

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 13/03/2026

FATTO

- In base alla denuncia in atti, il 15/07/2025 la ricorrente ha ricevuto un SMS da un numero non riconducibile all'intermediario resistente, in cui si prospettava l'esecuzione di operazioni fraudolente.
- La ricorrente ha, quindi, ricontattato il numero di telefono indicato nel messaggio: l'interlocutore si è presentato come un addetto dell'intermediario e ha sollecitato la ricorrente a trasferire con urgenza i fondi dal suo conto corrente a un diverso conto, asseritamente intestato alla stessa ricorrente.
- La ricorrente si è recata presso una filiale dell'intermediario e ha richiesto l'esecuzione di un bonifico istantaneo pari a 18.000,00 €.
- L'operatore allo sportello non ha formulato alcuna domanda né ha sollevato perplessità sull'operazione, nonostante l'importo significativo e il contesto anomalo.
- Uscita dalla filiale, la ricorrente si è resa conto dell'anomalia della situazione ed è rientrata immediatamente per richiedere il blocco dell'operazione.

- L'intermediario ha comunicato l'impossibilità di procedere al blocco, trattandosi di un bonifico istantaneo già eseguito.

Tanto premesso, la ricorrente domanda il rimborso della somma oggetto della frode, pari a 18.000,00 €. Nelle controdeduzioni l'intermediario eccepisce quanto segue.

- Il ricorso riguarda un bonifico istantaneo di 18.000,00 €, disposto personalmente dalla ricorrente in data 15/07/2025.

L'operazione è stata richiesta dalla ricorrente presso la filiale dell'intermediario, indicando quale causale "girofondi".

Prima dell'esecuzione, l'operatore di sportello ha coinvolto il proprio superiore per approfondire la volontà dispositiva della ricorrente. Il superiore ha tentato di dissuadere la ricorrente dal procedere. La ricorrente, dopo un temporaneo allontanamento dalla filiale, è rientrata e ha confermato la volontà di eseguire il bonifico.

- La ricorrente ha richiesto espressamente l'esecuzione dell'operazione in modalità istantanea.

Gli operatori hanno avvisato la ricorrente dell'irrevocabilità del bonifico. L'irrevocabilità è stata espressamente indicata nel modulo sottoscritto dalla ricorrente.

- L'operazione è stata eseguita previa identificazione della ricorrente e verifica della firma.

- Dopo che la ricorrente si è avveduta della frode, l'intermediario ha attivato tempestivamente la procedura interbancaria di recupero delle somme, con esito negativo.

Tanto premesso, l'intermediario osserva quanto segue.

- L'operazione deve qualificarsi come operazione autorizzata ai sensi dell'art. 5, commi 1 e 2, del D.lgs. 11/2010. Non trova applicazione il regime di tutela previsto per le operazioni non autorizzate.

L'intermediario si è limitato a dare esecuzione a un ordine regolarmente impartito. L'evento dannoso è imputabile esclusivamente alla condotta della ricorrente.

- La condotta della ricorrente integra colpa grave ai sensi degli artt. 7 e 12 del D.lgs. 11/2010. Infatti, ha seguito le istruzioni di soggetti sconosciuti senza effettuare verifiche preventive. Inoltre, la ricorrente ha disposto l'operazione nonostante gli avvertimenti forniti dal personale di filiale.

- Peraltro, non sussiste in capo all'intermediario un obbligo di monitoraggio o di blocco preventivo delle operazioni dispositive del cliente.

Ciò posto, chiede il rigetto del ricorso.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 15 luglio 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.- L'operazione contestata è un bonifico istantaneo di 18.000,00 € disposto il 15/07/2025 a valere sul conto corrente della ricorrente.

In base alla denuncia in atti, il 15/07/2025 la ricorrente ha ricevuto un SMS da un numero non riconducibile all'intermediario resistente, in cui si prospettava l'esecuzione di operazioni fraudolente.

La ricorrente ha, quindi, ricontattato il numero di telefono indicato nel messaggio e l'interlocutore si è presentato come un addetto dell'intermediario, convincendo la ricorrente a spostare d'urgenza i fondi presenti sul suo conto corrente su un altro conto indicato dal truffatore, apparentemente per metterli al sicuro da possibili frodi.

La ricorrente si è recata presso la propria filiale e ha richiesto l'esecuzione di un bonifico istantaneo di 18.000,00 € sul conto indicato dal frodatore.

La ricorrente lamenta che lo sportellista abbia eseguito il bonifico senza insospettirsi per l'entità del bonifico.

Al contrario, l'intermediario afferma che la ricorrente è stata messa in guardia dal personale della filiale, è uscita momentaneamente dall'edificio e, al suo ritorno, ha confermato la volontà di procedere al bonifico.

Dunque, l'operazione disconosciuta è stata pacificamente autorizzata in prima persona dal ricorrente, nella convinzione di evitare addebiti fraudolenti sul suo conto, seguendo le indicazioni fornite telefonicamente dal truffatore.

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 ricorrente sostiene, peraltro, che il bonifico avrebbe dovuto essere bloccato preventivamente a fronte del suo elevato ammontare.

Il bonifico riportava come beneficiaria la stessa ricorrente. Tuttavia, la verifica della corrispondenza tra beneficiario nominale di un bonifico e titolare del conto di destinazione è divenuta obbligatoria per gli intermediari solo a partire dal 09/10/2025 (cfr. art. 5-quater del Regolamento (UE) 260/2012, introdotto dal Regolamento (UE) 2024/886, c.d. Instant Payments Regulation), dunque successivamente ai fatti che formano oggetto del ricorso.

Per bonifici eseguiti prima del 09/10/2025 l'ABF ritiene che la responsabilità dei prestatori di servizi di pagamento sia esclusa dalla corretta esecuzione dell'operazione verso l'identificativo unico fornito dal pagatore, fermo restando un obbligo di diligenza professionale nell'attività, necessariamente

successiva, volta al recupero dei fondi per quanto possibile (cfr. art. 24 d.lgs. n. 11/2010 e Collegio di coordinamento, con decisione n. 162 del 12/01/2017).

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