

COLLEGIO DI ROMA

composto dai signori:

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

Relatore DOMENICO NASO

Seduta del 25/03/2026

FATTO

Con ricorso introduttivo del presente giudizio preceduto da reclamo del 04/03/2025, parte ricorrente esponeva di aver ricevuto in data 03/03/2025 una chiamata asseritamente proveniente da un numero che sembrava provenire dal servizio clienti della banca.

Il sedicente operatore allertava il ricorrente che sul proprio cellulare erano presenti dei malware, per eliminare i quali avrebbe dovuto scaricare una determinata APP.

Il ricorrente seguiva le indicazioni dell'operatore telefonico, il quale gli preannunciava che il giorno seguente lo avrebbe ricontattato.

Non avendo ricevuto alcuna telefonata, il ricorrente chiamava il servizio clienti, che gli comunicava l'avvenuta esecuzione di un bonifico di euro 6.300,00 da lui non autorizzato.

Il ricorrente chiedeva pertanto all'Arbitro Bancario Finanziario il rimborso della somma sottratta, oggetto di bonifico da lui sconosciuto.

Si costituiva l'intermediario resistente, il quale eccepiva che le operazioni sconosciute erano imputabili alla condotta del ricorrente, rimasto vittima di truffa mediante *vishing* a seguito dell'installazione di un'app malevola.

Rappresentava che l'operazione di pagamento veniva eseguita e correttamente autenticata dal ricorrente mediante il sistema a doppio fattore, quali l'inserimento del PIN (fattore di conoscenza) e del codice OTP (fattore di possesso).

Evidenziava l'Intermediario l'esclusiva responsabilità in capo al ricorrente, per aver seguito ingenuamente le istruzioni impartite dall'operatore telefonico, nonché per aver condiviso le proprie credenziali di accesso mediante download di una sconosciuta applicazione esterna, che ha verosimilmente consentito al terzo truffatore di controllare da remoto il dispositivo.

Concludeva pertanto per il rigetto del ricorso.

DIRITTO

Parte ricorrente chiede la restituzione della somma complessiva di euro 6.300,00 relativa all'esecuzione di un bonifico disconosciuto del 03/03/2025.

Nello specifico, in tale data il ricorrente ha seguito le indicazioni ricevute telefonicamente da un sedicente operatore bancario, installando un'app sul proprio dispositivo nella convinzione di rimuovere un presunto malware dal proprio cellulare.

Dopo due giorni dalla installazione dell'applicazione, il ricorrente si è avveduto dell'avvenuta esecuzione di un bonifico di euro 6.300,00 dal proprio conto corrente, che ha disconosciuto sostenendo di non aver mai eseguito.

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>>.*

In merito all'autenticazione del bonifico, l'intermediario afferma che l'operatività è riferibile al ricorrente e che dalla documentazione in atti non emerge l'enrollment dell'app bancaria su altro device, passaggio non reso necessario in forza dell'installazione della seconda app malevola sul telefono del ricorrente. L'utente ha, in particolare, effettuato il login alle ore 17:09 mediante inserimento di nome utente e codice pin, nonché proceduto alla verifica a due fattori mediante inserimento del PIN.

A ciò ha fatto seguito l'inserimento del bonifico alle ore 17:13 per l'importo contestato, con causale "asquisto panda", firmato con Pin e OTP generato da Mobile Token, a seguito del quale ha ricevuto e visualizzato la notifica push.

Secondo il condiviso orientamento di questo Collegio, è ritenuta *compliant* alla SCA una modalità autorizzativa che preveda la generazione di una OTP da mobile app (cfr. Collegio di Roma, decisione n. 19821/2021).

L'operazione disconosciuta è stata eseguita a seguito della installazione dell'app malevola sul device del ricorrente, con il quale è stato verosimilmente consentito ai terzi frodatori l'accesso all'applicazione. Avuto riguardo alle modalità della truffa, parte ricorrente deduce di aver ricevuto una chiamata in data 03/03/2025 da un numero riconducibile all'intermediario; pur tuttavia, non è stata fornita in giudizio alcuna evidenza della lista delle chiamate in entrata relativamente a quella asseritamente ascrivibile al resistente.

Per tali motivi, ritenendo la documentazione probatoria insufficiente, nella riunione del 04/12/2025 il Collegio ha deliberato di chiedere al ricorrente la produzione di copia delle schermate del registro chiamate del giorno della truffa.

In riscontro alla richiesta di integrazione, il ricorrente ha prodotto schermate che risultano tuttavia sprovviste di data e, nello specifico, non recano il giorno della truffa.

È stata fornita, difatti:

1. una schermata da cui si evincono chiamate in uscita e chiamate perse relative ad un numero riconducibile a un contatto dell'intermediario, ma prive di data;

2. una schermata recante il numero di un'utenza privata, asseritamente riconducibile al truffatore, del giorno 11/03/2026;

3. un sms riconducibile alla banca del 10/03/2026 e recante l'avviso di attivazione del mobile token.

I Collegi ABF ritengono la truffa esperita mediante *vishing caller ID spoofing* come maggiormente insidiosa rispetto al *vishing* classico, per la cui prova è richiesta l'allegazione della lista delle chiamate ricevute, al fine di poterne verificare l'insidiosità (cfr. Collegio di Roma, decisione n. 8749/2024).

In tali casi, può essere rilevata una forma di responsabilità dell'intermediario qualora quest'ultimo, sulla base delle evidenze documentali, abbia fornito un apporto causale alla verifica della truffa, quali: Mancata disponibilità (anche temporanea) del numero verde del PSP, che rende impossibile per l'utente la verifica della genuinità delle indicazioni fornite dal frodatore;

Mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP cui il pagatore si è rivolto esponendo le richieste del frodatore;

Mancato rilievo di indizi di frode, nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole della natura effettiva delle operazioni poste in essere.

Nel caso di specie, non sussiste alcuna delle ipotesi sopra indicate, non essendo configurabile alcuna responsabilità in capo alla Banca resistente, circostanza avvalorata dalla mancata produzione in giudizio, da parte del ricorrente, del registro chiamate.

Il medesimo ricorrente ha peraltro dichiarato di aver scaricato un'applicazione non riconducibile all'intermediario, dalla quale è presumibilmente stato dato avvio al controllo, da parte dei truffatori, del device e dell'applicazione della banca, con conseguente esecuzione del bonifico contestato.

Secondo il condiviso orientamento di questo Collegio <<[...] *in simili fattispecie, questo Arbitro riconosce la colpa grave dell'utente che, su indicazione del frodatore, installi un'applicazione "la cui funzionalità risiede [...] nel permettere l'accesso ed il controllo di pc e smartphone da remoto", consentendo in tal modo al frodatore di agire indisturbato e disporre i pagamenti (cfr. Collegio di Roma, decisione n. 7806/2023). 8. Inoltre, si osserva che non è stato prodotto il messaggio esca. 9. Secondo costante orientamento, questo Arbitro rigetta il ricorso in cui venga lamentata una frode riconducibile allo spoofing laddove il ricorrente "non produc[a] evidenza del messaggio ricevuto e non [sia] noto se abbia in passato ricevuto altri messaggi genuini dallo stesso mittente, che avrebbero potuto generare nell'utente un legittimo affidamento circa la genuinità del messaggio"* (cfr. Collegio di Roma, decisione n. 3032/2023).>> (Collegio di Roma, decisione n. 4317/2024).

Alla luce dei rilievi suesposti e della documentazione prodotta, la domanda di rimborso di parte ricorrente deve essere respinta, tenuto conto della colpa grave in capo all'utente per aver dato seguito alla truffa mediante installazione di un'applicazione ignota che ha verosimilmente consentito al frodatore il controllo dello smartphone e l'esecuzione del bonifico contestato.

PER QUESTI MOTIVI.

Il Collegio respinge il ricorso.

IL PRESIDENTE