COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	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) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA DELL ANNA MISURALE

Seduta del 01/10/2024

FATTO

Con ricorso del 23 maggio 2024 il cliente espone quanto segue:

- in data 05/02/2024, dopo le ore 13.00, riceveva una telefonata apparentemente proveniente dal numero verde dell'intermediario (contatto che, sulla base della dicitura presente sul sito, risulta essere il "servizio relazioni con la clientela");
- l'interlocutore, qualificatosi come operatore dell'intermediario, comunicava la necessità di aggiornare l'AppToken del cellulare e lo invitava ad installare l'applicazione dell'intermediario attraverso un link. Tale link perveniva sulla sua utenza attraverso un SMS;
- la conoscenza da parte del sedicente interlocutore dei suoi dati sensibili e la circostanza che l'app riportava i simboli e la sigla dell'intermediario lo inducevano a fidarsi dell'interlocutore e a seguirne le istruzioni, cliccando sul link;
- sottolinea che non ha mai dovuto comunicare al sedicente operatore alcun codice OTP e/o password;
- solo dopo una sua successiva verifica presso la filiale di riferimento, apprendeva di essere stato vittima di una frode informatica per € 24.901,00;
- alla luce delle circostanze sopra indicate appare evidente la responsabilità dell'intermediario per il perfezionamento della frode;
- prima di autorizzare l'operazione la banca avrebbe dovuto verificare la congruità della disposizione e appurare la riconducibilità della stessa al cliente, il quale in passato non ha mai eseguito operazioni così rilevanti in modalità *home banking nei confronti di soggetti sconosciuti.*

Chiede, pertanto, il rimborso della somma di € 24.901,00

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

- il ricorrente è intestatario del conto corrente n. ***490 al quale è collegato il servizio "Rapporti a distanza tra Banca e Cliente" c.d. *home banking;*
- dalle dichiarazioni del cliente, si evince che la frode è stata perpetrata con una ormai nota tecnica di "phishing";
- il cliente, non fornendo alcuna evidenza del contatto ricevuto, è venuto meno all'assolvimento dell'onere probatorio;
- il cliente avrebbe dovuto insospettirsi sin da subito, dal momento che non aveva personalmente richiesto di installare l'APP. Inoltre, lo stesso dichiara di aver seguito le istruzioni impartitegli dal sedicente interlocutore, istallando una APP (non quella genuina dell'intermediario) e inserendo le proprie credenziali di sicurezza, comportamento imprudente che integra la colpa grave del cliente;
- se il ricorrente avesse, subito dopo il primo ingaggio, telefonato lui stesso al servizio clienti della Banca chiedendo informazioni in merito alla "nuova App" che gli era stato richiesto di installare, avrebbe appreso che si trattava di una truffa ed avrebbe così evitato ogni danno a suo carico;
- inoltre, il cliente è incorso in colpa grave anche per non avere adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate dello strumento di pagamento;
- le operazioni, sia di attivazione del Mobile Token, sia di login che di bonifico, risultano correttamente autenticate, registrate ed eseguite mediante un sistema di autenticazione "forte", senza che sia emerso alcun malfunzionamento o compromissione dei sistemi della Banca;
- in merito al canale di provenienza del contatto noto al ricorrente come quello dell'intermediario, si segnala che non bisogna riporre troppa fiducia nel "caller ID" 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 invita gli operatori telefonici ad inibire questa funzionalità);
- a fronte dell'operazione eseguita, la Banca ha inviato al cellulare del ricorrente la relativa notifica push e l'SMS alert, ignorati dal ricorrente;
- inoltre, a seguito della segnalazione del cliente, la Banca si è subito attivata per il richiamo della somma oggetto di frode, ricevendo risposta negativa;
- in merito alla falla informatica, dichiarata ma non provata dal cliente, che avrebbe permesso al frodatore di venire a conoscenza dei dati sensibili, si sottolinea che non si sono mai verificati eventi di perdita di dati. I sistemi di banca sono costantemente monitorati e sono state introdotte ulteriori azioni di controllo a garanzia della sicurezza dei nostri dati.

Chiede, pertanto, il rigetto del ricorso.

Il cliente replica che:

- nessuna responsabilità può essergli imputata stante la complessa e raffinata ingegneria della truffa subita, Gli elementi genuinamente appartenenti all'intermediario escludono anche una colpa lieve;
- dalla schermata del dispositivo mobile si evince la cronologia delle chiamate; in particolare si desume chiaramente la telefonata ricevuta dal numero verde dell'intermediario alle ore 11:57 in data 06/02/2024;
- tale chiamata rappresenta il primo contatto dei truffatori e non lascia dubbi circa la genuinità e l'attendibilità della numerazione, trattandosi del numero verde dell'intermediario;

- in merito all'app Token, che l'intermediario disconosce, si evidenzia invece, dal raffronto tra l'icona originale e quella clonata, una totale corrispondenza delle immagini: sia i caratteri che le tonalità cromatiche sono riprodotte fedelmente e non sono per nulla distinguibili;
- a differenza di quanto dichiarato dall'intermediario in sede di controdeduzioni, non ha mai dovuto inserire User e password per accedere alla propria pagina riservata, i passaggi intermedi di comunicazione dei dati sensibili sono stati superati dall'installazione dell'applicazione clone;
- i sistemi di sicurezza dell'intermediario si sono dimostrati, quantomeno nella fattispecie in esame, gravemente fallaci;
- da ultimo si sottolinea la serialità di tale truffa ai danni dei clienti dell'intermediario nello stesso periodo (febbraio 2023) e con le stesse modalità attuative, rendendo altamente probabile un *vulnus* dei correntisti dell'istituto a causa di un'evidente falla nei sistemi di sicurezza che ha permesso ai frodatori di carpire i dati dei clienti e clonare l'applicazione ufficiale;

Insiste per l'accoglimento integrale del ricorso.
L'intermediario non deposita controrepliche.

DIRITTO

La questione rimessa all'esame del Collegio attiene all'esecuzione di un'operazione di bonifico disconosciuta dal cliente, che sostiene di essere stato vittima di una frode informatica
È in atti la denuncia presentata dal cliente in data 8.2.2024.
Alle fattispecie in esame deve dunque applicarsi la disciplina dettata dalla PSD2 (artt. 97 e 98) e dal D.lgs. n. 11/2010 nella versione oggi vigente. Ciò premesso, giova precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
Ebbene, per quanto attiene al primo profilo, l'intermediario resistente non ha fornito piena prova della corretta autenticazione dell'operazione disconosciuta dal ricorrente, conformemente ai criteri SCA.
L'intermediario sostiene che l'operazione è stata eseguita 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.
Dai log prodotti, tuttavia, non si ricava specifica evidenza dell'inserimento del PIN, il cui utilizzo risulta solo dalla descrizione attività utente perché la colonna "esito operazione" non è in alcun modo valorizzata.
La prova della SCA per quanto attiene alla fase prodromica all'esecuzione del bonifico non può reputarsi raggiunta in linea con la giurisprudenza di questo Collegio che, a fronte dei

medesimi log, ha ritenuto provata la SCA in fase di login soltanto quando, oltre alla presenza del PIN da attività utente, era presente il valore Y alla voce "esito" (v. *ex plurimis* Collegio di Milano, decisione n. 4760/24: "…*In relazione, invece, all'esecuzione delle operazioni disconosciute, pur essendo le stesse valorizzate, nei log prodotti dall'intermediario resistente, nella colonna "esito operazione" come eseguite, non risulta, tuttavia, evidenza dell'effettivo inserimento del codice PIN" - da ultimo cfr. altresì decisioni n. 9005/24 e n. 9152/24"*).

Del pari, con riferimento all'esecuzione dell'operazione di pagamento contestata sulla base delle evidenze prodotte è possibile osservare che non si rinviene nella documentazione in atti evidenza della notifica push e manca, ancora una volta, l'evidenza dell'avvenuto inserimento del PIN.

Ne segue che a fronte del fattore di autenticazione dato dall'inserimento del codice OTP (elemento di possesso), non emerge l'ulteriore fattore di autenticazione.

In linea con l'orientamento consolidato dei Collegi ABF, dal quale non vi è ragione di discostarsi, deve considerarsi fondata la domanda di rimborso, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius logico* rispetto alla prova di colpa grave dell'utente.

Solo per completezza, si osserva che, dato l'elevato importo della transazione, prima di autorizzare l'operazione, l'intermediario avrebbe dovuto verificare la congruità della disposizione rispetto alla normale movimentazione del cliente, il quale in passato (stando agli estratti del conto esibiti in atti) non aveva mai eseguito operazioni così rilevanti in modalità home banking. Tanto più che il beneficiario non rientrava tra i contatti abituali del cliente.

Sebbene, infatti, Il D.M. 112/2007 faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, per orientamento consolidato dei Collegi gli indici di frode ivi disciplinati possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici come nel caso di specie), in ragione della *ratio* sottesa a tale normativa.

Può pertanto reputarsi sussistere il diritto del ricorrente al rimborso dell'importo richiesto.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 24.901,00.

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