COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) DENOZZA

Seduta del 28/03/2024

FATTO

Il cliente afferma:

- in data 31 gennaio 2023 alle ore 18:30 riceveva sulla propria utenza telefonica una telefonata da parte del n. 02****01 durante la quale un sedicente operatore lo informava di un blocco di operatività del conto e gli chiedeva conferma del modello di cellulare in suo possesso e la generazione di codici;
- a tale ultima richiesta si opponeva e confermava il modello di cellulare in suo possesso;
- nei successivi giorni 1 e 2 febbraio 2023 veniva ricontattato e gli veniva richiesto di generare dei codici con il proprio *token*; si opponeva nuovamente;
- il numero dal quale ha ricevuto le telefonate corrisponde a quello di una filiale della banca a Milano; ha quindi subito un tipo di frode sofisticato;
- in data 6 aprile si è recato in banca per eseguire un'operazione e si è accorto che erano stati disposti 3 bonifici tra il giorno 31.01.2023 e il giorno 02.02.2023 per gli importi di € 4.850,00, € 4.999,00 ed € 4.999,00;
- ha presentato denuncia e domandato alla banca il rimborso di tali operazioni;
- la banca ha respinto la sua richiesta ed ha prodotto i log relative alle operazioni contestate affermando che le stesse risultano correttamente disposte;
- le operazioni sono state disposte con l'utilizzo di dati e codici riservati carpiti senza la sua responsabilità;

- ha agito in buona fede ed ha subito un attacco di tipo sofisticato;
- tale attacco quindi denota una carenza organizzativa da parte dell'intermediario, considerando che il numero di telefono era riconducibile alla banca;
- la banca ha l'obbligo di garantire la sicurezza delle transazioni elettroniche e di proteggere i dati dei clienti;
- inoltre la banca non ha bloccato le operazioni nonostante fossero anomale per la sua operatività e disposte per tre giorni consecutivi;
- chiede il rimborso di € 14.848,00 oltre interessi e rivalutazione e inoltre copia del contratto e della documentazione in possesso della banca.

L'intermediario afferma quanto segue:

- il cliente è titolare del conto corrente n.***300 sul quale sono attivi i servizi di banca telematica;
- in sede di sottoscrizione ha comunicato i propri contatti che sono stati associati alla sua utenza e non sono stati modificati nelle giornate in cui si è verificata la truffa;
- nel giugno del 2022 il cliente ha chiesto di ottenere un apposito *token* fisico che genera il codice OTP che serve per accedere ai servizi e disporre le operazioni;
- al momento dell'attivazione dei servizi di internet banking la banca ha fornito al cliente codice utente e password per poter accedete; tali dati sono essenziali per l'autenticazione e sono noti solo al cliente;
- tramite i contatti certificati la banca ha inviato al cliente la comunicazione relative all'esecuzione delle operazioni come attestano i log prodotti;
- non è stata riscontrata alcuna anomalia né manomissione o intrusione nei sistemi informatici della banca;
- le operazioni sono state correttamente contabilizzata, registrate e autenticate in quanto risulta che siano avvenute con il corretto inserimento delle credenziali;
- ne deriva che non è inverosimile ritenere che il cliente ha comunicato le proprie credenziali all'interlocutore, comunicato l'OTP generato di volta in volta dal *token*;
- tramite i log in atti è possibile ricostruire tutti i passaggi e le operazioni che sono state svolta dai truffatori con l'utilizzo di un dispositivo diverso rispetto a quello in uso al cliente;
- stante il sistema di autenticazione forte adottato dalla banca i frodatori hanno potuto effettuare le operazioni soltanto grazie alla piena collaborazione del cliente;
- il cliente ha ricevuto diverse telefonate ed ha tenuto un comportamento negligente collaborando attivamente con il frodatore;
- il cliente contesta specificamente la violazione dei dati personali da parte della banca;
- sul punto, fermo restando che non vi è stato alcun tipo di malfunzionamento o violazione, la banca non può essere considerata responsabile per il fatto che il cliente ha comunicato a terzi le proprie credenziali;
- ad ogni modo tale contestazione esula dalla competenza dell'ABF e quindi fa considerata inammissibile;
- quanto alla colpa del cliente si rileva che egli ha proposto una ricostruzione generica e sommaria; non ha prodotto evidenza delle telefonate ricevute e quindi non è possibile verificare l'effettiva origine di tali comunicazioni;
- la truffa si è svolta in più passaggi in quanto il cliente afferma di aver ricevuto almeno tra telefonate; gli orari delle stesse coincidono con quelli in cui si sono realizzati diversi accessi all'home banking come risulta dai log prodotti;
- se il cliente non avesse fornito i codici al truffatore non sarebbe stato possibile disporre le operazioni;

- il cliente inoltre non ha prestato la dovuta attenzione ai messaggi di notifica di esecuzione dei bonifici che la banca ha puntualmente inviato all'indirizzo email certificato e mai modificato dal cliente;
- la banca ha agito correttamente ed ha dimostrato di aver adottato un sistema di autenticazione forte;
- ha inviato specifiche richieste di *recall* dei bonifici ed in data 7 febbraio ha bloccato e poi revocato l'utenza del cliente al fine di tutelarlo;
- con riferimento alla richiesta di copia di documentazione bancaria avanzata dal cliente, ha prodotto in atti tutti i documenti richiesti.

Chiede che il ricorso sia dichiarato inammissibile, che sia respinto nel merito e in subordine l'accertamento di un concorso di colpa.

Il cliente conferma la propria richiesta e specifica quanto segue:
- il danno per la violazione dei propri codici e credenziali rientra nella materia della prestazione dei servizi di pagamento telematico, è compresa nella competenza dell'arbitro bancario;
- il riferimento non è al trattamento dati ma all'attività pericolosa relativa alla prestazione di servizi di pagamento e alla loro possibile violazione di sicurezza;
- la genesi del danno trae origine dalla pericolosità dell'attività della banca;
- il tipo di frode è stata correttamente descritta;
- dalla ricerca online risulta che il numero dal quale ha ricevuto la telefonata è riferibile ad una filiale dell'intermediario;
- la banca non ha dimostrato che ha comunicato i codici al truffatore;
- i log prodotti sono parziali e non certificati come conformi a quelli presenti nell'archivio da cui sono estratti;
- il telefono indicato come collegato alle operazioni fraudolente è diverso dal suo;
- le operazioni sono state effettuate da un diverso cellulare, ma la banca non ha provato l'autenticazione dell'app sul nuovo cellulare;
- c'è incongruenza sugli orari delle telefonate e quelli degli accessi.

L'intermediario ribadisce quanto già affermato e specifica che:
- i log prodotti dalla banca documentano il reale svolgimento dei fatti e la colpa grave del cliente;
- dall'analisi dei log emerge che il cliente ha consentito ad altri di disporre ed operare sul proprio conto corrente;
- dai file prodotti si ricavano tutti i passaggi necessari per effettuare il login e autorizzare le operazioni dispositive;
- nel caso di specie non si è registrata l'attivazione di una nuova *app*, in quanto le operazioni contestate sono state eseguite tramite *smartphone* accedendo al portale web;
- il cliente non ha prestato alcuna attenzione alle notifiche che la banca ha inviato in merito all'esecuzione delle operazioni contestate.

DIRITTO

Le operazioni disconosciute sono tre operazioni di bonifico. L'intermediario produce le relative contabili (allegato n. 4 alle controdeduzioni) ed i tentativi di richiamo dei bonifici. Il cliente in sede di denuncia presentata in data 06.02.2023, dichiara che:
- alle ore 18:30 del 31.01.2023 è stato contattato al telefono da un numero fisso;

- l'interlocutore gli riferiva di un blocco della operatività sul suo conto che era necessario effettuare alcune operazioni per poterlo sbloccare;
- l'interlocutore gli chiedeva di confermare il modello di cellulare in suo possesso; procedeva in questo senso;
- il presunto operatore gli chiedeva inoltre di generare dei codici con il *token* in suo possesso, ma si rifiutava di comunicare tali codici;
- l'interlocutore gli diceva quindi che il giorno successivo l'avrebbe chiamato nuovamente sul cellulare il cui modello era stato confermato poco prima; ha quindi inserito la *sim* all'interno del cellulare in questione;
- il giorno successivo alle ore 18:30 come da accordi è stato quindi contattato nuovamente dal presunto operatore che gli chiedeva nuovamente di generare i codici tramite il *token*;
- anche in tale occasione si rifiutava di comunicare i codici in questione; la stessa cosa è accaduta il giorno successivo, 02.02.2023;
- in data 06.02.2023 si è recato in banca per effettuare un bonifico ed a quel punto si è reso conto che ignoti avevano disposto dal suo conto n. 3 bonifici di € 4.840,00, € 4.999,00 ed € 4.999,00, a favore dello stesso beneficiario.

L'Intermediario afferma che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate. Tutte e tre le operazioni, stando a quanto affermato dall' intermediario si sono svolte secondo analoghe modalità e cioè mediante accesso all'home banking del cliente tramite APP e successiva esecuzione delle operazioni disconosciute. Tutte le operazioni risultano svolte con un dispositivo diverso rispetto a quello in uso al cliente.
L'intermediario produce evidenze relative allo svolgimento delle tre operazioni che sono sostanzialmente simili. Relativamente agli accessi all'internet banking l'intermediario afferma che per l'accesso è necessario il corretto inserimento del codice utente, della password e del codice OTP fornito dal dispositivo *token* in possesso al cliente.
Dall'esame delle evidenze prodotte dall'intermediario risulta però che:

- lo stato credenziali è indicato come "*password: modifica non necessaria (o non modificata)";*
- la seconda credenziale del LOGIN è identificata come OTP; non sembra però esserci evidenza dell'inserimento del codice OTP; nella schermata prodotta è riportato esclusivamente *"[...] seconda credenziale Login: OTP[...]";*

Quanto alle operazioni di bonifico l'autenticazione sarebbe avvenuta mediante inserimento del codice OTP generato dal *token* fisico in possesso al cliente. A sostegno l'intermediario allega evidenze dall'esame delle quali però si rileva che anche qui non sembra esserci prova certa dell'inserimento del codice OTP; nella schermata prodotta è riportato esclusivamente *"tipo credenziale OTP_SIGNATURE_PSD2[...]".*
Considerato che tutte le operazioni di bonifico sono avvenute all'interno della medesima sessione entro pochi minuti, e che quindi il login per l'accesso all'internet banking potrebbe essere considerato come primo fattore di autenticazione, il problema preliminare appare essere quello della sussistenza della prova di una autenticazione forte durante la fase del login.
A questo riguardo, 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, 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 in tali casi 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.
Quanto alla domanda relativa alla consegna della documentazione contrattuale ex art. 119 TUB, si rileva che l'intermediario ha prodotto copia dei contratti sottoscritti dal cliente e gli estratti conto aggiornati al 31.01.2023 ed al 28.02.2023 e la documentazione relativa ai log, agli accessi, le attivazioni ed i dettagli informativi relativi alle giornate del 31 gennaio, 1 e 2 febbraio 2023 durante le quali si è perpetrata la truffa ai danni del ricorrente. La domanda deve perciò considerarsi in parte soddisfatta; per quanto attiene alle richieste funzionali al completamento dell'istruttoria relativa al presente procedimento, assorbita; e per il resto non accoglibile.

PER QUESTI MOTIVI:

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 14.848,00, con buona valuta.
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