COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) TINA

Seduta del 04/07/2023

FATTO

Con il proprio ricorso all'Arbitro, il ricorrente ha riferito quanto segue:

- ha ricevuto, in data 07/03/2023, un SMS dall'emittente la propria carta di credito, che lo informava del blocco di carta/conto per mancata verifica della sua sicurezza;
- ha ricevuto la telefonata di un sedicente operatore dell'emittente, che gli chiedeva di accedere all'app dell'intermediario per sbloccare carta/conto;
- ha seguito le istruzioni dell'interlocutore;
- dopo aver aperto l'app installata sul suo device senza fornire dati sensibili, il sedicente operatore gli comunicava che il problema era stato risolto;
- è stato contattato, il 09/03/2023, dalla filiale dell'intermediario: l'interlocutore gli chiedeva conferma di tre bonifici conclusi il giorno prima;
- ha disconosciuto detti bonifici, apprendendo di essere stato vittima di phishing;
- la banca gli comunicava che il terzo bonifico era stato prontamente bloccato e che pertanto l'importo totale dei due bonifici fraudolenti era pari a Euro 5.000,00;
- ha sporto denuncia il 10/03/2023;
- ha infruttuosamente presentato reclamo;
- l'intermediario deve provare la colpa grave del cliente, la quale non può essere

presunta;
- è stato contattato dai canali ufficiali dell'emittente, fidandosi dunque delle comunicazioni ricevute.

Il ricorrente ha, quindi, chiesto il rimborso dell'importo di Euro 5.000,00, corrispondente alle operazioni disconosciute.

Con le proprie controdeduzioni, l'intermediario resistente ha precisato quanto segue:
- la ricostruzione dei fatti proposta dal cliente è incompleta e contraddittoria;
- il ricorrente, diversamente da quanto vorrebbe far credere, ha espressamente comunicato le OTP, trasmesse via SMS e email per l'installazione dell'app sul device del frodatore;
- la banca ha provato la corretta autenticazione del cliente, la corretta registrazione ed esecuzione dei bonifici contestati, l'assenza di malfunzionamenti nei propri sistemi informatici e la colpa grave del ricorrente;
- la banca ha informato per tempo il suo cliente, mediante diversi canali, sulle caratteristiche delle truffe più diffuse e sui modi per difendersi da queste;
- sono stati approntati idonei ed adeguati presidi di sicurezza.

DIRITTO

La questione rimessa all'esame del Collegio attiene all'esecuzione di due operazioni di pagamento effettuate on line con il servizio di home banking, per l'importo complessivo di Euro 5.000,00. Il ricorrente riferisce, in sintesi, di essere stato vittima di un caso di spoofing/vishing. Le operazioni contestate dal ricorrente sono avvenute il 7 marzo 2022 e sono, quindi, assoggettate alle disposizioni del D.lgs. n. 11/2010 nella versione oggi vigente.

Ciò premesso, giova precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Nel caso di specie, per quanto attiene al primo profilo sopra evidenziato, sebbene descriva un sistema di autenticazione conforme ai criteri SCA, l'intermediario resistente non ha fornito piena prova in ordine alla corretta autenticazione delle operazioni contestate.

Più in particolare, in relazione all'enrollment dell'app, tramite la quale le operazioni sono state eseguite, l'intermediario resistente fornisce evidenza dell'invio, via email, di un codice OTP (elemento di possesso), ma non fornisce, invece, evidenza dell'inserimento del codice utente e password (fattore di conoscenza). Anche in relazione alla successiva fase di accesso all'area personale dell'app, effettuato per la prima volta su un nuovo dispositivo, l'intermediario resistente non fornisce evidenza dei fattori di autenticazione utilizzati, che, peraltro, secondo la descrizione offerta dallo stesso intermediario, sarebbero tutti fattori dello stesso tipo: di conoscenza.

Non avendo fornito l'intermediario resistente piena prova della corretta autenticazione delle operazioni di pagamento disconosciute, sussiste il diritto del ricorrente al rimborso dell'intero importo corrispondente pari a Euro 5.000,00.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.000,00.
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