COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) DELL'ANNA MISURALE

Seduta del 15/07/2025

FATTO

Il cliente, con ricorso del 4 aprile 2025, espone quanto segue:
- in data 10.03.2024 al mattino gli veniva comunicato il blocco della carta;
- entrando nell'app della banca installata sul proprio telefono si avvedeva che fra le 2.51 e le ore 7.16 del medesimo giorno erano state effettuate 8 operazioni di pagamento da lui mai eseguite e mai autorizzate per un importo complessivo di € 2.291,00;
- si avvedeva in seguito della presenza di 5 bonifici non riconducibili e mai autorizzati dallo stesso, per un importo complessivo di € 3.670,00;
- procedeva a sporgere denuncia presso le Autorità;
- si attivava a disconoscere le operazioni fraudolente presso l'intermediario;
- in data 12.04.2024 la banca procedeva al rimborso di uno dei bonifici pari a € 1.000,00 a seguito del riscontro di anomalie;
- presentava reclamo all'intermediario che veniva riscontrato negativamente.

Chiede, pertanto, il rimborso della somma di € 4.961,00, "nonché delle somme attribuite a titolo di scoperto bancario conteggiate sino alla risoluzione della vertenza".

L'intermediario, riportato il fatto, afferma quanto segue:
- il cliente è titolare del conto corrente *7453 acceso presso l'intermediario e abilitato al servizio di Internet *banking*;
- il ricorso è inaccoglibile in quanto:

1) i bonifici sono stati disposti personalmente dal ricorrente seppur sotto raggiro di un terzo che lo convinceva ad eseguirli;
2) le operazioni con carta sono state eseguite dopo l'attività di *enrollment* su un nuovo dispositivo che è stata resa possibile tramite la cooperazione del cliente che ha riferito le proprie credenziali al truffatore;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto realizzate con il corretto inserimento delle credenziali;
- sussiste la colpa grave del cliente in quanto:
1) fornisce indicazioni generiche circa le modalità della truffa;
2) ha omesso di adottare tutte le cautele necessarie a custodire i codici di accesso e reso possibile l'acquisizione da parte dei malfattori delle credenziali necessarie per accedere al servizio della banca;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.
Chiede, pertanto, il rigetto del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di n. 12 operazioni, per un importo complessivo di € 4.961,00.
Si tratta di n. 4 bonifici e n. 8 operazioni con carta.
Le operazioni sono avvenute nelle date e per gli importi seguenti:
1) 7/03/2024 ore 23:36 € 420,00 (bonifico)
2) 8/03/2024 ore 00:03 € 850,00 (bonifico)
3) 9/03/2024 ore 00:18 € 800,00 (bonifico)
4) 10/03/2024 ore 01:19 € 600,00 (bonifico)
5) 10/03/2024 ore 02:51 € 200,00 (operazione con carta)
6) 10/03/2024 ore 04:20 € 321,00 (operazione con carta)
7) 10/03/2024 ore 05:11 € 200 (operazione con carta)
8) 10/03/2024 ore 05:12 € 500 (operazione con carta)
9) 10/03/2024 ore 05:16 € 500 (operazione con carta)
10) 10/03/2024 ore 05:18 € 500 (operazione con carta)
11) 10/03/2024 ore 06:58 € 50 (operazione con carta)
12) 10/03/2024 ore 07:16 € 20 (operazione con carta)

Sono in atti le denunce presentate in data 10/03/2024 e in data 12/03/2024.

Viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate.
Deve rilevarsi che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, n. 11. In particolare, le fonti normative applicabili alla fattispecie sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).
Nello specifico è richiesta l'autenticazione forte (SCA) quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti

tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Al riguardo, giova precisare che 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.
Ciò premesso, per quanto attiene al primo profilo sopra individuato, vale a dire l'onere di provare la SCA, l'intermediario fornisce dettagliata ricostruzione, confortata da documenti, dell'autenticazione delle operazioni.
In particolare, afferma che i bonifici disconosciuti sono stati autorizzati usando uno *smartphone* con sistema operativo IOS, identificato con codice univoco, mentre le operazioni di pagamento sono state autorizzate mediante uno *smartphone* con sistema operativo IOS, identificato con altro codice univoco.
Sussiste la prova dell'autenticazione forte con riferimento alle attività antecedenti all'esecuzione dei bonifici oggetto di disconoscimento. In particolare, con riguardo alla fase di accesso all'App, nonché a quella di *enrollment.*
Quanto all'autenticazione forte relativa all'esecuzione delle singole operazioni, risulta dalle evidenze prodotte in atti che con riferimento i bonifici questa sia avvenuta con doppio fattore tramite:
- elemento di possesso: OTP generato in APP sul *device*
- elemento di inerenza: fattore biometrico a seguito del quale è stato generato il codice OTP.

Con riferimento alle operazioni eseguite con carta, dalle tracciature in atti, risulta che per l'operazione di € 200,00 eseguita alle ore 2:51 del 10.03.24 l'autenticazione è avvenuta tramite:
- elemento del possesso: codice OTP generato in APP sul *device* registrato;
- elemento di inerenza: fattore biometrico a seguito del quale è stato generato il codice OTP.

Per tutte le altre sette operazioni (a partire da quella disposta alle ore 4:20 del 10.03.24 per giungere a quella delle ore 7:16 dello stesso giorno) dalle evidenze in atti emerge che sono state realizzate in ambiente e-commerce 3D Secure2 previa validazione del PIN, elemento di conoscenza precedentemente registrato su device abilitato, che invece rappresenta l'elemento del possesso.
Valutato positivamente assolto l'onere della prova relativo alla sussistenza della SCA, deve procedersi nell'esame del profilo soggettivo, incombendo sull'intermediario l'ulteriore onere di provare la colpa grave del cliente.
Il cliente non ha riferito nulla in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento. Nella denuncia e nel ricorso rappresenta solo di essersene accorto *dopo essere stato contattato dall'intermediario che lo avvisava del blocco dello strumento di pagamento.*

Peraltro, sebbene nel ricorso neghi di aver fornito le credenziali di sicurezza a terzi ignoti e di aver disposto le operazioni oggetto di disconoscimento, in sede di disconoscimento dei bonifici ha crociato la risposta affermativa al quesito contenuto nel modulo con il quale gli si chiedeva "Sei stato tu a disporre le operazioni selezionate?", aggiungendo di essere stato convinto da persona che lo induceva ad eseguirle.
Al riguardo si ha presente che i Collegi sono unanimi nel ritenere che nelle contestazioni di utilizzi fraudolenti on line di strumenti di pagamento in cui l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute e il sistema di pagamento risulta conforme alla *Strong Customer Authentication* (SCA), le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del cliente medesimo.
Con la responsabilità del cliente concorre tuttavia una responsabilità dell'intermediario per violazione degli obblighi di protezione posti a suo carico. In particolare, egli ha trascurato di inviare gli SMS *alert* relativi alle operazioni di bonifico laddove per lo meno per evitare il terzo e il quarto bonifico del complessivo valore di € 1.400,00 (realizzati a distanza di giorni dal primo), sarebbero stati certamente utili. Risultano, invece, inviate le notifiche *push* con riferimento alle operazioni con carta.

Sussistono, inoltre, gli indici di anomalia configurati con il D.M. n. 112/2007 con riferimento alle operazioni con carta.
Come noto, la necessità che gli intermediari operanti nel settore si dotino di sistemi di monitoraggio capaci di intercettare elementi sintomatici di un rischio di frode rispetto a operazioni c.d. sospette si evince dalle indicazioni contenute nel D.M. n. 112 del 2007, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento").
In particolare, l'art. 8 del D.M. 112/2007 identifica i casi di frode che, ai fini della normativa stessa, vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento. Secondo le posizioni condivise dell'Arbitro, le relative disposizioni non hanno un valore precettivo, ma rappresentano comunque utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente.
Sulla base delle evidenze in atti, risulta la sussistenza dei seguenti indici di anomalia/rischio:

- sette o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore (art. 8, lett. b, punto 1);
- tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita (art. 8, lett. a, punto 2);

Conseguentemente, in linea con i Collegi, devono essere rimborsate al cliente quattro operazioni con carta per l'ammontare complessivo di € 1.070,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.470,00.
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
ANDREA TINA