COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore PAOLO DI STEFANO

Seduta del 22/05/2025

FATTO

Parte ricorrente espone di avere ricevuto in data 12/11/2024 un sms, seguito da una telefonata da soggetto qualificatosi come operatore dell'intermediario, con il quale veniva avvisato del tentativo di accesso al proprio conto corrente da parte di terzi. Preoccupato dall'accaduto, il ricorrente si recava presso la propria filiale dove riferiva dell'accaduto al cassiere, il quale, presa visione dei messaggi inviati al cliente, lo rassicurava sulla provenienza degli stessi. Successivamente, sempre dalla medesima utenza, veniva ricontattato da un soggetto che, identificandosi come operatore dell'intermediario, lo informava della necessità di scaricare sul proprio dispositivo l'applicazione "Cleaner" utile, a suo dire, a garantire la protezione dell'apparato da frodi informatiche. Il giorno dopo, riceveva da altra utenza dei messaggi di testo con i quali veniva invitato a prendere immediato contatto con la propria filiale e gli veniva comunicato di essere stato vittima di una truffa con la quale è stata addebitata sul proprio conto corrente, la somma di € 19.761,00 a mezzo di n. 4 bonifici bancari on-line, della quale il ricorrente chiede la restituzione.
Si è costituito l'intermediario per chiedere il rigetto del ricorso. La resistente deduce che le operazioni disconosciute sono state disposte con modalità conformi a SCA, con inserimento del pin e dell'OTP generato dal mobile token, previo accesso con i medesimi

elementi e che la truffa è avvenuta per colpa grave del cliente. La banca fa presente di essersi comunque attivata operando il recall del bonifico, con esito negativo.
In sede di repliche, il ricorrente contesta le controdeduzioni avversarie, ribadendo la circostanza di essersi recato pochi minuti dopo la chiamata sospetta presso la filiale della banca dalla quale ha ricevuto rassicurazioni sull'attendibilità del messaggio ricevuto e solo dopo il cliente effettuava le operazioni disconosciute. Aggiunge di non avere ricevuto sms alert e di non avere fornito le proprie credenziali a nessuno.
La resistente deposita controrepliche rilevando che, al contrario di quanto asserito dal ricorrente, il gestore in servizio il 12 novembre 2024 ha confermato che il numero della banca è lo 06***0 ed ha ammonito il cliente di non dare mai codici a nessuno e di non cliccare nessun link. La resistente ha aggiunto che il 14 novembre 2024, in occasione dell'incontro in agenzia, i clienti sono stati nuovamente ammoniti circa l'inopportunità di proseguire con dichiarazioni prive di riscontro. Rimarca la sussistenza della colpa grave del ricorrente, come risulta dalla confessione operata in sede di denuncia, producendo le evidenze dei Log delle attività svolte dal cliente sulla propria app.

DIRITTO

La controversia rientra nell'ambito della disciplina dettata dal d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
In particolare, le fonti normative che regolano la strong customer authentication (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del dlgs. 10/2011, 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).
Le operazioni disconosciute constando di quattro bonifici eseguiti in data 12/11/2024, per un totale di Euro 19.761,00.
Tanto premesso, dalle evidenze informatiche in atti risulta che in data 12.11.2024 alle ore 16.29 vi sia stato l'accesso all'home banking mediante app, avvenuto a seguito inserimento del codice cliente e del pin tramite impronta digitale (fattor di conoscenza), digitazione del codice otp, generato con dispositivo mobile token (fattore di possesso). La prima operazione di pagamento è stata disposta tre minuti dopo e risulta essere stata autorizzata con la digitazione del pin (fattore di conoscenza) e inserimento OTP generato in modo silente dal Mobile Token (fattore di possesso); identica modalità di autenticazione è stata adottata per le altre tre operazioni dispositive.
Le videate informatiche e i log delle attività svolte, decifrate con il supporto di legenda esplicativa, indicano la sequenza delle operazioni susseguitesi senza anomalie e con digitazione dei codici sia in fase di accesso al conto, sia in fase di esecuzione dei bonifici, con metodo di autenticazione forte.
Fornita la prova da parte dell'intermediario di autenticazione delle operazioni a doppio fattore, occorre valutare l'eventuale colpa grave del ricorrente, in base alle modalità della truffa.
Sulla scorta di quanto dichiarato, risulta che le modalità di attacco informatico siano riconducibile allo smshing, spoofing, vishing, che l'utente abbia risposto ad un sms, che

l'utenza da cui provenuta la telefonata truffaldina sia riconducibile all'intermediario e che parte ricorrente abbia autorizzato terzi estranei all'utilizzo delle funzionalità di home banking, scaricando l'app "CLEANER" sul proprio dispositivo.
Rispetto all'sms che il ricorrente afferma di avere ricevuto dall'intermediario, il ricorrente non ne produce copia pur avendone l'onere allo scopo di consentire l'indagine sul livello di insidia che avrebbe caratterizzato l'operazione disconosciuta.
A tale riguardo si rappresenta che secondo le posizioni dei Collegi, nel caso di spoofing, la mancata allegazione, da parte del cliente, del messaggio civetta, osta all'accoglimento del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio.
A ciò si aggiunga, che non è stata prodotta copia neanche del registro chiamate.
Quanto all'attivazione dei sistemi alert, dalle evidenze in atti risulta che gli stessi siano stati attivati per tutte le operazioni contestate tramite notifiche push al numero di telefono del ricorrente. Sul punto è però d'obbligo rilevare che tutti i bonifici sono stati effettuati entro sei minuti.
Al fine di escludere del tutto la responsabilità dell'intermediario è infine necessario valutare la sussistenza di eventuali indici di anomalia ai sensi del D.M. 112/2007.
Difatti, può sempre essere rilevata una responsabilità concorrente del PSP quando, sulla base delle evidenze disponibili emerge che nella stessa giornata siano state eseguite tre operazioni verso uno stesso beneficiario.
Nel caso di specie sono stati eseguiti quattro bonifici verso lo stesso soggetto.
La fattispecie, quindi, può essere analogicamente ricondotta al rischio di frode delle tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, di cui al punto 2 della lett. a) dell'art. 8 del citato D.M..
Sebbene il D.M. faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche online) in ragione dell'unicità della ratio sottesa a tale normativa, stante che il principio della richiamata disposizione e suscettibile di applicazione in tutti i casi di effettuazione di operazioni fraudolente (ex plurimis Collegio di Palermo, decisione n. 1287/2023).
Avuto riguardo alla quantificazione del rimborso da riconoscere al ricorrente, si ritiene che la responsabilità dell'intermediario incida in ragione del 20% dell'ammontare degli importi disconosciuti, qui pari ad euro 19.761,00, dovendosi precisare che il D.M. non ha un valore precettivo in materia di disconoscimento delle operazioni non autorizzate e non è ravvisabile una diretta correlazione tra l'integrazione dell'indice di frode e il numero di operazioni da rimborsare.
Di conseguenza, la somma da restituire è pari a euro 3.952,20 (20% di Euro 19.761,00).

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 3.952,20.
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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI