COLLEGIO DI MILANO

composto dai signori:

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

Relatore FRANCESCO DENOZZA

Seduta del 06/06/2024

FATTO

Il cliente afferma quanto segue:

- in data 03/01/2024 riceveva un SMS da parte di un numero sconosciuto che faceva riferimento al suo rapporto bancario con l'intermediario e affermava di provenire da quest'ultimo;
- l'SMS lo invitava a cliccare su un link al fine di bloccare un accesso anomalo registrato sul suo conto dalla Francia;
- cliccava sul link che lo riportava ad una pagina del tutto identica a quella dell'intermediario, all'interno della quale inseriva il primo codice di accesso, il codice cliente e il numero di telefono personale;
- ad un certo punto fermava la procedura in quanto si accorgeva che la pagina era sospetta in quanto richiedeva documenti personali già in possesso della banca, pertanto avviava una chat tramite *chatbot* nell'app ufficiale dell'intermediario il quale gli rispondeva che a breve sarebbe stato contattato da un operatore;
- qualche minuto dopo riceveva la telefonata da parte di un soggetto che si qualificava come operatore dell'intermediario; il falso operatore lo induceva ad eseguire 2 operazioni chiedendogli per ogni transazione le due cifre del secondo codice segreto al fine di poter bloccare le operazioni in parola;

- non conoscendo la prassi autorizzava in buona fede le due transazioni da € 500,00 e rispettivamente da € 250,00 comunicando l'OTP ricevuto sul suo cellulare e il codice CVC della carta;
- la chiamata del truffatore giungeva solo a seguito della sua richiesta di assistenza formulata e partita dall'applicazione ufficiale;
- una volta accortosi della truffa telefonava immediatamente al numero verde dell'intermediario chiedendo il blocco della carta e procedeva a sporgere denuncia alle autorità competenti;
- tutti gli operatori bancari che aveva contattato gli avevano riferito che la contabilizzazione fosse una condizione necessaria per procedere con la richiesta di disconoscimento e rimborso;
- attendeva dunque 6 giorni lavorativi, a seguito dei quali inviava la richiesta di rimborso ottenendo però riscontro negativo.

Chiede la restituzione dell'importo sottratto e un adeguato risarcimento per la fuga dei dati personali.

L'intermediario afferma:

- la controversia riguarda l'utilizzo fraudolento della carta di debito n. ***6746 appoggiata sul conto corrente n.***0851;
- ha correttamente implementato sugli strumenti di pagamento da esso emessi il sistema di autenticazione forte richiedendo, ai fini del loro utilizzo online, innanzitutto l'attivazione di una password statica di 5 cifre scelta direttamente dal cliente nella propria area personale e successivamente l'autorizzazione dell'operazione mediante l'inserimento dei dati identificativi della carta, del M***Identity Check attivato in precedenza e del codice OTP;
- l'esecuzione delle operazioni in esame veniva tempestivamente comunicata al ricorrente mediante il servizio SMS alert;
- il cliente è stato vittima di phishing, nelle forme dello smishing e vishing in quanto sulla base di mere indicazioni ricevute telefonicamente da terzi non meglio identificati cooperava con evidente imprudenza al perfezionamento dell'operazione;
- il cliente cliccava sul link fraudolento inserendo codice cliente, primo codice segreto e numero di telefono, forniva le cifre del secondo codice segreto e comunicava i codici OTP autorizzativi delle operazioni disconosciute oltre che il CVC della carta bancomat;
- l'SMS ricevuto dal cliente non è riconducibile ai numeri dello scrivente istituto e non si inseriva nella chat ufficiale con quest'ultimo e il link non è assimilabile a quello ufficiale dell'intermediario né è ad esso riconducibile;
- il numero di telefono chiamante, riferibile ad un'utenza mobile normalmente usata da soggetti privati non è riconducibile né ad un prefisso della provincia dove ha la sede lo scrivente istituto né ad un eventuale numero verde dello stesso;
- è inveritiero l'assunto secondo cui sia stata proprio l'assistenza chatbot dell'intermediario a riferire che nel breve sarebbe stato contattato da un operatore in quanto alcuna comunicazione veniva in tal senso fornita al ricorrente;
- in presenza di una condotta improntata ai criteri di un'ordinaria diligenza alcun fatto criminoso si sarebbe verificato;
- il ricorrente riconosceva espressamente sia in sede di ricorso che in sede di denuncia che eseguiva personalmente le azioni necessarie all'autorizzazione delle operazioni contestate con conseguente non applicazione, al caso di specie, del d.lgs. 11/20120;

- le operazioni effettuate personalmente dal cliente, seppure in virtù di un consenso viziato dal raggiro subito ad opera di terzi, non possono essere configurate come operazioni non autorizzate.

Chiede il rigetto del ricorso.

DIRITTO

Le operazioni contestate sono 2 operazioni di pagamento di importo complessivo pari a € 750,00 effettuate in data 03/01/2024 alle ore 20:06 e 20:08.
È in atti la denuncia del cliente presentata in data 04/01/2024 in cui descrive la truffa nei medesimi termini del ricorso, specificando che:

- in data 03/01/2024 alle ore 19:38 riceveva sulla sua utenza telefonica un messaggio proveniente da un numero di telefono privato che lo informava di alcune operazioni effettuate all'estero e lo invitava a cliccare il link contenuto nel messaggio al fine di bloccare le stesse;
- cliccava sul link che lo riportava ad una pagina web molto simile a quella dell'intermediario e successivamente alle ore 19:52 riceveva una chiamata da un altro numero di telefono;
- il soggetto chiamante si qualificava come operatore dell'intermediario e lo guidava in alcune operazioni per attivare la protezione della carta;
- in seguito arrivavano sulla sua utenza telefonica due messaggi che lo avvisavano di due pagamenti avvenuti in rapida successione di € 500,00 e di € 250,00;
- subito dopo cercava di ricontattare il numero dal quale aveva ricevuto la telefonata senza ottenere alcuna risposta.

Venendo alla prova della esistenza dell'autenticazione, rileva in particolare il tema dell'attivazione e della utilizzazione della password statica "M***Identity check". A questo riguardo dall'analisi delle evidenze prodotte dall'intermediario si rileva che l'accesso al conto è avvenuto tramite app (cfr. colonna A, "Canale Accesso", valorizzata con "MOBILE APP") e che è stato effettuato un nuovo "login di primo livello". Dalla legenda non si evince però la definizione di "login di primo livello". L'intermediario riferisce poi che l'accesso all'area riservata del cliente è stato seguito dall'attivazione del *M***Identity check*, ossia di una password statica di 5 cifre.
Il Collegio nel complesso ritiene però che la documentazione prodotta non sia idonea a fornire una prova assolutamente certa della sussistenza della SCA per l'accesso all'home banking del cliente.
Anche relativamente alle singole operazioni il Collegio ritiene che le affermazioni dell'intermediario nelle controdeduzioni, secondo cui le operazioni sarebbero state autorizzate con il sistema 3ds2.0 e, pertanto, che il cliente avrebbe utilizzato, oltre ai dati identificativi della carta, l'SMS OTP e la password di 5 cifre, non siano sufficienti a provare l'inserimento del M***Identity Check (il codice di 5 cifre, attivato in precedenza – elemento di conoscenza).
Alla luce 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.
La domanda relativa al risarcimento del danno per fuga di dati personali, non può essere accolta in assenza di ogni prova in ordine alla colpevolezza della convenuta e alla sussistenza di danni.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 750,00.
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