). La domanda deve quindi dichiararsi inammissibile.

Passando ad esaminare il merito del ricorso, il Collegio constata che la domanda di rimborso di € 9.000,00 riguarda tre operazioni di prelievo ATM eseguite in data 23/09/2025, alle ore 15:52, per € 5.000,00; alle ore 15:54 per € 2.500,00 e alle ore 15:55 per € 1.500,00.

Le operazioni contestate risultano eseguite con la carta fisica consegnata ai truffatori (in particolare parte ricorrente ha lasciato la carta all’interno della cassetta della pubblicità del condominio, affinché venisse ritirata da un presunto corriere dell’intermediario). Detta consegna, è stata anticipata da un’interazione telefonica tra la parte ricorrente e il truffatore nel corso della quale sono state eseguite talune azioni sull’*home banking* della cliente con le quali sono stati aumentati i massimali della carta. A tale proposito, dalle evidenze in atti risulta che l’innalzamento dei massimali della carta è avvenuto mediante: “CHECK-FINGERPRINT” (elemento di inerenza) e “SENDPUSHNOTIFICATION” “CONTROLLO-MTOKEN” “PUSH STATUS: OK” (elemento di possesso).

L’innalzamento del massimale è, quindi, avvenuto con una corretta esecuzione della SCA.

Si ricorda in proposito che secondo i principi fissati dal D.lgs. 27/01/2010 n. 11, in materia di *strong customer authentication* (SCA): *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.

Passando ad esaminare la SCA con riferimento alle tre operazioni di prelievo, il Collegio constata quanto segue.

Quanto alla prima operazione di prelievo per € 5.000,00, dalle evidenze in atti emerge la corretta autorizzazione tramite i seguenti fattori: corretto inserimento PIN (elemento di conoscenza); lettura *CHIP* della carta (elemento di possesso) e invio SMS OTP (ulteriore elemento di possesso).

Quanto alla seconda e terza operazione di prelievo rispettivamente di € 2.500,00 e di € 1.500,00 dalle evidenze in atti emerge la corretta autorizzazione tramite i seguenti fattori: corretto inserimento PIN (elemento di conoscenza); lettura *CHIP* della carta (elemento di possesso).

Alla luce di quanto precede, tutte le operazioni in contestazione risultano autenticate mediante i fattori del possesso (la carta) e della conoscenza (il codice PIN). Peraltro, parte ricorrente in sede di denuncia ha dichiarato di aver inserito il proprio bancomat, all’interno di una busta, identificata da un codice fornito dal truffatore, nella cassetta della pubblicità del palazzo ove abita, affinché un presunto corriere dell’intermediario – in realtà il truffatore – la ritirasse, senza riferire di averla tagliata a metà per renderla inutilizzabile.

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.

Parte ricorrente riferisce di aver ricevuto tre chiamate dal numero fisso *115 (non riconducibile all’intermediario e segnalato sul *web* come fraudolento) da un falso operatore che segnalava operazioni sospette. Seguendo le istruzioni ricevute, ha autorizzato notifiche *push* per una presunta procedura di sicurezza e ha optato per il ritiro della carta a domicilio affinché venisse distrutta da un asserito centro antifrodi. Inoltre, nonostante i messaggi SMS ricevuti presentassero varie anomalie (intestazione generica, assenza di punteggiatura e sintassi errata), parte ricorrente ha riposto il bancomat integro in una busta nella cassetta postale del palazzo, permettendo ai malfattori di impossessarsene. Tale condotta ha consentito il primo prelievo alle ore 15:52, autorizzato tramite procedura rafforzata di inserimento codice OTP ricevuto via SMS (al cellulare verificato di parte ricorrente) e che risulta correttamente inserito.

Parte ricorrente, infine, afferma di avere contattato l’intermediario e chiesto il blocco della carta non appena accortasi della truffa. L’intermediario produce evidenza, da cui risulta che il blocco è stato disposto alle ore 15:59 del 23/09/2025 per sospetta frode (ossia solo 4 minuti dopo l’ultimo

prelievo disconosciuto delle ore 15:55). È presente in atti evidenza delle notifiche *push* di *alert* inviate alla parte ricorrente per tutte e tre le operazioni disconosciute.

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