Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

## COLLEGIO DI BARI

composto dai signori:

| | |
|---|---|
| (BA) TUCCI | Presidente |
| (BA) BARTOLINI | Membro designato dalla Banca d'Italia |
| (BA) VITERBO | Membro designato dalla Banca d'Italia |
| (BA) CIPRIANI | Membro di designazione rappresentativa degli intermediari |
| (BA) QUARTA | Membro di designazione rappresentativa dei clienti |

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 12/01/2026

## FATTO

La ricorrente riferisce di aver ricevuto in data 7 luglio 2025, nel pomeriggio, una chiamata dal numero del Servizio Clienti dell'intermediario (06***) nell'ambito della quale l'interlocutore le ha rappresentato che era in corso un attacco *hacker* ai suoi danni e l'ha invitata a disinstallare l'APP di *home banking* e ad installare un'APP denominata "*AVG Sicurezza*", rivelatasi poi atta a consentire il controllo da remoto del dispositivo.
Precisa di non avere fornito alcun codice personale e di essere stata richiamata dallo stesso numero il giorno dopo sempre per pretesi motivi di sicurezza sicché, insospettita, ha controllato i movimenti del conto e ha notato l'esecuzione a sua insaputa da parte di ignoti di un bonifico istantaneo di € 26.000,00 in favore di un soggetto da lei non conosciuto.
Precisa che non è stato possibile revocare l'operazione "*per mancanza di fondi sul conto ricevente*".
Tanto premesso, ritiene l'intermediario responsabile dell'accaduto per non aver adottato soluzioni idonee ad evitare l'uso fraudolento dei sistemi elettronici di pagamento e l'appropriazione delle credenziali. Evidenzia che la tecnica dello *spoofing* usata dal frodatore le ha ingenerato un legittimo affidamento sulla genuinità delle comunicazioni. Riferisce, in ultimo, che l'intermediario il 25 agosto 2025 le ha poi comunicato informalmente di avere recuperato l'importo parziale di € 1.500,00, tuttavia non riaccreditato.
Chiede, pertanto, il rimborso dell'importo fraudolentemente sottrattole, pari ad € 26.000,00.
Costituitosi, l'intermediario premette che il proprio servizio di *online banking* prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte", in linea con la normativa europea PSD2, e in particolare:

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

- per effettuare il *login* e le operazioni di *inquiry*, l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP (One Time Password), codice dinamico generato da *Mobile Token*;
- per disporre le operazioni, dopo avere effettuato il *login* e inserita l'operazione, la stessa deve essere confermata mediante l'inserimento del PIN + codice OTP (One Time Password), generato da *Mobile Token*.

Chiarisce, inoltre, che l'attivazione del *Mobile Token* è resa possibile solo con la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato *all'home banking*, indipendentemente dall'attivazione del servizio SMS *Alert*.
Tanto premesso, precisa che, nel caso di specie, dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi e l'operazione risulta correttamente autenticata, registrata e contabilizzata a valle della seguente attività:

- con l'utenza della cliente, alle 18:02:40 del 7 luglio 2025, è stato effettuato il *login* mediante inserimento di Id Utente e PIN da indirizzo IP 151.*** con il dispositivo (***LX1A) e verifica a 2 fattori, utilizzando l'OTP (604***) generato dal *Mobile Token*;
- alle 18:07:25 è stato inserito il bonifico di € 26.000,00 firmato con SCA, in particolare con PIN e OTP (615***) generato da Mobile Token da indirizzo IP 151.*** con il dispositivo (***LX1A).

In definitiva, chiarisce che l'operazione è stata correttamente eseguita con SCA, che ha previsto l'utilizzo di un fattore di conoscenza (PIN) e di un fattore di possesso (OTP).
Quanto alla condotta della ricorrente, osserva che la stessa ha dichiarato di aver installato un'APP di terze parti sul proprio dispositivo, che ha consentito il controllo da "*remoto*" del suo cellulare e, quindi, la conoscenza di tutti i suoi dati, seguendo tutte le istruzioni del truffatore e rileva che, a fronte di una simile richiesta, avrebbe dovuto immediatamente insospettirsi e chiamare il Servizio Clienti.
Soggiunge che, al fine di prevenire possibili frodi in danno alla clientela, conduce da tempo campagne informative in materia. Rileva, inoltre, che è altresì noto che non bisogna riporre eccessiva fiducia nel *caller id* che appare sul telefono in quanto non garantisce che la chiamata sia effettivamente collegabile all'utenza indicata sul *display*, giacché è possibile, con pochi passaggi, modificare il mittente di un numero telefonico da parte di terzi.
Riferisce di aver inviato a seguito dell'operazione appositi *alert* via *push* e SMS e di essersi attivato per il recupero dei fondi, riuscendo però a bloccare presso la banca corrispondente solo un importo parziale di € 1.500,00. A tale ultimo riguardo, precisa che la richiesta di recall non presuppone la restituzione automatica della somma in frode, poiché la banca corrispondente, per poterla addebitare sul conto corrente del beneficiario, deve essere autorizzata dal suo cliente oppure dal Giudice, tramite specifico provvedimento di sequestro.
Chiede, pertanto, di rigettare il ricorso.
In sede di repliche, la ricorrente fa presente che l'APP installata, in realtà, "*risultava essere proprio una applicazione apparentemente riconducibile all'istituto di credito resistente*", come attestato dalla denuncia alla polizia postale. Soggiunge che tale APP malevola non le ha consentito di prendere contezza degli *alert* che la banca le inviava mentre l'attaccante operava fraudolentemente sul conto, poiché dirottava l'inoltro degli SMS *alert* e delle notifiche *push*. Rileva che l'intermediario avrebbe dovuto adottare misure di tutela attive sospendendo l'esecuzione del bonifico alla luce dell'ingente importo e del fatto che avrebbe azzerato il saldo.
Insiste, quindi, per l'accoglimento del ricorso.

**DIRITTO**

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di bonifico istantaneo dell'importo di € 26.000,00 eseguita il 7 luglio 2025, successivamente contestata.

Il Collegio rileva preliminarmente che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13 gennaio 2018. Inoltre, tale operazione è stata eseguita successivamente all'entrata in vigore delle disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento della Banca d'Italia del 5 luglio 2011.

In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". Il comma 2 del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è, altresì, precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

Ai sensi del successivo art. 12, comma 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve, inoltre, ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione.

Si deve, altresì, rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

Al riguardo, il Collegio di Coordinamento ha in più occasioni precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia). La *ratio* di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coordinamento, decisioni n. 3947/2014 e, da ultimo, n. 22745/2019, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *ex* art. 10, comma 2, d.lgs. n. 11/2010).
Tratteggiato il quadro normativo di riferimento, occorre premettere che, nel caso di specie, l'intermediario resistente afferma che l'operazione contestata è stata eseguita mediante l'utilizzo dei seguenti fattori: PIN (fattore di conoscenza); e OTP generato da *Mobile Token* (fattore di possesso).
In particolare, l'intermediario fornisce una descrizione dettagliata dell'operazione intercorsa, secondo la quale, con l'utenza della cliente alle 18:02:40 del 07/07/2025, è stato effettuato il *login* mediante inserimento di Id Utente e PIN da indirizzo IP 151.*** con il dispositivo (***LX1A) e verifica a 2 fattori, utilizzando l'OTP (604***) generato dal *Mobile Token*; e alle 18:07:25 è stato inserito il bonifico di € 26.000,00 firmato con SCA, in particolare con PIN e OTP (615***) generato da *Mobile Token*, sempre da indirizzo IP 151.*** e con il dispositivo (***LX1A).
Tuttavia, il Collegio rileva che l'intermediario ha prodotto i log relativi alle suddette operazioni senza fornire allegazioni specifiche in ordine al *device* utilizzato per generare l'OTP e, in particolare, non ha chiarito né se sia il device storicamente registrato e utilizzato dalla ricorrente, né se sia un nuovo *device* registrato a ridosso dell'operatività contestata e se tale eventuale nuovo *enrollment* sia stato eseguito con SCA. Inoltre, dalle evidenze prodotte può evincersi soltanto che l'inserimento e l'autorizzazione del bonifico disconosciuto sia avvenuto da un *device* diverso da quello in precedenza registrato e con un *Mobile Token* recante un diverso seriale. Sul punto, non constano neppure dichiarazioni confessorie della ricorrente in merito alla validazione di *push* autorizzative o alla titolarità del *device* indicato nei *log* .
Stante l'incertezza in merito all'APP concretamente utilizzata per l'esecuzione dell'operazione disconosciuta, si deve confermare l'orientamento di questo Collegio (cfr. decisioni n. 2918/2025; n. 11625/2024; e n. 3749/23) che, in tali casi, non ha considerato assolto l'onere probatorio relativo all'autenticazione.
Orbene, secondo l'orientamento consolidato dell'Arbitro, la mancanza 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.
Ne consegue il riconoscimento del diritto della ricorrente al rimborso dell'importo oggetto dell'operazione di bonifico contestata.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

**P.Q.M.**

**Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 26.000,00.**
**Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE