

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO VERDICCHIO

Seduta del 13/01/2026

FATTO

Il ricorrente afferma di essere stato vittima di una truffa telefonica il 24/07/2025, all'esito della quale gli sono stati sottratti euro 4.942,80, tramite cinque operazioni non autorizzate a valere sulla carta di credito emessa dall'intermediario convenuto.

Riferisce di essere stato contattato da un sedicente operatore della polizia postale, il quale lo informava che la sua carta di credito era stata clonata e che indagini erano in corso; lo stesso gli rivolgeva domande relative al suo titolo di studio, alla condizione familiare e personale, senza però alcun riferimento ai dati bancari, invitandolo a rimanere in linea per agevolare le predette attività di indagini. La telefonata durava oltre un'ora, dopodiché lo stesso operatore lo invitava a recarsi presso un ufficio dell'intermediario per bloccare lo strumento di pagamento; una volta giunto all'ufficio, tale telefonata si interrompeva e a quel punto il ricorrente si avvedeva che erano state effettuate cinque operazioni da lui non autorizzate. Insoddisfatto della prodromica interlocuzione avuta con l'intermediario, si rivolge all'Arbitro per chiedere il rimborso delle operazioni sconosciute.

L'intermediario, ritualmente costituitosi, eccepisce che le operazioni in questione sono state regolarmente autorizzate tramite SCA e realizzate senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi. Precisa che la SCA risulta essere stata applicata in tutte le fasi, ovvero *enrollment*, login ed esecuzione delle operazioni.

Chiarisce che l'*enrollment* originario della carta non è stato modificato, mentre il login avvenuto in occasione delle disposizioni è stato effettuato con inserimento delle credenziali e successivo inserimento del codice ID. Infine, la fase dispositiva dell'operazione è stata autorizzata con inserimento

della password (fattore di conoscenza) e del codice segreto (fattore di possesso).

La convenuta precisa poi che non vi è stato alcun cambio dell'utenza telefonica associata alla carta né del dispositivo utilizzato; ricorda che il cliente riceve notifiche sulle operazioni tramite *push* in app oppure, in assenza dell'app, via SMS.

Ritiene dunque presumibile che il ricorrente, dopo aver risposto alla chiamata pervenuta sulla propria utenza, abbia anche eseguito le direttive dello sconosciuto interlocutore, approvando le operazioni oggetto del contendere. Evidenzia che, peraltro, il ricorrente non ha allegato alcun preciso elemento in merito alla frode subita, avendo semplicemente riferito di essere stato contattato da un sedicente operatore della polizia postale; ricorda, in proposito, il principio di diritto espresso dal Collegio di coordinamento nella decisione n. 897 del 2014, secondo il quale grava sul ricorrente l'onere di fornire elementi utili a provare che l'operazione sia stata realmente fraudolenta.

Nel rammentare le campagne divulgative svolte per la sicurezza delle operazioni di pagamento, effettuate mediante più canali informativi, chiede, in virtù degli elementi considerati, di rigettare il ricorso, dal momento che la condotta del ricorrente è stata caratterizzata da "colpevole credulità".

DIRITTO

Il Collegio precisa, *in limine*, che le operazioni disconosciute sono sottoposte alla disciplina recata dal d.lgs. n. 11/2010, modificato a seguito dell'entrata in vigore, in data 13/1/2018, del d.lgs. n. 218/2017, di recepimento della Direttiva (UE) 2015/2366 (c.d. PSD2), relativa ai servizi di pagamento nel mercato interno.

In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, 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 14/9/2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21/6/2019).

Ciò premesso, il ricorrente disconosce cinque (5) operazioni, costituite da quattro pagamenti on line e un bonifico istantaneo, tutti effettuati tramite App in data 24.07.2025, per un importo totale di euro 4.941,80, oltre a un ulteriore euro per l'addebitata commissione relativa al bonifico.

L'intermediario produce evidenza dell'onboarding del dispositivo alla carta, effettuato in data 27.06.2024, quindi oltre un anno prima delle operazioni disconosciute, per quanto riguarda l'App (qui convenzionalmente denominata) "Alfa".

V'è inoltre evidenza dell'enrollment di una nuova APP, denominata "App-up", avvenuta in data 24.07.2025, stesso giorno delle operazioni disconosciute, alle ore 13:55:40; si rileva, al riguardo, che la prima disposizione disconosciuta è successiva di poco più di 35 minuti.

L'intermediario allega evidenze relative all'accesso alle App avvenuto in occasione delle disposizioni poi disconosciute, e segnatamente:

la prima operazione, consistente in un bonifico dell'importo di euro 3.000,00, è avvenuta a mezzo di login e autenticazione effettuata mediante la app "Alfa", tramite codice ID, il cui enrollment – come già rilevato – era avvenuto sul device in uso al cliente un anno prima;

le altre disposizioni sono state effettuate a seguito di accessi avvenuti il 24.07.2025, alle ore 14:15 e 14:58, ed effettuati tramite l'applicazione "App-up", securizzata alle ore 13,55 dello stesso giorno, anche in questo caso utilizzando il codice ID come fattore di conoscenza.

Dalle evidenze in atti risulta che le operazioni disconosciute sono state regolarmente autorizzate con l'inserimento del codice ID mediante lettura dei dati biometrici da parte del device originariamente securizzato sia per l'operazione di bonifico sia per le operazioni di pagamento effettuate on line.

L'intermediario allega, inoltre, evidenza dei messaggi push inviati sul dispositivo del ricorrente.

A fronte dei suddetti riscontri, che paiono escludere ogni responsabilità in capo all'intermediario

resistente, il Collegio rileva che il cliente si è limitato a riferito di una pretesa telefonata da parte di un sedicente operatore della polizia postale, senza tuttavia allegare a sostegno lo screenshot di tale presunta chiamata.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE