

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 13.3.2025, alle ore 13:35, riceveva un SMS apparentemente proveniente dalla sua banca che lo metteva in allarme per una possibile frode in atto, invitandolo a contattare un numero di telefono indicato nel corpo del messaggio;
- il ricorrente, preoccupato, contattava l'utenza alle ore 14.00 e un sedicente operatore gli confermava che era in atto una frode;
- per bloccarla, l'operatore gli faceva una videochiamata e lo guidava all'interno dell'App, dandogli un appuntamento per una nuova chiamata alle ore 16:10;
- alle ore 16:10 ricontattava il ricorrente per fargli trasferire i suoi risparmi presenti in un conto deposito su un conto sicuro;
- il ricorrente, seguendo le istruzioni del frodatore, svincolava il conto deposito e disponeva così dal suo conto corrente un bonifico di euro 17.000,00;
- al termine della telefonata veniva invitato a disinstallare le App della banca;
- soltanto più tardi acquisiva consapevolezza di essere rimasto vittima di una frode.

Chiede il rimborso di euro 17.000,00.

L'intermediario resiste al ricorso ed eccepisce quanto segue.

- Nell'ambito della denuncia-querela presentata, l'odierno ricorrente riferisce di aver seguito tutte le indicazioni fornite da parte del sedicente operatore, di fatto autorizzando l'operazione di bonifico

oggetto del presente ricorso. Senza la inconsapevole, quanto colpevole, collaborazione del ricorrente, nessuna frode avrebbe potuto essere compiuta.

- La fattispecie non può essere ricondotta nell'alveo della normativa sulle operazioni di pagamento non autorizzate commesse a seguito di furto, smarrimento o uso indebito di uno strumento di pagamento, con la conseguenza che risulta preclusa l'operatività del relativo regime disciplinare.
 - 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.
 - È dimostrato che le operazioni sono state disposte dal device in possesso del ricorrente, con digitazione delle credenziali e con autorizzazione delle stesse.
 - Quando la banca esegue correttamente l'operazione di pagamento in conformità all'identificativo unico fornito, alcuna responsabilità le può essere attribuita.
 - Pervenuta in data 14 marzo 2025 richiesta di richiamo (c.d. recall) del bonifico, la resistente vi ha dato seguito in data 17 marzo 2025. Tale richiesta non ha avuto alcun esito. L'esito della richiesta di richiamo di un bonifico dipende esclusivamente dalla banca beneficiaria.
 - Il ricorrente ha dato pienamente credito al proprio interlocutore e 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 che consentono l'utilizzo dello strumento (art. 7, comma 2, D. Lgs. n. 11/2010).
 - Il ricorrente non solo non ha allegato alcuna evidenza dell'SMS che ha dato avvio alla vicenda truffaldina e delle chiamate ricevute, ma è altresì pacifico come non sia stato vittima di ID caller spoofing. Lo stesso infatti riferisce di aver ricevuto un SMS da un numero di cellulare, i.e. un canale non ufficiale e non sicuro che la banca non utilizza per interloquire con i propri clienti, di aver poi richiamato il numero sempre sconosciuto indicato nell'SMS e di aver ricevuto ulteriori telefonate/videochiamate sempre da numeri di cellulare.
- L'intermediario conclude chiedendo il rigetto del ricorso.

Il ricorrente in sede di repliche:

- insiste per l'applicazione del d.lgs. n. 11/2010, sottolineando che il suo consenso all'operazione è stato viziato da un raggirio, pur avendo egli stesso disposto il bonifico;
- invoca la sofisticatezza della frode, che riconduce all'SMS spoofing e al vishing caller ID;
- afferma che l'intermediario non ha dimostrato la sua colpa grave; peraltro, egli, non appena accortosi della frode, si è immediatamente attivato per limitarne gli effetti pregiudizievoli, contattando la banca con una chatbot;
- evidenzia che la chatbot non gli ha fornito un supporto effettivo e soltanto il giorno successivo è riuscito a mettersi in contatto con un operatore fisico;
- lamenta la mancata attivazione di sistemi di alert;
- lamenta altresì la previsione di un massimale molto alto per i bonifici (euro 50.000,00), solo in seguito ridotto;
- insiste per l'accoglimento del ricorso.

L'intermediario, in sede di controrepliche, insiste sulla mancata produzione di screenshot di SMS e telefonate ricevute.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita il 13 marzo 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.- Il ricorrente disconosce un bonifico di euro 17.000,00 del 13.3.2025. La provvista sul conto corrente è stata in parte alimentata mediante svincolo di un conto deposito di euro 14.500,00 con un giroconto dal conto deposito al conto corrente.

Il tentativo di richiamo del bonifico non è andato a buon fine. Il ricorrente ammette di aver eseguito egli stesso il bonifico controverso.

L'intermediario descrive dettagliatamente il proprio sistema di autenticazione nelle controdeduzioni e negli allegati F e G, recanti anche i log per l'operatività controversa.

Da tale documentazione si ricava che le operazioni sono state disposte con il device registrato del ricorrente con token attivo sin da ottobre 2022.

Il primo accesso è avvenuto con codice cliente, data di nascita e PIN quali credenziali statiche e con push autorizzativa sul dispositivo registrato.

Il giroconto, con cui il denaro è stato trasferito dal conto deposito al conto corrente è stato autorizzato a seguito di validazione con codice OTP (conoscenza) della notifica push ricevuta sul dispositivo del ricorrente (possesto).

Analogamente dicasi per il bonifico controverso.

5.- Il ricorrente descrive una frode realizzata a partire da un SMS in apparenza riferibile alla banca a seguito da telefonate e videochiamate su Whatsapp del frodatore.

Come eccepito dall'intermediario, il ricorrente nemmeno in sede di replica ha depositato evidenza degli SMS e delle telefonate ricevute, così da poterne verificare la provenienza.

Nella denuncia-querela sono riportati dei numeri di telefono che, da una ricerca sul web, non risultano riferibili all'intermediario. Peraltro, ed il rilievo appare dirimente, il messaggio esca proveniva da una utenza mobile (come dichiarato nella denuncia dal ricorrente) e, quindi, non riconducibile all'intermediario resistente.

6.- 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:

a) 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;

b) 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;

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.

7.- Nell'ambito della classica distinzione tra metodi tradizionali di frode e subdoli meccanismi di aggressione, il Collegio di Roma – richiamando un punto della motivazione della pronuncia del Collegio di Coordinamento n. 22745/2019 – ha ricondotto alla categoria delle frodi sofisticate le intrusioni truffaldine tramite "sms spoofed".

Come noto, si tratta di ipotesi di smishing in cui il messaggio 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).

Nei casi di spoofing i Collegi territoriali ABF hanno in generale evidenziato l'insidiosità del meccanismo di aggressione, consistente nell'invio dell'sms dall'utenza dell'intermediario, tale da rivelare criticità organizzative del servizio di pagamento offerto.

Tuttavia, hanno parimenti osservato che talvolta il testo del messaggio civetta presenta indizi di evidente inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario) che dovrebbero far allertare l'utente avveduto.

Si ritiene quindi che nelle fattispecie di spoofing non sia generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione, a meno che non si rinvenivano i suddetti indizi di inattendibilità o anomalia del messaggio.

In tale ultimo caso, secondo l'ABF si può configurare un concorso di colpa tra le parti, in relazione, da un lato, alla negligenza grave del cliente che agevola il compimento della truffa e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.

Quanto al vishing, la comunicazione per telefono da parte degli utenti dei codici dispositivi – in ipotesi in cui la telefonata non risulta parte di una frode più sofisticata, in combinazione con altre forme di captazione fraudolenta dei dati sensibili – è considerata dai Collegi quale indice di colpa grave della vittima della frode (Collegio di Roma, decisione n. 8728/2022).

8.- Nel caso in esame non è prodotta evidenza degli sms di adescamento; pertanto, non si può evincere se il messaggio da cui è partita la frode si sia inserito nella conversazione contenente i messaggi in precedenza inviati dall'intermediario.

Analoghe considerazioni valgono per il registro delle chiamate, non versato in atti, anche se i numeri indicati nella denuncia non sono riconducibili all'intermediario.

Nel caso in esame, la fattispecie sembra rientrare nella casistica dello spoofing "classico", avendo il ricorrente dedotto di aver ricevuto un SMS sul proprio cellulare inseritosi in coda ad altri genuini provenienti dall'intermediario.

Tuttavia, si rileva che il ricorrente non ha prodotto evidenza dell'SMS ricevuto (ed i numeri di telefono indicati nella denuncia non sono riconducibili alla banca resistente) e, pertanto, secondo il consolidato orientamento di questo Collegio, il ricorso dunque non può essere accolto in quanto non è possibile verificare se abbia in passato ricevuto altri messaggi genuini dallo stesso mittente, che avrebbero potuto generare nell'utente un legittimo affidamento circa la genuinità del messaggio (Coll. Roma, dec. n. 1008/2020; Collegio di Roma, decisione n. 4570/2024).

L'operazione inoltre è stata eseguita personalmente dal ricorrente (in ogni caso, l'intermediario dimostra di essersi dotato di un sistema di autenticazione a due fattori, in linea con la normativa di settore sopra ricordata). Ne deriva che la parte ricorrente non ha diritto alla restituzione dell'importo richiesto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE