

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) SANTARELLI

Seduta del 24/03/2026

FATTO

Parte ricorrente agisce in relazione ad alcune operazioni truffaldine effettuate a debito del suo conto corrente n. *953. Riferisce, in proposito, di aver ricevuto in data 12.06.2025, alle ore 15:48, mentre era impegnato al lavoro, una mail da noreply@i*.it che lo avvisava di una nuova attivazione dell'App I* su di un dispositivo iP**16ProiMax a lui del tutto sconosciuto e di aver ricevuto pochi minuti dopo, alle ore 16:03, altra mail dal medesimo servizio *alert* che gli comunicava come dal suo conto corrente fosse stato inviato un bonifico istantaneo per l'importo di € 850,00 ad una persona a lui sconosciuta. Poiché in quel momento era impegnato in un cantiere, aveva modo di leggere la posta elettronica solo qualche decina di minuti più tardi, quando, gli veniva negato l'accesso all'app della propria banca. Chiamata immediatamente la filiale di riferimento, apprendeva che sul suo conto corrente risultava effettuata sia l'operazione di bonifico citata sia altra operazione non meglio identificata e che risultava poi essere un pagamento POS. L'accesso all'App veniva bloccato e gli veniva indicato che doveva procedere ad una nuova installazione. Apprendeva successivamente che il totale sottratto ammontava a complessivi € 1.500,00, oltre a commissioni bancarie per € 0,50. Ciò premesso, parte ricorrente afferma di non aver concorso in alcun modo al compimento delle operazioni sconosciute, di non aver fornito a nessuno le proprie credenziali, all'evidenza, carpite da terzi mediante il probabile accesso abusivo ai sistemi telematici della banca e/o dell'operatore del servizio App, ovvero I*. Afferma, altresì, che le operazioni

contestate non sono state autenticate e che le misure di sicurezza predisposte dall'intermediario si sono dimostrate del tutto insufficienti anche sotto il profilo della buona fede nell'esecuzione del contratto. Infine, ritiene dimostrata la sua estrema diligenza, dal momento che, nel giro di meno di venti minuti dall'alert ricevuto via mail, si è attivato per avvertire la filiale dell'intermediario, così scongiurando danni ulteriori. Di qui la domanda di restituzione dell'importo sottrattogli oltre alle relative commissioni.

L'intermediario chiede il rigetto del ricorso nonché, in via subordinata, l'accertamento del concorso di colpa di parte ricorrente con quantificazione "*della minor somma eventualmente dovuta*". Questa la sintesi delle prospettazioni e delle ragioni fatte valere: (a) il servizio di *internet banking* prevede informative preventive sui requisiti tecnici, sulle modalità d'uso e sui rischi connessi, nonché la consegna di credenziali personali e l'obbligo per l'utente di adottare misure idonee alla loro protezione; (b) l'accesso e l'operatività *online* risultano subordinati ai sistemi di autenticazione forte, mediante credenziali statiche abbinate a codici dinamici o strumenti biometrici, come contrattualmente previsto; (c) le verifiche tecniche evidenziano la comunicazione a terzi, da parte del ricorrente, delle credenziali associate alla postazione di *internet banking*, circostanza che ha consentito l'*enrollment* su un nuovo dispositivo e la successiva operatività fraudolenta; (d) i *log* dimostrano la ricezione, da parte del ricorrente, degli avvisi relativi al cambio dispositivo tramite app e tramite e-mail, senza che sia stato disposto alcun blocco della postazione; (e) l'*enrollment* ha permesso al terzo di abilitare la biometria e autorizzare sia un'operazione di pagamento *e-commerce* sia un bonifico, eseguiti mediante i nuovi sistemi di autenticazione; (f) la condotta di parte ricorrente integra violazione degli obblighi contrattuali di custodia e riservatezza delle credenziali nonché mancata attenzione agli *alert* ricevuti, con conseguente contributo determinante alla realizzazione della frode; (g) sono state effettuate campagne informative sul rischio di frodi, pubblicate tramite sito aziendale, piattaforme *online* e comunicazioni alla clientela, idonee a sensibilizzare l'utente sull'uso prudente degli strumenti dispositivi.

Parte ricorrente ha replicato per osservare che: (i) l'evento generatore delle operazioni oggetto del contendere consiste nell'abusiva attivazione dell'app di *home banking* su un dispositivo mai utilizzato dal lui, mediante una procedura fraudolenta avvenuta senza alcun suo intervento; (ii) l'intera sequenza operativa non avrebbe potuto realizzarsi senza il preliminare abuso consistente nel trasferimento della *app* su un dispositivo estraneo, circostanza che ha consentito al terzo un accesso privo di ostacoli; (iii) l'intermediario sostiene che l'installazione della app sul nuovo dispositivo sarebbe stata autorizzata dall'inserimento, da parte del cliente, di un codice OTP ricevuto sul proprio device, circostanza che non corrisponde alla realtà dei fatti; (iv) la migrazione della *app* dovrebbe presupporre la disinstallazione dal dispositivo originario e non risulta coerente, per finalità di sicurezza, il rilascio di un unico codice OTP destinato alla nuova installazione; (v) l'intermediario ammette che il trasferimento della *app* e il completo accesso del terzo possano essere stati consentiti attraverso l'inserimento di un solo codice OTP, meccanismo manifestamente insufficiente a garantire la sicurezza del servizio; (vi) la scansione temporale degli eventi dimostra l'assenza di alcuna colpa a suo carico, giacché tra l'avviso di trasferimento della app e le operazioni fraudolente sono trascorsi soltanto pochi minuti, tempo insufficiente per qualunque intervento utile; (vii) la ricostruzione dell'intermediario risulta smentita anche quanto alla presunta comunicazione delle credenziali a terzi, non avendo mai ricevuto alcun SMS, ma esclusivamente e-mail, alle quali ha reagito nell'immediato contattando la filiale per il blocco dell'app; (viii) la documentazione prodotta dall'intermediario non prova che la richiesta di attivazione, la ricezione del codice OTP e il relativo inserimento siano avvenuti sul suo dispositivo, risultando anzi

evidente che il destinatario degli avvisi fosse un diverso identificativo; (ix) dagli atti emerge che notifiche e codici sono stati indirizzati allo stesso identificativo estraneo, poi utilizzato per autorizzare le operazioni contestate; (x) l'intermediario, pur dichiarando di conoscere il fenomeno diffuso delle frodi tramite app di *home banking*, non ha predisposto adeguati meccanismi di controllo atti a rilevare l'evidente anomalia delle operazioni, in violazione dei doveri di correttezza e buona fede contrattuale; (xi) tali doveri risultano ulteriormente rafforzati in presenza di un rapporto con un consumatore, imponendo specifiche cautele informative e tecniche sulla natura irrevocabile delle operazioni dispositive online; (xii) nella specie tali doveri non sono stati rispettati: non ha ricevuto alcun SMS, come confermato dall'assenza di riscontri documentali, con conseguente inidoneità dell'invio di semplici e-mail a garantire un adeguato livello di sicurezza nei casi di trasferimento fraudolento dell'app; le notifiche inviate sulla app trasferita o clonata non assicurano alcuna protezione, risultando quindi inefficaci nel prevenire l'illecito utilizzo dei servizi di *home banking*. Dunque, secondo parte ricorrente, l'insieme delle circostanze evidenzia la responsabilità esclusiva dell'intermediario nella gestione dell'autenticazione e della sicurezza, con conseguente obbligo di rimborso integrale del danno subito dal cliente.

L'intermediario ha a sua volta replicato per sottolineare quanto segue: (a) l'assenza di diligenza nella custodia delle credenziali di sicurezza contrasta con le obbligazioni contrattuali previste per l'utilizzo dei servizi dispositivi; (b) la normativa e l'orientamento dell'Arbitro Bancario Finanziario indicano che la violazione degli obblighi di custodia configura condotta negligente dell'utilizzatore e può fondare la sua responsabilità per operazioni non autorizzate; (c) la prova della regolare autenticazione tramite SCA e la mancata allegazione di circostanze alternative da parte del ricorrente costituiscono elementi presuntivi di colpa grave; (d) l'attivazione dell'App dedicata ai servizi dispositivi risulta effettuata tramite corretto inserimento di credenziali statiche e codice OTP inviato all'applicazione certificata associata all'utenza telefonica del ricorrente; (e) le comunicazioni relative all'attivazione dell'App risultano trasmesse tramite notifica *push* ed e-mail inviata all'indirizzo indicato in contratto; (f) l'applicazione utilizzata per la ricezione dei codici OTP risulta installata in data antecedente e associata al numero di telefono indicato in contratto; (f) l'inserimento del codice OTP per l'installazione dell'App sul dispositivo dal quale sono state disposte le operazioni contestate conferma il rispetto delle procedure di Strong Customer Authentication; (g) le operazioni successive, eseguite tramite carta di debito e conto corrente, risultano autorizzate mediante credenziali statiche, PIN o biometria, con conferme inviate tramite notifiche *push* ed e-mail; (h) l'operazione e-commerce risulta preceduta da accesso autenticato e successivamente autorizzata con PIN/biometria, con conferma generata dall'applicazione notifiche; (i) il bonifico istantaneo oggetto di contestazione risulta disposto previo accesso autenticato, con inserimento dei dati e autorizzazione mediante biometria, e risulta seguito da conferma tramite notifica e comunicazione via e-mail; (j) le notifiche relative alle operazioni risultano inviate al dispositivo certificato associato al ricorrente, mentre il *token* notifiche risulta attivo durante le operazioni e modificato solo successivamente per aggiornamento automatico del sistema; (k) le risultanze tecniche confermano l'accesso alla piattaforma e l'esecuzione delle operazioni mediante dispositivo e utenza riconducibili al ricorrente, senza evidenza di malfunzionamenti dei sistemi dell'intermediario; (l) l'assenza, nel ricorso e nella denuncia, di qualsiasi descrizione delle modalità della presunta frode costituisce elemento valutato costantemente dall'ABF quale indice rilevante ai fini dell'integrazione della colpa grave; (m) la prova della corretta autenticazione e la mancata descrizione delle modalità

della frode da parte del ricorrente determinano la presunzione di colpa grave e l'insussistenza del diritto al rimborso delle somme contestate.

DIRITTO

Materia del contendere sono due operazioni - un bonifico e un pagamento *online* - per l'importo complessivo di € 1.500,00 (€ 650,00 + 850,00) + € 0,50 per commissioni, effettuate il 12.06.2025 rispettivamente alle ore 15:51 (€ 650,00) e ore 16:03 (€850,00). Come è ormai noto, sull'intermediario, in applicazione dei principi che regolano le operazioni fraudolente ai sensi del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17, grava l'onere di provare l'autenticazione forte non solo delle operazioni disconosciute, ma anche di tutti i passaggi precedenti necessari alla loro esecuzione è la eventuale colpa grave del cliente. Restano fermi gli oneri di allegazione e prova dei fatti che hanno portato alla truffa in capo al cliente.

Partendo dall'autenticazione, sulla base della documentazione prodotta dall'intermediario risulta anzitutto quali dispositivi fossero associati all'utenza di parte ricorrente ed il fatto che in data 12.06.2025 alle ore 15:48 l'App è stata installata su un nuovo dispositivo (Ip*** 16ProMax). L'*enrollment* del tale nuovo dispositivo risulta effettuato tramite OTP inviato sul *device* di parte ricorrente e correttamente inserito. Agli atti risultano anche la notifica inviata a parte ricorrente in relazione a tale *enrollment* via SMS e via e-mail. Sempre dai *log* e relativa legenda risulta che alle 15.48 del 12/06/2025 è stato effettuato un *login* sul dispositivo del ricorrente con inserimento di password/ biometria e *User ID*. Poco dopo il *login* risulta altresì evidenza della attivazione della SCA biometrica sul nuovo dispositivo abilitato. Dunque, dalle evidenze prodotte emerge che l'*enrollment* sul nuovo dispositivo è stato effettuato mediante accesso all'App già installata sul dispositivo originario, tramite autenticazione con *userID* e *password* ovvero tramite fattore biometrico (fattore di conoscenza/inerenza), come desumibile dalla lettura congiunta delle tracciatore informatiche e della relativa legenda interpretativa. Successivamente, il processo di attivazione è stato perfezionato mediante l'inserimento del codice OTP inviato al dispositivo precedentemente certificato (fattore di possesso). La prima operazione – un pagamento *e-commerce* – presuppone, secondo le spiegazioni fornite dall'intermediario la seguente procedura standard: inserimento dei dati della carta sul sito dell'esercente; la ricezione di una richiesta di autenticazione sull'App I*; la visualizzazione all'interno dell'App dei dettagli dell'operazione; ed infine la convalida del pagamento tramite biometria. Da quanto prodotto dall'intermediario risulta che la carta pan 463345*****391 utilizzata era associata all'utenza telefonica certificata n. *863 e che è stata attivata la SCA BIOMETRICA (senza evidenza di fattori di autenticazione *ad hoc*) abilitando la funzionalità di "Autorizzazione rapida" delle operazioni di pagamento e-commerce, previo accesso all'area riservata tramite App I*. Quindi il 12.06.2025 alle ore 15:50 è stata inviata tramite app I* nel frattempo caricata dai truffatori (come detto sopra) una notifica *push* per l'autenticazione dell'operazione di pagamento e-commerce di € 650,00, autenticazione poi intervenuta con fattore biometrico dall'App in uso ai truffatori alle ore 15:51. Agli atti risulta anche evidenza della notifica *push* relativa all'intervenuto pagamento. Dunque, l'autenticazione risulta avvenuta mediante i due fattori previsti dalla SCA: da un lato il possesso del dispositivo mobile associato all'utenza telefonica certificata (viene indicato il modello "Ip*** 16Promax" appena prima 'enrollato' e in uso ai truffatori), necessario per ricevere la notifica *push* sull'App I*, e dall'altro la biometria, utilizzata per confermare l'operazione tramite impronta digitale o riconoscimento facciale.

Quanto alla seconda operazione, in atti vi è evidenza che alle ore 16:02 del 12.06.2025 è stato effettuato il *login* di accesso sul dispositivo in uso ai truffatori tramite SCA costituita dal 'possesso' del nuovo dispositivo mobile previamente *enrollato* - che costituisce l'elemento necessario per ricevere e gestire l'accesso all'app - e l' 'inerenza', rappresentata dalla verifica biometrica (impronta o volto) con cui l'utente ha effettuato l'accesso prodromico all'operatività. Quanto all'operazione - un bonifico istantaneo dell'importo di € 850,00 – inserito alle ore 16:03, risulta autorizzato tramite biometria (riconoscimento facciale) dovendosi ritenere che il secondo fattore sia rappresentato dal fattore impiegato per il login e cioè nella specie il fattore di possesso (device su cui è stata installata l'App) inserito in fase di login. Anche in questo caso in atti vi è evidenza della notifica *push* inviata dall'intermediario.

Verificata la prova della SCA per le due operazioni, deve essere esaminata la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa grave.

Dalla denuncia e dalla sua integrazione emerge che parte ricorrente il 12 giugno 2025, mentre stava lavorando, ha ricevuto una prima e-mail di alert da "*noreply@i*.it*" che gli segnala l'attivazione dell'app I* su un iP*** 16 Pro Max (quello dei truffatori di cui si è esaminato sopra l'*enrollment*). Dopo pochi minuti, parte ricorrente riceveva una seconda e-mail dallo stesso servizio, che lo avvisa che dal suo conto è stato effettuato un bonifico istantaneo di € 850,00. Parte ricorrente ha dichiarato in proposito che, essendo impegnato in un cantiere, non è riuscito a leggere subito gli avvisi e che, quando lo ha potuto fare, ha provato ad accedere alla sua app bancaria, scoprendo che l'accesso era bloccato, perché i truffatori avevano preso il controllo dell'*account*. Dalla documentazione prodotta risulta che parte ricorrente ha ricevuto l'email relativa all'installazione dell'App su un nuovo dispositivo alle ore 15:48 e che alle ore 15:51 è stata effettuato il primo pagamento. Tuttavia, né dalla denuncia né dal ricorso è dato apprendere molto delle circostanze in cui si è inserita la truffa patita – ad esempio in relazione alla ricezione dell'OTP - e quindi quali siano i fatti che hanno portato all'esecuzione delle operazioni disconosciute a fronte (i) della prova della SCA; (ii) del fatto che il conto risulta essere stato bocciato alle 16:36 mentre la carta di pagamento lo è stata per un'anomalia rilevata dall'intermediario alle ore 15:57; (iii) dell'invio della mail con cui parte ricorrente è stata informata dell' *enrollment* del nuovo dispositivo e del bonifico di € 850,00 nonché della notifica *push* contenente l'OTP necessaria per perfezionare detto *enrollment* al dispositivo in uso a parte ricorrente così come delle notifiche alert; (iv) del brevissimo lasso temporale in cui sono state effettuate le due operazioni contestate (le ore 15:51 e 16:03 del 12.06.2025). Il quadro così rappresentato non consente di accogliere il ricorso né di ravvisare una responsabilità concorrente dell'intermediario (anche in carenza di circostanze che valgano a evidenziare artifici che possano aver agevolato equivoci in ordine alla genuinità di eventuali messaggi ricevuti), non valendo in proposito l'argomento addotto da parte ricorrente in relazione ai fattori di autenticazioni richiesti per l'*enrollment* di un nuovo dispositivo, fattori che rispecchiano i requisiti di legge, per quanto è stato possibile apprendere dalla documentazione prodotta.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE