COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERSANO

Seduta del 08/05/2025

FATTO

Nel presente procedimento, la parte ricorrente afferma quanto segue:

- il 12/11/2024 alle ore 11:17 riceveva una chiamata dall'utenza telefonica 060* della banca, da cui abitualmente riceveva le comunicazioni;
- con la chiamata l'interlocutore, qualificatosi come operatore della banca, le comunicava che il suo conto corrente era oggetto di attacco hacker e che i truffatori stavano eseguendo un bonifico da € 4.900,00;
- sebbene l'interlocutore la invitasse a contattare l'utenza 02*753, non effettuava alcuna chiamata;
- successivamente riceveva una nuova chiamata dall'utenza 060* e l'interlocutore, qualificatosi come operatore antifrode della banca, la informava della presenza di un bonifico sospetto e le indicava che il suo conto era stato clonato;
- il sedicente operatore la informava anche che l'app non era più sicura, perché oggetto di attacco hacker, e quindi disinstallava e reinstallava l'app su sua indicazione,
- in data 15/11/2024 riceveva altre chiamate dall'utenza 060* e, in quella circostanza, si accorgeva di un bonifico non autorizzato di € 4.980,00;
- contattava il numero 060* e l'operatore le confermava di essere stata vittima di truffa;

- precisa di non aver mai ceduto ai sedicenti operatori nessuno dei codici personali di accesso all'*home banking* o OTP;
- la banca avrebbe dovuto porre in essere strumenti di verifica dell'effettiva titolarità di chi compiva le operazioni bancarie, attività che invece non è stata svolta;
- nessun avviso relativo all'accesso da un dispositivo non autorizzato e comunque diverso da quelli usuali veniva segnalato;
- procedeva a presentare denuncia-querela presso le Autorità in data 18/11/2024;
- presentava reclamo all'intermediario in data 07/01/2025, che veniva riscontrato negativamente in data 13/01/2025.

La ricorrente chiede, dunque, all'Arbitro, di accertare il proprio diritto ad ottenere il rimborso dell'importo che ritiene esserle stato fraudolentemente sottratto.

Nelle proprie controdeduzioni, l'intermediario domanda il rigetto del ricorso, eccependo quanto segue:

- la ricorrente è intestataria del conto corrente n. *872, al quale è collegato il servizio di *home banking*;
- la ricorrente ha, altresì, attivato dal 2020, senza interruzioni, il servizio SMS *Alert* collegato al suo numero di telefono cellulare n. *129;
- il rimborso richiesto di € 4.980,00 corrisponde ad un bonifico inserito con modalità "bonifico Sepa", eseguito online a debito del conto corrente n. *872;
- nella denuncia la ricorrente ha dichiarato di aver prima ricevuto un messaggio, che segnalava la presenza di un "bonifico sospetto" e la necessità di contattare un numero non riconducibile alla banca (02*753) per bloccare tale operazione e di aver ricevuto successivamente una telefonata dall'utenza 060*;
- dell'app che la ricorrente ha installato secondo le modalità dettate non si rinviene evidenza;
- per quanto attiene al canale di provenienza degli SMS e delle telefonate, come più volte segnalato alla clientela tramite gli avvisi sulla sicurezza, non si deve riporre troppa fiducia nel "*caller ID*" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display ed è infatti possibile modificare il mittente di un numero telefonico da parte di terzi;
- la ricorrente ha, invece, seguito in modo pedissequo e acritico le istruzioni ricevute al telefono da persona a lei sconosciuta che l'ha guidata al download di un'applicazione esterna, disconosciuta dalla banca e che non viene offerta in visione alla banca, per poi eseguire comandi non meglio specificati;
- è una circostanza anomala e illogica che, per bloccare un'operazione di bonifico a debito del proprio conto corrente, si debba scaricare un'applicazione esterna alla banca;
- a fronte di una tale richiesta la ricorrente avrebbe dovuto subito insospettirsi, interrompere la telefonata, verificare personalmente il proprio conto corrente, richiamare il servizio clienti, così da rendersi conto del raggiro in atto ed impedire il danno economico subìto con il suo comportamento gravemente colposo;
- le dichiarazioni di natura confessoria riportate in denuncia confermano che la ricorrente, assecondando colpevolmente le istruzioni ricevute al telefono dal suo sconosciuto interlocutore, abbia seguito le indicazioni ricevute, consentendo l'installazione di app "malevola" e rendendo così possibile l'accesso al suo dispositivo da soggetto terzo;
- è assente l'allegazione di qualsivoglia dettaglio utile alla comprensione e alla qualificazione dei fatti narrati come frode, non avendo la ricorrente depositato agli

atti del ricorso alcuna evidenza del download dell'app esterna scaricata, e detta condotta è sanzionata da tutti i Collegi ABF con il rigetto del ricorso in quanto tale omissione è ritenuta assorbente di ogni altra circostanza;
- dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi e l'operazione risulta correttamente autenticata, registrata e contabilizzata (così come previsto dall'art. 10 del D.lgs. n. 11/2010), con le credenziali di sicurezza della ricorrente, come dimostrato nelle evidenze *log*;
- la ricorrente, per l'operazione dispositiva inserita, ha ricevuto SMS e notifica *push*;
- ricevuta notizia, sia pure tardiva, della frode si è attivato per la *recall* con esito negativo.

Successivamente, la cliente, in sede di repliche, richiamati i propri scritti, precisa ulteriormente che:

- è insussistente la sua colpa grave, come invece eccepito dall'intermediario nelle proprie controdeduzioni, perché l'intrusione di un hacker nel sistema bancario non le può essere attribuita in quanto non era in grado di riconoscere l'origine fraudolenta dell'operazione;
- tale violazione, invece, evidenzia la significativa inconsistenza dei sistemi di sicurezza bancari, penetrati da soggetti truffatori;
- la sua condotta non può ritenersi gravemente colposa in quanto non aveva una evidente ragione di insospettirsi, secondo l'ordinaria diligenza, in considerazione del fatto che il raggiro è avvenuto in modo articolato e sofisticato, con modalità sempre più difficili da individuare al momento anche da parte di chi ha una media conoscenza informatica;
- i truffatori hanno agito come di solito operano gli operatori della banca ed erano in possesso di tutti i suoi dati sensibili, circostanza che la truffa è partita in seno alla banca, o per il tramite di dipendenti infedeli o per il tramite di *data bridge*;
- rileva la responsabilità della banca per una carenza di tutela dei dati personali della clientela fondata sul fatto che terzi truffatori ne sono venuti in possesso ed hanno conseguentemente inoltrato messaggi ed effettuato telefonate spacciandosi per operatori della banca;
- dal documento in allegato alle controdeduzioni riportante i *log* delle operazioni, l'operazione afferente al bonifico oggetto della controversia risulta solo presa in carico ma non eseguita, pertanto, non risulta dimostrato in atti il perfezionamento materiale da parte della ricorrente stessa dell'effettuazione del bonifico stesso;
- risulta documentalmente comprovato che le transazioni fraudolente erano state classificate dal sistema di monitoraggio come caratterizzate da "*high risk score above threshold*", circostanza che avrebbe dovuto determinare il blocco automatico delle operazioni da parte dell'intermediario ma che quest'ultimo ha colpevolmente omesso di attuare;
- l'applicazione fraudolenta è stata scaricata direttamente dallo store ufficiale, recante i medesimi loghi e *claim* della banca e, a completamento della condotta fraudolenta, gli autori della truffa hanno imposto la disinstallazione della predetta applicazione, impedendo l'acquisizione di screenshot.

Inoltre, con le repliche, la ricorrente, rispetto alla domanda formulata in sede di ricorso, chiede altresì: "*In subordine e nella denegata ipotesi – di cui non si ravvedono le circostanze, considerato quanto esaustivamente esplicato in merito alle responsabilità della banca e alla tenuità della colpa della ricorrente - dovesse ravvisarsi un profilo di responsabilità in capo al nostro assistito, si chiede, ex art. 1227 c.c., una valutazione proporzionale che tenga conto dell'incidenza causale e della graduazione della colpa*."

L'intermediario, per contro, non ha presentato le controrepliche.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di un'operazione bancaria non autorizzata dell'importo complessivo di € 4.980,00 effettuata in data 12/11/2024 alle ore 12:16.

Alla data dell'operazione era vigente il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU.

In forza di tale disciplina, in caso di contestazione delle operazioni, grava sull'intermediario l'onere di provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza di aver applicato un c.d. "Sistema di autenticazione forte" (strong customer authentication o SCA), posto che ai sensi del comma 2-bis dell'art. 12 d. lgs. n. 11/2010, come inserito dal d. lgs. n. 218/2017, "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 beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente". L'intermediario, inoltre, è anche tenuto a 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 (art. 12, co. 2-ter e s., d. lgs. n. 11/2010).

Con riferimento alla strong customer authentication (c.d. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'art. 10-bis del D. Lgs. 10/2011, nelle 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 (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

In riferimento all'autenticazione forte – SCA – con riferimento alle azioni antecedenti all'esecuzione dell'operazione contestata, l'intermediario rappresenta che l'accesso all'*home banking* avviene mediante fattore di conoscenza (PIN) e fattore di possesso (OTP generato da Mobile Token).

Con riferimento alla fase di accesso all'*internet banking* del 12/11/2024, l'intermediario produce evidenze, sulla base delle quali si rileva il fattore di possesso, ma non vi è prova dell'effettivo inserimento del PIN.

Pertanto, non risulta possibile verificare la corretta applicazione della SCA.

Dalle evidenziate lacune probatorie quanto all'autenticazione, alla corretta registrazione e alla contabilizzazione delle operazioni mediante un c.d. "Sistema di autenticazione forte" consegue che, ad avviso del Collegio, l'intermediario resistente non ha provato di aver adottato gli standard di sicurezza corrispondenti alla disciplina oggi applicabile come sopra

individuata, dovendosi altresì ricordare che secondo il disposto dell'art. 10, co. 1, d.lgs. n. 11/2010 *"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"*.

A tale riguardo e in siffatto contesto, a differenza di quanto accade per la colpa grave dove si deve ammettere la possibilità di ricorrere alle presunzioni, per la SCA la prova non può essere indiziaria o indiretta, ma deve avere ad oggetto specificamente i singoli fattori di autenticazione, dovendo il prestatore di servizi di pagamento offrire puntuale evidenza di quali siano stati quelli in concreto ed effettivamente utilizzati, nonché del completo processo attraverso cui sono stati utilizzati (in questo senso, vd. ABF-Coll.- Milano n. 6881 del 5 luglio 2023 e n. 6933 del 6 luglio 2023).

Ciò premesso, rispetto alla mancanza anche parziale della prova di autenticazione, i Collegi sono unanimi nel ritenere che in tali casi il ricorso venga accolto integralmente, posto che il difetto di tale prova è risolutivo e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova di colpa grave dell'utente.

Questo Collegio ritiene che la documentazione allegata dalla parte resistente non sia esaustiva circa la prova dell'avvenuta autenticazione delle operazioni contestate; da ciò consegue che ogni ulteriore valutazione in merito alla sussistenza o meno della colpa grave in capo al ricorrente è del tutto irrilevante e la domanda restitutoria deve essere accolta.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.980,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA