

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

Il ricorrente, in qualità di “titolare di rivendita sali e tabacchi”, afferma che, in data 02/09/2025 (alle ore 15:55), riceveva una e-mail fraudolenta riconducibile all’intermediario, che lo esortava ad entrare sul proprio account di pagamento per aggiornare i dati anagrafici. Dopo aver “cliccato il pulsante giallo, con la scritta “ACCEDI AL TUO CONTO” deduce di essere stato “rimandato al [...] conto personale che giornalmente consult[a] al fine di controllare la [...] situazione bancaria”; Dichiarava di “aver inserito i dati di accesso” e di essersi così avveduto della sottrazione fraudolenta di € 3.131,00.

Afferma di aver sporto denuncia e di aver compilato il modulo di disconoscimento.

Pertanto, chiede la restituzione della somma indebitamente sottratta.

Costitutosi ritualmente, l’intermediario precisa che il ricorrente disconosce un bonifico istantaneo di € 3.131,00.

Contesta le circostanze a fondamento dell’avversa pretesa in quanto “insufficienti, prive di allegazioni probatorie e comunque infondate nel merito”.

Rileva che l’operazione è stata autorizzata previo accesso alla mobile app, tramite un dispositivo non in precedenza autenticato. Dichiarava che, in tale contesto, l’utente deve innanzitutto procedere

all'installazione dell'applicazione effettuando un primo accesso per la registrazione, tramite username e password.

Aggiunge 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 al ricorrente sia effettivamente associato un conto di pagamento attivo.

Rappresenta che successivamente, quale ulteriore livello di controllo, la mobile application verifica se il device in uso risulta essere certificato innescando, ove non sia così, un processo che, in piena conformità agli orientamenti ABF (cfr. ex multis, Collegio di Bari, decisione n. 1086/2023), è basato su SCA con inserimento in app di una OTP inviata via SMS al numero di cellulare del ricorrente 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 di specie, il 02/09/2025 alle ore 16:10:47 veniva effettuato, previo inserimento di username e password (credenziali che solo il ricorrente poteva conoscere), un accesso all'area personale da un dispositivo non certificato in precedenza.

Alle ore 16:10:51 l'app rilevava che il device utilizzato (44a3*****7970) era diverso da quello utilizzato dal ricorrente (5384*****7d5b).

Dunque, alle ore 16:11:45, veniva avviato il processo di certificazione di un nuovo device, mediante generazione di una OTP, inviata tramite SMS al numero di comprovata appartenenza del ricorrente. Conseguentemente, il ricorrente digitava il codice OTP e, dopo la verifica dell'OTP, veniva certificato il nuovo device (44a3*****7970) alle ore 16:11:56.

Osserva che, dal nuovo device certificato, risulta che il ricorrente veniva ricondotto sulla pagina di login dell'app, e provvedeva al reinserimento delle credenziali di accesso.

Da quanto emerso, previa inclusione di un PIN precedentemente creato dal ricorrente, si evince la correttezza della procedura ai fini della SCA, completata con autenticazione a due fattori alle ore 16:12:35.

Precisa che il ricorrente, previo login al portale web, accedeva alla sezione "home banking" (con inserimento di username e password), attivando così una nuova procedura SCA mediante notifica push sul nuovo device e PIN (precedentemente impostato).

A seguito del buon esito della procedura, l'utente veniva abilitato ad operare sul Conto di pagamento. Fa presente che, eseguito detto login, veniva successivamente disposto il bonifico oggetto di ricorso alle ore 16:20:03, utilizzando il device certificato/notifica push come elemento di possesso e il PIN come elemento di conoscenza.

Ritiene quindi di aver fornito la prova della SCA per tutte le fasi relative all'operatività contestata. Infatti, la ricostruzione degli eventi sopra riportata, suffragata dai documenti prodotti, conferma che si tratta di operazioni autorizzate tramite l'utilizzo delle credenziali di sicurezza e di un codice OTP che solo il ricorrente poteva aver ricevuto e utilizzato (o comunicato) per autorizzare l'esecuzione delle transazioni.

Richiama la decisione n. 5646/2023 del Collegio di Palermo secondo cui "l'evidenza dell'invio del codice OTP al numero di cellulare del ricorrente con orario compatibile con quello dell'operazione vale come prova del fattore di autenticazione, ancorché non consti in atti il contenuto del messaggio".

In merito alla colpa grave, afferma che il cliente si limita a dichiarare di non aver autorizzato l'operazione di bonifico in questione, senza entrare nel merito della truffa subita. Richiama, in tal senso,

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

Dichiara, infine, di aver disposto il blocco cautelativo della carta e di aver tentato le procedure di richiamo delle operazioni (c.d. recall), che, tuttavia, non hanno sortito alcun effetto.

Pertanto, chiede il rigetto del ricorso. In via subordinata, nella denegata ipotesi in cui il Collegio dovesse ravvisare profili di responsabilità dell'intermediario, chiede di graduare la propria responsabilità, ai sensi dell'art. 1227 c.c.

Il ricorrente, in sede di repliche, esclude la sussistenza della colpa grave in quanto afferma di aver inserito le credenziali di accesso su un sito "esteticamente identico a quello ufficiale" e di aver comunicato i codici OTP nell'ambito di una procedura in apparenza legittima "anche a seguito di contatto proveniente da numero recante il nome o il servizio clienti della banca".

Osserva di non disporre delle competenze tecniche necessarie per avvedersi della truffa ed insiste per il rimborso della somma sottratta.

L'intermediario, in sede di controrepliche, rileva che il ricorrente non ha fornito, anche in sede di repliche, prova della e-mail fraudolenta e del dedotto contatto telefonico.

Si riporta, per il resto, a quanto già esposto e concluso.

DIRITTO

La controversia riguarda un'operazione di pagamento non autorizzata, consistente in un bonifico istantaneo di euro 3.131,00 eseguito in data 02/09/2025.

L'operazione contestata è stata eseguita a seguito di una truffa informatica riconducibile a tecniche di phishing, verosimilmente combinate con smishing e/o vishing. Il ricorrente dichiara, infatti, di aver ricevuto una comunicazione apparentemente proveniente dal servizio clienti della banca, contenente un link a un sito clone della piattaforma di home banking. Convinto dell'autenticità della comunicazione, il ricorrente ha inserito le proprie credenziali dispositive e, successivamente, ha digitato l'OTP ricevuta sul proprio telefono, ritenendo di star completando una procedura di sicurezza richiesta dall'intermediario per prevenire accessi fraudolenti. Solo in un secondo momento, a seguito della consultazione del conto e/o della ricezione di un SMS di alert, il ricorrente ha constatato l'avvenuta esecuzione del bonifico istantaneo non voluto. Ha quindi segnalato l'operazione come non autorizzata e presentato reclamo all'intermediario, rimasto senza esito soddisfacente. Il ricorrente ha quindi adito l'Arbitro Bancario Finanziario, chiedendo:

- la declaratoria di non autorizzazione dell'operazione;
- la condanna dell'intermediario al rimborso integrale della somma di euro 3.131,00.

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 l'operazione disconosciuta consiste in un bonifico istantaneo di euro 3.131,00 disposto alle ore 16:20:03 del 02/09/2025. Non risulta allegata la lista movimenti o l'estratto conto. Il blocco della carta è avvenuto in data 02/09/2025, dunque nello stesso giorno dell'operazione

fraudolenta. L'operazione disconosciuta è stata, quindi, 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. PSD2), entrata in vigore il 13/01/2018. Il Collegio rileva che, nella denuncia presentata il 02/09/2025, il ricorrente ricostruiva i fatti nei seguenti termini:

- alle ore 15:58 dello stesso giorno prendeva visione di una e-mail, apparentemente proveniente dalla banca convenuta, con cui gli veniva richiesto di "aggiornare le mie informazioni il prima possibile come misura contro il riciclaggio";
- successivamente, dopo aver prestato il consenso, si avvedeva della sottrazione di euro 3.131,00 dal conto corrente.

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, e ricostruiva la truffa in termini sostanzialmente analoghi a quanto dichiarato in denuncia e nel ricorso.

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 16:10:47 è stato effettuato, previo inserimento di username e password, un accesso all'area personale del ricorrente da un dispositivo non precedentemente certificato;
- alle ore 16:10:51 l'app ha riconosciuto l'accesso da un device (n. *970) non associato al ricorrente e ha avviato il processo di certificazione;
- all'utente è stato chiesto di impostare un PIN di 6 cifre numeriche, da utilizzare per confermare le operazioni tramite SCA, in alternativa alla biometria;
- alle ore 16:11:45 la piattaforma ha inviato un codice OTP al numero di telefono riferibile al ricorrente, ai fini dell'associazione del nuovo dispositivo;
- alle ore 16:11:56, verificata la correttezza dell'OTP ricevuta e inserita, l'intermediario ha provveduto a certificare il nuovo dispositivo (n. *970);

- alle ore 16:12:21 l'utente ha effettuato il login nell'app inserendo username e password e, verificato che il device (n. *970) risultava certificato, l'app ha richiesto l'inserimento del PIN, correttamente digitato;
- alle ore 16:16:31 l'utente ha effettuato il login sul sito web e, alle ore 16:16:36, è stata inviata una notifica push al predetto device, autorizzata tramite l'inserimento del PIN precedentemente impostato;
- eseguito tale login, alle ore 16:20 è stato disposto il bonifico sconosciuto, utilizzando il device certificato, sul quale è pervenuta la notifica push, poi autorizzata con l'inserimento del PIN.

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 del bonifico contestato.

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 al bonifico 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, il bonifico è stato autorizzato 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. Il cliente ha infatti inserito username,

password e codice OTP nella pagina raggiunta tramite la e-mail fraudolenta, consentendo così ai truffatori di entrare in possesso dei codici dispositivi.

Lo stesso ricorrente, del resto, ha confermato tale circostanza nella dichiarazione contenuta nella denuncia, alla quale deve essere riconosciuto valore confessorio.

Il ricorrente riferisce di aver inserito le credenziali dopo aver ricevuto una e-mail apparentemente riconducibile all'intermediario, contenente un link che lo ha indirizzato a una pagina web identica a quella ufficiale. In sede di repliche, ha ribadito che "le credenziali sono state inserite su un sito esteticamente identico a quello ufficiale" e che "i codici OTP sono stati comunicati nell'ambito di una procedura apparentemente legittima, anche a seguito di contatto proveniente da numero recante il nome o il servizio clienti della banca". Tuttavia, agli atti non risulta prodotta copia di tale e-mail. Sul punto, il Collegio richiama l'orientamento dell'Arbitro secondo cui la mancata allegazione del messaggio civetta (o della registrazione della telefonata ricevuta) non consente di accertare se sussistano o meno gli estremi di un legittimo affidamento dell'utente circa la genuinità dell'interlocuzione con l'intermediario.

Per completezza, il Collegio precisa che, essendo stata posta in essere una sola operazione, l'eventuale mancata attivazione di presidi di sicurezza ex post da parte dell'intermediario (quali SMS alert o strumenti assimilabili) deve ritenersi irrilevante.

Alla luce di quanto sopra esposto, il Collegio ritiene che non possa configurarsi alcuna responsabilità in capo all'intermediario resistente e che, conseguentemente, la domanda del ricorrente non possa essere accolta.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE