

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 06/03/2026

FATTO

La parte ricorrente espone quanto segue.

- i) In data 11/09/25 riceveva un sms dal numero ***190 che la avvertiva di una richiesta di pagamento, con invito a chiamare il numero antifrode ivi contenuto.
 - ii) La ricorrente chiamava il numero riportato nel messaggio ma, insospettita, riagganciava subito dopo.
 - iii) Provava a contattare il numero verde della Banca, senza successo.
 - iv) Pochi minuti dopo veniva ricontattata dal numero ***472 e l'interlocutore, spacciandosi per operatore della banca, le riferiva che sarebbe stata, di lì a breve, richiamata dal numero riportato sulla carta bancomat.
 - v) Effettivamente riceveva la chiamata da tale numero.
 - vi) Nel corso di tale ultima chiamata l'operatore le riferiva di un tentativo di prelievo che doveva essere bloccato e la guidava nella asserita operazione di blocco.
 - vii) A tal fine, il finto operatore la invitava ad accedere nella home banking e a controllare il saldo e i massimali. Una volta verificato il limite, Le chiedeva di disporre un bonifico, al fine di effettuare lo storno dell'operazione sospetta. Le forniva, quindi, i dati necessari per l'esecuzione del bonifico.
 - viii) Una volta disposto il bonifico, la invitava a non aprire l'app perché erano in corso delle operazioni di aggiornamento.
 - ix) Avendo compreso di essere stata vittima di frode, la ricorrente contattava il numero verde della banca e l'operatore Le riferiva che non era più possibile disporre il blocco dell'operazione in quanto erano state superate le ore 20:00.
 - x) Il giorno successivo si recava presso la filiale e tentava il richiamo del bonifico, senza successo. L'intermediario resiste al ricorso e, premessi cenni in fatto, eccepisce quanto segue.
- i) Il messaggio iniziale non proveniva dalla banca.
 - ii) L'operazione è stata correttamente autenticata, registrata e contabilizzata.
 - iii) La ricorrente ha eseguito il bonifico in conformità alle istruzioni ricevute dal sedicente operatore bancario e la banca ha eseguito le disposizioni impartite dalla cliente.

iv) Le operazioni di bonifico sono state, seppur inconsapevolmente, disposte dalla Cliente autonomamente tramite la propria banca multicanale a seguito di corretta digitazione delle credenziali solo a lei note. Pertanto, non è applicabile la PSD2.

v) La banca si è prontamente attivata per il richiamo del bonifico, che ha avuto esito negativo per mancanza di fondi.

vi) Non sussiste alcuna responsabilità della banca per quanto occorso.

Per concludere, la banca chiede il rigetto del ricorso.

Nelle repliche la parte ricorrente aggiunge quanto segue.

i) Alle ore 21:20 dell'11 settembre 2025 (giorno della truffa) essendo stata trattenuta al telefono fino alle ore 20,20 circa dal truffatore, contattava immediatamente il numero verde della banca, che comunicava l'impossibilità di revocare l'operazione poiché era stato superato l'orario di cut-off (ore 20:00).

ii) Il giorno dopo si recava immediatamente in filiale per chiedere formalmente il richiamo.

iii) Nonostante la tempestività delle richieste, la banca non è riuscita a bloccare il bonifico.

iv) La banca avrebbe potuto – e dovuto – disporre misure idonee a sospendere l'esecuzione dell'operazione.

v) Pochi giorni dopo, il 1° ottobre 2025, un'altra cliente della banca è stata vittima di una truffa identica per modalità e orario (si allega la sua autocertificazione). In quel caso, la banca ha bloccato tempestivamente l'operazione e inviato messaggi di allerta alla cliente, impedendo che la truffa andasse a buon fine. Nel mio caso, invece, la filiale non ha attivato alcuna misura preventiva o automatica, pur trattandosi di un'operazione chiaramente anomala. Ciò dimostra una disomogeneità nella gestione interna della sicurezza e un deficit di diligenza professionale.

La ricorrente chiede quindi:

- di accertare la responsabilità della banca per la mancata adozione di misure di sicurezza adeguate;
- di disporre il rimborso integrale della somma di € 4.890,00, oltre ad interessi legali dalla data dell'operazione;
- in subordine, di riconoscere la corresponsabilità della banca, con rimborso parziale secondo equità.

Nelle controrepliche la banca eccepisce quanto segue.

i) La presentazione di nuovi elementi, quali la testimonianza di un terzo, è inammissibile.

ii) Il personale della banca agisce in ottemperanza a precise politiche aziendali, nel rispetto delle Leggi e delle Direttive vigenti, ed è tenuto a osservare comportamenti conformi alla diligenza, correttezza e trasparenza.

iii) Nel caso che ci occupa bonifico è stato disposto personalmente dalla cliente, in data 11/09/2025 alle ore 18:55. Trattandosi di un bonifico ordinario, il termine ultimo stabilito per procedere alla revoca dello stesso (cut-off) sono le ore 20:00.

i) Trascorso tale orario, è possibile richiedere il "recall" del bonifico alla Banca del beneficiario, così come avvenuto il giorno seguente.

Infine, la banca rinnova le considerazioni svolte nelle controdeduzioni e insiste per il rigetto del ricorso.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 11 settembre 2025. Risulta pertanto effettuata dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata

in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) 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. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-bis, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "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. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-bis), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "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".

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

4.- Nel caso in esame, la parte ricorrente chiede il rimborso della somma di € 4.890,00, pari al controvalore di un bonifico eseguito in data 11/09/2025 a seguito di truffa perpetrata mediante la tecnica dello smishing.

Infatti, la ricorrente afferma di aver ricevuto un sms che, preannunciando una richiesta di pagamento, la invitava a contattare il numero di telefono ivi contenuto.

La ricorrente contattava il numero riportato nel messaggio e riagganciava poco dopo.

Dopo pochi minuti, sarebbe stata contattata da un sedicente operatore della banca, dapprima da un numero fisso riconducibile alla banca e, successivamente, da un'utenza privata mobile.

A riprova di quanto dedotto, la parte ricorrente produce la copia della schermata contenente il messaggio truffaldino.

Il messaggio esca proviene da un numero privato non riconducibile alla banca.

La ricorrente riferisce che la seconda chiamata è avvenuta da un numero di telefono riconducibile alla banca. Manca in atti il registro delle chiamate.

5.- La ricorrente ammette di aver disposto in prima persona l'operazione in contestazione.

Secondo l'orientamento condiviso tra i Collegi, 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 PSD2.

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").

In questi casi, dunque, non è configurabile una responsabilità oggettiva del PSP.

Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:

mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;

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

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

Tenuto conto di quanto precede, non si è proceduto alle verifiche richieste dalla normativa speciale di cui al d.lgs. 27 gennaio 2010, n. 11, per come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento (spec. la verifica della c.d. strong customer authentication). Si precisa, tuttavia, che l'intermediario ha comunque fornito la prova dell'autenticazione forte, allegando alle controdeduzioni la relativa documentazione tecnica.

6.- Dall'esame istruttorio è emerso che, nel caso di specie, non risultano sms truffaldini provenienti dal canale ufficiale della banca.

Tali elementi confermano il difetto di alcun apporto causale alla frode da parte della banca resistente, che esclude pertanto un concorso di colpa tra le parti: «[...] In base alle allegazioni di parte la transazione sconosciuta sembra sia stata posta in essere a seguito di frode informatica perpetrata con la tecnica del sito clone, tramite il quale non sono stati tuttavia veicolati messaggi truffaldini apparentemente provenienti dalla banca; infatti, nello specifico, il ricorrente pare aver inserito i dati della carta e le credenziali per il pagamento sul sito clone della piattaforma di compravendita, quindi al di fuori dei canali ufficiali della banca. Ciò posto, occorre valutare se la tecnica truffaldina utilizzata in danno dell'odierno ricorrente sia annoverabile tra quelle non sofisticate o viceversa tra quelle particolarmente insidiose: nel primo caso, alla stregua del phishing, sussisterebbe la colpa grave, che invece nel secondo caso sarebbe esclusa (cfr. Collegio di Coordinamento, decisione n. 3498 del 26 ottobre 2012). [...]» (cfr. Collegio di Roma, decisione n. 6534/2024).

Alla luce dei suddetti principi, tenuto conto della estraneità dell'intermediario resistente alla frode perpetrata, non può ravvisarsi alcuna colpa in capo allo stesso, essendo ravvisabile una esclusiva responsabilità della parte ricorrente, per aver dato seguito con ingenuità alla truffa perpetrata (Collegio di Roma, decisione n. 7622 del 1/08/2025).

7.- La banca deduce di essersi attivata per il recall del bonifico il giorno successivo alla frode. La procedura ha avuto esito negativo per mancanza di fondi.

Al riguardo, secondo il costante orientamento dell'ABF, una volta che l'ordine di pagamento è divenuto irrevocabile ai sensi dell'art. 17, 1° comma, d.lgs. n. 11/2010 (cioè quando esso è "ricevuto dal prestatore di servizi di pagamento del pagatore"), il rimborso dell'operazione è subordinato al buon esito della procedura di recall, che presuppone il consenso del beneficiario (Collegio di Bari, decisioni

nn. 7363/2024 e 15198/2022; Collegio di Milano, decisione n. 16506/2022). In ogni caso, il rimborso non può essere disposto se i fondi sul conto del beneficiario risultano insufficienti (Collegio di Napoli, decisione n. 21846/2021).

Al di fuori dei casi indicati, il recupero della somma sembrerebbe essere possibile soltanto con un'azione di ripetizione nei confronti del beneficiario, secondo le regole generali in materia di ripetizione dell'indebito (cfr. Collegio di Roma, decisione n. 904 del 30.01.2023).

8.- Alla luce di quanto esposto, il Collegio ritiene che la domanda non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE