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

Il ricorrente è intestatario di un conto corrente presso l'intermediario, al quale sono associati una carta di debito ed una carta di credito.
In data 21 marzo 2025 a partire dalle ore 17:04, il ricorrente riceveva diversi SMS sul proprio telefono cellulare da un'utenza telefonica riconducibile all'intermediario, i quali informavano che erano state autorizzate delle operazioni in uscita dal conto e avvisavano di contattare un numero fisso per il disconoscimento. Il ricorrente, verificando che il numero fisso presente nell'SMS corrispondeva all'Ufficio Antifrode dell'intermediario, contattava il numero comunicato nei messaggi. Il sedicente operatore dell'intermediario che rispondeva alla telefonata indicava al ricorrente alcune operazioni da effettuare per ottenere lo storno degli addebiti, e gli suggeriva altresì di bloccare subito le carte di pagamento. In seguito a tali operazioni, che il cliente effettuava su istruzione dell'interlocutore e che comprendevano la dettatura del numero della carta di credito, riceveva dei messaggi whatsapp da un numero telefonico che venivano immediatamente eliminati; e riceveva dal medesimo numero vari SMS con i quali venivano confermati gli storni delle transazioni. Alle ore 22:00 circa il ricorrente si insospettiva, in quanto riceveva ulteriori messaggi relativi ad addebiti di operazioni. Non riusciva, tuttavia, ad accedere all'home banking sino alle ore 00.00. Una volta sbloccato l'accesso, verificava la lista dei

movimenti sul conto corrente e l'effettuazione di operazioni non autorizzate per complessivi € 7.253,56, avvedendosi di essere rimasto vittima di una truffa.
In data 26 marzo 2025 presentava formale denuncia e disconosceva le operazioni presso l'intermediario. In data 8 aprile 2025 inviava reclamo all'intermediario chiedendo il rimborso della somma di € 7.253,56, riscontrata negativamente dall'intermediario reclamo del cliente.
Con ricorso all'ABF del 6 maggio 2025, il ricorrente ha chiesto il rimborso di € 7.253,56, affermando la responsabilità dell'intermediario, quale soggetto che ha il dovere contrattuale di tutelare il cliente consumatore, avendo l'obbligo di rimborsare allo stesso gli importi derivanti da operazioni disconosciute dal cliente.
Con le controdeduzioni l'intermediario ha chiesto il rigetto del ricorso. Afferma di aver prodotto documentazione che attesta che le operazioni sono state correttamente contabilizzate, registrate e autenticate tramite il corretto inserimento di un doppio fattore di autenticazione. Rileva che i messaggi truffaldini ricevuti sembravano provenire dal numero ufficiale della banca, ma in realtà indicavano un numero non riconducibile all'istituto e che il cliente stesso ha contattato un numero falso e ha seguito le istruzioni di un sedicente operatore antifrode, fornendo durante la chiamata dati sensibili, comunicando le credenziali di sicurezza e attivando un secondo Mobile Token, autorizzando così le operazioni fraudolente. Avrebbe quindi tenuto un comportamento gravemente colposo, avendo agevolato il perfezionamento della truffa. Rileva infine come il ricorrente abbia ricevuto SMS che confermavano l'esecuzione dell'operatività contestata nonché che il cliente ha ignorato le notifiche *push* e gli SMS di *alert* inviati dalla banca.
Con repliche alle controdeduzioni il ricorrente contesta quanto affermato dall'intermediario. Rileva come gli SMS erano inseriti nella chat genuina dell'intermediario, così come il numero riportato sembrava riconducibile allo stesso intermediario, circostanze che escludono la colpa grave in carico al cliente. Il sedicente operatore, durante la prima telefonata, richiedeva al cliente di disinstallare l'applicazione di home banking e di reinstallarla: in seguito, il cliente non riceveva più alcuna notifica *push*.
L'intermediario nelle controrepliche afferma che il ricorrente ha ammesso di aver fornito all'interlocutore il numero delle carte e di aver seguito tutte le istruzioni fornitegli al telefono dall'interlocutore. Inoltre, rileva come le operazioni contestate sono state autorizzate dal cliente nel corso delle telefonate truffaldine, a seguito della chiamata a un numero non genuino effettuata da parte del cliente stesso, che comunicava le sue credenziali di sicurezza all'interlocutore oltre al codice pervenuto tramite SMS, relativo all'attivazione del secondo Mobile Token. Ritiene di aver attuato tutte le misure di sicurezza e prevenzione idonee al fine di tutelare il cliente.
L'intermediario, per mera finalità transattiva, è disponibile al rimborso di € 3.340.22 (comprensivo di € 20,00 per spese di presentazione ricorso) a fronte della sottoscrizione della manleva da parte del cliente.

DIRITTO

Oggetto del ricorso è la richiesta del rimborso di n. 13 operazioni per complessivi € 7.253,56 (compresi € 4,00 di commissioni), di cui: n. 8 operazioni di pagamento online con carta di credito in data 21 marzo 2025 alle ore 18:43 per € 990,00, alle ore 18:47 per € 1.999,00, alle ore 19:14 per € 303,00, alle ore 19:19 per € 292,90, alle ore 19:50 per € 500,00, alle ore 19:53 per € 416,00, alle ore 19:56 per € 499,00, alle ore 20:01 per € 480,00; n. 2 operazioni di pagamento con carta di debito in data 21 marzo 2025 alle ore 20:22 per € 500,00, alle ore 20:30 per € 458,54; n. 1 operazione di pagamento CBILL in data 21 marzo 2025 alle ore 21:53 per € 611,12; n. 2 operazioni di prelievo ATM "per te" in

data 21 marzo 2025 alle ore 22:51 per € 100,00 e in data 22 marzo 2025 alle ore 0:23 per € 100,00.

Le operazioni che il ricorrente afferma di non aver autorizzato 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 già 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 di 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.

L'intermediario afferma che le operazioni sarebbero state regolarmente eseguite con autenticazione (anche forte) del cliente e non avrebbero subito le conseguenze del malfunzionamento delle procedure necessarie per l'esecuzione o di altri inconvenienti.

Con riferimento all'enrollment del nuovo device, l'intermediario afferma che, trattandosi di nuovo device, non viene richiesta la generazione di un OTP virtuale, bensì si attiva la procedura di enrollment di un nuovo dispositivo che prevede l'invio di un OTP al dispositivo in precedenza certificato dal cliente. Dalla documentazione in atti emergono il dispositivo n. *161, modello device CPH*577 (presumibilmente quello del truffatore), ed il dispositivo n. *219, modello SM*018 (quello del ricorrente).

Dalle evidenze prodotte, corredate di legenda esplicativa, si ricava che:

- alle ore 17:24 del 21 marzo 2025 è stato eseguito un tentativo di accesso con ID utente (riconducibile al numero associato al ricorrente) e PIN;
- nella colonna IP si alternano due indirizzi, presumibilmente due IP associati al collegamento del ricorrente e del truffatore; mentre nella colonna device si alternano due dispositivi, presumibilmente anch'essi associati rispettivamente al ricorrente e al truffatore;
- in merito all'inserimento del PIN (elemento di conoscenza), si evidenzia che l'utilizzo del PIN risulta: dalla descrizione attività utente ("Tentativo di accesso con ID utente e PIN"), dalla dicitura "PIN INVIATO": "sì" e "PIN VERIFICATO: Verifica ok";
- a seguito dell'inserimento del PIN su nuovo device, risulta avviata la procedura di invio di un OTP via SMS (elemento di possesso). Nel file "** log attività cliente" allegato alle controdeduzioni compare, alle ore 17:24, un'indicazione dell'invio OTP via mail, ma non è presente una evidenza al riguardo e l'intermediario non fa menzione di tale modalità nelle controdeduzioni;
- alle ore 17:26 risulta completata l'attivazione del Mobile Token.

L'orientamento dei Collegi per valutare l'assolvimento dell'onere della prova della SCA, tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte,

prevede che possano essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione; hanno altresì rilievo eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c..
Tutto quanto ciò premesso, il Collegio ritiene provata la SCA in relazione all'enrollment del nuovo device.
Con riferimento al Login/accesso all'area riservata, prodromico alle operazioni contestate, occorre precisare che, dalle controdeduzioni dell'intermediario, risulta prodromico unicamente alle operazioni di pagamento online con carte e pagamento CBILL. L'intermediario rappresenta che l'accesso all'home banking da app e da sito web, come nel caso di specie, avviene mediante fattore di conoscenza (PIN) e fattore di possesso (OTP generato da Mobile Token).
Dall'evidenza prodotta, correlata di legenda esplicativa, si ricava che:

- in data 21 marzo 2025 alle ore 18:36 è stato eseguito l'accesso all'home banking con ID utente e Pin e generazione in app dell'OTP c.d. silente (vd. colonna OTP popolata e relativa legenda esplicativa).
- alla luce della legenda si rileva che: *(i)* l'inserimento dell'ID Utente risulta dalla relativa colonna popolata; *(ii)* 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");
- alla colonna ID Utente compare il numero cliente associato al ricorrente;
- la colonna User Agent (corrispondente all' "App utilizzata e relativa versione") risulta l'app dell'intermediario versione android;
- la colonna "esito operazione" non è valorizzata;
- in merito all'inserimento del PIN (elemento di conoscenza), si evidenzia che l'utilizzo del PIN risulta dalla descrizione attività utente e dalle colonne popolate "PIN Inviato" e "PIN Verificato".

Si osserva, inoltre, che il codice OTP virtuale risulta generato (vd. relativo campo popolato): tale circostanza può verificarsi solo a seguito dell'inserimento del PIN.
Alla luce delle evidenze in atti e della necessità di considerare tutti gli elementi esplicativi forniti dall'intermediario, il Collegio ritiene che questi siano idonei a verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione che, pertanto, risulta fornita dall'intermediario.
Con riferimento alla/alle operazione/operazioni contestate, occorre distinguere il tipo di operazioni.
Con riferimento alle operazioni di pagamento con carta di credito e ai pagamenti online con carta di debito e al pagamento CBILL, sulla base delle evidenze prodotte e sopra riportate è possibile osservare che:

- l'operazione di pagamento con carta di credito è avvenuta in data 21 marzo 2025 alle ore 18:43; l'operazione di pagamento con carta di debito e i pagamenti CBILL sono avvenuti in pari data alle ore 20:22;
- alla colonna ID Utente compare il numero del cliente;
- la colonna "OTP", che – in base alla legenda fornita dall'intermediario – corrisponde all' "OTP transazionale generato dal Mobile Token utilizzato", è popolata e questo dimostra che la dispositiva è stata firmata con l'utilizzo del Mobile Token come da norma PSD2;
- nella colonna User Agent (corrispondente all' "App utilizzata e relativa versione") risulta l'app dell'intermediario versione android 6.1.17;

- i campi “Pin inserito” e “Pin verificato” non sono valorizzati;
- l’esito dell’operazione non è valorizzato;
- in merito all’inserimento del PIN (elemento di conoscenza), si evidenzia che l’utilizzo del PIN risulta dalla descrizione attività utente. Si osserva, inoltre, che il codice OTP virtuale risulta generato (vd. relativo campo popolato): tale circostanza può verificarsi solo a seguito dell’inserimento del PIN.

In virtù di quanto sopra, pertanto, risulta che:

- un fattore di autenticazione è dato dalla validazione della notifica *push* ricevuta sul device, con conseguente generazione del codice OTP transazionale c.d. silente (elemento di possesso);
- l’utilizzo del PIN (elemento di conoscenza) per la validazione della *push* risulta dalla descrizione attività utente e risulta, inoltre, evidenza dell’OTP transazionale silente, generatosi a seguito del suo inserimento. Tuttavia, le colonne “pin inserito”, “pin verificato” ed “esito” non sono popolate.

In casi analoghi il Collegio di Milano non ha ritenuto provata la SCA. Tuttavia, come già detto sopra, il Collegio ritiene doversi ammettere il “riutilizzo” del fattore di conoscenza (PIN) precedentemente impiegato per l’apertura della sessione. Deve pertanto ritenersi provata l’autenticazione forte anche in relazione alle operazioni di pagamento con carta di credito e ai pagamenti online con carta di debito e ai pagamenti CBILL.

Per quanto riguarda, invece, i due prelievi ATM “per te”, nelle controdeduzioni viene affermato che si tratta di una particolare tipologia di prelevamento, eseguito attraverso un codice di sicurezza ottenuto da App o da sito web, per una somma precedentemente prenotata. Accedendo alla App o al sito web dell’intermediario il cliente può selezionare la funzione “Prelievo x Te”, decidendo quale importo prenotare e su quale conto addebitarlo. L’importo massimo prenotabile è di € 100,00 per operazione (con l’aggiunta di € 1,00 di commissioni) ed è possibile effettuare solo una prenotazione al giorno. In pochi secondi, il cliente può visualizzare il riepilogo dell’operazione e il codice che serve per prelevare. Il prelievo può essere eseguito recandosi presso un ATM dell’intermediario, e dopo aver selezionato il tasto “3”, è necessario inserire il codice ricevuto sul cellulare per completare l’operazione.

Per il primo prelievo risultano le evidenze dell’accesso all’APP avvenuto con Pin e OTP (ore 23.50) e subito dopo il primo prelievo contestato (ore 23.51), autorizzato tramite OTP. Si ritiene, pertanto, che la SCA risulti provata anche relativamente all’autorizzazione al prelievo, riutilizzando uno dei fattori di autenticazione utilizzati nella fase di accesso all’APP e, nello specifico, il Pin in combinato con l’OTP (conoscenza + possesso).

Per la seconda operazione contestata è stata prodotta evidenza nei log solo di un accesso avvenuto all’App alle ore 23.01; da altra documentazione prodotta risulta poi che l’operazione di prelievo è avvenuta alle ore 00.23 del giorno successivo tramite OTP. Non è possibile pensare quindi al riutilizzo del fattore PIN considerato che tra le due operazioni sono trascorsi 1 ora e 22 minuti e tenuto conto delle norme dell’EBA. Ne consegue che, quanto alla seconda operazione, non pare autorizzata la SCA.

Premesso quanto precede e passando all’esame dell’eventuale sussistenza di colpa grave in capo alla ricorrente, risulta dalla documentazione in atti che sarebbe stata vittima di SMS *spoofing* e *vishing*.

Come noto, i Collegi in casi di SMS *spoofing* – ovvero di truffa particolarmente insidiosa consistente nell’invio di SMS “civetta” dall’utenza dell’intermediario – nonostante la maggiore diffusione di campagne informative sul tema, lo *spoofing* conservi ancora il carattere di insidiosità. In particolare, con riferimento alle comunicazioni in apparenza provenienti dagli intermediari, che inducono il cliente ad abbassare la sua soglia di attenzione, si ritiene che l’eventuale colpa grave del cliente sia desumibile, ad esempio,

dall'inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta nonché da evidenti errori grammaticali o di sintassi sempre contenuti nel messaggio civetta. Resta salva la possibilità di individuare, anche in questi casi, una responsabilità concorrente dell'intermediario. Sempre secondo l'orientamento condiviso tra i Collegi, sia quando il messaggio civetta si inserisca in una "conversazione" o "chat" contenente precedenti messaggi genuini provenienti dall'intermediario, sia quando sussista un singolo messaggio civetta che risulti apparentemente proveniente dall'intermediario in relazione alla simulazione del nome del mittente, occorre valutare caso per caso eventuali profili di colpa grave del cliente, non potendosi ipotizzare automatismi di sorta circa il riparto di responsabilità tra le parti (es. presenza di errori grammaticali nel testo del messaggio civetta).

Nel caso di specie, quanto alla valutazione della colpa grave del ricorrente, sulla base delle evidenze prodotte risulta che, quanto agli SMS ricevuti dal ricorrente, la denominazione della chat in cui sono inseriti i messaggi è riferibile all'intermediario; nella medesima chat sono altresì presenti prima e dopo gli SMS truffaldini, altri messaggi genuini. Peraltro, occorre rilevare che tali SMS non contengono errori grammaticali e sono presenti errori lessicali e di punteggiatura, anche se non macroscopici. Gli SMS non presentano link da cliccare ma un numero telefonico da chiamare che il ricorrente afferma essere riconducibile all'intermediario, anche se produce schermata di un sito generico T*, non riconducibile all'intermediario, che riporta tre recensioni positive del numero in questione (presumibilmente inserite per conto dei truffatori, al fine di rendere maggiormente credibile la truffa).

Quanto alla condotta dell'intermediario si evidenzia quanto segue.

Nel caso di specie l'invio di *alert* per le operazioni effettuate dal truffatore è da ritenersi del tutto irrilevante posto che sono stati ricevuti dal device registrato dal truffatore e non da quello della ricorrente.

Quanto invece alla sussistenza di indici di frode alla luce di quanto previsto dal D.M. 112/2007, nel caso di specie sono state effettuate sette o più richieste di autorizzazione sulla stessa carta di credito, effettuate nelle 24 ore (art. 8, lett. b, punto 1) dell'art. 8 del DM 112/2007) e, pertanto, l'intermediario avrebbe dovuto rilevare l'anomalia/rischio di frode. In ipotesi simili, il Collegio di Milano è solito ravvisare una responsabilità concorrente dell'intermediario, valorizzando gli obblighi di protezione gravanti sull'intermediario stesso ai sensi dell'art. 1375 c.c., che impongono l'adozione di misure idonee a monitorare l'utilizzo degli strumenti di pagamento dei clienti e a prevenire truffe a danno di questi ultimi. In particolare, il Collegio ritiene che rientri tra i doveri dell'intermediario l'adozione di adeguati presidi automatici di sicurezza, che consentano il blocco delle operazioni non in linea con una normale operatività.

Alla luce di tutto quanto precede da un lato la truffa subita dal cliente presenta caratteri di insidiosità tali da averla indotta ad abbassare la sua soglia di attenzione alla luce della collocazione dell'SMS nella chat genuina con l'intermediario, seppur il numero di telefono da cui proveniva la telefonata dell'operatore non è riconducibile all'intermediario. Dall'altro lato l'intermediario, pur avendo rilevato il rischio di frode, non sembra avere adottato cautele sufficienti al fine di evitare quantomeno la realizzazione dell'ottava operazione di pagamento con carta di credito.

In virtù di tutto quanto precede, il Collegio ritiene che l'intermediario debba rimborsare alla ricorrente la seconda operazione di prelievo ATM "per te" per mancata prova della SCA, nonché la settima e ottava operazione di pagamento online con carta di credito, per mancata rilevazione degli indici di frode. Rigetta nel resto il ricorso, ritenendo il comportamento della cliente affetto da colpa grave.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.079,00.
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