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 25 settembre 2024 alle ore 16:57 la ricorrente riceveva una telefonata da un numero apparentemente riconducibile all'intermediario. L'interlocutore si qualificava come operatore dell'intermediario e comunicava alla cliente che era stata presentata una richiesta di modifica del dispositivo associato alla sua utenza. Non avendo effettuato tale richiesta, la ricorrente seguiva le indicazioni dell'interlocutore al fine di bloccare l'operazione. L'interlocutore riferiva alla ricorrente che avrebbe dovuto scaricare un'applicazione "Certificato Web" e seguire le indicazioni che apparivano, acconsentendo alle richieste di autorizzazione richieste da tale applicazione. Nel procedimento l'app dell'home banking non risultava più presente sul dispositivo della ricorrente. Prima di terminare la telefonata l'interlocutore dava appuntamento telefonico alla ricorrente per il giorno successivo, spiegando che occorrevano 24 ore per completare la procedura.
La ricorrente riferisce che essendosi insospettita provvedeva a contattare il numero dell'assistenza ma cadeva la linea.
Veniva poi ricontattata da altro presunto operatore dell'intermediario il quale le chiedeva se avesse contattato l'assistenza, rassicurandola che, se non avesse comunicato le credenziali a terzi, non avrebbe dovuto preoccuparsi; lo stesso riferiva anche di non continuare a chiamare l'assistenza o recarsi in filiale per non rallentare la procedura.

Il giorno successivo la ricorrente, recandosi in filiale, si avvedeva che era stato effettuato un bonifico per € 6.800,00 e che l'applicazione che i truffatori le avevano chiesto di scaricare era finalizzata ad entrare nel dispositivo della ricorrente per carpire le sue credenziali. La ricorrente provvedeva quindi a presentare denuncia alle Autorità in data 26 settembre 2024 ed a disconoscere il bonifico non autorizzato presso l'intermediario.
Il disconoscimento ed il reclamo della ricorrente sono stati rigettati dall'intermediario con lettere del 14 e 29 ottobre 2024.
Con ricorso all'ABF del 15 novembre 2024, la ricorrente ha chiesto il rimborso della somma complessiva di € 6.801,00 oggetto dell'operazione non autorizzata e disconosciuta, comprensiva delle spese di bonifico. Riferisce di non aver mai comunicato le proprie credenziali personali e/o i dati essenziali per l'esecuzione dell'operazione contestata e, pertanto, ciò varrebbe a ritenere che i sistemi di sicurezza della banca siano gravemente carenti.
Ne consegue che l'intermediario è tenuto a risarcire la cliente.

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 riposto ingiustificata fiducia nel "*caller ID*" che appare su telefono in quanto risaputo che non garantisce che la chiamata provenga effettivamente dall'utenza indicata sul display. Precisa inoltre che, seguendo le indicazioni dell'interlocutore telefonico, la ricorrente ha affermato di aver scaricato un'applicazione dal funzionamento sconosciuto e non riferibile in alcun modo alla banca, per mezzo della quale verosimilmente i truffatori hanno assunto il controllo del suo dispositivo, assecondando altresì le istruzioni e le richieste di consenso provenienti da tale app.

Nelle repliche alle controdeduzioni la ricorrente ha riferito di non aver ricevuto alcun *SMS-alert* dall'intermediario, né ha potuto constatare la truffa, non potendo più accedere all'home banking, se non nel momento in cui si è recata alla filiale dell'intermediario. Precisa, infine, che il bonifico sarebbe del tutto anomalo in quanto avrebbe svuotato tutto il conto corrente.

L'intermediario, con le controrepliche, insiste per il rigetto del ricorso, richiamandosi a quanto già dedotto.

DIRITTO

Oggetto del ricorso è la richiesta del rimborso di n. 1 operazione di bonifico online per complessivi € 6.801,00, comprensivi delle spese di commissioni bonifico pari ad € 1,00.

Il Collegio rileva che l'operazione di pagamento contestata rientra 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 decreto legislativo, 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 decreto legislativo, 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 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 all'operazione contestata, 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 17:29:27 del 25 settembre 2024 è stato eseguito l'accesso all'home banking con ID utente e PIN (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 "*non viene è evidenziato in chiaro come avviene per i codici OTP in quanto a differenza di questi ultimi, che hanno valenza per la sola operazione per cui sono stati generati, il codice PIN rimane valido sempre o almeno sino a quando il cliente non decide di modificarlo*".

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.
Tuttavia, occorre rilevare che l'intermediario ha affermato che il PIN è stato attivato mediante impronta digitale ma dai log prodotti non è possibile confermare tale affermazione, né è presente alcuna valorizzazione alla voce "esito operazione".

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 integrale del ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 6.801,00.
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