

ARBITRO BANCARIO FINANZIARIO

Risoluzione Stragiudiziale Controversie

Prot. N° 0008175/26 del 09/09/2026

COLLEGIO DI ROMA

(Dati personali e identificativi oscurati ai fini della pubblicazione)

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 degli intermediari	Membro di designazione rappresentativa
(RM) NOTARO dei clienti	Membro di designazione rappresentativa

Relatore


DOMENICO BONACCORSI DI PATTI

Seduta del 14/07/2026

Esame del ricorso n. [OMISSIS] del 07/10/2025

proposto da [RICORRENTE]

nei confronti di [INTERMEDIARIO]

FATTO

Parte ricorrente rappresenta di essere titolare di conto corrente bancario presso l'intermediario resistente e che in data 04.06.2024 ha ricevuto sul proprio telefono cellulare, dal numero utilizzato dalla banca per comunicazioni ufficiali, una serie di SMS mediante i quali le veniva comunicata l'avvenuta autorizzazione di tre pagamenti – una ricarica presso [OMISSIS] di euro 500,00 e due transazioni verso «[OMISSIS]» rispettivamente di euro 990,00 e euro 870,00 – mai disposti dalla ricorrente. Rappresenta che pochi minuti dopo, riceveva un ulteriore SMS proveniente dallo stesso numero, con il quale le veniva segnalato un contatto da parte dell'«Ufficio Antifrode» della banca e, in particolare, un numero da richiamare.

In seguito a tale messaggio, riceveva una telefonata da un soggetto che si qualificava come operatore antifrode, il quale le comunicava che risultavano movimenti sospetti riconducibili alle stesse transazioni di cui sopra, inducendola a ritenere di trovarsi in contatto effettivo con la propria banca. Terminata la telefonata, in data 05.06.2024 e 06.06.2024, venivano effettuati due bonifici non autorizzati dal suddetto conto corrente per importi pari a euro 5.000,00 e euro 495,00, entrambi a favore di [OMISSIS].

Riferisce che nella mattinata del 05.06.2024, fin dalle prime ore di apertura della filiale della banca resistente, la ricorrente – impossibilitata a recarsi personalmente in loco per documentati motivi di salute – tentava insistentemente di contattare telefonicamente il personale di filiale, senza tuttavia ottenere alcuna risposta.

In data 10.06.2024, non avendo ricevuto comunicazioni, la ricorrente contattava il numero verde della banca, apprendendo solo in tal momento, per la prima volta, che in data 04.06.2024 erano state effettuate tre operazioni Bancomat (non corrispondenti ai bonifici enunciati nei messaggi dai truffatori) di importi pari rispettivamente a euro 298,67, euro 299,70 e euro 299,80, a beneficio di una sedicente società denominata «[OMISSIS]», inizialmente rimborsati e successivamente stornati dall'intermediario all'insaputa della ricorrente.

La ricorrente chiede il rimborso degli importi sottratti in via fraudolenta.

L'intermediario nelle proprie controdeduzioni rileva che le operazioni contestate risultano correttamente autorizzate, contabilizzate e registrate. Dalle analisi svolte risulta che l'accesso e le disposizioni sono avvenute con il corretto riconoscimento delle credenziali e delle password dispositive e, dal punto di vista tecnico, senza forzature o violazione dei sistemi. Dalla dinamica

riferita emerge poi che la ricorrente ha fornito tutti gli elementi utili ad eseguire un'attivazione illecita dell'App a suo nome su un dispositivo nelle disponibilità dei frodatori, compresa una password necessaria all'autenticazione ed inviata via SMS al numero di telefono verificato. Risulta dunque l'inapplicabilità alla fattispecie della PSD2 in ragione delle dichiarazioni confessorie rese dalla ricorrente, tali da escludere per le operazioni disconosciute il difetto di autorizzazione da parte della cliente e ogni responsabilità della banca. L'intermediario chiede il rigetto del ricorso.

Nella riunione del 13 marzo 2026 il Collegio ha assegnato un termine di 15 giorni all'intermediario per la produzione di «copia della documentazione comprovante l'enrollment del dispositivo e la descrizione del relativo procedimento, compresi i fattori di autenticazione forte utilizzati». L'intermediario ha adempiuto nel termine assegnato.

DIRITTO

La controversia ha ad oggetto 3 operazioni di pagamento tramite carta e 2 operazioni di bonifico on line per un totale di euro 6.393,17. Le operazioni contestate sono state effettuate 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).

Come riportato in fatto, nella riunione del 13 marzo 2026 il Collegio ha assegnato un termine di 15 giorni all'intermediario per la produzione di «copia della documentazione comprovante l'enrollment del dispositivo e la descrizione del relativo procedimento, compresi i fattori di autenticazione forte utilizzati». L'intermediario ha adempiuto nel termine assegnato. Nello specifico, a seguito dell'integrazione documentale prodotta risulta che l'enrollment dell'app sul nuovo dispositivo utilizzato dai frodatori sia avvenuta con l'impiego: i) di un fattore di possesso, costituito dall'OTP generato dal token fisico in possesso del ricorrente; ii) presumibilmente, di un fattore di conoscenza utilizzato per effettuare il log in nell'home banking. Tale secondo fattore, tuttavia, non viene menzionato espressamente dall'intermediario nella propria scarsa descrizione della procedura di enrollment.

Con riferimento alle singole operazioni, eseguite a seguito dell'enrollment sul dispositivo dei frodatori, i bonifici risultano essere stati effettuati mediante accesso alla App Mobile (fattore di possesso) e autorizzati tramite MPIN (fattore di conoscenza). La ricorrente afferma di aver ricevuto alcuni SMS fraudolenti (in rosso) provenienti da un numero apparentemente riconducibile a quello dell'intermediario – e che pertanto si andavano a inserire in una sequela

di messaggi genuini – i quali la avvertivano di alcune operazioni sospette e la invitavano a contattare l'Ufficio Antifrode. Produce screenshot della chat relativa all'intermediario.

Secondo il più recente orientamento del Collegio di Roma in materia, nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvenivano indici di inattendibilità o anomalia del messaggio. Nel caso di specie, tuttavia, l'intermediario non fornisce prova circa il fattore di conoscenza utilizzato per effettuare l'enrollment sul dispositivo in possesso dei frodatori.

Si osserva che con riferimento al difetto di prova ovvero della prova non esaustiva di autenticazione (forte), i Collegi sono unanimi nel ritenere che in tali ipotesi il ricorso debba essere accolto integralmente, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente. Il ricorso dunque merita di essere accolto.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 6.393,17 oltre interessi legali dalla richiesta al saldo. Respinge nel resto.

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

Firmato digitalmente