

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) BULLO	Membro designato dalla Banca d'Italia
(BO) LUCARELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore STEFANO TRAVERSI

Seduta del 10/02/2026

FATTO

Con ricorso presentato in data 28 settembre 2025, il ricorrente chiede il rimborso dell'importo di euro 1.819,00, relativo a una operazione di pagamento online eseguita in data 5 agosto 2025 e da lui disconosciuta.

Espone che, alle ore 19:42 di tale data, riceveva una chiamata da un soggetto qualificatosi come operatore bancario, il quale lo informava della presenza di transazioni sospette sul conto e lo induceva a comunicare i codici OTP ricevuti via SMS, rappresentando che fossero necessari per bloccare presunte frodi in corso. Riferisce che, alle ore 19:54, riceveva un SMS antifrode relativo alla transazione di euro 1.819,00 e che rispondeva "NO", ma che l'operazione risultava comunque eseguita.

Precisa che ulteriori due operazioni di importo minore sono state rimborsate dall'intermediario.

Il ricorrente qualifica l'evento come caso di vishing, deducendo di essere stato vittima di manipolazione psicologica e sostenendo che la comunicazione dell'OTP sotto inganno non costituirebbe prova di autorizzazione consapevole dell'operazione. Afferma, inoltre, che il numero chiamante risultava pubblicamente associato a un soggetto appartenente allo stesso gruppo bancario e che la pressione

esercitata nel corso della telefonata gli avrebbe impedito una lettura attenta degli SMS ricevuti. Sostiene che incomberebbe sull'intermediario l'onere di provare la colpa grave.

L'intermediario si è costituito chiedendo il rigetto del ricorso, deducendo che l'operazione è stata correttamente autenticata in regime di Strong Customer Authentication, mediante inserimento di password e OTP inviato al numero certificato del ricorrente.

Rappresenta che, poco prima dell'operazione, è stato effettuato un accesso all'internet banking da un nuovo dispositivo, associato all'account tramite OTP regolarmente inviato e validato.

Produce le evidenze relative ai log di accesso, all'associazione del nuovo dispositivo, all'invio e alla verifica degli OTP, nonché alla corretta contabilizzazione dell'operazione.

L'intermediario evidenzia altresì di aver messo a disposizione della clientela un presidio di sicurezza – il c.d. “bollino di sicurezza” – che consente di verificare in tempo reale, accedendo all'home banking, se la chiamata provenga effettivamente da un operatore autorizzato.

Deduce di aver informato la clientela circa tale funzionalità attraverso diversi canali comunicativi e deduce che il ricorrente ha comunicato a terzi i codici OTP ricevuti via SMS e che tale condotta integra violazione degli obblighi di custodia previsti dall'art. 7 del d.lgs. 11/2010.

Dalla documentazione in atti risulta che:

- alle ore 19:49–19:50 del 5 agosto 2025 è stato effettuato un accesso all'internet banking mediante inserimento di credenziali corrette e OTP inviato al numero di telefono del ricorrente, con associazione di un nuovo dispositivo all'account;
- alle ore 19:53 è stata disposta l'operazione online di euro 1.819,00, autenticata tramite password e OTP;
- il ricorrente ha ricevuto SMS e notifiche relativi sia all'associazione del nuovo dispositivo sia all'operazione;
- non emergono anomalie tecniche nei sistemi dell'intermediario né indici di anomalia ai sensi della normativa richiamata.

DIRITTO

La controversia è disciplinata 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 (PSD2).

Ai sensi dell'art. 10 del citato decreto, incombe sull'intermediario l'onere di provare che l'operazione di pagamento sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito malfunzionamenti. Nel caso di specie, tale onere risulta assolto, avendo l'intermediario fornito evidenza dell'autenticazione mediante credenziali corrette e OTP inviato al numero certificato del ricorrente, nonché della corretta associazione del nuovo dispositivo e dell'assenza di anomalie nei sistemi.

Resta dunque da verificare se la perdita possa essere imputata all'intermediario ovvero se ricorra un'ipotesi di dolo o colpa grave dell'utilizzatore, ai sensi dell'art. 12 del medesimo decreto.

È pacifico che il ricorrente abbia comunicato a terzi le proprie credenziali e i codici OTP ricevuti via SMS. La fattispecie si inquadra nel fenomeno del c.d. vishing, ossia nella sollecitazione telefonica volta a indurre l'utente a rivelare dati riservati. L'orientamento consolidato dei Collegi ABF ritiene che, in presenza di comunicazione volontaria di codici dispositivi strettamente personali, la condotta integri, di regola, una colpa grave, atteso il carattere notorio e diffuso di tali modalità fraudolente.

Nel caso concreto assumono particolare rilievo ulteriori elementi:

- l'avvenuta associazione di un nuovo dispositivo, preceduta da invio di OTP al numero certificato del ricorrente;
- la ricezione di notifiche e SMS relativi sia all'enrollment del device sia all'operazione;
- la disponibilità del presidio del "bollino di sicurezza", che consente al cliente, accedendo all'home banking, di verificare in tempo reale l'effettiva provenienza della chiamata da un operatore autorizzato.

Il ricorrente stesso riferisce di aver interagito con il sedicente operatore nel corso dell'accesso all'applicazione; in tale contesto, avrebbe potuto avvalersi del presidio sopra indicato per verificare l'autenticità del contatto. La presenza di tale strumento, oggetto di preventiva informazione alla clientela e idoneo a consentire una verifica immediata dell'autenticità del contatto, rende concretamente attuabile una condotta improntata a ordinaria diligenza, anche in un contesto di sollecitazione telefonica.

La diffusione del fenomeno del phishing, compreso quello che si realizza mediante chiamate telefoniche (c.d. vishing) è tale che, pacificamente, i Collegi ABF ormai ritengono da tempo che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa (ex multis, Collegio di Milano, decisione n. 887 del 07 febbraio 2019, Coll. Bologna, dec. n. 26184 del 12/12/2019).

La dedotta pressione psicologica, pur comprensibile sul piano soggettivo, non appare idonea, alla luce delle circostanze oggettive sopra richiamate, a escludere la gravità della negligenza, in quanto il ricorrente ha fornito a terzi tutti gli elementi necessari per l'accesso e l'autorizzazione dell'operazione, nonostante i plurimi alert ricevuti.

Ne consegue che la perdita economica derivante dall'operazione contestata deve essere imputata al ricorrente, ricorrendo un'ipotesi di colpa grave ai sensi dell'art. 12 del d.lgs. 11/2010.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE