



COLLEGIO DI ROMA

composto dai signori:

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

Relatore DOMENICO NASO

Seduta del 08/09/2025

FATTO

Con ricorso introduttivo del presente giudizio preceduto da reclamo del 03/04/2024, parte ricorrente esponeva di aver ricevuto in data 26/03/2024 un sms proveniente dall'utenza telefonica riferibile a quella della sua banca, aparendo peraltro in coda ai precedenti messaggi già ricevuti dall'Intermediario resistente.

Nell'sms ricevuto, il ricorrente veniva informato del tentativo di accesso alla sua app bancaria ed invitato, in caso di disconoscimento, a contattare l'utenza telefonica indicata nel messaggio.

Il ricorrente seguiva le indicazioni contenute nell'sms, chiamava il numero e poco dopo veniva ricontattato da un'utenza apparentemente riconducibile alla banca.

Il giorno successivo, insospettito da alcune irregolarità in sede di accesso all'app, il ricorrente contattava il servizio clienti, dal quale apprendeva dell'avvenuta esecuzione il giorno precedente di un bonifico di euro 47.600,00 in favore di un soggetto terzo, a lui sconosciuto.

Il ricorrente richiamava invano la disposizione di pagamento.

Parte ricorrente chiedeva pertanto all'Arbitro Bancario Finanziario la restituzione dell'importo di euro 47.600,00, corrispondente all'importo dell'operazione di pagamento disconosciuta.

L'Intermediario resisteva al ricorso eccependo preliminarmente il mancato assolvimento dell'onere della prova da parte del ricorrente in ordine alla allegazione del messaggio "civetta", che le operazioni disconosciute sarebbero state correttamente autenticate, registrate e contabilizzate e che il sistema per le transazioni online prevede l'utilizzo di un doppio fattore di autenticazione SCA *compliant*.

Precisava la Banca resistente che l'operazione contestata veniva eseguita personalmente dal ricorrente con colpa grave, mediante inserimento di un codice statico (PIN – fattore di conoscenza) e uno dinamico (OTP – fattore di possesso).

Nelle proprie repliche, il ricorrente specificava che l'esecuzione della truffa era resa possibile grazie alla sofisticatezza del raggio perpetrato nei suoi danni e che la responsabilità doveva rinvenirsi nei soli confronti della banca, per non aver introdotto sistemi di sicurezza tali da impedire l'evento.

La Banca resistente, nelle proprie controrepliche, ribadiva quanto precedentemente affermato ravvisando un'ipotesi di colpa grave nei soli confronti del ricorrente, per aver contattato il numero indicato nell'sms senza prima verificare l'attendibilità e la genuinità della richiesta.

DIRITTO

1. Parte ricorrente chiede la restituzione della somma complessiva di euro 47.600,00 relativa ad un'operazione di bonifico non autorizzata, disposta in data 26/03/2024 a seguito di ricezione di SMS proveniente da un numero apparentemente riconducibile a quello della Banca resistente.

2. L'operazione contestata è stata effettuata dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.

In particolare, ai fini della verifica del rispetto della Strong Customer Authentication (c.d SCA), affinché l'Intermediario possa andare esente da responsabilità dovrà fornire prova, oltre che dell'insussistenza di malfunzionamenti, dell'adozione di un sistema di sicurezza adeguato e della corretta registrazione, autenticazione e contabilizzazione delle operazioni contestate.

Come sancito dal Collegio di Coordinamento con la decisione n. 22745/19: *<<...la previsione di cui all'art. 10, comma 2, del D.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'Intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente>>.*

Con riferimento alle modalità di autenticazione dell'operazione di pagamento, l'Intermediario afferma che l'operazione è stata eseguita verosimilmente dai truffatori che hanno attenuato il controllo da remoto del dispositivo del ricorrente mediante un'applicazione scaricata il giorno precedente l'esecuzione del pagamento.

In ordine a tale circostanza, l'Intermediario produce in giudizio i Log che attestano che l'accesso al conto è avvenuto il 26.03.2024 alle ore 147:06, con inserimento di ID utente e codice PIN (fattore di conoscenza) e l'utilizzo del mobile token per la generazione del codice OTP (fattore di possesso).

L'operazione dispositiva è stata autorizzata alle ore 17:10 della medesima giornata con PIN (fattore di conoscenza) e OTP generata in maniera silente dal Mobile Token (fattore di possesso), pertanto in modalità *compliant* alla SCA, secondo il consolidato orientamento del Collegio (*cfr. Collegio di Roma, decisione n. 19821/2021*).

3. Avuto riguardo alle modalità della truffa, il ricorrente affermava di aver ricevuto in data 26.03.2024 un sms apparentemente riconducibile a quello della banca, che lo avvisava di un tentativo di accesso alla sua app bancaria e lo invitava a contattare il numero ivi indicato.

Dopo aver chiamato il numero indicato, il ricorrente veniva ricontattato dall'utenza della Banca resistente, la quale gli riferiva che era necessario completare la configurazione del telefono per la verifica dell'identità, operazione che richiedeva anche un tempo di 24 ore.

Il giorno successivo il ricorrente, impossibilitato ad entrare nell'App della Banca, contattava il servizio clienti che gli comunicava l'avvenuta esecuzione di un bonifico di euro 47.600,00 nei confronti di un terzo soggetto sconosciuto.

Dalla documentazione prodotta in atti risulta che gli sms, inseriti in coda a messaggi genuini dell'Intermediario, sono riconducibili al numero della Banca, traendo pertanto in inganno il ricorrente.

Unitamente a ciò, il ricorrente riceveva una chiamata proveniente dal numero del servizio clienti della Banca.

Secondo l'orientamento condiviso dei Collegi ABF, nelle fattispecie di *sms - spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione.

Tuttavia, qualora il testo del messaggio civetta presenti indici di evidente inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (anche dell'operatività rispetto alle movimentazioni storiche del ricorrente), il Collegio ritiene configurarsi un concorso di colpa tra le parti, individuando da un lato la negligenza grave dell'utente che agevola il compimento della truffa, mentre dall'altro ai limiti organizzativi della Banca in ordine al servizio di pagamento offerto.

Sul punto, il Collegio di Coordinamento ha espresso i seguenti principi in tema di colpa grave del ricorrente a seguito di ricezione di <<[...] un sms "civetta" sulla medesima chat abitualmente utilizzata dall'intermediario; ha cliccato sul link contenuto nell'sms e ha fornito le proprie credenziali e comunicato

*il successivo SMS OTP al truffatore; ha poi ricevuto un ulteriore SMS che le confermava l'attivazione della sua carta sul wallet "A**** pay" senza porsi il problema di contattare l'intermediario per chiedere spiegazioni. In questa situazione, il fatto che il primo sms fosse contenuto nella chat dell'intermediario costituisce un elemento che rende la truffa particolarmente sofisticata e che in parte potrebbe giustificare l'aver dato seguito al link in esso contenuto. Tuttavia, nel concreto svolgimento della vicenda, l'inerzia di fronte al successivo messaggio di conferma dell'attivazione della carta sul wallet ha costituito un elemento assolutamente decisivo, la cui autonoma efficienza causale ai fini della riuscita della truffa è stata tale da far ritenere sussistente la colpa grave della ricorrente e da porre a suo carico tutte le conseguenze dannose della vicenda [...]»>> (cfr. Collegio di coordinamento, decisione n. 9559/2024).*

In senso conforme il Collegio di Roma, con decisione n. 451/2025, ha ravvisato un'ipotesi di colpa grave in capo al ricorrente per negligenza nell'aver agevolato la truffa in presenza di evidenti indici di inattendibilità: << *In presenza di una frode di questo tipo, secondo un orientamento consolidato dei diversi Collegi territoriali, non si ritiene ravvisabile la colpa grave della parte ricorrente, a meno che non siano rinvenibili indici di inattendibilità o anomalie del messaggio truffaldino, in considerazione dei quali si ritiene la sussistenza di un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa e, dall'altro, alle criticità organizzative del servizio di pagamento offerto dall'intermediario (cfr., ad es., Coll. Roma, dec. n. 13521 del 2022 e dec. n. 13110 del 2022). Ora, nel caso di specie, il messaggio truffaldino appare proveniente dall'intermediario, ma si caratterizza per un contenuto approssimativo, per un impiego improprio della punteggiatura e delle maiuscole e per il passaggio da un tono informale a uno formale. Il link contenuto nel messaggio, inoltre, presenta un identificatore (URL) inattendibile, senza protocollo di trasferimento di sicurezza (https) e non riconducibile in alcun modo all'intermediario resistente. Sussisterebbe dunque gli estremi per il riconoscimento di un concorso di colpa della parte ricorrente. Bisogna però considerare anche che il primo messaggio truffaldino è stato seguito da una comunicazione che informava la parte ricorrente che stava procedendo all'attivazione un ulteriore token mobile non richiesto. Il dato è di rilievo. Infatti, secondo un orientamento consolidato dei diversi Collegi territoriali, in ipotesi di questo tipo, quando ricorrono altresì elementi di anomalia del messaggio truffaldino, deve ritenersi la colpa grave dell'utente in via esclusiva. In effetti, in una recente decisione, anche il Collegio di coordinamento ha rigettato un ricorso in cui risultava che il primo messaggio truffaldino con falsificazione dell'identità del mittente era stato però seguito da una comunicazione*

autentica dell'intermediario che confermava l'attivazione dello strumento di pagamento su un wallet (cfr. Coll. coordinamento, dec. n. 9559 del 2024). Si è ritenuto infatti che quest'ultima comunicazione avrebbe dovuto richiamare l'attenzione del cliente sull'operazione che stava per autorizzare. È stata quindi riconosciuta la sua colpa grave per non essersi neppure posto il problema di contattare l'intermediario e chiedere spiegazioni su quanto stava accadendo, consentendo così di fatto ai malfattori di portare a termine il piano criminoso. [...]>>.

Nel caso di specie, i messaggi ricevuti dal ricorrente da parte di un numero apparentemente riconducibile a quello della Banca, recavano l'indicazione di un accesso non autorizzato, invitando il cliente a contattare il servizio clienti.

A ciò faceva seguito la telefonata da parte del servizio clienti al ricorrente, circostanza ascrivibile all'ipotesi del cd. *vishing caller ID*, che, secondo i Collegi, dà luogo ad un <<...concorso colposo delle parti, imputando all'intermediario la colpa di "non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo" (così Collegio di Milano, decisione n. 17467/2021). Si richiede a tal fine solo l'allegazione da parte del ricorrente della lista delle chiamate ricevute, onde poter verificare la corrispondenza del numero utilizzato dal truffatore con il numero verde dell'intermediario (così Collegio di Milano, decisione n. 22105/2021). La frode, così congegnata, non sembra in effetti differire in maniera significativa dalle ipotesi di "spoofing", ossia dalle ipotesi di *smishing* in cui il messaggio "esca" reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario). E, secondo la più recente posizione condivisa dai Collegi territoriali dell'ABF, nelle fattispecie di spoofing è al più ravvisabile "un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario" (in questi termini v., per esempio, Collegio di Roma, decisione n. 1625/2022)>>.

4. Quale ulteriore elemento di valutazione si consideri che, dalla documentazione prodotta, emerge che l'App che ha consentito il controllo da remoto è stata scaricata dal ricorrente il giorno precedente la truffa.

In tali ipotesi, quando la frode risulta attuata tramite installazione di app di terze parti, i Collegi affermano la colpa grave del ricorrente; tuttavia, laddove la truffa prende le mosse da un sms di

spoofing, il Collegio ha ritenuto che l'installazione dell'app e la ricezione dell'sms di *spoofing* concorrono alla realizzazione dell'operazione truffaldina e che pertanto non può rinvenirsi un'ipotesi di responsabilità esclusiva del cliente, bensì una forma di concorso di colpa tra le parti (cfr. *Collegio di Roma, decisione n. 1896/2025; Collegio di Roma, decisione n. 3362/2025*).

5. Ai fini dell'individuazione della responsabilità concorrente dell'Intermediario, è evidente dallo *screenshot* prodotto dal ricorrente che il numero dal quale ha ricevuto l'sms, nonché la successiva chiamata, sono riconducibili a quello ufficiale dell'Intermediario.

Secondo gli orientamenti condivisi dei Collegi ABF, in presenza di un sms o chiamata che si inserisca in una conversazione precedente con l'Intermediario, non è ravvisabile un concorso di colpa grave del ricorrente <<...data l'insidiosità del meccanismo di aggressione e nonostante la maggiore diffusione di campagne informative sul tema; e per analogia si deve ritenere che la chiamata da un numero apparentemente della banca non insospettisca il cliente. Solo nel caso in cui il testo del messaggio civetta presenti indici di evidente inattendibilità (quali ad esempio evidenti errori grammaticali o sintattici) o di anomalia (inequivoca non riconducibilità all'intermediario del link ivi contenuto) che dovrebbero far allertare l'utente avveduto, è stato ritenuto che possa rilevarsi un concorso di colpa a suo carico per aver agevolato il compimento della truffa e, analogamente, occorre valutare le richieste telefoniche dei malintenzionati, le quali possono generare allarme solo in quanto irragionevoli...>> (Collegio di Torino, decisione n. 12068/2024).

La Banca avrebbe pertanto dovuto adottare sistemi di sicurezza tali da evitare la riconducibilità del numero di provenienza dell'sms a quello dell'Intermediario, al fine di evitare che il ricorrente potesse essere tratto in inganno agendo in buona fede.

A ciò deve aggiungersi che sono valorizzabili ulteriori indici di frode relativi alla operatività anomala dell'operazione rispetto alle movimentazioni storiche del ricorrente, il quale avrebbe dovuto ricevere una specifica segnalazione da parte della Banca in merito alla anomalia rilevata (cfr. *Collegio di Roma, decisione n. 7491/2024; Collegio di Roma, decisione n. 11288/2024*).

6. Alla luce dei suddetti principi, deve essere ravvisato un concorso di colpa tra le parti, tenuto conto da un lato della negligenza grave del ricorrente che ha agevolato il compimento della truffa, dall'altro dell'iter organizzativo della Banca che, non impedendo l'attivazione di sms e della chiamata, entrambi riconducibili al numero del medesimo intermediario, non ha consentito al ricorrente di percepire la truffa in corso.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 30.000,00, 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

Firmato digitalmente da
PIETRO SIRENA