

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore ENZO SCANNELLA

Seduta del 31/03/2026

FATTO

Dopo aver invano esperito la fase di reclamo, con ricorso pervenuto in data 29.12.2025, il ricorrente chiede la restituzione della somma di euro 14.980,00, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati. Parte ricorrente avanza altresì domanda di restituzione degli interessi.

Parte ricorrente riferisce che/di:

- In data 26/09/2025 alle ore 19:20 riceveva un sms che si inseriva nella cronologia di comunicazione ufficiale della resistente, a seguito del quale intratteneva una conversazione telefonica con utenza riconducibile a quella del numero dell'intermediario;
- Il sedicente operatore forniva al cliente una serie di informazioni per confermare la sua identità e lo informava di un tentativo di clonazione della carta a Madrid, città in cui il ricorrente era stato durante l'anno;
- Seguivano le operazioni contestate senza consenso del cliente per la somma complessiva di euro 27.891,00 ed in particolare:
 - bonifico istantaneo di euro 10.000,00 in favore dello stesso ricorrente;
 - bonifico ordinario di euro 12.911,00, anch'esso in favore dello stesso ricorrente;
 - Pagamento mediante carta di euro 4.980,00;
- Il ricorrente, una volta avvedutosi delle operazioni provvedeva al disconoscimento richiedendo la revoca e la resistente non ha mai fornito risposta;
- In data 22/10/2025 riceveva l'accredito della somma di euro 12.911,00;

- Il ricorrente richiede dunque la differenza pari ad euro 14.980,00;
 - Deduce che ai sensi dell'art 5 del D.lgs. n. 11/2010 le operazioni non sono state eseguite con il consenso del ricorrente;
 - La banca ha violato i propri obblighi di vigilanza e controllo sulle operazioni disposte atteso che le stesse presentavano chiari indici di anomalia considerando i normali pattern operativi del cliente, tra le quali l'azzeramento delle giacenze;
 - In particolare, specifica che in relazione al bonifico istantaneo indirizzato allo stesso ricorrente, il cliente successivamente alla frode ha simulato la medesima operazione di bonifico alle stesse coordinate IBAN e ha visualizzato il seguente messaggio "i dettagli non corrispondono al conto del beneficiario. Ciò potrebbe essere dovuto a informazioni errate o a un tentativo di frode. Verifica nuovamente i dettagli rima di continuare", ritiene dunque che la banca se avesse posto in essere tale misura al momento della frode quest'ultima non si sarebbe verificata.
 - Ne consegue che l'omessa attivazione di procedure di verifica da parte della banca costituisce una condotta negligente;
 - La carenza di colpa grave del cliente in quanto il ricorrente ha ricevuto messaggi di testo che si inserivano in coda a quelli "genuini" e ciò non integra colpa grave del cliente in quanto trattasi di truffa sofisticata;
 - La malagestione da parte della banca dei propri sistemi di sicurezza inerenti i servizi di pagamento in quanto al cliente non sono stati offerti sistemi di alert o di notifica, cosicché lo stesso non si è potuto avvedere in tempo dello svuotamento del conto da parte dei malfattori.
- L'intermediario, con le controdeduzioni, eccepisce che/di:
- Dalle tracciate informatiche in possesso della Banca, è stato appurato che, il ricorrente ha autorizzato in-app le n. 2 operazioni contestate tramite il dispositivo mobile in suo esclusivo possesso ed unicamente associato al suo conto, in conformità con i requisiti previsti dalla c.d. SCA;
 - le transazioni in questione sono state autenticate dal ricorrente in data 26 settembre 2025 rispettivamente alle ore 17:40 UTC (19:40 ora locale) e alle ore 18:00 UTC (20:00 ora locale) in seguito all'inserimento delle credenziali e all'utilizzo dell'App installata sul proprio dispositivo mobile personale ed associata in via esclusiva al proprio conto;
 - Il ricorrente ha agito con colpa grave, in violazione delle disposizioni di legge e delle previsioni contrattuali, attenendosi alle istruzioni impartite dai soggetti fraudolenti e autorizzando l'operazione successivamente disconosciuta, nonostante fosse stato previamente informato dei rischi connessi al phishing mediante una campagna informativa promossa dalla banca a beneficio della clientela, nella quale erano altresì illustrate possibili modalità di realizzazione della frode analoghe a quelle riscontrate nel caso di specie;
 - il caso in esame esula dal regime di protezione previsto dal D. Lgs. n. 11/2010 in caso di operazioni non autorizzate, posto che, affinché un'operazione possa dirsi tale, deve difettare il requisito del "consenso del pagatore" di cui all'art. 5 del medesimo decreto, requisito che invece nel caso di specie sussiste;
 - la puntuale ricostruzione della vicenda è stata resa possibile unicamente a seguito dell'esame della denuncia-querela trasmessa dal ricorrente alla banca in data 27 settembre 2025 (che la resistente produce), tale denuncia non risulta allegata al ricorso introduttivo, né il relativo contenuto è stato fedelmente riportato;
 - la dinamica dei fatti rappresentata in sede di ricorso non collima con quella emergente dalla denuncia stessa.
 - il ricorrente riferisce che in data 26 settembre 2025, intorno alle ore 19:20, riceveva sul proprio numero di telefono cellulare un messaggio SMS apparentemente riconducibile all'intermediario. Il messaggio "civetta" invitava a contattare con urgenza un numero telefonico di rete mobile assolutamente non riconducibile alla banca, invito al quale il ricorrente aderiva spontaneamente;

- Il ricorrente, dopo aver autonomamente contattato il numero indicato nel messaggio civetta, entrava in comunicazione con un soggetto che si qualificava come operatore, il quale sottoponeva il medesimo ad alcune domande di verifica dell'identità e faceva riferimento a presunte operazioni anomale, tra cui un tentativo di clonazione della carta asseritamente avvenuto a Madrid;
 - Il sedicente operatore rappresentava la necessità, per asserite ragioni di sicurezza, di trasferire i fondi dal conto corrente del ricorrente, avente IBAN tedesco, a un presunto nuovo conto corrente italiano, chiedendo al ricorrente di disporre un bonifico istantaneo di euro 10.000,00, formalmente intestato a sé medesimo, fornendo le relative coordinate bancarie;
 - Il ricorrente, come espressamente ammesso in sede di denuncia, procedeva autonomamente all'esecuzione dell'operazione di bonifico, autorizzandola tramite l'App;
 - Nel corso della conversazione, il ricorrente veniva altresì indotto a effettuare un pagamento di prova di euro 1,00 per verificare il corretto funzionamento della carta, pagamento che veniva poi rimborsato;
 - Successivamente, a fronte delle perplessità manifestate dal ricorrente in relazione a un ulteriore trasferimento di fondi, il sedicente operatore lo rassicurava prospettando una richiamata dal numero verde della banca. Dopo pochi minuti, il ricorrente dichiarava di aver ricevuto una chiamata proveniente da un numero asseritamente riconducibile alla convenuta; circostanza che, tuttavia, non risulta adeguatamente provata, atteso che parte ricorrente non ha prodotto in allegato al ricorso alcuno screenshot del registro delle chiamate idoneo a comprovare l'effettiva provenienza della chiamata;
 - Con riferimento all'operazione contestata in sede di ricorso, pari a euro 4.980,00, eseguita a favore dell'esercente M***, il ricorrente non ha specificato le modalità di autorizzazione dell'operazione, limitandosi ad affermare di essersi avveduto di tale addebito solo successivamente alla ricezione della chiamata truffaldina;
 - in data 29 settembre 2025, il dipartimento competente comunicava al ricorrente l'impossibilità di procedere al rimborso delle somme oggetto di controversia, atteso che, dall'analisi dei log informatici emergeva che le transazioni risultavano predisposte e autorizzate dal ricorrente tramite il proprio dispositivo mobile associato al conto, nel pieno rispetto dei requisiti di autenticazione previsti dall'art. 10-bis del d.lgs. n. 11/2010;
 - In data 6 ottobre 2025 veniva attivata la procedura di recall nei confronti di altro istituto di credito, il quale, in data 27 ottobre 2025, comunicava l'esito negativo della richiesta di recall a causa dell'avvenuta estinzione del conto del soggetto beneficiario;
 - dalla ricostruzione dei fatti così come rappresentata dalla parte ricorrente, nonché dall'analisi delle tracciate informatiche nella disponibilità della Banca, emergono chiari e univoci indizi di colpa grave imputabili al ricorrente;
 - il ricorrente non ha prodotto alcuna prova documentale idonea a suffragare le proprie allegazioni: difettano, in particolare, gli screenshot relativi alla presunta telefonata "civetta";
 - La banca esegue periodicamente delle campagne antifrode.
- In conclusione, l'intermediario chiede al Collegio di rigettare il ricorso in quanto infondato.
- Parte ricorrente, in sede di repliche, riferisce che:
- La mera produzione dei log informatici non è sufficiente a dimostrare che le operazioni siano state effettivamente autorizzate dal ricorrente;
 - Per ciò che concerne le argomentazioni di parte resistente relative alla colpa grave, replica che lo stesso ha prodotto gli screenshot attestanti gli sms truffaldini incardinati nello stesso canale di comunicazione dell'intermediario e rileva di avere prodotto evidenza della chiamata truffaldina riferibile alla banca;
 - Di non avere mai riferito di avere contattato il numero indicato nell'SMS;
 - Di non avere mai autorizzato le operazioni contestate;
 - Di non avere contattato il truffatore, ma di avere ricevuto la chiamata dallo stesso;
 - Non è provato che la banca abbia inoltrato al ricorrente delle e-mail di sensibilizzazione;

-Che l'SMS, il quale si inseriva nell'abituale canale di comunicazione con la resistente, ha ingenerato un legittimo affidamento in capo al cliente avallato dalla comunicazione di fatti realmente riconducibili allo stesso ricorrente comunicati dal truffatore;

-A riprova della carenza di colpa grave in capo al ricorrente, richiama il rapporto della Banca d'Italia sulle operazioni fraudolente di agosto 2025, secondo cui nel secondo semestre 2024 le frodi da manipolazione hanno rappresentato per i bonifici il 67% del valore ed il 49% del numero delle frodi totali;

-La banca non contesta di non avere offerto sistemi di alert o di notifica cosicché non è stato possibile avvedersi della frode subita e ciò rappresenta una violazione dell'obbligo di diligenza gravante sulla banca;

-La banca non contesta l'indice di anomalia consistente nell'importo considerevole delle operazioni oggetto di ricorso, non abitualmente eseguiti dal ricorrente e tutte concentrate in breve distanza di tempo;

-Ulteriore indice di anomalia è l'azzeramento del conto;

-In ordine al bonifico di euro 10.000,00, questo risultava essere indirizzato allo stesso ricorrente; tuttavia, il cliente successivamente alla fronte ha simulato un ulteriore bonifico al medesimo IBAN di quello oggetto di ricorso ed indicando sé stesso come beneficiario e visualizzava un alert di non corrispondenza tra intestatario del conto e beneficiario. Sul punto asserisce che se tale alert fosse stato adottato durante la frode non si sarebbe verificata la sottrazione illecita di denaro;

-In ordine al recall del bonifico di 10.000,00 euro contesta che la banca ha attivato la procedura di recall solo in data 06/10/2025, ossia dieci giorni dopo la segnalazione del ricorrente avvenuta in data 26/09/2025. Tale ritardo ha pregiudicato la possibilità di recupero delle somme dato che il conto del beneficiario è stato estinto durante questo lasso di tempo.

Parte resistente, in sede controrepliche, afferma che:

-Con riferimento alle contestazioni formulate in ordine alla presunta inidoneità probatoria dei log informatici prodotti dalla resistente, rileva che i log prodotti costituiscono estrazioni dirette dei sistemi informatici generate nell'ambito dell'ordinaria operatività dei sistemi di registrazione delle transazioni, e rappresentano la tracciatura tecnica ufficiale delle operazioni effettuate sul conto del ricorrente, evidenzia che sul punto parte ricorrente non individua alcuna concreta anomalia, limitandosi a contestazioni assertive. Qualora la contestazione riguardi il formato Excel in cui le tracciate relative alle operazioni disconosciute sono state rappresentate, rileva che tale circostanza non incide in alcun modo sulla loro attendibilità;

-circa la presunta produzione dello screenshot attestante la provenienza della chiamata truffaldina dalla convenuta, ribadisce che tale circostanza non trova riscontro nella documentazione versata in atti, dalla quale non risulta screenshot del registro delle chiamate idoneo a comprovare l'effettiva provenienza della telefonata;

-l'affermazione secondo cui il ricorrente non avrebbe contattato proattivamente il frodatore, non trova riscontro negli atti. Dalla denuncia presentata dallo stesso ricorrente in data 27 settembre 2025, prodotta quale Allegato n. 5 alle controdeduzioni, emerge infatti che il ricorrente ha dichiarato di aver ricevuto un messaggio apparentemente proveniente dalla banca che lo invitava a contattare gli uffici della banca, aggiungendo espressamente di aver provveduto a farlo ("...mi invitava a contattare i loro uffici, cosa che facevo prontamente");

-la Banca ha dimostrato di aver trasmesso alla propria clientela una serie di e-mail di sensibilizzazione sul fenomeno del phishing nel periodo compreso tra il 18 febbraio 2020 e il 13 settembre 2024, nonché di aver diffuso messaggi informativi;

-il richiamo operato dalla difesa della parte ricorrente al Rapporto della Banca d'Italia sulle operazioni di pagamento fraudolente risulta non pertinente ai fini della decisione della presente controversia. Il dato statistico richiamato, relativo alla diffusione delle frodi da manipolazione, non è idoneo in alcun

modo a escludere la colpa grave del cliente nel caso concreto, dovendo quest'ultima essere valutata alla luce delle specifiche circostanze fattuali della vicenda;

-per ciò che concerne la censura formulata dalla difesa della parte ricorrente circa la presunta mancata predisposizione da parte della Banca di un sistema di "sms alert" dichiara di avere adottato un sistema di notifiche push in-app, che – richiamando l'orientamento dell'Arbitro Bancario Finanziario – è ritenuto equivalente al sistema di sms alert ai fini dell'informazione del cliente sulle operazioni effettuate;

-Nel caso di specie, le notifiche push relative alle operazioni contestate sono state regolarmente inviate al dispositivo mobile personale del ricorrente associato al suo conto, consentendogli di essere informato delle operazioni effettuate. In ogni caso, ribadisce che la censura risulta inconferente anche sotto altro profilo, atteso che il ricorrente ha ammesso in denuncia di aver personalmente disposto le operazioni di bonifico. In particolare, ha dichiarato di aver proceduto al trasferimento di euro 10.000,00 e successivamente di euro 12.911,00 verso il presunto nuovo conto, ritenendo di operare su indicazione dell'operatore. Con riferimento all'operazione contestata in sede di ricorso, pari a euro 4.980,00, eseguita a favore dell'esercente M***o mediante carta di debito osserva che l'eventuale sistema di alert non avrebbe comunque potuto spiegare alcuna efficacia preventiva, trattandosi di un'unica. In ordine alla presunta difformità tra l'IBAN indicato e il nominativo del beneficiario evidenzia che i PSP non sono tenuti a verificare la corrispondenza tra IBAN indicato dall'ordinante e intestatario del conto, essendo il bonifico uno strumento basato sull'identificativo unico IBAN. L'obbligo di verifica della corrispondenza tra IBAN e beneficiario è stato introdotto solo successivamente dal Regolamento (UE) 2024/886, con applicazione dal 9 ottobre 2025, mentre l'operazione oggetto di contestazione è anteriore a tale data;

-In ordine alla censura attorea secondo cui la banca avrebbe dovuto rilevare indizi di anomalia e sospendere le operazioni contestate. Eccepisce che le operazioni sono state predisposte e autorizzate direttamente dal ricorrente mediante SCA e pertanto non sussisteva alcun obbligo normativo di bloccarne l'esecuzione. Né l'importo delle operazioni può essere considerato di per sé indice di anomalia, anche perché la parte ricorrente non ha prodotto documentazione relativa alla propria abituale operatività;

-Avere attivato la procedura di storno prevista dalle prassi interbancarie, pur in assenza di uno specifico obbligo in tal senso e nonostante l'operazione risultasse regolarmente autorizzata tramite i presidi di SCA. Evidenzia che il bonifico oggetto di contestazione, avendo natura di bonifico istantaneo, è stato eseguito entro i tempi previsti dal SEPA Instant Credit Transfer Scheme, divenendo pertanto irrevocabile al momento stesso della sua esecuzione.

DIRITTO

Parte ricorrente chiede la restituzione della somma corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.

Le operazioni contestate sono state 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. PSD 2), entrato in vigore il 13/1/2018.

Ai sensi dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare:

A. l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

In particolare, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente.

Parte ricorrente lamenta l'esecuzione fraudolenta di un'operazione di bonifico istantaneo di euro 10.000,00 e di un'operazione di pagamento online di euro 4.980,00 entrambe avvenute in data 26/09/2025:

- Bonifico istantaneo di euro 10.000,00;

- In ordine all'operazione di pagamento online di euro 4.980,00, il ricorrente non produce evidenza ma la stessa non è contestata dalla convenuta e la stessa produce i log dai quali risulterebbe l'esecuzione della suddetta operazione. Pertanto, il punto è pacifico tra le parti.

Ne consegue, che il presente ricorso ha ad oggetto la restituzione complessiva di euro 14.980,00.

In sede di controdeduzioni l'intermediario afferma che le operazioni disconosciute sono state eseguite personalmente dal cliente, così come dallo stesso ricorrente sembrerebbe affermato in sede di querela, la quale risulta allegata in atti dalla resistente. Tale circostanza non sembrerebbe però confermata in sede di ricorso.

Si precisa che, secondo l'orientamento del Collegi ABF, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD.

Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni sotto dettatura”).

Al contempo, i Collegi sono concordi nell'affermare che, viceversa, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è solo parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD e disposizioni di recepimento), prescindendo dalla nozione civilistica di “consenso”, dispone che quest'ultimo deve essere prestato nella forma convenuta tra il pagatore steso e il PSP.

Alla luce di quanto sopra esposto e tenuto conto delle evidenze prodotte dall'intermediario, il Collegio ritiene che l'operazione è stata predisposta dai truffatori e il cliente abbia cooperato inconsapevolmente nella realizzazione della stessa.

In merito alla autenticazione delle operazioni e modalità: valutazione di conformità ai requisiti della SCA, le fonti normative che regolano la strong customer authentication (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D.lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).

Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Con riferimento alla autenticazione forte all'accesso all'app, preliminarmente si rileva che gli accessi in app propedeutici alle due operazioni contestate sono due: a tal proposito l'intermediario produce analoga documentazione per entrambi.

Con riferimento alla fase di accesso in app, l'intermediario rappresenta devono essere osservate le seguenti modalità:

- credenziali personali (indirizzo e-mail di registrazione e password) o, in alternativa, ID biometrico (riconoscimento facciale o impronta digitale) - elementi, rispettivamente, nella categoria della conoscenza e inerenza;

-utilizzo dell'App installata sul dispositivo associato in via esclusiva al conto del cliente - elemento nella categoria del possesso.

Precisa altresì che una volta predisposto un determinato ordine di pagamento oppure un'operazione di pagamento online attraverso carta di debito per la quale viene richiesta l'autenticazione forte (SCA) da parte dell'esercente, questo tipo di transazione deve essere necessariamente autorizzata all'interno della App installata sul dispositivo mobile associato al conto corrente tramite apposita notifica push, quale ulteriore elemento nella categoria del possesso, e dopo avervi effettuato l'accesso mediante credenziali personali o ID biometrico.

Pertanto, parrebbe che la SCA in relazione alla fase di accesso sia provata avendo riguardo ai seguenti fattori autentificativi:

- l'inserimento di username + password proverebbe il fattore di conoscenza;
- l'aver agito all'interno dell'app autenticata proverebbe il fattore di possesso.

Con riferimento all'operazione di bonifico istantaneo di euro 10.000,00, l'intermediario rappresenta che all'interno della sessione di accesso precedentemente analizzata, seguiva la fase dispositiva del bonifico, autorizzato con riferimento ai seguenti fattori:

- digitazione del PIN di conferma precedentemente creato dal Ricorrente (fattore di conoscenza);
- l'utilizzo dell'app, cliccando sull'apposito pulsante "Conferma il bonifico". In tale schermata - oltre al testo integrale della notifica contenente i dettagli di pagamento (ivi incluso il codice IBAN del beneficiario e il relativo importo) - appare chiaramente indicato il dispositivo autorizzativo a cui tale notifica è stata inviata e che equivale allo smartphone personale in uso esclusivo al ricorrente (fattore di possesso).

Sulla base delle evidenze prodotte e sopra riportate, risulta che:

- in data 26/09/2025, alle ore 17:57 viene disposto un bonifico istantaneo di euro 10.000,00;
- tale face, avviene nella medesima sessione di accesso precedentemente analizzata;
- la dicitura "PIN Validation" presente indica che l'operazione è stata predisposta in seguito alla digitazione del PIN di conferma creato dal Ricorrente;
- dall'analisi delle evidenze che mostrano l'interfaccia in app visualizzata dall'utente, è possibile desumere che l'operazione veniva convalidata in app mediante l'impiego del device autenticato cliccando sull'apposito pulsante "Conferma il bonifico".

Pertanto, è possibile desumere che la SCA parrebbe provata con riferimento ai seguenti fattori autentificativi:

- l'impiego del PIN proverebbe il fattore di conoscenza;
- l'aver agito all'interno dell'app autenticata proverebbe il fattore di possesso.

Con riferimento all'autorizzazione di un'operazione di pagamento online di euro 4.980,00, la resistente riferisce che la stessa applica il processo di sicurezza 3D Secure e una richiesta di autenticazione viene trasmessa da parte dell'esercente alla stessa convenuta.

Sulla base dei dettagli relativi all'operazione per cui è trasmessa la richiesta, i sistemi informatici della Banca effettuano l'analisi degli elementi di rischio dell'operazione di pagamento, per determinare se la transazione in questione debba essere soggetta ad autenticazione forte da parte del cliente (c.d. "Challenged").

In tal caso, viene richiesta conferma dell'operazione al cliente stesso esclusivamente attraverso l'App installata sul dispositivo mobile associato al conto corrente. In sostanza, viene trasmessa al cliente una specifica notifica push attraverso la quale viene indirizzato all'apertura della schermata iniziale dell'app. Il cliente è quindi tenuto ad effettuare il login nell'App come sopra già illustrato.

Una volta effettuato l'accesso nell'area riservata dell'App, al cliente viene presentata una schermata contenente i dettagli della transazione e la richiesta di autorizzare o meno l'operazione entro un tempo massimo di 5 minuti.

La conferma della operazione determina l'autorizzazione attraverso un elemento rientrante nella categoria del possesso, in quanto dà luogo a una verifica nel back end - attraverso la private key

conservata all'interno del dispositivo del cliente e un sistema di private key linking - che l'autenticazione dell'operazione avviene dall'App installata sul dispositivo associato al conto e che causa il rigetto dell'operazione laddove tale circostanza non sia soddisfatta.

Nel caso di specie, l'operazione è stata dunque autenticata previa notifica push, attraverso l'accesso al conto tramite l'inserimento delle credenziali di login (nome utente e password) (fattore di conoscenza) all'interno dell'App installata sul dispositivo del Ricorrente univocamente associato al suo conto (fattore di possesso).

La resistente, deduce dunque che alla ricezione della push, questa viene autenticata mediante accesso in app.

Alla luce di quanto prodotto, è possibile desumere che:

- Alle ore 18:06 l'utente ha ricevuto la Push sul device autenticato, la quale parrebbe peraltro descrivere l'operazione che si sta autorizzando;

- L'accesso in app è avvenuto alle ore 18:00;

- Potrebbe ritenersi, così come riferito anche da parte della convenuta; che l'autorizzazione sia avvenuta durante una sessione di accesso in app già avviata.

Pertanto, parrebbe ammettersi che l'operazione di pagamento online sia provata avendo riguardo ai seguenti fattori autenticativi;

- L'invio della push sul device autenticato proverebbe il fattore di possesso;

- L'autorizzazione della stessa mediante credenziali di accesso (username + password) proverebbe il fattore di conoscenza.

Preliminarmente, si precisa che la colpa grave del ricorrente assume rilievo solo se l'intermediario fornisce la prova di autenticazione delle operazioni che – secondo l'orientamento condiviso dai Collegi – rappresenta, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente (cfr. Collegio di Coordinamento, con decisione n. 22745/2019).

In merito alle modalità della truffa e sussistenza degli indizi di colpa grave in capo all'utilizzatore, alla luce di quanto riferito da parte ricorrente in sede di querela, parrebbe che:

1. In data 26/09/2025 alle ore 19:20 riceveva sul proprio cellulare un messaggio che si inseriva nel canale di comunicazione abituale della banca;

2. Detto sms invitava il ricorrente a contattare i loro uffici, il quale riferisce di avere dato seguito a tale richiesta;

3. Rispondeva un presunto operatore, il quale avvertiva il cliente di un tentativo di clonazione della carta in una città in cui il ricorrente era effettivamente stato da breve tempo;

4. Il truffatore richiedeva al cliente di effettuare un bonifico di euro 10.000,00 intestato allo stesso ricorrente al fine di mettere in sicurezza i propri fondi; tale bonifico è oggetto di ricorso;

5. Sembrerebbe che il ricorrente abbia eseguito il bonifico;

6. Successivamente il truffatore gli comunicava la necessita di effettuare un altro bonifico, generando nel cliente perplessità;

7. A tale punto della vicenda il truffatore comunicava al cliente che l'avrebbe contattato dal numero ufficiale della banca;

8. Dopo pochi minuti, riceveva un'ulteriore chiamata dal numero ufficiale della resistente;

9. Procedeva al trasferimento di euro 12.911,00 al presunto nuovo conto sempre indicando egli stesso come beneficiario; tale bonifico non è oggetto di ricorso;

10. Visualizzava come destinatario un soggetto terzo e insospettito chiamava il numero 112;

11. Pur non descrivendone le modalità, il cliente contattava la resistente contestando altresì un pagamento di euro 4.980,00, oggetto di ricorso;

12. La modalità di attacco parrebbe essere un mix tra spoofing sms, phishing e spoofing ID Caller in combinazione tra loro;

13. Da quanto riferito in sede di querela, non prodotto dal ricorrente bensì dall'intermediario, parrebbe che le operazioni contestate siano state personalmente autorizzate, tuttavia in sede di ricorso e repliche, lo stesso insiste per la natura fraudolenta e non autorizzativa delle operazioni.

Il ricorrente allega copia dell'sms civetta. L'sms parrebbe essere in coda a dei messaggi genuini e non parrebbe presentare gravi indici di inattendibilità; tuttavia, non è possibile visualizzare il mittente.

Quanto alla fattispecie cui è riconducibile il caso esaminato, secondo le posizioni dei Collegi nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del cliente, a meno che non si rinvenivano indici di inattendibilità o anomalia del messaggio [errori grammaticali e/o lessicali, presenza di link non riferibile all'intermediario]; in tale caso, potrà essere ravvisato 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 particolare, con riferimento alle comunicazioni in apparenza provenienti dagli intermediari, che inducono il cliente ad abbassare la sua soglia di attenzione, i Collegi hanno convenuto che l'eventuale colpa grave del cliente è desumibile, ad esempio, dall'inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta nonché da evidenti errori grammaticali o di sintassi sempre contenuti nel messaggio civetta. Resta salva la possibilità di individuare, anche in questi casi, una responsabilità concorrente dell'intermediario.

Il ricorrente riferisce di avere ricevuto una chiamata dal numero ***361, effettivamente riconducibile alla resistente, tuttavia non produce evidenze al riguardo.

La chiamata sarebbe precedente rispetto all'esecuzione delle operazioni contestate.

Si rappresenta che è oggetto di contestazione tra le parti se il numero truffaldino indicato nell'sms sia stato contattato spontaneamente dal ricorrente o se questi abbia ricevuto la chiamata dal truffatore.

Il ricorrente insiste per la spontanea ricezione della chiamata. La resistente adduce che il ricorrente abbia contattato detto numero. Quanto sostenuto dalla resistente parrebbe confermato da quanto dichiarato dal ricorrente in sede di querela. Pertanto, parrebbe provato che il ricorrente abbia spontaneamente contattato il numero indicato nell'sms truffaldino.

Non parrebbe che sia stato richiesto il blocco della carta.

Parte ricorrente non ha specificamente contestato il superamento del plafond, ma ha contestato l'azzeramento del conto. Non è comunque versato in atti in contratto contenente il limite del plafond.

Con riferimento alla contestazione da parte del ricorrente circa la mancata attivazione dei sistemi alert, l'intermediario contesta

1. che tale censura sia priva di fondamento, posto che lo stesso ricorrente ha ammesso in sede di denuncia di aver personalmente disposto le operazioni di bonifico.

- dai log informatici prodotti in atti, risulta che le notifiche push relative alle operazioni contestate sono state regolarmente inviate al dispositivo mobile personale del Ricorrente associato al suo conto, consentendogli di essere informato delle operazioni effettuate. In merito, parte resistente produce evidenze in atti.

Secondo l'orientamento del Collegio, in presenza di messaggi contenenti i codici autorizzativi (OTP) che avvisano l'utente del tipo, dell'importo e del destinatario dell'operazione che sta per autorizzare (c.d. SMS parlante), non rileva l'attivazione o meno di sistemi di alert ex post (in senso conforme, v. Collegio di Palermo, decisione n. 4894/25 - non ancora pubblicata sul sito esterno- ; Collegio di Palermo, decisione n. 13859/2022; Collegio di Palermo, decisione n. 5893/2023, Collegio di Torino, decisione n. 1344/2023).

Non sono rinvenibili nel caso di specie gli indici di anomalia di cui all'art. 8 del DM 112/2007.

Tuttavia, il ricorrente evidenzia l'anomalia degli importi, in relazione alla propria abituale attività.

A tal fine, produce evidenze dell'estratto conto a far data dal 2019 sino all'anno 2024.

In proposito si osserva che le operazioni contestate sono avvenute con modalità distinte:

1. Pagamento mediante carta;

2. bonifico

Nella stessa giornata era stato eseguito un ulteriore bonifico di euro 12.911,00 poi restituito e, quindi, non oggetto di domanda.

Si fa presente che, secondo l'orientamento dei Collegi, i principi del D.M. 112/2007 non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario. Il Collegio Abf può quindi valorizzare anche indici di frode ulteriori a quelli del D.M. 112/2007 in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.

I Collegi hanno inoltre precisato che, sebbene il D.M. faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche online) in ragione dell'unicità della ratio sottesa a tale a tale normativa.

Per quanto concerne infine la quantificazione del rimborso da riconoscere all'utente, i Collegi hanno convenuto che la valutazione della responsabilità del PSP debba essere formulata in un giudizio sintetico che tenga conto della sua condotta complessiva e di tutti gli altri elementi desumibili dal caso concreto: la base di calcolo per la liquidazione della somma oggetto di condanna è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti. Infatti, il D.M. non ha un valore precettivo in materia di disconoscimento delle operazioni non autorizzate e non è ravvisabile una diretta correlazione tra l'integrazione dell'indice di frode e il numero di operazioni da rimborsare.

Si rammenta che il Collegio di Palermo, decisione n. 4200 del 05 aprile 2024, in conformità all'orientamento di cui sopra, ha stabilito che vanno restituite tutte le operazioni al 20% salvo una diversa distribuzione in concreto del concorso di colpa tra le parti. Negli stessi termini Collegio di Palermo, decisione n. 4148 del 05 aprile 2024.

Pertanto, la somma da restituire sarebbe pari a euro 2.996,00 (20% di 14.980,00).

Parte ricorrente contesta come il bonifico di euro 10.000,00 risulta eseguito in favore di un soggetto diverso rispetto a quello risultante dalla distinta della banca. In tali circostanze, l'intermediario avrebbe dovuto avvisare il ricorrente in ordine alla discrepanza fra i beneficiari indicati, così come previsto dal Regolamento UE 2024/886.

Sul punto si osserva che, come rilevato dall'intermediario, tutte le operazioni sono state eseguite il 26.09.2025, mentre l'obbligo di verifica della corrispondenza tra IBAN e beneficiario è entrato in vigore a partire dal 9 ottobre 2025.

Parte resistente non ha domandato l'applicazione della franchigia.

Sono state attivate procedure di recall in data 06/10/2025 con esito negativo per avvenuta estinzione del conto del beneficiario.

La resistente, a riprova dell'osservanza dell'obbligo di diligenza in capo ad essa, riferisce di avere periodicamente inviato delle e-mail relative alla campagna anti-phishing al ricorrente. Produce evidenze in atti.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto a corrispondere l'importo complessivo di € 2.996,00, oltre interessi legali dalla data del reclamo.

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