COLLEGIO DI MILANO

composto dai signori:

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

Relatore DANIELE PERSANO

Seduta del 20/05/2025

FATTO

Nel presente procedimento, la parte ricorrente afferma quanto segue:

- in data 01/10/2024 subiva un attacco informatico al proprio computer con accessi anomali ai suoi diversi account;
- a tal proposito, riceveva diverse e-mail da tali profili, che segnalavano la presenza di login effettuati su altri dispositivi e geolocalizzati in località diverse da quella in cui si trovava e si muoveva nell'immediato per tutelarsi;
- in data 02/10/2024 alle ore 18:00 circa riceveva una chiamata dall'utenza 060*, riconducibile alla banca;
- il sedicente operatore lo informava di movimenti sospetti sul suo conto e mostrava di essere a conoscenza delle ultime operazioni eseguite e della filiale di riferimento;
- confidando nella genuinità della chiamata, si fidava del sedicente operatore e forniva un codice OTP per bloccare le transazioni anomale;
- non riceveva, come solitamente accade, notifiche tramite SMS, e-mail o *pop up* nell'applicazione per le operazioni in uscita sospette;
- terminata la telefonata, non riusciva ad accedere all'applicazione della banca con le proprie credenziali;

- contattava quindi il numero verde della banca e, svolgendo un'operazione simile a quella della chiamata precedente, veniva a conoscenza dell'esecuzione di n. 4 operazioni di pagamento tramite bollettini e n. 1 bonifico bancario, che veniva immediatamente bloccato;
- i bollettini, che erano stati effettuati digitalmente tramite il servizio di *home banking* per gli importi di € 1.490,00, € 1.500,00, € 1.500,00 ed € 1.500,00, non potevano essere bloccati in quanto modalità di pagamento immediate e non richiamabili;
- i bollettini non venivano bloccati all'origine, nonostante sia previsto che l'esecutore del pagamento debba essere uguale al titolare del conto e nel caso di specie l'esecutore fosse diverso dal titolare del conto;
- non poteva accertarsi che il sedicente operatore della prima chiamata fosse un truffatore, in quanto era a conoscenza dei suoi dati sensibili e le informazioni richieste risultavano simili a quelle richieste in una conversazione genuina con la banca;
- gli elevati importi e le modalità delle operazioni eseguite sono insoliti rispetto alle movimentazioni che era solito compiere;
- in data 03/10/2024 presentava denuncia presso le Autorità competenti e disconosceva, ottenendo il rigetto della propria richiesta da parte della banca, le operazioni.

Il ricorrente chiede, dunque, all'Arbitro, di accertare il proprio diritto ad ottenere il rimborso dell'importo che ritiene essergli stato fraudolentemente sottratto, complessivamente pari ad € 6.000,00.

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

- il rimborso chiesto dal ricorrente corrisponde a n. 4 bollettini postali, disconosciuti, autorizzati online dal sito web della banca con le credenziali del ricorrente a debito del conto corrente n. *121;
- le operazioni oggetto di contestazione non sono revocabili in quanto bollettini;
- la richiesta di rimborso è stata oggetto di reclamo il 03/10/2024 e di replica il 21/11/2024, ritualmente riscontrati dalla banca il 21/10/2024 e il 20/12/2024;
- il ricorrente è intestatario del conto corrente *121, al quale è collegato il servizio di *home banking* che consente ai clienti di effettuare le operazioni di *inquiry* e *dispositive* su tutti i conti correnti personali a loro riferibili utilizzando il cellulare o internet;
- il ricorrente ha altresì attivato dal 2022, senza interruzioni, il servizio di SMS-*alert* collegato alla sua utenza telefonica *759;
- nella denuncia il ricorrente ha dichiarato di aver intrattenuto una conversazione con l'interlocutore, qualificatosi come operatore della banca, della chiamata ricevuta dal numero 060* e di aver seguito le istruzioni del sedicente operatore, tra cui quella di comunicare il codice ricevuto tramite app;
- è bastato ai frodatori chiedere il codice del Mobile Token al fine di effettuare delle verifiche per ottenerlo senza alcuna obiezione;
- non è stato assolto l'onere della prova posto a carico del ricorrente *ex* art. 2967 c.c., che viene sanzionato da tutti i Collegi ABF;
- stanti le modalità di esecuzione delle dispositive per come narrate dal ricorrente in denuncia, che evidenziano la piena consapevolezza dell'operatività posta in essere dal ricorrente, non può trovare applicazione il regime di protezione previsto dal D.lgs. n. 11 del 2010, in quanto trattasi di pagamenti eseguiti volontariamente dal ricorrente, come da sua stessa ammissione;

- ha inviato al ricorrente le comunicazioni, via SMS ed e-mail, in merito all'attivazione del Mobile Token;
- è evidente che il ricorrente ha abboccato ad una telefonata di *phishing*, che rappresenta un tipo di frode ormai diffusa, conosciuta come strumento di approfittamento della credulità delle vittime, quindi inescusabile e ritenuta elemento qualificabile come colpa grave da parte dei Collegi ABF.

Successivamente, il cliente, in sede di repliche, richiamati i propri scritti, insiste nella richiesta di restituzione delle somme fraudolentemente sottratte, precisando ulteriormente che:

- ha ricevuto la chiamata truffaldina in data 02/10/2024 alle ore 18:00 circa;
- si è allarmato quando ha ricevuto l'SMS-*alert* relativo all'inserimento del bonifico bancario, che è stato bloccato;
- non ha tenuto una condotta negligente in quanto confidava di interloquire con un operatore dell'intermediario, non notando alcuna anomalia nell'attività richiesta e confidando nella genuinità delle operazioni;
- i truffatori erano già in possesso di tutti i dati necessari per utilizzare l'app della banca, presumibilmente a causa dell'hackeraggio del pc;
- non ha ricevuto tramite SMS o e-mail o notifica *push* nell'applicazione le notifiche che lo informavano che erano in corso operazioni in uscita sospette, poiché i messaggi sono giunti sul telefono del truffatore;
- la colpa grave è esclusa dinnanzi a forme di truffa dal carattere sofisticato come quella in specie, in cui l'insidiosità del meccanismo di aggressione consiste nell'utilizzo di canali di comunicazione apparentemente riferibili all'intermediario;
- trattandosi di pagamenti effettuati digitalmente tramite il servizio di *home banking*, l'esecutore del pagamento deve essere uguale al titolare del conto o comunque un delegato ad agire sullo stesso;
- la successione di n. 4 pagamenti in pochi minuti, subito dopo un cambio *device*, di importo elevato non ha fatto scattare nessun *alert* nei sistemi della banca, denotando questo una grave carenza dei sistemi di controllo della banca determinante ai fini della riuscita della truffa;
- l'elenco dei log mostra una successione di indirizzi IP, l'IP *185 è a lui riferibile e l'IP *231 è riferibile al truffatore, ed è impossibile che il cliente si sia spostato da un luogo all'altro nell'arco di pochi secondi;
- prima della telefonata truffaldina ha visto comparire dei messaggi a tendina dall'app della banca per dei tentativi di login e immissione pagamento, circostanza che prova che i truffatori stavano già cercando di infiltrarsi nella sua applicazione di *home banking*;
- nessun operatore dell'intermediario ha contattato l'assistito per chiedere l'autenticità di operazioni anomale;
- la truffa subita è stata causata dalle carenze dei sistemi di sicurezza della banca e dall'inerzia dell'intermediario.

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

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di n. 4 operazioni bancarie non autorizzate dell'importo complessivo di € 5.999,60 effettuate in data 02/10/2024.

Nello specifico si tratta delle seguenti operazioni:
1) 02/10/2024 alle ore 18.09: € 1.492,40;
2) 02/10/2024 alle ore 18.10: € 1.502,40;
3) 02/10/2024 alle ore 18.17: € 1.502,40;
4) 02/10/2024 alle ore 18.21: € 1.502,40.

Il ricorrente chiede il rimborso della somma di € 6.000,00, ottenuta arrotondando per eccesso l'importo di € 5.999,60.

Tale importo è dato dalla somma delle operazioni eseguite tramite bollettino, incluse le commissioni applicate per € 1,20/cad.

Alla data delle operazioni 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 relazione all'autenticazione forte – SCA – con riguardo alle azioni antecedenti all'esecuzione dell'operazione contestata, in via generale, l'intermediario rappresenta che l'accesso da APP 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*, l'intermediario produce evidenze, sulla base delle quali si rileva il fattore di possesso, ma non vi è prova dell'effettivo inserimento del PIN da parte del cliente.

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 € 6.000,00.
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