COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore GIORGIO CORNO

Seduta del 18/02/2025

FATTO

La ricorrente è titolare di conto corrente presso l'intermediario. In data 5 agosto 2024 alle ore 14:07 la ricorrente riceveva un SMS sulla sua utenza telefonica con il quale veniva informata che il suo conto era stato sospeso e veniva invitata a contattare un numero di telefono indicato nel predetto SMS. In data 6 agosto 2024 la ricorrente provvedeva a contattare il numero indicato nell'SMS, senza successo. Alle ore 17:00 del medesimo giorno veniva contattata dal numero in questione e l'interlocutore - qualificatosi come operatore dell'intermediario - le proponeva di proseguire la telefonata tramite WhatsApp al fine di porre rimedio alla situazione di blocco del conto. Alle ore 18:00 riceveva telefonata WhatsApp alla quale non rispondeva e alle 18:08 provvedeva personalmente a ricontattare il numero.
Nel corso del colloquio l'operatore la invitava a scaricare una applicazione "APKAP" asseritamente necessaria a rendere sicure le operazioni bancarie e, infine, le comunicava che l'avrebbe ricontattata il giorno successivo non essendo riuscito a risolvere la problematica. In data 7 agosto 2024 riceveva una nuova chiamata e l'operatore la invitava a seguire le istruzioni riferendo, infine, la presenza di ulteriori problemi che non riusciva a risolvere. In data 9 agosto 2024 alle ore 11:40 la cliente riceveva un'ulteriore chiamata da un soggetto qualificatosi come operatore dell'intermediario che la avvisava di una possibile truffa.

La ricorrente - terminata la chiamata senza fornire informazioni - si recava in filiale avvedendosi dell'effettuazione di n. 10 operazioni per complessivi € 48.047,50 che sostanzialmente azzeravano la disponibilità presente sul suo conto. Provvedeva quindi a presentare denuncia presso le Autorità competenti in data 9 agosto 2024 e reclamo all'intermediario in data 27 agosto 2024, riscontrato negativamente in data 18 ottobre 2024.
Con ricorso all'ABF del 28 ottobre 2024, la ricorrente chiede l'immediato riaccredito di tutte le somme oggetto di truffa, il risarcimento del danno nella misura che sarà ritenuta equa dal Collegio e la messa a disposizione del tracciato delle notifiche da parte dell'intermediario.
La ricorrente afferma che la banca avrebbe dovuto riconoscere l'anomalia delle operazioni e pertanto, almeno il 7 agosto 2024, avrebbe dovuto bloccare il conto evitando la prosecuzione della truffa; lamenta inoltre che sono state disposte operazioni per un importo superiore al limite disponibile.

Con le controdeduzioni l'intermediario chiede il rigetto del ricorso.
Produce documentazione che attesta che l'operazione è stata correttamente contabilizzata, registrata e autenticata tramite il corretto inserimento di un doppio fattore di autenticazione. Afferma che la ricorrente ha seguito le istruzioni ricevute al telefono dal suo interlocutore, persona a lei sconosciuta, digitando le credenziali di sicurezza della propria home banking, previa installazione di un'app "malevola" (non riferibile in alcun modo alla banca), rendendole così note al malintenzionato.
Precisa inoltre che, in merito al canale di provenienza degli SMS ed alla telefonata, si tratta di numeri ad essa non riferibili, nonché di non servirsi per le sue comunicazioni di telefonate via WhatsApp ma solo di canali ufficiali.
Evidenzia inoltre come la frode si è articolata in due giorni ma la ricorrente non si è colpevolmente premurata di verificare dal suo estratto conto disponibile sul suo home banking l'esecuzione dei bonifici sin dal primo giorno della frode che, peraltro, è stata oggetto di notifiche *push* e/o *SMS-alert*.

Nelle repliche alle controdeduzioni la cliente afferma che gli SMS e le notifiche *push* prodotte dall'intermediario non provano l'effettiva ricezione degli stessi da parte della ricorrente, con tutta probabilità intercettati dal truffatore. Contesta la carenza di sicurezza nel sistema dell'intermediario e afferma di non aver mai digitato le proprie credenziali.

DIRITTO

Oggetto del ricorso è la richiesta del rimborso di n. 10 operazioni di bonifico per complessivi € 48.047,50 (comprensive di € 7,50 di spese di commissione), in particolare: in data 6 agosto 2024 alle ore 18:18 per € 4.880,00, alle ore 18:19 per € 4.960,00 e alle ore 18:21 per €4.720,00 , alle ore 18:22 per € 4.840,00, alle ore 18:24 per € 4.400,00, alle ore 18:26 per € 4.720,00; e in data 7 agosto 2024 alle ore 18:24 per € 4.960,00, alle ore 18:26 per € 4.890,00, alle ore 18:27 per € 4.920,00, alle ore 18:29 per € 4.750,00.
La ricorrente chiede altresì il risarcimento del danno nella misura che sarà ritenuta equa dal Collegio e la messa a disposizione del tracciato delle notifiche da parte dell'intermediario.

Quanto all'ultima domanda, non viene riproposta in sede di repliche alle controdeduzioni in quanto l'intermediario ha prodotto la documentazione richiesta in allegato alla propria memoria.

Il Collegio rileva che le operazioni di pagamento contestate rientrano nell'ambito applicativo del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218. Poiché il ricorrente, quale utente di servizi di pagamento, ha negato di aver autorizzato le operazioni di pagamento eseguite, è onere dell'intermediario, ai sensi dell'art. 10 del medesimo D.lgs., quale prestatore di servizi di pagamento, provare che tali operazioni sono state autenticate, correttamente registrate e contabilizzate e che non hanno subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o altri inconvenienti. Ai sensi dell'art. 10-bis del ricordato D.lgs., i prestatori di servizi di pagamento sono tenuti ad applicare modalità di autenticazione forte del cliente (*strong customer authentication*, SCA) quando l'utente: a) accede al suo conto di pagamento online; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.
Nel caso di avvio di un'operazione di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico. L'autenticazione forte (SCA) è richiesta sia nella fase di (i) accesso al conto/*enrollment* dell'app/registrazione della carta sul *wallet*, sia nella fase di (ii) esecuzione delle singole operazioni; e 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.
Alla luce del disconoscimento delle operazioni da parte del cliente, è altresì onere dell'intermediario di fornire prova della frode, del dolo o della colpa grave dell'utente.

Nel caso di specie, la prova della corretta autenticazione, corretta registrazione e contabilizzazione dell'operazione di pagamento disconosciuta dal cliente deve avere ad oggetto le diverse fasi della realizzazione della truffa ovvero: (i) il login/accesso all'area riservata prodromico all'operazione contestata; e (ii) l'esecuzione dell'operazione contestata.
Quanto al login/accesso all'area riservata prodromico alle prime cinque operazioni effettuate in data 6 agosto 2024, l'intermediario afferma che sarebbe stato effettuato con inserimento dell'ID utente e PIN (elemento di conoscenza) e OTP generato con il *device* della ricorrente (elemento di possesso). A tal fine produce evidenza dalla quale si ricava che alle ore 18:09:38 del 6 agosto 2024 è stato eseguito l'accesso all'home banking con ID utente e PIN (elemento di conoscenza) (cfr. colonna Attività "Accesso con ID Utente e Pin con verifica a due fattori con OTP da Mobile Token") e generazione in app dell'OTP cosiddetto silente (cfr. colonna OTP popolata e relativa legenda esplicativa).

Alla luce della legenda si rileva che:

- l'inserimento dell'ID Utente risulta dalla relativa colonna popolata;
- la generazione dell'OTP silente risulta dalla relativa colonna popolata ("OTP transazionale generato dal Mobile Token utilizzato. Questo dimostra che la dispositiva è stata firmata con l'utilizzo del Mobile Token come da norma PSD2") (elemento di possesso);

- quanto all'inserimento del PIN (elemento di conoscenza), si evidenzia che l'utilizzo del PIN risulta dalla descrizione attività utente e dalle dichiarazioni dell'intermediario, il quale precisa che "*il codice PIN, la cui digitazione è confermata nella colonna attività, essendo un codice noto solo al cliente, che la Banca non conosce, non può essere decodificato*".

Si osserva, inoltre, che il codice OTP virtuale risulta generato (cfr. relativo campo popolato): tale circostanza può verificarsi solo a seguito dell'inserimento del PIN. Occorre tuttavia rilevare che, dai log prodotti, non è possibile confermare tale affermazione, né è presente alcuna valorizzazione alla voce "esito operazione".
Medesima documentazione è stata prodotta con riguardo al login/accesso all'area riservata prodromico all'ultima operazione effettuata in data 6 agosto 2024 e al login/accesso all'area riservata prodromico alle operazioni del 7 agosto 2024.

Il Collegio di Milano, in casi come quello in esame, non ritiene provata la SCA in fase di login in quanto non è documentato l'inserimento del PIN e non sono ritenute sufficienti le dichiarazioni dell'intermediario negli atti del procedimento.
Ciò di per sé non consente di ritenere provata da parte dell'intermediario la corretta autenticazione, corretta registrazione e contabilizzazione delle operazioni di pagamento disconosciute dal cliente, con conseguente accoglimento del ricorso per € 48.048,00 (dal 1 ottobre 2020, con l'entrata in vigore delle modifiche alle Disposizioni ABF, gli importi contenuti nelle pronunce di accoglimento sono arrotondati all'unità di euro).

La ricorrente chiede altresì il risarcimento del danno nella misura che sarà ritenuta equa dal Collegio.
Dagli atti del procedimento emerge che la ricorrente non ha fornito alcuna prova del concreto pregiudizio economico asseritamente subìto, né con riguardo all'*an* né sul *quantum* del pregiudizio lamentato. È principio consolidato nella giurisprudenza di questo Arbitro che il risarcimento del danno è sempre commisurato all'effettivo pregiudizio subito dal titolare del diritto e non può mai degradare a ristoro - come nel caso di specie - per un danno *in re ipsa* (così Collegio di Coordinamento, decisione n. 1642/2019).
Tantomeno questo Collegio può operare una quantificazione equitativa ai sensi dell'art. 1226 c.c., posto che essa può operare unicamente laddove sia stata dimostrata l'esistenza del danno risarcibile, ma sia impossibile o comunque eccessivamente difficile quantificarlo esattamente.
Da ultimo, questo Arbitro ha condiviso i consolidati indirizzi della Suprema Corte, secondo cui è consentita la risarcibilità dei danni non patrimoniali soltanto nelle ipotesi previste dalla legge, nonché in caso di lesione di un interesse di rilevanza costituzionale, laddove la lesione sia grave e il danno non sia futile.

Non è pertanto accoglibile la richiesta risarcitoria formulata dalla ricorrente.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 48.048,00.
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