

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) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 22/01/2026

FATTO

La ricorrente espone quanto segue.

Venerdì 09.05.2025 il sig. A.S., cointestatario con la ricorrente del conto n. *312, riceveva notifiche sull'app della banca relative a tentativi di pagamento non andati a buon fine dell'importo di € 0,01.

Ritenendo tali operazioni sospette, per precauzione, i clienti contattavano il numero ufficiale di assistenza clienti della banca, il cui operatore riscontrava effettivamente dei tentativi di pagamento provenienti dall'estero e bloccava la carta di debito.

Il lunedì successivo, 12.05.2025, il sig. A.S., mentre si trovava a lavoro, prima di potersi recare in filiale per ritirare la nuova carta, alle ore 11:20 circa, veniva contattato dallo stesso numero dell'assistenza clienti e l'operatore, presentandosi come membro del team della banca, lo informava di presunti movimenti anomali dall'estero, ragione per cui affermava essere assolutamente necessario attivare una procedura per bloccare tali tentativi.

A tal punto, l'operatore invitava il sig. A.S. ad effettuare un primo bonifico istantaneo di € 1.490,00 con descrizione ben precisa (Restituzione 001), convincendolo che tale descrizione e tale procedura fossero necessari per riottenere l'accredito di alcuni bonifici.

In ultimo, l'operatore comunicava al sig. A.S. che avrebbe contattato anche la cointestataria del conto in quanto era necessario attivare la procedura anche con lei per ragioni di sicurezza.

A tal punto, l'operatore, sempre con numero identico a quello ufficiale di assistenza, contattava la ricorrente e, spiegando anche a lei dei tentativi di pagamento fraudolenti effettuati con il loro conto, la invitava a seguire le istruzioni per bloccare tali operazioni.

Pertanto, anche lei riceveva numerose notifiche di autorizzazione relative a pagamenti presso diversi esercenti e l'operatore le chiedeva di accettare le notifiche e di pronunciare "non sono stata io" per ogni operazione.

A queste seguivano notifiche di pagamento non riuscito.

Durante la chiamata, la linea cadeva più volte e veniva ricontattata sempre dal numero apparentemente dell'intermediario.

In seguito, l'istante scopriva di aver subito una truffa e che erano state autorizzate tre operazioni per complessivi euro 1.990,00.

Ritiene di non essere in colpa grave, poiché non ha fornito codici utente, codici personali quali pin e/o codici OTP, non ha ricevuto sms, link e non ha mai fornito i numeri delle proprie carte, ragione per cui non ha avuto alcun sospetto. In particolare, l'istante evidenzia che è stato indotto in errore dalla chiamata ricevuta dal numero di assistenza ufficiale, che tra l'altro aveva realmente contattato per bloccare la carta il venerdì precedente.

Chiede il rimborso delle somme sottratte per un totale di € 1.990,00 oltre interessi legali e spese.

L'intermediario resiste al ricorso ed eccepisce quanto segue.

La ricorrente ha ammesso di aver eseguito, seppur sotto indicazioni del truffatore, le operazioni sconosciute.

Ravvisa colpa grave dell'utente per aver dato seguito alle istruzioni ricevute dallo sconosciuto interlocutore.

Le operazioni risultano correttamente autenticate tramite l'APP installata sul device della ricorrente con fattore biometrico (FINGERPRINT_FACEID). In particolare, la cliente ha ricevuto la richiesta di autorizzazione delle transazioni oggetto di contestazione tramite push notification sul suo device.

Dopo di che le transazioni sono state autenticate mediante inserimento del Fattore biometrico tramite il device stesso e quindi combinando due fattori di autenticazione indipendenti tra loro: il device ove è installata la APP utilizzata come canale di SCA (possesso) e la conferma attraverso digitazione del Fattore biometrico (fattore di inerenza).

L'intermediario deposita gli SMS Alert delle tre transazioni eseguite e di quelle tentate e non andate a buon fine. Evidenzia che le notifiche ricevute dalla cliente non sono falsi SMS di addebiti e finti storni delle transazioni inviati per corroborare la truffa. Durante la telefonata alla ricorrente pervenivano solo i messaggi (autorizzativi e SMS Alert) genuini della resistente che l'avvisavano delle transazioni di pagamento in corso e che la cliente ha invece ignorato, con sua evidente colpa grave.

Non ricorrono nel caso in esame profili di rischio ex DM 112/2007, atteso che si è trattato di tre transazioni che non hanno esaurito il plafond, prive pertanto di indici di rischio, anomalia o sospetto.

La banca informa i propri clienti sui rischi di frode informatica.

Chiede il rigetto del ricorso; in via subordinata l'applicazione della franchigia.

Con le repliche si ribadisce che a convincere ulteriormente i ricorrenti della veridicità della procedura vi era il fatto che a ogni operazione andata a buon fine, seguivano immediate notifiche di operazioni non andate a buon fine che accrescevano la convinzione che si trattasse di uno storno delle disposizioni e che la procedura effettuata fosse corretta e legittima.

L'istante nega di aver ricevuto i messaggi di alert.

Ravvisa responsabilità della banca per non aver rilevato l'anomalia delle operazioni avvenute in un'unica giornata e dirette al totale svuotamento del conto in poche ore.

Insiste per il rimborso della somma sottratta, oltre interessi e rivalutazione.

Nelle controrepliche l'intermediario precisa quanto segue.

L'istante non fornisce riscontro documentale dei presunti messaggi di storno delle transazioni che, come affermato da controparte, l'avrebbero indotta a convincersi della veridicità della procedura.

I messaggi che la parte ricorrente ha prodotto infatti sono gli SMS Alert delle transazioni tentate dai truffatori riportate nel LOG ed altri messaggi addirittura con date successive.

DIRITTO

1.- Le tre operazioni di pagamento online sconosciute dalla parte ricorrente sono state eseguite il 12 maggio 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 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)*".

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.- La controversia ha ad oggetto il disconoscimento di tre operazioni eseguite il 12.5.2025 tra le ore 12:40 e le 12:45 per complessivi 1.990,00 euro.

Sembra che le operazioni siano state inserite dal truffatore e poi autorizzate dalla ricorrente tramite app. In caso di operazioni autorizzate con l'intervento parziale del pagatore, secondo l'orientamento condiviso tra i Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è 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 (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.Lgs. 11/2010.

5.- L'intermediario afferma che le operazioni sono state correttamente autenticate e contabilizzate.

Le operazioni risultano correttamente autorizzate tramite l'APP installata sul device della ricorrente e autenticate con fattore biometrico. In particolare, la cliente ha ricevuto la richiesta di autorizzazione delle transazioni oggetto di contestazione tramite push notification. Dopo di che le transazioni sono state autenticate mediante inserimento del fattore biometrico.

Il sistema di autenticazione predisposto dall'intermediario per l'esecuzione dell'operazione è stato ritenuto compliant alla SCA da questo Collegio (Collegio di Roma, decisione n. 19734/2021).

6.- La parte ricorrente afferma di aver ricevuto una chiamata da un numero apparentemente proveniente dalla banca.

A supporto la ricorrente produce lo screenshot delle chiamate ricevute da un numero effettivamente riconducibile all'intermediario resistente.

7.- Il ricorrente contesta il carattere anomalo delle operazioni che avrebbe portato allo svuotamento del conto in poche ore.

L'intermediario afferma che non ricorrono nel caso in esame profili di rischio ex DM 112/2007, atteso che si è trattato di tre transazioni che non hanno esaurito il plafond, prive pertanto di indici di rischio, anomalia o sospetto.

Le operazioni contestate sono tre ricariche disposte online il 12.5.2025 tra le 12:40 e le 12:45 a favore del medesimo beneficiario per complessivi euro 1.990,00.

Occorre valutare se in tali ipotesi sia possibile applicare l'orientamento condiviso tra i Collegi secondo cui "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 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. È stato 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 normativa (Collegio di Milano, decisione n. 5805/24).

Ed invero nel caso di specie non emergono anomalie tali ritenere che l'intermediario non si sia attivato tempestivamente.

Peraltro, l'intermediario afferma di aver inviato i messaggi di alert. La ricorrente nega la ricezione.

Invero, la questione della mancata attivazione del servizio di alert non viene in rilievo in caso di unica operazione contestata ovvero di più transazioni effettuate a distanza di pochi minuti l'una dall'altra, in

quanto la ricezione dell'alert non potrebbe in concreto limitare il pregiudizio dell'utente (Collegio di Roma, decisione n. 1831/2023).

La ricorrente sostiene di aver dato seguito alle istruzioni dell'interlocutore poiché riceveva notifiche di annullamento delle presunte operazioni sospette. Ciò ha rafforzato la convinzione dei ricorrenti di trovarsi davanti a un operatore che stava cercando di bloccare accessi illeciti.

Tuttavia, l'intermediario replica che i messaggi che la parte ricorrente ha prodotto sono messaggi di alert delle transazioni anche tentate dai truffatori riportate nel LOG ed altri messaggi addirittura con date successive.

8.- Pertanto, ad avviso del Collegio la truffa deve ritenersi integrare un'ipotesi di vishing callerID, che costituisce una frode più insidiosa sostanzialmente assimilabile allo spoofing per la quale i Collegi territoriali ABF pervengono all'accoglimento parziale del ricorso accertando un concorso colposo delle parti. In particolare, imputano alla banca la colpa poiché deve addossarsi sull'intermediario il rischio d'impresa relativo alla modalità di comunicazione adottata, propedeutica rispetto all'operazioni di disposizioni poi avvenute (cfr. ex multis Collegio di Roma, decisione n. 8749/24; Collegio di Roma, decisione n. 8185/25).

9.- La ricorrente chiede la corresponsione degli interessi e la rivalutazione dalla data dell'operazione fino al loro effettivo rimborso.

Per quanto attiene alla domanda di interessi legali, il Collegio è solito accogliere la richiesta in caso di esplicita domanda (cfr. Collegio di Roma, decisione n. 12223/23).

È noto, invece, l'orientamento dei Collegi ABF che escludono la rivalutazione monetaria sui debiti di valuta (cfr., tra le molte, Collegio di Palermo, decisione n. 7131 del 4.4.2018; Collegio di Bari decisione n. 6948 del 28.3.2018; Collegio di Napoli, decisione n. 1941 del 23.1.2018; Collegio di Torino, decisione n. 628 del 12.1.2018; Collegio di Roma, decisione n. 8192/2024).

10.- Alla luce di quanto sopra esposto il Collegio valuta il concorso tra le parti e liquida in via equitativa in favore della ricorrente a titolo risarcitorio l'importo di € 1.000,00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 1.000,00, determinata in via equitativa. Respinge nel resto. 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