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 ricorrente allega denuncia e successiva integrazione della denuncia nelle quali espone che:

- alle ore 16:35 del giorno 24/10/2023 riceveva un sms che sembrava provenire dall'intermediario in quanto inseritosi nello storico delle comunicazioni genuine inviategli precedentemente dall'intermediario;
- l'sms civetta gli comunicava che l'intermediario aveva "*limitato la sua carta/conto per mancata verifica della sicurezza web*", e indicava un *link* attraverso il quale poteva "riattivarla";
- a questo punto provvedeva a cliccare su tale *link*, che lo reindirizzava a una schermata che sembrava essere quella dell'intermediario;
- su tale schermata gli veniva richiesto l'inserimento di alcune credenziali che, a mente del cliente, potrebbero essere il codice cliente e il numero di telefono cellulare;
- inserite le credenziali richieste, la schermata gli segnalava un'anomalia del sistema e gli comunicava che sarebbe stato contattato da un operatore dell'intermediario "*in merito alla nuova sicurezza web*";
- alle ore 16:40 riceveva, dunque, una telefonata dal numero +39***060, che corrispondeva al numero del Servizio Clienti dell'intermediario, ad opera di un sedicente operatore che si qualificava come "*A********* B******, Codice operatore 2287*";

- il sedicente operatore gli spiegava che l'avrebbe supportato nel completamento della procedura di aggiornamento della sicurezza *web* associata al conto corrente acceso presso l'intermediario, attraverso la disinstallazione dell'*App* dal suo cellulare e – una volta completati gli aggiornamenti sulla sicurezza informatica – la successiva reinstallazione dell'*App*;
- dunque, guidato dal truffatore, eseguiva la procedura attraverso il suo pc, inserendo il codice cliente e il codice pin di accesso al suo *home banking*, senza mai comunicarli al malfattore;
- il sedicente operatore fissava, al fine di concludere tale procedura, un appuntamento telefonico per la mattina successiva e trasmetteva un ulteriore messaggio, anch'esso apparentemente proveniente dall'intermediario, a conforto di quanto appena sostenuto;
- si avvedeva di essere stato vittima di una truffa quando il giorno seguente – 25/10/2023 – alle ore 15:11 veniva contattato da un addetto del Nucleo Antifrode Internet dell'intermediario, che gli comunicava che erano stati effettuati tramite il suo *home banking* n. 3 bonifici, per un ammontare complessivo di € 2.535,00, a favore di S***** N*******, il cui nominativo risultava già inserito dalla banca nell'elenco dei soggetti sospetti;
- vi è stato un ritardo nell'intervento del Nucleo Antifrode Internet dell'intermediario, nonostante il beneficiario dei n. 3 bonifici fosse inserito nell'elenco dei soggetti sospetti;
- da parte dell'intermediario non è stata data alcuna conferma telefonica o tramite sms *Alert* in relazione all'esecuzione di tali operazioni;
- in data 11/04/2024 è stato nuovamente destinatario di un sms civetta apparentemente proveniente dall'intermediario, riscontrando dunque un ulteriore mancato presidio di sicurezza informatica da parte dell'intermediario.

Chiede la restituzione di € 2.535,00.

L'intermediario afferma:

- il cliente è cointestatario del conto corrente n. 1***2 al quale è stato collegato il servizio di *home banking* che, a sua volta, risulta collegato all'utenza cellulare del cliente n. ****2012;
- a tale utenza sono state inviate le notifiche *push* relative alle operazioni disconosciute, delle quali si chiede il rimborso e l'sms "parlante" contenente il codice OTP indispensabile per attivare il *Mobile Token,* con l'indicazione di non comunicarlo a nessuno, né inserirlo in un eventuale *link* o pagina *web* e di prestare attenzione alle frodi;
- il cliente non produce prova né relativa al messaggio civetta, né alla cronologia delle telefonate, né della schermata "clone";
- la mancata allegazione di tali prove documentali comporta il mancato assolvimento dell'onere della prova a carico del cliente e l'impossibilità per il Collegio di qualificare i fatti narrati come fraudolenti;
- sulla base delle dichiarazioni rilasciate dal cliente, è possibile desumere che cliccando sul *link* dell'sms truffaldino il cliente abbia consentito al malfattore di assumere il controllo del suo *device*, permettendogli – così – di carpire le credenziali di sicurezza editate successivamente per autorizzare l'accesso all'*home banking* ed anche il codice OTP necessario per attivare il *Mobile Token* ricevuto via sms dal cliente sul suo cellulare (e inviato solo a lui dall'intermediario);
- le operazioni risultano correttamente autenticate, registrate e contabilizzate, senza il riscontro di alcun malfunzionamento o compromissione dei sistemi;

- il comportamento del cliente integra la colpa grave per aver cliccato un *link* non ufficiale della banca e per aver assecondato acriticamente le istruzioni di un interlocutore;
- inoltre, il comportamento del cliente integra la colpa grave per non aver adempiuto con la richiesta diligenza ai suoi compiti di custodia e protezione delle credenziali di sicurezza e del codice OTP indispensabile per completare l'attivazione del *Mobile Token*;
- ha posto in essere tutte le misure di sicurezza e prevenzione idonee al fine di tutelare il cliente, rese inefficaci dal suo comportamento;
- raccomanda da tempo la massima cautela nell'utilizzo dei canali telematici, pubblicando specifici avvisi nella pagina di accesso al portale, sull'*App* e sugli schermi degli ATM ed ha, inoltre, inviato alla clientela una comunicazione contenente "Regole e Comportamenti per operare in sicurezza".

Chiede la reiezione del ricorso.

DIRITTO

Le operazioni contestate sono 3 bonifici on line, per un ammontare complessivo pari a € 2.535,00 effettuati il 24/10/2023 alle ore 18:11 (€ 890,00) 18:12 (€ 895,00) e 18:14 (€ 750,00). È in atti la denuncia-querela del cliente presentata in data 02/11/2023. È, altresì, in atti l'integrazione della denuncia-querela del cliente presentata in data 17/04/2024.
Circa le modalità di esecuzione delle operazioni in questione, 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, con riferimento alla fase di login e di attivazione del *mobile token*, l'intermediario produce evidenza, corredata da legenda esplicativa da cui risulta che alle ore 16:45:23 è stato eseguito un tentativo di accesso. L' "IdUtente" corrisponde, secondo quanto preliminarmente allegato dall'intermediario, al numero cliente abbinato al ricorrente.
Non vi è però diretta evidenza dell'inserimento del PIN, il cui utilizzo risulta solamente dalla descrizione attività utente, e la colonna "Esito Operazione" non è in alcun modo valorizzata.
L 'intermediario in verità specifica 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 fino 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.
Per quanto concerne l'attivazione del *Mobile Token*, sulla base delle evidenze e della legenda prodotte, si rileva che vi è evidenza del codice OTP che risulta dalla relativa colonna popolata ("*OneTimePWD* = OTP transazionale generato dal *Mobile Token* utilizzato. Anche qui non vi è però diretta evidenza dell'inserimento del PIN, il cui utilizzo risulta solamente dalla descrizione attività utente, e la colonna "Esito Operazione" non è in alcun modo valorizzata.
Trattandosi di un'operazione svolta 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.
Analoghi problemi in ordine alla prova dell'effettivo inserimento del PIN si riscontrano con riferimento alle operazioni di login prodromiche ai bonifici fraudolenti e agli stessi ordini di bonifico.
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 € 2.535,00.
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