

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore DILETTA FULCHERI

Seduta del 24/04/2026

FATTO

Con ricorso del 3.09.2025, la ricorrente riferisce che il 04.02.2025, riceveva alcune telefonate da un numero apparentemente riferibile alla banca resistente e l'operatore telefonico cercava di farle comunicare i dati del conto corrente e delle carte a lei intestate, che non forniva. Tuttavia, dopo un controllo sull'app bancaria apprendeva di un addebito di euro 1.431,97 sulla carta emessa dall'intermediario resistente. Chiede la restituzione dell'importo di euro 1.431,97.

Nelle controdeduzioni, l'intermediario eccepisce come l'operazione contestata risulti autorizzata conformemente a SCA; ritiene presumibile che mentre la ricorrente era al telefono con il presunto operatore provvedeva ad autorizzare la notifica push inviata dalla banca. Precisa di aver inviato al cellulare del cliente il messaggio relativo alla richiesta di autorizzazione delle operazioni e, successivamente, il messaggio SMS e la notifica push dell'avvenuto pagamento. Conclude per il rigetto del ricorso.

DIRITTO

La controversia ha ad oggetto un'operazione fraudolenta eseguita in data 04.02.2025 alle ore 15:13 su un sito di e-commerce per la somma di € 1.431,97, effettuata sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).

In tema di autenticazione, l'intermediario documenta come le operazioni siano state effettuate online su sito che opera in modalità sicura e validate mediante Pin e OTP generata da mobile token.

Al fine di generare l'OTP silente è stato necessario approvare una notifica push o conferire apposita autorizzazione dalla "lista delle autorizzazioni" presente sull'APP dell'intermediario, mediante touch ID. Per questo Collegio il processo di autenticazione sopra descritto, che prevede l'utilizzo di un fattore di conoscenza (PIN) o ineranza (touch o face id) e di un fattore di possesso (OTP generato dal mobile token) è ritenuto conforme a SCA.

Venendo alla dinamica della truffa, la ricorrente riferisce di aver ricevuto una telefonata apparentemente proveniente dalla banca resistente e, in tale occasione, l'operatore telefonico le

avrebbe chiesto di comunicare i dati dei suoi conti correnti e delle carte a lei intestate, che tuttavia riferisce di non aver comunicato.

Senonché la ricorrente non ha indicato il numero da cui proveniva la telefonata né allegato il registro chiamate, nemmeno a fronte della richiesta di integrazione istruttoria formulata da questo Collegio.

In tale contesto, la frode sembra essere riconducibile all'ipotesi "phishing" in cui *"il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di internet"* (in linea con la decisione n. 3498/2012 del Collegio di Coordinamento).

Avendo riguardo alle circostanze del caso concreto, la credulità del ricorrente appare non scusabile, in quanto le modalità con cui la truffa è stata perpetrata rientrano tra quelle più diffuse, che qualunque cliente dotato di normale avvedutezza e prudenza deve essere in grado di individuare, non facendosi trarre in inganno. Tutto ciò premesso, allo stato delle risultanze agli atti, ne consegue che nel comportamento della ricorrente è ravvisabile la colpa grave che non consente di accogliere la richiesta di rimborso della somma indebitamente sottratta.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE