

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) ROBUSTELLA	Membro di designazione rappresentativa dei clienti

Relatore CARMELA ROBUSTELLA

Seduta del 30/03/2026

FATTO

La ricorrente, titolare di un conto bancario intrattenuto con la resistente, riferisce che in data 22/10/2025 accedeva al conto online e constatava la presenza di due bonifici istantanei eseguiti tra le ore 16:20 e 16:25 del 20/10/2025, rispettivamente di € 4.500,00 e di € 1.736,00 in favore di terzi sconosciuti.

Precisa di non aver mai consegnato o rilasciato i codici di accesso del conto a estranei. Osserva che per l'esecuzione dei bonifici è necessaria la generazione di codici OTP che, nel caso di specie, non sono stati generati.

Ritiene dunque che via stato un problema nel sistema informatico dell'intermediario.

Chiede pertanto il rimborso delle somme sottratte pari a € 6.236,00, nonché la refusione delle spese legali.

Costitutosi ritualmente, l'intermediario precisa che la ricorrente - titolare di un conto funzionale all'erogazione di servizi presso la propria attività - disconosce due bonifici disposti dal proprio conto il 20/10/2025, dell'importo di € 4.500,00 ed € 1.736,00.

Preliminarmente rileva la carenza di allegazione e di prove da parte della ricorrente, la quale non fornisce elementi utili e idonei a circostanziare le modalità dell'esecuzione delle operazioni contestate,

lasciando presupporre una partecipazione, quantomeno gravemente colposa, della stessa nell'esecuzione delle operazioni contestate.

Ad ogni modo, osserva che le transazioni disconosciute sono state eseguite regolarmente, senza alcuna anomalia, previo accesso all'app tramite un dispositivo non in precedenza autenticato.

Dichiara che, in tale contesto, l'utente deve innanzitutto procedere all'installazione dell'applicazione effettuando un primo accesso per la registrazione, fase in cui viene richiesto di indicare le credenziali di riferimento (username e password).

Saggiunge che, dopo aver verificato la correttezza delle credenziali, il sistema associa l'ID esercente alla sessione (previa generazione di apposito token di sessione restituito all'app) e verifica che all'esercente sia effettivamente associato un conto di pagamento attivo.

Rappresenta che successivamente, quale ulteriore livello di controllo, la *mobile application* verifica altresì se il *device* in uso dall'utente risulta essere certificato, innescando, ove non sia così, un processo di certificazione del dispositivo che, in piena conformità agli orientamenti ABF (cfr. ex multis, Collegio di Bari, decisione n. 1086/2023), è basato su SCA e avviene tramite inserimento in app di una OTP inviata via SMS al numero di cellulare dell'esercente quale secondo fattore di autenticazione.

Segnala che, una volta autenticato, l'utente può compiere operazioni dispositive solo per il tramite di quel device, mediante i seguenti fattori di autenticazione forte: User ID/password (fattore di conoscenza) e identificativo univoco del *device* certificato associato tramite OTP alla sua utenza/notifica push (fattore di possesso).

Fa presente che, nel caso in esame, dall'analisi condotta circa l'utenza della ricorrente si evince che il 20/10/2025, alle ore 16:20:02, veniva effettuato, previo inserimento di *username* e *password* (credenziali che solo l'esercente poteva conoscere), un accesso all'area personale da un dispositivo non certificato in precedenza.

Osserva che alle ore 16:20:05 l'app rilevava correttamente che il *device* in uso (**48b) non era certificato e avviava così il processo di certificazione di un nuovo dispositivo, con generazione di una OTP (8 caratteri numerici randomici) e l'invio della stessa tramite SMS all'esercente.

Evidenzia che alle ore 16:20:26 la piattaforma inviava, come confermato anche dalla ricorrente, detto codice OTP al numero riferibile all'esercente, dalla stessa fornito sia in sede di sottoscrizione del contratto sia in sede di denuncia, ai fini dell'associazione del nuovo dispositivo e detto codice veniva poi inserito sull'app.

Fa presente che, nel verificare la correttezza dell'OTP ricevuto e inserito, alle ore 16:20:35 procedeva a certificare il nuovo dispositivo (**48b) secondo le richieste, debitamente autorizzate, della ricorrente.

Osserva che dal nuovo *device* certificato l'utente veniva ricondotta sulla pagina di *login* dell'app per un ulteriore inserimento delle credenziali, che venivano effettivamente inserite alle ore 16:22:56, consentendo, previa inclusione di un PIN precedentemente creato dall'utente, di completare la SCA alle ore 16:23:39, con registrazione dell'avvenuta autenticazione a due fattori alle ore 16:23:40.

Rileva che, successivamente, previo login al portale web alle ore 18:11:36, mediante inserimento di *username* e *password*, l'utente accedeva alla sezione "home banking" attivando una nuova procedura SCA, ricevendo notifica push sul nuovo device certificato alle ore 18:11:50 e inserimento del PIN precedentemente impostato, così completando il flusso SCA alle ore 18:11:52.

Fa presente che, eseguito detto *login*, venivano successivamente disposti i bonifici oggetto di ricorso, rispettivamente alle ore 18:32:46 e 18:55:33, utilizzando il *device* certificato/notifica *push* come elemento di possesso e il PIN come elemento di conoscenza (oltre ad aver già inserito in sessione le credenziali).

Ritiene di aver fornito la prova della SCA per tutte le fasi (cita ex multis, Collegio di Bari, decisione n. 6954/2024 e Collegio di Bologna, decisione n. 23216/21).

Segnala che, sebbene l'esercente lamenti di non aver autorizzato i bonifici, la ricostruzione degli eventi sopra riportata, suffragata dai documenti prodotti, conferma che si tratta di operazioni dallo stesso autorizzate, dato l'utilizzo delle credenziali di sicurezza personalizzate, che solo la ricorrente poteva conoscere, e di un codice OTP che solo la stessa può aver ricevuto utilizzato, o comunicato, per autorizzare il procedimento che ha poi portato all'esecuzione delle transazioni.

Segnala che, nell'intercettare prontamente un'attività potenzialmente sospetta, ha comunque disposto il blocco cautelativo del conto dell'esercente in data 22/10/2025, al fine di prevenire, se del caso, ulteriori movimentazioni fraudolente. Saggiunge di aver attivato anche l'opportuna procedura di *recall* delle operazioni.

Quanto alla colpa grave, ribadisce che la ricorrente si è limitata a sostenere di non aver eseguito i bonifici oggi contestati, ma non ha riferito né provato di essere stata vittima di alcun tipo di frode e che pertanto non è possibile comprendere se la truffa stessa vi sia effettivamente stata.

Richiama l'orientamento dei Collegi secondo cui – in mancanza della produzione di elementi da cui sia possibile evincere la tecnica truffaldina – sussiste la colpa grave della ricorrente per negligente cooperazione con i frodatori (cita Collegio di Roma, decisione n. 6301/2023).

Ad ogni buon conto, fa presente che l'eventuale truffa è stata possibile solo grazie alla collaborazione fornita dalla ricorrente.

Evidenzia che la ricorrente è stata destinataria di specifiche campagne informative, *alert* e attività di formazione, mirate a sensibilizzarla in modo particolare sulle più comuni tecniche di frode informatica e sulle corrette modalità di protezione di credenziali e dati sensibili.

In particolare, richiama la PEC inviata all'esercente il 22/01/2025 e il 16/10/2025, quindi in prossimità della truffa subita, volta a sollecitare l'attenzione su «*crescenti e sempre più sofisticati tentativi di truffa legati a fenomeni di phishing e spoofing*».

Infine, ritiene infondata la domanda di rifusione delle spese legali.

Pertanto, chiede il rigetto del ricorso e, in via subordinata, nella denegata ipotesi in cui il Collegio dovesse ravvisare profili di responsabilità dell'intermediario, chiede di graduare la propria responsabilità in ragione delle responsabilità imputabili alla ricorrente.

In sede di repliche, la ricorrente afferma di aver evidenziato, nel modulo di disconoscimento inviato il 22/10/2025, che: - alle ore 16:20 del 20/10/2025 effettuava un accesso al conto per verificare movimenti e saldo; - andando alla barra dei movimenti, compariva il pulsante "adeguata verifica"; - cliccava su tale pulsante e eseguiva la verifica; - dopodiché effettuava il log out.

Precisa che tale accesso veniva eseguito dal computer in dotazione alla propria attività e andando direttamente sul sito dell'intermediario e "non sul link arrivato via mail", né da un dispositivo non in precedenza autenticato.

Saggiunge di aver ricevuto alle ore 16:23 tramite SMS solo due codici OTP, uno per l'accesso alla piattaforma e uno per l'adeguata verifica.

Rileva che per effettuare l'accesso ad un nuovo dispositivo occorrono almeno quattro codici OTP.

Contesta che la colpa grave dell'utente non può essere presunta o desunta implicitamente dalla sola circostanza che le sue credenziali siano state utilizzate per autorizzare l'operazione.

Ritiene che la semplice prova della regolarità formale dell'operazione, attestata dai log informatici, non è di per sé sufficiente a esonerare la banca dalla sua responsabilità.

Insiste nel sostenere che la responsabilità dell'accaduto ricada sull'intermediario, rientrando nel suo rischio professionale la possibilità di utilizzazione fraudolenta dei codici da parte di terzi.

Soggiunge inoltre che la banca avrebbe dovuto attivare sistemi di allarme e adottare cautele ulteriori, quali il blocco preventivo o il contatto diretto con il cliente, dato il carattere anomalo delle operazioni in questione.

Insiste per l'accoglimento del ricorso.

L'intermediario, in sede di controrepliche, eccepisce che la ricorrente nelle repliche non allega ulteriori elementi utili a circoscrivere la truffa. Evidenzia che la ricorrente, oltre ad aver fornito le proprie credenziali, ha ricevuto alle 16:20 un sms con l'OTP per la certificazione di un nuovo device che ha evidentemente comunicato a terzi.

Precisa che alle successive 16:23 e 16:27 la ricorrente ha ricevuto due SMS contenenti OTP utilizzati per accedere alla piattaforma web ed effettuare l'aggiornamento dell'adeguata verifica, completato alle ore 16:29.

Ribadisce di aver provato l'adozione della SCA in tutte le fasi che hanno portato all'esecuzione dei bonifici contestati; nonché che la disposizione dei bonifici è stata autorizzata mediante l'utilizzo di informazioni che potevano essere – e dovevano certamente rimanere – nella esclusiva disponibilità della ricorrente.

Insiste pertanto per il rigetto del ricorso.

DIRITTO

La controversia riguarda due operazioni di pagamento non autorizzate, consistenti in due bonifici istantanei di euro 4.500 e di euro 1.736,00 eseguiti in data 20/10/2025

Il ricorrente nella denuncia sporta riferisce che in data 22/10/2025 accedeva al conto online e constatava la presenza di due bonifici istantanei, rispettivamente, di € 4.500,00 e di € 1.736,00 eseguiti in favore di terzi sconosciuti.

Precisa di non aver mai consegnato o rilasciato i codici di accesso del conto a estranei. Osserva che per l'esecuzione dei bonifici è necessaria la generazione di codici OTP che, nel caso di specie, non sono stati generati.

Ritiene dunque che via stato un problema nel sistema informatico dell'intermediario.

Ha quindi segnalato le operazioni come non autorizzate e adisce l'Arbitro Bancario Finanziario, chiedendo:

- la declaratoria di non autorizzazione dell'operazione;
- la condanna dell'intermediario al rimborso delle somme sottratte pari a € 6.236,00, nonché la refusione delle spese legali.

L'intermediario, dal canto suo, sostiene di aver correttamente applicato i presidi di sicurezza previsti dalla disciplina sui servizi di pagamento, in particolare l'autenticazione forte del cliente, mediante l'utilizzo congiunto di credenziali statiche, OTP via SMS e dispositivo registrato. A suo dire, la riconducibilità dell'operazione alle credenziali del ricorrente, unitamente al corretto inserimento dell'OTP, dimostrerebbe l'esecuzione conforme alle istruzioni del cliente. Chiede pertanto il rigetto del ricorso e, in subordine, la riduzione dell'eventuale risarcimento ai sensi dell'art. 1227 c.c., ove venga accertata una sua qualsivoglia responsabilità.

Il Collegio accerta che le operazioni disconosciute consistono in due bonifici istantanei di euro € 4.500,00 e di € 1.736,00 eseguiti tra le ore 16:20 e 16:25 del 20/10/2025. Le operazioni disconosciute sono state, quindi, eseguite 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. PSD2), entrata in vigore il 13/01/2018. Il Collegio rileva che, nella

denuncia presentata il 22/10/2025, la ricorrente ricostruisce i fatti in modo analogo al ricorso. Nel modulo di disconoscimento, il ricorrente negava di aver ceduto a terzi le credenziali di sicurezza o di averle comunicate tramite SMS, telefono o e-mail.

L'intermediario, per parte sua, espone, in via generale, che l'utente, per utilizzare l'applicazione mobile, deve procedere alla sua installazione ed effettuare un primo accesso per la registrazione, fase in cui gli viene chiesto di indicare le credenziali di riferimento (username e password).

Successivamente, la mobile application verifica se il dispositivo in uso risulti già certificato; in caso contrario, viene avviato un processo di certificazione basato sull'inserimento, all'interno dell'app, di una OTP inviata via SMS al numero di cellulare del cliente, quale secondo fattore di autenticazione.

Una volta autenticato, l'utente può compiere operazioni dispositive solo tramite quel dispositivo, mediante i seguenti fattori di autenticazione forte:

- User ID e password (fattore di conoscenza);
- identificativo univoco del device certificato, associato tramite OTP alla sua utenza, e/o notifica push (fattore di possesso).

Nel caso di specie, l'intermediario afferma che l'operatività disconosciuta sarebbe stata preceduta da un accesso effettuato da un dispositivo "non in precedenza autenticato".

Dalle dichiarazioni rese emerge che il giorno della truffa (02/09/2025) si sono succedute le seguenti fasi:

1. certificazione di un nuovo device;
2. login;
3. autorizzazione del bonifico.

L'intermediario produce i log di sistema, corredati da note esplicative, descrivendo così l'operatività intercorsa:

- alle ore 16:20:02 del giorno della truffa è stato effettuato, previo inserimento di *username* e *password*, un accesso all'area personale della ricorrente da un dispositivo non certificato in precedenza;
- alle ore 16:20:05 l'app ha riconosciuto l'accesso da un *device* (n. ***48b) non associato alla ricorrente e ha avviato il processo di certificazione;
- all'utente è stato quindi chiesto di impostare un PIN composto da 6 caratteri numerici, da utilizzare per confermare le operazioni tramite SCA, in alternativa alla biometria;
- alle ore 16:20:06 la piattaforma ha inviato un codice OTP al numero riferibile all'esercente ai fini dell'associazione del nuovo dispositivo e detto codice è stato poi inserito sull'app;
- alle ore 16:20:35 nel verificare la correttezza dell'OTP ricevuto e inserito, l'intermediario ha provveduto a certificare il nuovo dispositivo;
- alle ore 16:20:56 l'utente ha eseguito il log in nell'app dal nuovo device certificato, inserendo *username* e *password*, e verificato che il device dell'utente risultava certificato, l'app ha richiesto l'inserimento del PIN, correttamente effettuato dall'utente;
- alle successive 18:11:36 è stato registrato un accesso dal portale web con inserimento di *username* e *password* e l'attivazione della voce di menu "home banking" da web, autorizzato tramite push notification e inserimento del PIN precedentemente impostato;
- alle ore 18:11:56 si è completato il flusso SCA per autorizzare l'accesso all'home banking e l'utente è stato abilitato ad operare sul conto di pagamento;
- sono stati successivamente disposti da web i bonifici disconosciuti, rispettivamente alle ore 18:32:46 e alle 18:55:33, utilizzando il device certificato, su cui l'utente riceve una notifica push e autorizza l'operazione inserendo il PIN, precedentemente impostato.

È prodotta evidenza dell'OTP SMS inviata per autorizzare l'accesso da un nuovo dispositivo. Il numero di telefono indicato coincide con quello presente nell'anagrafica del ricorrente e da lui stesso comunicato in sede di denuncia.

L'intermediario allega, inoltre, ulteriori log da cui risultano i passaggi che hanno portato all'esecuzione dei bonifici contestati.

Dalla descrizione offerta emerge che la certificazione del nuovo device del truffatore (e, nell'ambito di tale attività, l'impostazione del nuovo PIN) è avvenuta tramite l'inserimento congiunto di:

- una password (fattore di conoscenza);
- una OTP SMS (fattore di possesso).

Il login prodromico ai bonifici è avvenuto mediante inserimento della password (fattore di conoscenza) e autorizzazione della notifica push inviata al device precedentemente certificato (fattore di possesso). Una volta effettuato tale login, i bonifici sono stati autorizzati in forza del riconoscimento, da parte del sistema, del device certificato (fattore di possesso), sul quale è pervenuta la notifica push, e dell'inserimento del PIN precedentemente impostato, con riutilizzo della password di accesso (fattore di conoscenza).

Il Collegio, in proposito, rammenta che, secondo l'orientamento condiviso dai Collegi, la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte. Ai fini della valutazione dell'assolvimento dell'onere probatorio relativo alla SCA, possono essere considerati, oltre ai log, anche ulteriori elementi esplicativi, quali la legenda e/o le difese del prestatore di servizi di pagamento, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova dell'autenticazione. I Collegi hanno, inoltre, precisato che eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c. Sulla base di quanto sopra, il Collegio ritiene che l'intermediario abbia assolto l'onere probatorio di cui all'art. 10 d.lgs. 11/2010, dimostrando che il bonifico istantaneo di euro 3.131,00 del 02/09/2025 è stato eseguito mediante un sistema di autenticazione forte conforme alla disciplina PSD2, correttamente funzionante e privo di malfunzionamenti.

Chiarito ciò, il Collegio richiama il principio di diritto enunciato dal Collegio di Coordinamento con la pronuncia n. 22745/19 del 10/10/2019, secondo cui: "[...] 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 interpretata 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 riguardo all'ulteriore requisito della colpa grave del cliente, il Collegio ritiene che l'intermediario abbia fornito elementi sufficienti a comprovarne la sussistenza. In particolare, l'intermediario eccepisce che la ricorrente non ha fornito elementi utili alla ricostruzione dell'accaduto.

Effettivamente, in sede di ricorso la ricorrente non descrive le modalità della frode, limitandosi a disconoscere le operazioni fraudolente in questione e a chiederne il rimborso.

In sede di repliche, si limita ad affermare di aver ricevuto il giorno della truffa alle 16:23 solo due codici OTP, uno per autorizzare l'accesso al conto e uno per l'adeguata verifica e di non aver ricevuto nessun altro codice OTP.

Il Collegio, inoltre, rileva che in sede di repliche la ricorrente fa genericamente riferimento ad un "*link arrivato tramite mail*". Sul punto, il Collegio richiama le posizioni condivise dai Collegi secondo cui nelle contestazioni di utilizzi fraudolenti *on line* di strumenti di pagamento in cui:

- a) l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute;
- b) il sistema di pagamento risulta conforme alla *Strong Customer Authentication* (SCA);
- c) non risultano indici di anomalia delle operazioni e/o ulteriori elementi

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo.

Ciò premesso, il Collegio rileva che l'intermediario non ha fornito alcuna deduzione in merito all'eventuale invio di notifiche sms alert relative alle operazioni oggetto di ricorso, né ha prodotto documentazione sul punto. Il Collegio di Coordinamento, con decisione n. 24366/2019, ha chiarito che tra gli obblighi di protezione dell'utente gravanti sull'intermediario rientra anche la fornitura del servizio di sms alert (o strumenti equivalenti), dal quale l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente. Le conseguenze della mancata attivazione del servizio devono poi essere valutate alla luce delle circostanze concrete del caso.

Nel caso di specie, le operazioni disconosciute sono state effettuate nell'arco di circa venti minuti: la prima alle ore 18:33 e la seconda alle ore 18:55 del 20/10/2025. L'attivazione di tale rilevante presidio di sicurezza avrebbe verosimilmente consentito di evitare quantomeno la seconda operazione fraudolenta. Il mancato funzionamento del sistema di sms alert integra, pertanto, una disfunzione organizzativa imputabile all'intermediario, con conseguente responsabilità concorrente rispetto al comportamento gravemente negligente del ricorrente.

Alla luce di quanto precede, il Collegio ritiene configurabile la responsabilità dell'intermediario resistente in relazione alla seconda operazione non autorizzata e, per l'effetto, lo condanna alla restituzione di € 1.736,00.

La ricorrente ha inoltre richiesto la rifusione delle spese legali. Il Collegio, anche alla luce dei principi recentemente espressi dal Collegio di Coordinamento con decisione n. 4580/2025 — secondo cui tali spese possono essere riconosciute solo in presenza di condotte particolarmente scorrette o dilatorie dell'intermediario, ovvero quando la complessità della controversia renda oggettivamente necessaria l'assistenza di un professionista — ritiene che, nel caso di specie, sussistano i presupposti per procedere a una liquidazione equitativa, nella misura di € 200.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 1.736,00. Il Collegio dispone inoltre che l'intermediario corrisponda al ricorrente l'importo di € 200,00 a titolo di rifusione delle spese di assistenza professionale.

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