Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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) MODICA

Seduta del 06/05/2026

FATTO

Il cliente dichiara che: in data 24 maggio 2024, riceveva un SMS che sembrava provenire dall'intermediario con cui gli veniva comunicato che il suo numero di telefono certificato (***350) era stato disattivato e, contestualmente, era stato attivato un numero a lui sconosciuto (***334). Immediatamente dopo, un secondo SMS gli comunicava che era stato ripristinato il recapito telefonico corretto (ossia ***350). Nei giorni successivi, soggetti terzi hanno perpetrato un attacco di phishing altamente sofisticato, inducendolo in errore e disponendo 3 operazioni fraudolente, per un totale di € 17.806,00. In data 30 maggio 2024, l'intermediario lo contattava per segnalare un'"anomala operatività", procedendo al blocco del conto; in data 11 giugno 2024, disconosceva le operazioni e, in data 18 giugno 2024, sporgeva denuncia alle Autorità;procedeva a bloccare la carta e a presentare denuncia presso le Autorità; presentava formale reclamo all'intermediario in data 14 ottobre 2025, che veniva riscontrato negativamente in data 28 novembre 2025.
Chiede la restituzione di € 17.806,00, oltre interessi legali.
L'intermediario dichiara che, in data 29 maggio 2024, contattava il cliente per chiedere chiarimenti in merito alle operazioni e, a fronte delle sue risposte, bloccava il conto corrente; in data 21 giugno 2024, provvedeva al riaccredito dell'importo complessivo di € 17.806,06, informando contestualmente il cliente che la banca si sarebbe riservata di svolgere le necessarie verifiche a conclusione delle quali avrebbe provveduto, qualora avesse accertato che le operazioni erano state

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

correttamente autorizzate, al riaddebito; essendo state le operazioni correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali, veniva effettuato il menzionato riaddebito. Eccepisce, in via pregiudiziale, l'inammissibilità del ricorso in ragione dell'inosservanza, da parte del cliente, del termine minimo decorrente dal ricevimento del reclamo. Nel merito, ritiene che il cliente sia rimasto vittima di smishing; le operazioni contestate, come detto, sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; anche l'operazione di modifica del numero di cellulare risulta essere stata autorizzata dal cliente, il quale avrebbe dichiarato di aver cliccato sul link presente nell'SMS truffaldino e avrebbe inserito i propri codici di autenticazione, per poi essere contattato da un finto operatore. Ritiene sussistente la colpa grave del cliente, che avrebbe posto in essere una serie di comportamenti imprudenti che hanno determinato il verificarsi del danno lamentato, tra cui l'aver cliccato sul link truffaldino, l'aver volontariamente fornito le credenziali al frodatore e l'aver autorizzato personalmente il cambio di utenza associata alla propria posizione.
Chiede sia dichiarata la inammissibilità del ricorso o, in subordine, il rigetto del ricorso.
Il cliente, richiamati i propri scritti, replica, con riferimento all'eccezione di inammissibilità del ricorso riguardo alla scadenza dei termini previsti a seguito del ricorso, che la posizione dell'intermediario era già stata chiaramente e inequivocabilmente espressa con la comunicazione dell'8 novembre 2024, con cui si negava il rimborso e si procedeva al riaddebito delle somme. Aggiunge che l'SMS originario del 24 maggio 2024 si sarebbe inserito nella cronologia dei messaggi autentici provenienti dall'intermediario, configurando quindi un complesso caso di spoofing. Insiste nell'accoglimento del ricorso.
L'intermediario, riportandosi alle conclusioni in atti, controreplica, con riferimento all'SMS civetta, che lo screenshot allegato dal cliente in sede di denuncia non riporta alcun riferimento in merito all'ora e alla data; che neppure in sede di repliche, il cliente ha prodotto la documentazione completa in merito alla frode subita. Insiste nel rigetto del ricorso.

DIRITTO

Il cliente disconosce tre operazioni eseguite a valle di una truffa e chiede la restituzione dei relativi importi.
L'intermediario eccepisce in via preliminare la inammissibilità del ricorso per mancato rispetto dei termini di presentazione.
L'eccezione è infondata.
La Sezione VI, paragrafo 1, delle Disposizioni Banca d'Italia del 18 giugno 2009, dispone che: "Per i servizi di pagamento, i tempi massimi di risposta non sono superiori a 15 giornate lavorative dalla ricezione del reclamo. Se, in situazioni eccezionali, l'intermediario non può rispondere entro 15 giornate lavorative, invia al cliente una risposta interlocutoria, in cui indica in modo chiaro le ragioni del ritardo e specifica il termine entro il quale il cliente riceverà la risposta definitiva, comunque non superiore a 35 giornate lavorative. L'intermediario individua nell'ambito delle procedure interne le situazioni eccezionali, allo stesso non imputabili, al ricorrere delle quali è possibile rispondere oltre il termine delle 15 giornate lavorative".

Stando a quanto dichiarato dalle parti, le operazioni risalgono al 27 e al 28 maggio 2024, disconosciute dal cliente in data 11 giugno 2024. Il successivo 21 giugno, l'intermediario ha provveduto al riaccredito dell'importo complessivo ma, in data 8 novembre 2024, a seguito di ulteriori verifiche, revocava l'accredito. Il 14 ottobre 2025, il difensore del cliente presentava formale reclamo, senza, tuttavia, allegare la procura alle liti necessaria ai fini della sua legittimazione; in data 28 ottobre 2025, il cliente provvedeva a inviare la procura. L'intermediario sostiene di aver potuto prendere in carico il reclamo solo ricevuta la procura, appunto in data 28 ottobre 2025. Il cliente presentava ricorso all'ABF il 13 novembre 2025; l'intermediario riscontrava negativamente il reclamo il 18 novembre 2025.
Secondo l'intermediario, assumendo il 28 ottobre 2025 come *dies a quo*, il termine di 15 giorni lavorativi sarebbe scaduto in data 18 novembre 2025. Non può tacersi tuttavia che l'intermediario ha atteso ben 14 giorni dal reclamo, cioè fino al 28.10.2025, per inviare una risposta interlocutoria, nella quale rilevava la mancanza della procura e ne chiedeva la produzione. Non emerge, fra l'altro, che l'intermediario abbia invocato la mancanza della procura per il prolungamento del termine di risposta a 35 gg come consentito dalle Disposizioni di Trasparenza. Reputa allora questo Collegio che vada individuato come *dies a quo* il 14 ottobre 2025, data in cui il cliente ha inoltrato il reclamo pur sprovvisto di procura; conseguentemente, il termine di 15 giorni previsto dalla normativa vigente risulta rispettato.

Il cliente contesta 3 operazioni eseguite il 27/05/2024 alle ore 12:56, il 28/05/2024 alle ore 13:38, il 28/05/2024 alle ore 13:53, per complessivi € 17.806,06. Le operazioni ricadono sotto il raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2). Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente" (decisione n. 22745/2019). Il Collegio, richiamati gli artt. 97 e 98 della PDS2, l'articolo 10 bis del D. Lgs. 11/2010, le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come

"un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione". L'autenticazione forte è richiesta nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet; nella fase di esecuzione delle singole operazioni; rispetto a qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Nel caso di specie, l'intermediario ha fornito prova di autenticazione con impiego di doppio fattore. Con riferimento alla fase di accesso all'Home Banking in data 24 maggio 2024 alle ore 19:01, ha fornito evidenza dell'impiego di un fattore di conoscenza (credenziali di accesso) e di un fattore di possesso (numero di telefono associato all'utenza). Con riferimento alla fase di modifica dell'utenza telefonica, alla luce dei log allegati, risulta che, alle ore 19:05:10, il cliente ha iniziato l'operazione di cambio dell'utenza telefonica associata; alle ore 19:05:51, il cliente ha effettuato il cambio di utenza mediante Secure Call sul suo precedente numero di telefono e l'inserimento del codice PIN; alle ore 19:05:54, il cliente completa l'operazione di cambio dell'utenza telefonica. Appaiono pertanto correttamente provati il fattore di conoscenza (Codice PIN) e il fattore di possesso (precedente numero di telefono associato all'utenza). Dai log, inoltre, risulta che un ulteriore accesso in Home Banking è avvenuto il 26 maggio 2024 tra le ore 16:06:49 e le ore 16:07:11 e che un altro cambio di utenza telefonica è avvenuto tra le ore 16:09:05 e le ore 16:09:46. Quanto alla fase dispositiva, per la prima operazione risulta che il 27 maggio 2026 alle ore 12:55:31, il cliente (o il truffatore) ha iniziato a disporre il bonifico; alle ore 12:56:16, ha autorizzato il bonifico mediante Secure Call sul suo numero di telefono e l'inserimento del codice PIN. Risultano pertanto correttamente provati sia il fattore di conoscenza (codice PIN) sia il fattore di possesso (numero di telefono associato all'utenza).

Del pari provata appare la colpa grave del cliente, vittima di un banale smishing cui avrebbe potuto sottrarsi con l'impiego di una media diligenza. Le modalità attuative delle operazioni disconosciute riflettono uno schema tipico e ormai noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza. Tenuto conto delle circostanze, il ricorrente deve essere considerato vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle più diffuse e conosciute, che qualunque fruitore di servizi on line, dotato di normale avvedutezza e prudenza, deve essere in grado di riconoscere ed evitare (cfr. Collegio di Coordinamento n. 3498 del 26/10/2012). A rafforzare il giudizio sulla colpa grave sta pure la mancata allegazione del messaggio civetta: secondo l'orientamento dei Collegi, la mancata allegazione, da parte del cliente, del messaggio civetta, determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio.

La riconosciuta colpa grave del cliente, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della fattispecie, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius* anche *sub specie* di mancata gestione di eventi che segnalino la possibilità di frodi o anomalie; profili che, nella vicenda in esame, non ricorrono. Nel caso di specie, la mancata attivazione di un servizio di alert risulta in concreto ininfluente dal momento che i truffatori, come detto, avevano provveduto a modificare l'utenza cellulare del cliente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE