COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) CORNO

Seduta del 23/09/2025

FATTO

La cliente è titolare di un conto corrente presso l'intermediario convenuto, sul quale sono associati diversi strumenti di pagamento elettronico. In data 7 dicembre 2023, alle ore 17:48, la ricorrente riceveva una chiamata da un numero che sembrava corrispondere al servizio clienti della banca.
L'interlocutore, presentandosi come un operatore della banca, comunicava alla cliente di aver rilevato sospetti tentativi di pagamento verso l'estero dal suo conto, suggerendo di simulare dei bonifici per dimostrare la genuinità del conto. Seguendo le istruzioni ricevute, la cliente accreditava sul proprio conto la somma complessiva di € 5.300,00, prelevandola da altro conto allo stesso intestato. Tuttavia, nel tentativo di predisporre i bonifici in uscita dal conto dell'intermediario convenuto, non riusciva ad accedere alla propria app di home banking. L'operatore, rassicurandola, si rendeva disponibile a completare l'operazione da remoto, e predisponeva, quindi, due bonifici e due ordini di pagamento su carta di credito per un importo complessivo di € 4.218,91. La cliente riceveva alcuni codici di autenticazione tramite SMS (alcuni dei quali, peraltro, pervenuti anteriormente all'ora della chiamata), ma senza riuscire a interrompere l'operazione in corso. Una volta terminata la chiamata, la cliente, accortasi dell'irregolarità, contattava il servizio clienti della banca, scoprendo di essere stata vittima di una truffa. In data 2 gennaio 2024, la cliente sporgeva denuncia presso le autorità competenti. Nella denuncia, tuttavia, la cliente descriveva

alcuni dettagli in modo parzialmente difforme rispetto a quanto esposto nel ricorso. In particolare, riferiva che, dopo aver eseguito i bonifici da un altro conto in essere presso un diverso intermediario, non riusciva ad accedere alla propria app di home banking; che il truffatore predisponeva direttamente le operazioni contestate; e che lei si limitava a constatare l'arrivo di alcuni SMS contenenti codici di autenticazione. In data 11 marzo 2025, la cliente inviava un reclamo all'intermediario, rimasto privo di riscontro.
Con ricorso all'ABF, la cliente ha chiesto la condanna della banca al rimborso della somma di € 4.218,91, oltre al pagamento delle spese legali, sostenendo che la responsabilità dell'intermediario risiede nell'inadeguatezza dei sistemi di sicurezza e nella mancata adozione di misure idonee a prevenire accessi fraudolenti e operazioni non autorizzate. La ricorrente contesta la mancata attivazione da parte della banca dei meccanismi di controllo previsti per rilevare operazioni anomale, in particolare in ragione della rapidità, dell'entità e della natura delle transazioni eseguite. La ricorrente contesta altresì di aver richiesto alla banca la documentazione necessaria per comprendere la dinamica delle operazioni fraudolente e come, nonostante alcune informazioni fossero state fornite, la banca non abbia prodotto prova dell'avvenuta corretta autenticazione delle operazioni contestate, né ha indicato le procedure di sicurezza previste in caso di sospetto di frode.
L'intermediario si è costituito chiedendo il rigetto del ricorso.
Afferma che le operazioni sono state correttamente registrate, autorizzate e autenticate tramite inserimento delle credenziali e codici OTP ricevuti sul numero di cellulare associato al conto corrente della ricorrente. Contesta che vi sia stato un malfunzionamento dei sistemi e imputa la responsabilità della frode alla condotta colposa della cliente, che avrebbe fornito tali codici al truffatore durante la telefonata. Sostiene inoltre che la tecnica di *spoofing* telefonico è nota e già comunicata ai clienti mediante informative, e non può essere imputata all'intermediario.
Nelle repliche, la ricorrente ribadisce la propria estraneità all'esecuzione delle operazioni e contesta la mancanza di prova dell'effettiva comunicazione dei codici OTP al truffatore, evidenziando la mancata attivazione di alert, la vulnerabilità del sistema della banca, e l'assenza di una dimostrazione documentale esaustiva in ordine alla corretta procedura di autenticazione. Insiste sull'obbligo dell'intermediario di dimostrare l'autenticità delle operazioni e la presenza di eventuale colpa grave dell'utente, richiamando orientamenti giurisprudenziali e regolamentari.
L'intermediario, nelle controrepliche, ribadisce che l'autenticazione forte è stata eseguita correttamente e che le operazioni non avrebbero potuto essere eseguite senza la collaborazione della cliente. A tal fine produce una mail e una notifica push concernenti l'accesso da un nuovo dispositivo associato all'account, invitando la ricorrente a contattare il numero verde qualora non lo riconoscesse. Esclude qualsiasi malfunzionamento o violazione dei propri sistemi di sicurezza e ritiene evidente la colpa grave della cliente per aver condiviso i codici ricevuti e aver agevolato l'accesso non autorizzato.

DIRITTO

Oggetto del ricorso è la richiesta del rimborso di n. 4 operazioni per complessivi € 4.218,91, di cui: n. 2 ordini di pagamento online con carta di credito in data 7 dicembre 2023 alle ore 18:00 per € 454,92 e alle ore 18:12 per € 1.763,99; n. 2 operazioni di bonifico in data 7 dicembre 2023, entrambe alle ore 18:18, per importi pari rispettivamente a € 1.000,00 ciascuna.
Il Collegio evidenzia 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 (SCA *strong customer authentication*) quando l'utente: a) accede al suo conto di pagamento on-line; 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.

Dalla documentazione in atti e, in particolare nelle controrepliche dell'intermediario, a fronte della contestazione della cliente in merito alla mancata attivazione del servizio di SMS alert, l'intermediario produce evidenza di un'e-mail e di una notifica push concernenti l'accesso da un nuovo dispositivo. Da tale documentazione, peraltro, risulta che:

- alle ore 17:27 del 7 dicembre 2023 è avvenuto un cambio password mediante inserimento di 2 cifre del PIN (fattore di conoscenza) e OTP (fattore di possesso);
- in seguito (alle ore 17:27, 17:45, 17.54 e 17:55) si registrano ulteriori accessi effettuati con il solo inserimento di username e password;
- l'accesso delle ore 17:55 è prodromico alla generazione del CVV dinamico, quest'ultima avvenuta" con inserimento password (fattore di conoscenza) e inserimento di OTP;
- l'accesso delle ore 18:01 è prodromico alla modifica dei massimali della carta e non avvenuto con i due fattori; questa ultima modifica invece è avvenuta con inserimento password (fattore di conoscenza) e inserimento di OTP.

Tuttavia, l'intermediario nulla riferisce in merito al possibile enrollment da un nuovo dispositivo, né dagli alert prodotti è possibile ricavare evidenza dei fattori di autenticazione per l'enrollment del nuovo dispositivo.

Poiché la prova della corretta autenticazione, corretta registrazione e contabilizzazione delle operazioni disconosciute dalla cliente deve avere ad oggetto anche l'enrollment del nuovo dispositivo e, considerato che non è stata fornita dall'intermediario resistente, il Collegio non ritiene assolto l'onere della prova in capo all'intermediario, con conseguente accoglimento integrale dalla richiesta di rimborso delle operazioni disconosciute. L'importo ritenuto rimborsabile viene arrotondato all'unità di euro, in considerazione delle modifiche alle Disposizioni ABF in vigore dal 1° ottobre 2020.

Parte ricorrente chiede infine genericamente il pagamento delle spese legali, richiesta che non può essere accolta dal Collegio in quanto non provata (v. Collegio Coordinamento n. 3498/2012).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.219,00.
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