COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) CESARE

Seduta del 15/05/2025

FATTO

La cliente afferma che riceve una chiamata dal numero *60, riconducibile all'intermediario. L'interlocutore si identifica con nominativo e matricola, qualificandosi come operatore dell'intermediario chiede di poter compiere delle verifiche. La cliente installa su indicazione del sedicente operatore un nuovo antivirus e una volta installato si accorge che le app della banca sono state cancellate, per cui successivamente contatta nuovamente l'interlocutore che effettua le verifiche del caso e la informa che avendo installato l'antivirus, il problema si stava risolvendo. Dopo circa due ore, la ricorrente richiama l'intermediario per accertarsi della situazione, rendendosi poi conto di essere stata vittima di truffa in quanto le sono stati effettuati n. 4 bonifici istantanei di circa € 4.000,00.
Per queste motivazioni, la cliente domanda il rimborso integrale delle somme che le sono state fraudolentemente sottratte. Gli autori della frode hanno utilizzato strumenti ed espedienti atti a trarre in inganno i ricorrenti, utilizzando il numero di telefono riconducibile all'intermediario, dal quale non solo provenivano le chiamate, ma al quale hanno risposto quando hanno richiamato per verificare l'autenticità della chiamata. Specificando quindi, che la banca non solo non ha adottato cautele adeguate a proteggere i dati dei propri clienti, ma ha omesso di comunicare ai clienti il fatto di essere stata vittima di un attacco informatico, cosa che se fosse accaduta, avrebbe certamente messo in guardia i clienti stessi. Tra la documentazione prodotta ci sono estratti di notizie reperite in rete sull'attacco informatico in questione.

Nelle controdeduzioni l'intermediario afferma che la ricorrente è cointestataria del conto corrente n. *300 al quale è collegato il servizio di home banking, che consente ai clienti di effettuare le operazioni di **inquiry** e dispositive sui conti correnti personali utilizzando il telefono cellulare o internet. La ricorrente ha altresì attivato dal 2005, senza interruzioni, il servizio SMS-alert collegato al suo numero di telefono cellulare n. *087. Il rimborso richiesto di complessivi € 19.110,00 corrisponde a n. 4 operazioni inserite con modalità "bonifico ordinario", disconosciute ed eseguite on-line in data 28/08/2024 con le credenziali di sicurezza della ricorrente a debito del conto corrente n. *300 e la richiesta di rimborso è stata oggetto di reclamo in data 03/09/2024, riscontrata dalla banca con lettera dell'8/10/2024.

La banca aggiunge che ai truffatori è bastato ventilare l'abbinamento di un nuovo dispositivo all'home banking, verificabile immediatamente anche consultando l'app, per acquisire consenso e fiducia nella ricorrente, che procedeva a scaricare un'applicazione dal funzionamento a lei sconosciuto. L'intermediario sostiene che se la ricorrente avesse telefonato al Servizio Clienti della banca, digitando direttamente lo *60, e avesse chiesto informazioni in merito alla nuova app che le era stata proposta prima di scaricarla, avrebbe appreso che si trattava di una truffa ed avrebbe così evitato ogni danno a suo carico. Per quanto attiene al canale di provenienza degli SMS e delle telefonate, come più volte segnalato dalla banca alla propria clientela, non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display ed è infatti possibile, con pochi passaggi, modificare il mittente di un numero telefonico da parte di terzi.

Dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi e le operazioni risultano correttamente autenticate, registrate ed eseguite mediante sistema di autenticazione "forte". Sulla tesi della ricorrente di essere stata vittima di frode a seguito di attacco informatico, l'intermediario contesta il contenuto dell'articolo non riferibile direttamente alla banca e antecedente alla frode subita dalla ricorrente, mentre il comunicato interno distribuito da alcune sigle sindacali di categoria esprime contestazioni che non riguardano i sistemi di sicurezza delle transazioni. La banca a fronte di ciascuna operazione ha inviato al cellulare della ricorrente le relative notifiche *push* e/o gli SMS-alert e, ricevuta notizia della frode, si è attivata per la *recall* con esito sinora negativo. Per queste ragioni l'intermediario chiede che questo ricorso venga respinto in quanto infondato.

DIRITTO

Il ricorso riguarda la contestazione di quattro bonifici fraudolenti per un totale di € 19.110,00, eseguiti mediante tecniche di *social engineering* che hanno indotto la cliente a installare un'applicazione malevola sul proprio dispositivo. La materia è regolata dal D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. n. 218/2017 di attuazione della direttiva 2015/2366/EU (PSD2). Nel caso di specie, la cliente è stata raggiunta telefonicamente da sedicenti operatori della banca che, sfruttando la tecnica dello *spoofing* del *caller ID* (simulazione del numero ufficiale dell'istituto bancario), l'hanno indotta a installare un'applicazione presentata come antivirus, che in realtà ha permesso ai truffatori di assumere il controllo del dispositivo e di disporre bonifici non autorizzati. L'intermediario sostiene che le operazioni siano state autenticate correttamente mediante sistema di

autenticazione forte (SCA) e che il comportamento della cliente sia stato gravemente negligente per aver scaricato un'applicazione sconosciuta e non aver contattato direttamente il servizio clienti prima di procedere. Secondo la normativa vigente e l'orientamento consolidato dell'ABF, l'onere della prova circa la corretta autenticazione, registrazione e contabilizzazione delle operazioni contestate ricade sull'intermediario, il quale deve dimostrare anche la colpa grave dell'utilizzatore per liberarsi da responsabilità (art. 10 D.lgs. 11/2010).

Nel caso in esame, benché l'intermediario abbia fornito i *log* relativi alle operazioni contestate, non ha prodotto evidenze sufficienti a dimostrare che la cliente abbia personalmente inserito i fattori di autenticazione forte richiesti per l'esecuzione delle operazioni. Infatti, considerando che la cliente ha installato un'applicazione malevola, è plausibile che i fraudatori abbiano potuto intercettare o bypassare i sistemi di sicurezza predisposti. Inoltre, il caso specifico si inquadra nella fattispecie del "furto di identità digitale" piuttosto che in quella dell'"induzione all'errore" (*vishing* classico), poiché la cliente non ha eseguito volontariamente le operazioni contestate, ma ha subito un'intrusione nel proprio dispositivo mediante un *malware* che ha consentito ai truffatori di operare autonomamente.

La comunicazione preventiva inviata dall'intermediario alla clientela circa i rischi di *spoofing*, pur meritoria, non è sufficiente ad esonerarlo dalla responsabilità, in quanto l'adempimento degli obblighi informativi non implica automaticamente la colpa grave dell'utilizzatore, specialmente in casi di frodi sofisticate come quella in esame. Per questi motivi, la domanda di rimborso deve essere accolta integralmente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 19.110,00.
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