COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore CORRADO BALDINELLI

Seduta del 14/01/2025

FATTO

Si riporta di seguito quanto affermato dal cliente nella denuncia in quanto nel ricorso la vicenda non è descritta in modo dettagliato:

- il 13/09/2023 il ricorrente riceveva un messaggio di allerta che lo avvisava dell'enrollment di un nuovo dispositivo dalla Polonia;
- il messaggio, inserito all'interno della chat con l'intermediario, conteneva un link con l'invito ad aprirlo e seguire la procedura indicata al fine di bloccare il nuovo dispositivo;
- dopo aver cliccato sul link, temendo una possibile truffa, chiudeva immediatamente la pagina;
- dopo pochi minuti, veniva contattato telefonicamente da un sedicente operatore che lo invitava a concludere la procedura, il recapito telefonico utilizzato era lo stesso utilizzato normalmente dall'intermediario e, pertanto, confidando sulla bontà della telefonata, dava corso alla procedura coadiuvato dal sedicente operatore;
- al termine della procedura, su suggerimento dell'interlocutore, disinstallava l'app dell'intermediario;
- in data 19/09/203 riceveva un ulteriore SMS che notificava l'inserimento di un ordine di bonifico pari a € 19.900,00 e, immediatamente dopo, un messaggio che notificava lo storno della disposizione;

- alle ore 16.39 riceveva un ulteriore messaggio che lo invitava ad un appuntamento telefonico con l'operatore n. 8704 per il giorno successivo;
- il giorno 21/09/2023, non avendo ricevuto la telefonata programmata, si recava in filiale e apprendeva che dal suo conto erano stati disposti 6 bonifici (gli ultimi 5 istantanei), tutti a favore di un beneficiario sconosciuto, per un totale di € 24.660,00;
- precisa di non aver ricevuto gli SMS alert degli ultimi 5 bonifici;
- lo stesso giorno si recava presso la Stazione dei Carabinieri per sporgere formale denuncia;
- presentava reclamo il 21/09/2023 e successivamente, tramite il proprio procuratore, il 27/12/2023 ha presentato formale istanza di risarcimento. L'intermediario ha negato, in entrambi i casi, il rimborso.

L'intermediario, riportato il fatto, afferma quanto segue:

- il ricorrente è intestatario del conto corrente n.***68, al quale è collegato il servizio di home banking;
- il servizio di home banking risulta collegato alla utenza cellulare del ricorrente n. ***63, lo stesso dichiarato nella denuncia/querela, al quale nei giorni 13,19 e 20 settembre 2023 ha regolarmente inviato le notifiche push relative alle operazioni di cui si chiede il rimborso, oltre all'sms contenente il codice OTP indispensabile per attivare il Mobile Token;
- dalle dichiarazioni rilasciate dal ricorrente si evince che la frode è stata perpetrata con una ormai nota tecnica di "phishing " c.d. smishing/spoofing + vishing che si realizza mediante l'invio di messaggi ad un pc o smartphone e che inducono il ricevente a ritenere che lo stesso sia stato inviato da una fonte attendibile, alla quale ha fatto seguito una telefonata da parte di un operatore spacciatosi per dipendente della banca, attraverso le quali vengono carpite al malcapitato le credenziali di sicurezza o lo stesso viene guidato all'inserimento di operazioni dispositive;
- il ricorrente non avrebbe dovuto cliccare sul link ricevuto in quanto non corrispondente a quello ufficiale della banca;
- prima di accedere al link "malevolo" il ricorrente avrebbe, almeno, dovuto contattare il Servizio Clienti dell'intermediario per avere maggiori informazioni, oppure verificare il link sul web per accertarsi della sua genuinità;
- per quanto attiene al canale di provenienza degli SMS e delle telefonate, come più volte segnalato dalla banca alla propria clientela tramite gli avvisi sulla sicurezza, l'intermediario segnala che 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 (è infatti possibile, con pochi passaggi, modificare il mittente di un numero telefonico da parte di terzi);
- è plausibile ritenere che, per accedere al link, il ricorrente abbia dovuto editare le proprie credenziali di sicurezza dell'home banking e successivamente anche il codice OTP necessario per attivare il Mobile Token ricevuto via sms sul proprio cellulare, rivelando di fatto i codici al suo interlocutore;
- il ricorrente ha avuto tutto il tempo, prima dell'esecuzione dei bonifici, per verificare presso la banca, la genuinità delle operazioni eseguite il 13/09/2023. Oltretutto, neppure il 19/09/2023, dopo la ricezione dell'sms che gli comunicava l'esecuzione del bonifico di € 19.900,000, si è preoccupato di chiamare l'intermediario; se lo avesse fatto avrebbe almeno evitato i 5 bonifici eseguiti il giorno successivo;

- il comportamento tenuto dal ricorrente integra la sua colpa grave per non avere adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del suo strumento di pagamento, delle quali il PIN è noto solo al cliente, così come il codice OTP, indispensabile per completare l'attivazione del Mobile Token, consegnato dall'intermediario tramite sms "parlante" al suo cellulare;
- precisa che dalle verifiche effettuale non è emerso alcun malfunzionamento o compromissione dei sistemi e che le operazioni risultano correttamente autenticate, registrate e contabilizzate con le credenziali di sicurezza della ricorrente, come dimostrato nelle evidenze LOG;
- una volta avuta conferma del disconoscimento dei bonifici ha avviato l'azione di recall verso la banca corrispondente, che purtroppo ha avuto esito negativo.

Il cliente, richiamati i propri scritti, replica che:

- non è sufficiente paventare una regolarità di accessi e di operatività del conto, ma serve dimostrare che non ci siano state violazioni del sistema informatico che hanno permesso a terzi di intervenire e movimentare il conto;
- il disconoscimento dell'operazione determina l'obbligo, in capo all'intermediario, di dimostrare l'integrità e l'inviolabilità del sistema informatico;
- non è il correntista ad essere tenuto a dimostrare di avere eseguito i controlli e/o accertamenti, bensì – anche in base al principio di vicinanza della prova – è la Banca che deve provare di aver monitorato gli accessi e la sicurezza del sistema informatico.

Insiste per l'accoglimento integrale del ricorso.

DIRITTO

Alla data delle operazioni, trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.
Le operazioni disconosciute si sostanziano in 6 bonifici per un importo di € 24.660,00 oltre € 13,50 per le commissioni; si addiviene così a un ammontare complessivo di € 24.673,50 (somma richiesta dal cliente). Tali bonifici sono avvenuti il 19/09/2023 alle ore 16:37 e il 20/09/2023 alle ore 16:34, 16:45, 16:56, 17:07, 17:17. È in atti la denuncia del cliente presentata in data 21/09/2023 e integrata dalla querela presentata in data 24/11/2023.
Con riferimento alla strong customer authentication (cd. SCA), le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA 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. Per un elenco esemplificativo dei fattori di autenticazione compliant con la PSD2, cfr. Opinion EBA del 21 giugno 2019.
L'intermediario, preliminarmente, rileva che in relazione al conto corrente intestato al

cliente è attivo il servizio "Rapporti a distanza tra Banca e Cliente" (c.d. home banking). Questo prevede l'accesso alle funzioni di inquiry e dispositive mediante un sistema di autenticazione "forte" che in caso di utilizzo tramite APP include:

- per effettuare il login e funzioni di inquiry e dispositive, inserimento delle credenziali di accesso (numero cliente + PIN) + codice OTP (One Time Password), generato da mobile token;
- per disporre le operazioni, dopo aver effettuato il login ed inserita l'operazione, la stessa deve essere confermata mediante inserimento del PIN + codice OTP generato da mobile Token.

Il codice OTP è generato in modo silente da Mobile Token integrato nella APP che il cliente ha attivato sul proprio device. Il testo della notifica, che appare sul device e sul quale l'utente deve fare "tap" per autorizzare, indica in chiaro quale operazione/attività si sta autorizzando. Il MobileToken è una soluzione digitale studiata per garantire elevati standard di sicurezza dei pagamenti online; esso permette di generare automaticamente delle password valide per un solo utilizzo, One Time Password (OTP), direttamente sul proprio smartphone (o Tablet), protegge le credenziali di accesso all'Area Clienti e tutte le operazioni dispositive e di pagamento. L'attivazione del Mobile Token avviene tramite autenticazione "forte", infatti, essa è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'home banking, indipendentemente dall'attivazione del servizio SMS Alert.

Fatte queste premesse, e precisato che la banca non conosce le credenziali dei clienti, ad eccezione del Numero Cliente/Id Utente che viene assegnato in fase di sottoscrizione del servizio Rapporti a Distanza tra Banca e Cliente, l'intermediario ricostruisce i singoli passaggi esecutivi dell'operazione fraudolenta, fornendo quindi una schematizzazione della frode, nei termini che seguono:

- è plausibile ritenere che per accedere al link il ricorrente abbia dovuto digitare le proprie credenziali di sicurezza dell'home banking;
- successivamente, inserendo il codice OTP, ricevuto via SMS sul proprio cellulare, nella pagina web, ha permesso al truffatore di installare il Mobile Token sul proprio dispositivo ed eseguire i bonifici.

L'intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate.

Dalle evidenze prodotte dall'intermediario, correlate di legenda esplicativa, si ricava che:

- alle ore 15:40:45 del 13/09/2023 è stato eseguito un tentativo di accesso all'home banking con ID utente e Pin senza generazione in app dell'OTP c.d. silente (vd. colonna OTP non popolata);
- alla colonna ID Utente compare il numero cliente associato al ricorrente;
- l'operazione è stata eseguita con il device "a04s" con indirizzo IP 37.159.74.112;
- la colonna "esito dell'operazione" non risulta popolata, ma il tentativo di accesso appare andato a buon fine, posto che è stato possibile svolgere le operazioni successive "visualizzazione Mobile Token attivi" e "invio via mail OTP attivazione Mobile Token";
- la colonna User Agent (corrispondente all' "App utilizzata e relativa versione") risulta popolata con l'indicazione dell'app dell'intermediario versione android 6.1.1;

Non è presente specifica evidenza dell'inserimento del PIN, il cui utilizzo risulta solo dalla descrizione "attività utente". La colonna "esito operazione" non è valorizzata. Non risulta la generazione in app dell'OTP c.d. silente.

Anche riguardo al login prodromico alla prima, seconda, terza, quarta, quinta, sesta

operazione di bonifico poste in essere, non è presente specifica evidenza dell'inserimento del PIN, il cui utilizzo risulta solo dalla descrizione "attività utente". La colonna "esito operazione" non è valorizzata.
Sulla prova di autenticazione, si richiamano gli orientamenti condivisi dei Collegi in base ai quali la suddetta prova, in aderenza al dato normativo, rappresenta un antecedente logico rispetto alla prova della colpa grave dell'utente. Nel caso di specie, questo Collegio ritiene, come detto, che la documentazione allegata dalla parte resistente non sia esaustiva circa la prova dell'avvenuta autenticazione delle operazioni contestate; da ciò consegue che ogni ulteriore valutazione in merito alla sussistenza o meno della colpa grave in capo al ricorrente è del tutto irrilevante e la domanda restitutoria deve essere accolta integralmente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 24.674,00.
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