COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore NICOLA RIZZO

Seduta del 17/09/2024

FATTO

Il ricorrente chiede che venga riconosciuto il suo diritto ad ottenere il rimborso da parte dell'intermediario dell'operazione fraudolenta eseguita in data 12/2/2024.
Nel reclamo, al quale il cliente si richiama integralmente, il procuratore del cliente riferisce quanto segue: che in data 12/02/2024 il cliente riceveva una chiamata apparentemente proveniente dal numero verde dell'intermediario (servizio relazioni con la clientela); che il sedicente interlocutore era in possesso dei dati sensibili del cliente, circostanza che ingenerava affidamento in capo al cliente; che l'interlocutore comunicava la necessità di aggiornare l'app TOKEN del cellulare ed invitava, pertanto, il cliente ad accedere al proprio sito di play store e scaricare l'applicazione; che il cliente non dubitando circa l'affidabilità dell'interlocutore procedeva con l'installazione dell'applicazione.
Il cliente non ha dovuto fornire alcun codice OTP o/e password; che il sedicente operatore concludeva la telefonata fissando un appuntamento per il giorno successivo per verificare la corretta installazione dell'applicazione; che il giorno dopo il cliente contattava il numero verde dell'intermediario che lo aveva contattato il giorno prima, ma dopo un iniziale contatto con l'operatore, la chiamata si concludeva con la caduta della linea; che, dopo ripetuti tentativi di contatto, la filiale di riferimento, informava il cliente dell'emissione di un bonifico di € 11.001,00 a favore di un soggetto al cliente sconosciuto; il cliente

disconosceva l'operazione e presentava denuncia alla stazione dei Carabinieri; che, nella fattispecie in esame, rilevano alcuni elementi che integrano la colpa grave dell'intermediario: a. il numero da cui è stato contattato il cliente è genuinamente riconducibile all'intermediario; b. la somma sottratta appare ingente rispetto l'effettiva disponibilità del cliente, in quale ha subito la perdita della quasi totalità delle proprie finanze; c. prima di autorizzare l'operazione l'intermediario avrebbe dovuto verificare la congruità della disposizione e appurare la riconducibilità della stessa al cliente; d. il cliente dichiara di aver sempre avuto attivo sul proprio conto il servizio di alert, ma nel caso in esame non risulta inviato al numero del cliente alcun messaggio, invio che gli avrebbe consentito di intervenire tempestivamente per evitare il perfezionamento della frode.
Da ultimo si evidenzia che la truffa perpetrata ai danni del cliente si è realizzata con le medesime modalità nei confronti di altri correntisti dell'intermediario convenuto.
Il ricorrente domanda, quindi, il rimborso della somma sottratta.

L'intermediario convenuto, riportato il fatto, afferma quanto segue: che il cliente è contitolare insieme ad altro nominativo, del conto corrente n. ***604, al quale è collegato il servizio "Rapporti a distanza tra Banca e Cliente", c.d. home banking; che il cliente è venuto meno all'assolvimento dell'onere probatorio della prova a suo carico, non allegando al ricorso alcuna evidenza del contatto che il ricorrente sostiene aver ricevuto; che il cliente ha colposamente seguito pedissequamente ed acriticamente le istruzioni di un interlocutore a lui sconosciuto, senza nutrire alcun dubbio sulla natura della richiesta ricevuta; che, dalle dichiarazioni di natura confessoria del ricorrente, si evince che la frode è stata perpetrata con una, ormai nota, tecnica di "phishing"; che il cliente in sede di denuncia ammette di aver confermato tramite link, l'operazione indicatagli dall'interlocutore al telefono, senza accertarsi della natura di questa richiesta, integrando la sua colpa grave; che, inoltre integra colpa grave del ricorrente anche il fatto che il cliente non ha adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del proprio strumento di pagamento; che la Banca in data 30 giugno 2022 ha inviato a tutta la clientela, unitamente all'estratto del conto corrente, la comunicazione delle "Regole e comportamenti per operare in sicurezza" relativamente al comportamento da adottare per la sicurezza dei dati bancari; che è evidente, infatti, che il ricorrente ha "abboccato" ad una telefonata di phishing, che rappresenta un tipo di frode considerato conosciuto come strumento di approfittamento della credulità dei malcapitati, quindi inescusabile e ritenuta elemento qualificabile come colpa grave da parte dei Collegi ABF; che, ai fini della eventuale responsabilità della banca conferma che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi, l'operazione risulta correttamente autenticata, registrata e contabilizzata; che la banca ha inviato al cellulare del cliente le notifiche push relative all'inserimento e all'esecuzione delle operazioni; che, inoltre, appena è venuta a conoscenza della frode, ha tentato il richiamo del bonifico, ricevendo esito negativo; che, in merito al canale di provenienza dei messaggi SMS e poi del successivo contatto, asseritamente provenienti dal numero della banca noto al ricorrente, segnaliamo nuovamente 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 (si veda delibera AGCOM n.12/23/CIR); che, infine, nessuna falla nel sistema della banca (peraltro solo dichiarata non provata dal ricorrente), ha permesso a terzi di venire a conoscenza dei dati sensibili del cliente.
L'intermediario convenuto domanda, quindi, il rigetto del ricorso in quanto infondato in fatto e in diritto.

DIRITTO

Oggetto della presente controversia è un bonifico online a debito del conto corrente del cliente, per un importo complessivo di € 11.000,00 + € 1,00 di commissione, posto in essere il 12/02/2024 alle ore 16:13:25.
Alla data dell'operazione 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.
È in atti la denuncia presentata dal cliente, in data 13/02/2024.
L'intermediario sostiene che le operazioni sono state eseguite dall'APP installata sul device del cliente con il doppio fattore di autenticazione: Token + PIN e autorizzate con OTP silente generato dall'applicazione a seguito di "tap" sulla notifica apparsa sul device e contenente gli estremi dell'operazione inserita.
Dall'evidenza prodotta agli atti dall'intermediario, correlata di legenda esplicativa, si ricava che: alle ore 16:08:59 del 12/02/2024 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: 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"); la colonna User Agent (corrispondente all' "App utilizzata e relativa versione") risulta l'app dell'intermediario versione android 6.1.8; non si ha diretta evidenza dell'inserimento del PIN che viene indicato solo nel campo attività.
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. Infatti, il log evidenzia solamente il codice OTP e, nonostante la descrizione dell'attività in legenda, non vi è evidenza che il PIN sia stato digitato.
Quanto alla fase successiva di esecuzione dell'operazione contestata, dalle evidenze prodotte risulta che: un fattore di autenticazione è dato dall'inserimento del codice OTP (elemento di possesso); non emerge alcuna evidenza relativa all'inserimento del PIN quale ulteriore fattore di autenticazione.
Tuttavia, trattandosi di un'operazione autenticata nell'ambito della sessione precedentemente aperta, potrebbe ammettersi il "riutilizzo" di uno dei fattori di autenticazione precedentemente impiegati per l'apertura della sessione, in relazione ai quali, come già osservato, non si rinviene però la prova dell'inserimento del PIN.
Quanto procede porta questo Collegio a concludere che l'intermediario convenuto non abbia soddisfatto l'onere, di cui il D.lgs. n. 11 del 2010 lo grava, di provare l'autenticazione forte dell'operazione contestata in tutte le fasi, prodromiche e attuative, di svolgimento della stessa.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 11.001,00.

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
FLAVIO LAPERTOSA