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 afferma:

- il giorno 24 aprile riceve un SMS dall'intermediario che la sua carta di credito è stata utilizzata in un negozio a Roma;
- successivamente riceveva una telefonata proveniente, apparentemente dal numero verde dell'intermediario convenuto, il sedicente operatore lo informava circa l'utilizzo fraudolento della sua carta di credito, la chiamata era finalizzata di tali operazioni;
- ha esposto reclamo in data 8 maggio 2024, riscontrato dall'intermediario, con lettera di risposta, in data il 13 maggio 2024.

Chiede lo storno dell'operazione.

L'intermediario afferma:

- il cliente è venuto meno all'assolvimento dell'onere della prova posto a suo carico ex art. 2697 c.c.;
- la contestazione è stata oggetto di reclamo inviato l'8 maggio 2024, riscontrato con lettera di risposta inviata il 13 maggio 2024;

- nella denuncia, il cliente, dichiara di essere stato contattato inizialmente da un numero di cellulare (351***86), il quale non è riconducibile ad alcuna utenza dell'intermediario;
- successivamente, il secondo contatto era proveniente da un numero apparentemente appartenente all'intermediario, e un sedicente operatore di banca gli ha comunicato che la sua carta di credito era stata usata fraudolentemente;
- per stornare tali operazioni, il cliente doveva fornire all'interlocutore alcuni dati personali e anche alcuni codici;
- il ricorrente, nel primo contatto, ha avuto dei dubbi sulla genuinità di tali richieste, e ha chiuso la telefonata;
- dopo l'ultima operazione, il cliente si è insospettito e ha chiuso la telefonata, contattando lui stesso il numero di assistenza clienti, e in tal modo è venuto a conoscenza della frode subìta;
- nel corso del secondo contatto, proveniente apparentemente dal numero dell'intermediario, gli è stato chiesto di comunicare i codici OTP contenuti nei messaggi a lui pervenuti, e il cliente ha seguito tutte le indicazioni dell'interlocutore;
- la ricostruzione degli accadimenti riportata in denuncia integra la colpa grave del ricorrente che ha comunicato i propri dati; inoltre, durante il secondo colloquio avuto col sedicente operatore, ha autorizzato lui stesso l'esecuzione delle operazioni (pensando di stornarle), il cliente non ha pertanto custodito con diligenza le proprie credenziali;
- la transazione addebitata è stata eseguita il 24/04/2024, con la carta di credito n. ***0467, a lui intestata, come risulta dall'estratto della carta al 21/05/2024;
- la carta di credito è stata bloccata il 24/4/2024 alle ore 18:05, come da schermate blocco carta;
- in occasione della richiesta del blocco della carta da parte del cliente il 24/4/2024, l'operazione contestata era stata già regolarmente approvata tramite notifica push autorizzativa;
- il ricorrente, "abboccando" ad un contatto di "phishing", ha seguito le indicazioni fornite dalla persona che l'ha contattato (per ben due volte, di cui la prima da un numero non di riferibile all'intermediario), seguendo le indicazioni fornitegli, e comunicando le sue credenziali di sicurezza e anche tutti i dati sensibili della sua carta di credito.
- il sistema di autenticazione "forte" adottato dall'intermediario è in linea con la normativa europea PSD2, pertanto, le eccezioni sollevate nel ricorso sono da ritenere infondate;
- la banca ha predisposto e messo a disposizione del cliente tutti i dispositivi utili a prevenire il verificarsi di eventi fraudolenti, resi inefficaci dal comportamento del ricorrente;
- in merito al canale di provenienza della telefonata: non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display: è infatti possibile, con pochi passaggi, modificare il mittente di un numero telefonico da parte di terzi; tale modalità è nota da tempo e sul web esistono, molteplici servizi ed "app" per i dispositivi mobili, sia per Android che per iPhone, che permettono all'utente di effettuare una chiamata esponendo un numero telefonico che non è il proprio;
- dalle dichiarazioni rilasciate dal ricorrente, e dalla ricostruzione dell'evento, si può desumere che gli elementi fattuali che hanno portato al concretizzarsi della frode sono tutti estranei alla banca e riferibili al ricorrente;

- l'operazione disconosciuta è stata regolarmente autenticata, registrata ed eseguita mediante un sistema di autenticazione "forte", senza che sia emerso alcun malfunzionamento o compromissione dei sistemi della banca;
- risulta palese l'incauta custodia, ovvero l'aver consentito - fornendo le proprie credenziali di sicurezza e i dati sensibili della carta di credito e autorizzando lui stesso l'operazione -, in occasione del secondo contatto avuto con l'interlocutore, qualifica la sua condotta come gravemente colposa o comunque rientrante nella ipotesi del "social hacking";
- l'operazione di pagamento oggetto del ricorso, è stata approvata dallo stesso ricorrente; e da ciò consegue che la controversia si colloca al di fuori del perimetro applicativo della normativa in materia di operazioni di pagamento non autorizzate, cui fa riferimento la particolare disciplina protettiva contenuta nel d. lgs. 11/2010 (art. 10 e seguenti); per operazione non autorizzata, infatti, si intende un'operazione non imputabile al cliente, in quanto estranea alla sua condotta volitiva e, pertanto, suscettibile di essere rimborsata.

Chiede la reiezione del ricorso.

DIRITTO

L'operazione contestata, dell'importo di € 1.940,00, è stata effettuata il 24/04/2024 alle ore 17:00. Trattasi di una disposizione di pagamento online effettuata con carta di credito. In atti è presente l'integrazione alla denuncia presentata dal ricorrente, in data 15/05/2024. L'intermediario convenuto, nelle controdeduzioni, riporta la denuncia presentata dal ricorrente, in data 29/04/2024,

Relativamente alle modalità di esecuzione dell'operazione contestata, 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 all'accesso relativo alla operazione di pagamento contestata, dall'evidenza prodotta, corredata di legenda esplicativa, si ricava che alle ore 16:58:15 del 24/04/2024 è stato eseguito l'accesso all'home banking.

Alla luce della legenda si rileva che l'inserimento dell'ID Utente risulta dalla relativa colonna popolata e la generazione dell'OTP silente risulta dalla relativa colonna popolata. Quanto invece al PIN, l'unica evidenza relativa è quella del campo "attività" in cui risulta che l'accesso sia avvenuto con ID Utente e Pin. Non sono presenti ulteriori evidenze in merito al PIN. In effetti il log evidenzia solamente il codice OTP e nonostante la

descrizione dell'attività in legenda, non risulta esserci evidenza che il PIN sia stato correttamente digitato.
Con riferimento all'operazione di pagamento contestata, dalle evidenze prodotte risulta che l'operazione è avvenuta in data 24/04/2024 alle ore 17:00 e che sarebbe stata autenticata con l'inserimento del codice OTP come primo fattore. Quale sia il secondo fattore di autenticazione non è però chiaro. L'intermediario fa riferimento al PIN, in relazione al quale sottolinea peraltro che il codice 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. La descrizione attività fa però riferimento, come potenziale secondo fattore di autenticazione, al FaceID, mentre non emerge alcuna evidenza relativa all'inserimento del PIN quale ulteriore fattore di autenticazione. 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 alla operazione 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 € 1.940,00.
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