COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) DENOZZA

Seduta del 23/09/2024

FATTO

Il cliente espone:

- è cointestatario di un conto corrente n. ****6146, acceso presso l'intermediario;
- in data 20/03/2024 alle ore 17:31 riceveva un sms apparentemente proveniente dall'intermediario che riportava l'indicazione: "*Richiesta di accesso *** in data 20/03/2024, se non sei tu contattaci al numero ****0018*";
- preoccupato per un eventuale accesso non autorizzato, contattava il numero indicato nell'SMS;
- l'interlocutore, qualificatosi quale operatore dell'intermediario, lo avvisava di un probabile subentro di problemi di sicurezza relativi alla gestione dell'*App* e gli comunicava che avrebbe dovuto disinstallarla e che per le 24 ore successive l'*App* non sarebbe stata operativa;
- durante la telefonata truffaldina, gli veniva inviato un sms – sempre apparentemente proveniente dall'intermediario – contenente un *link* al quale veniva invitato ad accedere al fine di completare l'operazione e certificare l'*App*;
- l'*App* dell'intermediario veniva, dunque, disinstallata da remoto;
- non comunicava al sedicente operatore alcuna credenziale di sicurezza o accesso;
- il sedicente operatore gli indicava di non effettuare movimenti per le successive 24 ore;
- riceveva un ulteriore sms civetta che gli comunicava un appuntamento telefonico per il giorno seguente al fine di verificare il corretto funzionamento dei servizi *online*;

- effettivamente, il giorno seguente veniva contattato dal numero ***060. Ritenendo che tale chiamata provenisse dal medesimo interlocutore del giorno precedente, chiedeva di essere ricontattato dopo alcuni minuti;
- tuttavia, non avendo più ricevuto alcun contatto, il giorno seguente, 22/03/2024, provvedeva a richiamare il numero ***060, al quale rispondeva un vero operatore dell'intermediario e solo in tale occasione si avvedeva della truffa consumata a suo danno;
- contestualmente chiedeva di bloccare il conto corrente;
- l'operazione fraudolenta di cui è controversia è un bonifico pari a € 19.981,75 che, considerata la normale operatività del conto dal quale è stato eseguito, avrebbe dovuto allertare la banca inducendola ad attivare i necessari controlli.
  Chiede il rimborso della somma oggetto dell'operazione non autorizzata.

L'intermediario, afferma:

- il cliente è cointestatario del conto corrente n. ***6146 al quale è stato collegato il servizio di *home banking* che, a sua volta, risulta connesso all'utenza cellulare del cliente n. ****2115;
- in base a quanto dichiarato dal cliente, si può evincere che la frode è stata perpetrata con una tecnica di "*pishing*";
- il cliente ha contattato un numero di telefono a lui sconosciuto e non riconducibile all'intermediario;
- il cliente ha, inoltre, ammesso di aver cliccato su un *link*, che non risulta un *link* ufficiale dell'intermediario;
- il cliente ha seguito acriticamente le istruzioni di un sedicente operatore, il quale adducendo pretestuosi problemi di sicurezza, ha guidato il ricorrente a scaricare una nuova *App* mediante la quale ha assunto il controllo del suo *device*, lo ha indotto ad accedere sul conto corrente sul quale operare direttamente, gli ha fatto disinstallare l'*App* ufficiale, presumibilmente per impedirgli di monitorare tempestivamente il suo conto corrente;
- per quanto concerne il canale di provenienza degli sms, non si deve riporre troppa fiducia nel "*caller ID*" poiché, attraverso servizi e *App* disponibili sul web, è possibile modificare il mittente di un numero di telefono da parte di terzi (sul tema, è recentemente intervenuta anche l'AGCOM con delibera n. 12/23/CIR, invitando gli operatori telefonici ad inibire questa funzionalità);
- ad ogni modo, la cronologia degli sms depositata in atti non è univocamente riconducibile all'intermediario;
- la ricostruzione dei fatti riportata dal cliente integra la colpa grave a suo carico poiché ha confidato nella genuinità di sms e istruzioni ricevute da un interlocutore a lui sconosciuto, assecondandone acriticamente e, dunque, colpevolmente le richieste, vanificando ogni presidio di sicurezza posto in essere dalla banca;
- l'operazione risulta correttamente autenticata, registrata e contabilizzata con un sistema di autenticazione forte, senza che sia emerso alcun malfunzionamento o compromissione;
- il modello di *device* utilizzato per l'operazione di cui si chiede il rimborso è lo stesso utilizzato dal ricorrente nei giorni precedenti per autorizzare transazioni internet non disconosciute;
- ha inviato al ricorrente la notifica *push* relativa al bonifico disconosciuto;
- avendo il cliente disconosciuto l'operazione fraudolenta due giorni dopo l'esecuzione, non era più possibile procedere al blocco del bonifico;

- ha comunque avviato l'azione di *recall* verso la banca corrispondente, con esito negativo;
- ha messo a disposizione del cliente tutti i dispositivi utili a prevenire il verificarsi di eventi fraudolenti, che sono stati resi inefficaci dal suo comportamento.

Chiede la reiezione del ricorso

Il cliente, richiamati i propri scritti, replica che:

- mai ha comunicato o digitato credenziali, password, o altri dati necessari per compiere disposizioni di pagamento;
- invero, non gli è mai stata richiesta e non ha mai eseguito alcuna operazione che esigesse l'inserimento dei dati necessari a compiere operazioni di trasferimento di somme di denaro;
- ha dimostrato di aver ricevuto un sms da un numero riconducibile alla banca, il medesimo dal quale aveva ricevuto precedenti comunicazioni ufficiali;
- in tale messaggio non erano presenti errori grammaticali o evidenze che potessero far dubitare della genuinità dell'avviso;
- non ha mai ricevuto l'sms *Alert* che segnalava l'intervenuta operazione, il quale gli avrebbe permesso di avere contezza dell'accaduto e di bloccare l'operazione;
- vi è stato un mancato funzionamento del sistema di sicurezza.

L'intermediario, riportandosi alle conclusioni in atti, nelle controrepliche specifica che:

- i log provano la riconducibilità dell'operazione disconosciuta al ricorrente, la cui identità viene verificata mediante la combinazione corretta tra IdCliente, Pin e codice OTP;
- l'invio dell'sms *Alert*, trattandosi di una sola operazione, non sarebbe servito ad evitarla e, in ogni, ha inviato al ricorrente la notifica *push* relativa all'operazione contestata;
- non è stato necessario comunicare le credenziali al terzo, in quanto l'operazione è stata autorizzata dal ricorrente;
- per quanto attiene agli "applicativi antifrode" in grado di rilevare le operazioni anomale, con una recente decisione ABF, il Collegio di Roma ha stabilito: *"[…] non è necessario che questi organismi operino in tempo reale, con la conseguenza che l'intermediario non è obbligato a sottoporre a controllo, sulla base di questi parametri, tutte le operazioni avviate dal cliente, prima della loro esecuzione. Può invece limitarsi a un monitoraggio delle frodi ex post […]*".

DIRITTO

L' operazioni contestata di importo complessivo pari a € 19.981,75 (di cui € 0.75 di commissioni) è stata effettuata in data 20/03/2024 alle ore 17:58:45. È in atti la denuncia del cliente presentata in data 23/03/2024.
Venendo all'esame delle modalità di esecuzione delle operazioni contestate, l'intermediario rileva che il conto corrente cointestato al cliente è collegato al servizio "*Rapporti a distanza tra Banca e Cliente*", c.d. *home banking*.Tale servizio di *home banking* prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte" che in caso di accesso tramite *App* prevede, per effettuare il *login e* funzioni di *inquiry*, l' inserimento delle credenziali di sicurezza (numero cliente + PIN) + codice OTP, generato da *Mobile Token* e per disporre le operazioni, dopo aver effettuato il *login* ed inserita l'operazione, la conferma 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 cliente può attivare il *Mobile Token*, contemporaneamente su due dispositivi (2 *smartphone* oppure 1 *smartphone* + 1 *tablet*) ed inoltre è libero di sostituire il proprio *device* senza dover comunicare il nuovo modello alla banca se il numero di cellulare resta invariato. 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 email e via sms, indipendentemente dalla attivazione del servizio sms *Alert*.
Fatte queste premesse, l 'intermediario anzitutto riporta, nelle controdeduzioni, il numero cliente associato al ricorrente. Sulla base della documentazione prodotta, tuttavia, risulta che il numero di telefono associato al cliente non corrisponde all'utenza da lui indicata nel modulo del ricorso. Tale numero di telefono non corrisponde neppure al numero al quale è collegato il servizio di *home banking*.
Per quanto concerne l'operazione di login prodromica al bonifico fraudolento, sulla base dell'evidenza e della legenda prodotte, si ricava che alle ore 17:54:02 del 20/03/2024 è stato eseguito un accesso. L' "IdUtente" corrisponde, secondo quanto preliminarmente allegato dall'intermediario, al numero cliente abbinato al ricorrente. Vi è evidenza del codice OTP che risulta dalla relativa colonna popolata. Non si ha però diretta evidenza dell'inserimento del Pin e la colonna "Esito Operazione" non risulta in alcun modo popolata.
L 'intermediario, in proposito, in sede di controdeduzioni afferma *che il codice PIN non viene evidenziato in chiaro, come avviene per i codici OTP (onetime password), in quanto a differenza di questi ultimi, che hanno valenza per la sola operazione per cui sono stati generati, il codice PIN rimane valido sempre, o almeno, sino a quando il cliente non decide di modificarlo.*
Il Collegio ritiene tuttavia, in conformità con altre precedenti decisioni, che la SCA possa considerarsi provata soltanto quando, oltre alla presenza del PIN da attività utente, sia presente il valore Y alla voce esito.
Con riferimento all'operazione contestata sulla base delle evidenze e della legenda prodotte, è possibile rilevare che l'operazione è avvenuta in data 20/03/2024 alle ore 17:58:45. Vi è evidenza del codice OTP che risulta dalla relativa colonna popolata. In atti non vi è però evidenza relativa alla notifica *push* e non vi è diretta evidenza dell'inserimento del Pin.
Trattandosi di un'operazione autenticata nell'ambito della sessione precedentemente aperta, potrebbe teoricamente ammettersi il "riutilizzo" di uno dei fattori di autenticazione precedentemente impiegati per l'apertura della sessione. Nel caso di specie vanno tuttavia, richiamate le riserve sopra esposte con riferimento al login.
Sulla base di quanto precede, considerata l'assoluta rilevanza che nell'impianto della disciplina dettata dalla Direttiva PSD2 assume l'elemento della doppia autenticazione, rilevato che anche da tale considerazione deriva la necessità di un rigoroso assolvimento da parte dell'intermediario dell'onere su di lui gravante di provare la sussistenza in ogni caso concreto di tale elemento, onere che non appare peraltro sproporzionato, considerato che l' intera fase di autenticazione si colloca nell'ambito di controllo (e di conseguente "vicinanza alla prova") dell'intermediario stesso, il Collegio ritiene che nella specie non sia stata fornita prova sufficientemente certa della sussistenza della c.d. SCA.
Va allora ricordato che in presenza di mancanza anche parziale della prova di autenticazione, i Collegi sono unanimi nel ritenere che il ricorso debba essere accolto integralmente, 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.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 19.982,00.
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