

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore DILETTA FULCHERI

Seduta del 17/04/2026

FATTO

Con ricorso del 4.10.2025, il ricorrente riferisce che il 25.04.25, intorno alle 12.00, veniva contattato da un soggetto che si presentava come un operatore dell'intermediario. Contemporaneamente riceveva un SMS riconducibile all'intermediario, che confermava che un operatore stava cercando di contattarlo. Dopo poco più di un minuto, dalla stessa chat arrivava un ulteriore messaggio contenente il codice di verifica dell'intermediario. L'operatore dimostrava di essere a conoscenza di informazioni personali e menzionava l'esistenza di una transazione avvenuta dalla carta da un dispositivo che in quel momento si trovava a Copenaghen. Il ricorrente, entrato nell'app, verificava che, effettivamente, risultava una transazione di € 3,99 avvenuta in quella stessa mattinata e un'autorizzazione al pagamento di 1 centesimo da lui non autorizzate. Il finto operatore spiegava che al fine di bloccare i truffatori il ricorrente avrebbe dovuto attivare un'altra carta. Una volta creata la carta virtuale, l'operatore chiedeva informazioni sulla stessa e faceva pronunciare al ricorrente il codice per attivarla. Poco dopo la

telefonata si interrompeva e il ricorrente si avvedeva che con la carta in argomento erano stati effettuati due prelievi presso ATM. Il primo di 1.016,00 euro e il secondo di 969,00 euro.

Alla luce di quanto sopra, il ricorrente richiede il risarcimento del danno ed il rimborso delle somme prelevate fraudolentemente pari a €1.985,00.

Con le controdeduzioni, l'intermediario eccepisce come il ricorrente abbia collaborato con i truffatori, registrando la nuova carta e collegandola direttamente al conto, permettendo quindi ai truffatori di accedere liberamente al Conto stesso. Precisa che dalle tracciature interne della Banca, emerge che la carta non è stata generata illegittimamente tramite il conto del ricorrente, bensì essa era già in possesso dei truffatori, che l'avevano precedentemente acquisita mediante i distributori automatici di carte che possono essere successivamente attivate solo mediante il collegamento a un account regolarmente registrato. Contesta come l'utenza da cui presumibilmente sia stato contattato il ricorrente non risulti in alcun modo riconducibile all'intermediario e ritenendo la condotta del ricorrente connotata da colpa grave, conclude per il rigetto del ricorso.

DIRITTO

La controversia attiene la richiesta di rimborso dell'importo sottratto attraverso due prelievi ATM disconosciuti, pari a €1.985,00, comprensivo delle commissioni di prelievo presso l'ATM, e il risarcimento del danno arrecato.

L'intermediario afferma che le operazioni contestate risultano correttamente autenticate, conformi agli obblighi normativi e prive di anomalie.

Secondo quanto risulta dalle tracciature interne della banca, la carta era già in possesso dei truffatori, che l'avevano precedentemente acquisita mediante i distributori automatici di carte che possono essere successivamente attivate solo mediante il collegamento a un account della banca regolarmente registrato.

In particolar modo, per attivare la carta deve essere effettuata una transazione con chip e PIN. Il PIN viene mostrato agli utenti nel momento in cui provvedono a collegare la carta al conto.

Dai log prodotti, emerge che il ricorrente ha fatto accesso al conto, dal proprio device certificato in uso dal 2024, mediante riconoscimento biometrico facciale (fattore di inerenza) sull'app precedentemente registrata (fattore di possesso) ed ha poi associato la carta al rapporto inserendo il numero della stessa. L'associazione della carta è stata confermata mediante l'app precedentemente registrata (fattore di possesso) e riconoscimento biometrico facciale (fattore di inerenza).

Successivamente il ricorrente ha, tramite l'apposita sezione sull'Applicazione, visualizzato il codice PIN (invero poi comunicato ai frodatori).

A questo punto sono stati effettuati i prelievi con CHIP – fattore di possesso e PIN – fattore di conoscenza, conformemente a SCA.

Venendo alla dinamica della truffa, dalla documentazione versata in atti emerge come la frode si sia svolta attraverso c.d. *vishing* misto a *spoofing*.

Il giorno 25.04.2025 il ricorrente riceveva una chiamata da un numero non riferibile all'intermediario e, in simultanea, un SMS da un mittente con nome dell'intermediario in cui si specificava che un operatore stesse cercando di contattarlo.

L'interlocutore, presentatosi come operatore della banca, avvertiva il ricorrente che erano state eseguite due transazioni sospette rispettivamente da 3,99 euro e 0,01 euro da un dispositivo a Copenaghen che il ricorrente dichiara di aver effettivamente constatato depositando la lista delle transazioni.

L'operatore induceva il ricorrente ad attivare una carta virtuale al fine di bloccare ulteriori operazioni di terzi. Il ricorrente afferma che una volta creata la carta virtuale, l'operatore chiedeva informazioni su di essa e gli faceva comunicare un codice, a suo dire per attivarla.

Orbene, nel caso di specie appare dirimente il fatto come la truffa sia stata perpetrata anche per il tramite del c.d. SMS spoofing. Ed infatti se è vero, come pure contestato dall'intermediario che il numero da cui il ricorrente è stato contattato non è riconducibile alla banca, tuttavia questa è stata accompagnata dal contestuale ricevimento di un SMS proveniente da un contatto avente il nome dell'intermediario.

Dall'esame della schermata degli SMS emerge che il primo messaggio della chat è il messaggio esca, mentre gli altri due messaggi appaiono genuini, posto che il primo contiene un codice OTP di verifica per l'attivazione della carta ed il secondo conferma l'associazione del numero di telefono all'account.

Nei casi di *spoofing* i Collegi territoriali ABF hanno in generale evidenziato l'insidiosità del meccanismo di aggressione, consistente nell'invio dell'sms dall'utenza dell'intermediario, tale da rivelare criticità organizzative del servizio di pagamento offerto. Ritengono quindi che nelle fattispecie di *spoofing* non sia generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvenano i suddetti indici di inattendibilità o anomalia dei messaggi.

Dall'esame dell'sms civetta non emergono indici di anomalia posto che il testo non contiene conclamati errori grammaticali; d'altro canto il ricorrente ha agevolato il compimento della truffa seguendo le indicazioni del sedicente operatore.

In tal senso il Collegio ritiene esservi un concorso di colpa tra le parti e, pertanto, ritiene di poter liquidare in via equitativa l'importo di euro 1.000,00 in favore del ricorrente.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 1.000,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE