

COLLEGIO DI ROMA

composto dai signori:

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

Relatore MARCO MARINARO

Seduta del 30/04/2026

FATTO

Il ricorrente, correntista della banca, nella denuncia-querela e nel ricorso, riferisce che:

- il 9.1.2025, alle ore 11:17, riceveva una prima telefonata in apparenza dalla sua banca;
 - un sedicente consulente dell'intermediario lo metteva in allarme per operazioni sospette sul suo conto;
- a riprova dell'autenticità del contatto gli inviava due SMS, che apparivano provenire dalla banca;
- seguiva una seconda telefonata alle ore 11:18, in cui il medesimo soggetto lo induceva ad eseguire tre bonifici, rispettivamente di euro 12.450,00 (ore 11:48), 11.490,00 (ore 12:01) e 13.890,00 (ore 13:04), per complessivi euro 37.830,00;
 - riceveva un altro SMS che lo rassicurava sul rimborso della somma;
 - seguivano altre due telefonate per rassicurarlo, una delle ore 12:32 del sedicente consulente e una delle ore 13:14 in apparenza proveniente dalla Polizia postale;
 - soltanto in seguito si avvedeva di essere stato vittima di una frode.

Il ricorrente nel ricorso riconduce la frode al vishing caller ID e precisa di aver disposto i bonifici nella convinzione dell'autenticità dei contatti telefonici, avendo verificato i numeri chiamanti su internet. Chiede il rimborso di euro 37.830,00.

L'intermediario resiste al ricorso e propone i seguenti argomenti difensivi.

- Senza la inconsapevole, quanto colpevole, collaborazione del ricorrente, la frode non avrebbe potuto essere compiuta.
- Le operazioni disconosciute sono state eseguite senza alcuna anomalia e personalmente dal ricorrente, seguendo le istruzioni fornite al telefono da un soggetto che si era qualificato come incaricato della banca.
- La fattispecie non può essere ricondotta alla normativa sulle operazioni di pagamento non autorizzate commesse a seguito di furto, smarrimento o uso indebito di uno strumento di pagamento.
- Adotta un sistema di autenticazione forte di accesso all'Area Riservata e di autorizzazione delle disposizioni di pagamento, nel pieno rispetto delle previsioni normative di settore.
- Il ricorrente ha attivato il Servizio Token in data 30 aprile 2021 sullo smartphone al quale vengono inviate tutte le push.
- Con specifico riferimento all'operatività del giorno 9 gennaio 2025, alle ore 11:42:37 il ricorrente digita il proprio codice cliente e la propria data di nascita e conferma i dati. La banca controlla che il codice cliente sia esistente e che la data di nascita digitata sia corretta e coerente con il codice. La banca mostra il PinPad sul quale digitare il PIN. Alle ore 11:42:39 il ricorrente digita le tre cifre del PIN e conferma. Il PIN è stato validato. Alle ore 11:42:48 ricorrente prepara la push per autorizzare l'accesso all'Area Riservata e la invia al dispositivo registrato. Alle ore 11:42:59 il ricorrente autorizza l'accesso all'Area Riservata mediante riconoscimento del volto (FaceID).
- Il processo di autenticazione si è completato correttamente, tutti i controlli hanno dato esito positivo e alle ore 11:43:00 la banca registra l'avvenuto accesso all'area riservata da Web. Nel caso di specie, i passaggi sin qui descritti hanno soddisfatto sia il primo dei fattori della Strong Customer Authentication (inerenza: il ricorrente ha autorizzato l'operazione attraverso i suoi dati biometrici) che il secondo (possesso: il ricorrente ha ricevuto ed ha autorizzato la push sul suo smartphone).
- Il ricorrente inserisce i dati del primo bonifico e conferma l'operazione. Il bonifico ha superato i controlli previsti, pertanto la banca mostra al ricorrente la pagina di riepilogo con la richiesta di autorizzazione. Alle ore 11:46:20 prepara la push per autorizzare il bonifico, infine invia la push al dispositivo registrato. Il ricorrente non riceve la push e quindi ricorre alla autorizzazione con la generazione di un OTP. La banca presenta sullo schermo del PC il codice OTP che il ricorrente digita sulla App e conferma. Sulla App viene generato un Codice Token che il cliente inserisce nella apposita voce della schermata del PC e conferma.
- Nel caso di specie, i passaggi sin qui descritti hanno soddisfatto sia il primo dei fattori della Strong Customer Authentication (conoscenza: il ricorrente ha autorizzato l'operazione digitando sul suo smartphone il codice OTP e digitando sullo schermo del PC il Codice Token generato dalla App registrata sul suo smartphone) che il secondo (Possesso: il ricorrente ha operato sul suo smartphone).
- Il secondo ed il terzo bonifico sono stati disposti analogamente.
- Ha provato la corretta contabilizzazione, registrazione e autenticazione dei bonifici disconosciuti, depositando a tal fine i log e le evidenze delle operazioni da cui si evince che le stesse sono state autorizzate e autenticate applicando un sistema di autenticazione forte.
- Trattandosi di bonifici istantanei, il ricorrente non ha potuto annullarli.
- Pervenuta il 9 gennaio 2025 richiesta di richiamo (c.d. recall) delle operazioni di bonifico, vi ha dato tempestivamente seguito in data 10 gennaio 2025. Tale richiesta, tuttavia, non ha ricevuto alcun esito.
- Nella tipologia di frode del tipo di quella occorsa, seppur il/i frodatore/i abbia utilizzato tecniche di social engineering ed efficacia persuasiva tale da indurre il ricorrente a ritenere (erroneamente) che la conversazione si stesse svolgendo con un reale operatore della banca, il ricorrente stesso, dando pienamente credito alla telefonata apparentemente proveniente dal numero della banca ha, di fatto, consentito la consumazione della fattispecie di truffa ai propri danni, con ciò violando il dovere di tenere un comportamento idoneo a garantire la sicurezza dei dispositivi personalizzati (art. 7, comma 2, D. Lgs. n. 11/2010).

- L'SMS ricevuto dal ricorrente, ritenuto da lui genuino, non si inseriva in una precedente chat con l'intermediario.
 - Con riguardo, infine, al numero di provenienza della telefonata truffaldina, non si può imputare alla banca la manipolazione dei dati del mittente, tale da far apparire il messaggio proveniente da un'utenza della banca.
- L'intermediario conclude chiedendo il rigetto del ricorso.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 9 gennaio 2025. Risultano pertanto effettuate 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 tale operazione è altresì successiva 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)”*.

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

4.- Il ricorrente disconosce tre bonifici istantanei del 9.1.2025, rispettivamente di euro 12.450,00 (ore 11:48), 11.490,00 (ore 12:01) e 13.890,00 (ore 13:04), per complessivi euro 37.830,00.

I tentativi di richiamo dei bonifici non sono andati a buon fine.

L'intermediario descrive dettagliatamente il proprio sistema di autenticazione nelle controdeduzioni e nell'allegato G, recante anche i log per l'operatività controversa.

Da tale documento si ricava che le operazioni sono state disposte con il device registrato del ricorrente. L'accesso è avvenuto con codice utente, data di nascita e PIN quali credenziali statiche e con push autorizzativa sul dispositivo registrato.

I tre bonifici sono stati tutti autorizzati a seguito di validazione con codice OTP (conoscenza) della notifica push ricevuta sul dispositivo della ricorrente (possession).

5.- Il ricorrente descrive una frode che ha preso avvio con una telefonata da un numero in apparenza riconducibile alla banca. Nel corso della frode si susseguivano più telefonate dal medesimo chiamante. Il ricorrente deposita con il ricorso uno screenshot in cui non compare il numero chiamante, ma direttamente il nome della banca.

Al fine di rafforzare il convincimento del ricorrente sull'autenticità del contatto instaurato, i frodatori gli recapitavano due SMS che in apparenza provenivano dalla banca.

Il ricorrente deposita con il ricorso uno screenshot in cui compaiono i due SMS; tuttavia, non si evince se si inserissero nella medesima conversazione già in essere con la banca o se si tratti di una nuova conversazione.

In aggiunta, il ricorrente dichiara di aver ricevuto una telefonata da un numero corrispondente a quello di un commissariato di polizia, che aveva modo di verificare stesso durante la telefonata. Non deposita però uno screenshot da cui possa evincersi tale telefonata.

6.- Il ricorrente disponeva in autonomia i tre bonifici controversi, come da dichiarazioni rese nella denuncia-querela, nella convinzione di mettere i propri risparmi al riparo da una frode.

Secondo l'orientamento condiviso dai 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, 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: [...] c) 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.

Nel caso di specie sono stati disposti in rapida sequenza tre bonifici istantanei il 9.1.2025, rispettivamente di euro 12.450,00 (ore 11:48), 11.490,00 (ore 12:01) e 13.890,00 (ore 13:04), per complessivi euro 37.830,00.

I Collegi tendono a valorizzare la ricorrenza di alcuni indici di anomalia come il numero elevato delle operazioni, la rilevanza dell'importo oggetto di disposizioni di pagamento e il lasso temporale ravvicinato (Collegio di Roma, decisione n. 4805/2024).

7.- Nel corso della riunione del 10 aprile 2026, il Collegio invitava la parte ricorrente a produrre copia del registro delle chiamate con evidenza del numero chiamante e copia integrale degli SMS relativi al giorno della truffa.

In data 13 aprile 2026 la parte ricorrente ha riscontrato la richiesta del Collegio.

Quanto al registro delle chiamate, nelle schermate depositate dal ricorrente compare un numero che, da una ricerca sul web, pare riferibile alla banca resistente. La frode sembra dunque aver preso avvio mediante vishing caller ID.

Quanto agli SMS, il ricorrente deposita la conversazione con i messaggi truffaldini (tra i quali anche quelli di storno). Non pare, tuttavia, che nella chat siano presenti anche SMS genuini.

8.- All'esito dell'esame istruttorio, ad avviso del Collegio nel caso di specie la parte ricorrente deve ritenersi essere rimasta vittima di una fattispecie delittuosa riconducibile al c.d. "vishing caller ID".

Al riguardo, secondo un recente orientamento del Collegio, la chiamata proveniente da un numero apparentemente riconducibile all'intermediario (vishing caller id) è equiparabile all'sms spoofing e ove ne ricorrano i presupposti è possibile ravvisare un concorso di colpa (Collegio di Roma, decisione n. 8749/2024).

In particolare, la parte ricorrente produce lo screenshot della schermata dello smartphone contenente i riferimenti della chiamata truffaldina, da cui si evince che il numero di telefono corrisponde ad uno di quelli del servizio clienti dell'intermediario.

In simili ipotesi, l'orientamento prevalente tra i Collegi territoriali dell'ABF ravvisa un concorso colposo delle parti, imputando all'intermediario la colpa di "non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo" (così Collegio di Milano, decisione n. 17467/2021). Si richiede a tal fine solo l'allegazione da parte del ricorrente della lista delle chiamate ricevute, onde poter verificare la corrispondenza del numero utilizzato dal truffatore con il numero verde dell'intermediario (così Collegio di Milano, decisione n. 22105/2021).

La frode, così congegnata, non sembra in effetti differire in maniera significativa dalle ipotesi di "spoofing", ossia dalle ipotesi di smishing in cui il messaggio "esca" reca, quale mittente, la denominazione dell'intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario). E, secondo la più recente posizione condivisa dai Collegi territoriali dell'ABF, nelle fattispecie di spoofing è al più ravvisabile "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 questi termini v., per esempio, Collegio di Roma, decisione n. 1625/2022).

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 20.000,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE