

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PICARO	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 13/02/2026

FATTO

La parte ricorrente espone quanto segue.

- Nella giornata del 19.5.2025, alle ore 19.26, riceveva sulla sua utenza telefonica una telefonata da parte di un numero apparentemente riconducibile a quello ufficiale della Banca convenuta, di cui è correntista.
- L'interlocutore dopo essersi identificato come dipendente dell'ufficio antifrode le riferiva che le sue credenziali erano state collegate ad un altro telefono cellulare ed erano stati effettuati dei bonifici.
- A questo punto, domandava all'interlocutore come mai fosse stata contattata a quell'ora e lo stesso le riferiva che lavorava presso un ufficio esterno e si occupava di phishing ed inoltre su esplicita domanda si presentava come S.A., della sede di Viale Europa a Roma. Per conquistare la sua fiducia l'interlocutore rivelava l'esatto saldo del conto corrente al momento della telefonata nonché l'iban associato ad esso e al nome e cognome della ricorrente, tutti dati in possesso solo ed esclusivamente all'intermediario, tranquillizzando così la ricorrente.
- Guardando la messaggistica del proprio telefono cellulare, la ricorrente si accorgeva che tra i messaggi ricevuti, tramite il numero ufficiale della Banca e nella conversazione quotidiana con la banca, vi era un messaggio riportante "Servizio bonifico istantaneo sospeso per 24 ore" "Dispositivo Samsung Galaxy S10 rimosso correttamente"; contestualmente l'interlocutore la rassicurava dicendole che aveva provveduto a rimuovere il dispositivo Samsung Galaxy S10 da cui veniva effettuato l'accesso fraudolento.
- A questo punto il sedicente operatore riferiva alla ricorrente che avrebbe dovuto effettuare i bonifici per stornare quelli che erano stati fatti precedentemente tramite il cellulare Samsung Galaxy S10.
- Tratta in inganno, la ricorrente effettuava nr. 5 bonifici istantanei: 490,00 euro a beneficio di T. sull'iban nr. finale-46; 490,00 euro a beneficio di T. sull'iban nr. finale-98; 495,00 euro a beneficio di C.

sull'iban nr. finale-00.; 490,00 euro a beneficio di T. sull'iban nr. finale-98; 490,00 euro a beneficio di C. sull'iban nr. finale-00.

Per ogni bonifico, il presunto operatore inviava un messaggio di testo con riportato "Bonifico istantaneo di euro 490,00 bloccato. Storno numero ...".

- La ricorrente si rendeva conto di essere stata vittima di una truffa poiché con l'ultimo bonifico effettuato non riceveva il messaggio di storno e ricontattando il numero ufficiale della Banca, rispondeva un operatore che, venuto a conoscenza di quanto era accaduto, le riferiva che era stata truffata, motivo per il quale bloccava le credenziali di accesso all'area riservata e la invitava a recarsi presso la banca nonché presso un ufficio di Polizia per formalizzare querela in merito.
- Per tutta la durata della telefonata nessun avviso le è giunto dal sistema antifrode dell'home banking.
- Il giorno 20/05/2025 la ricorrente effettuava il disconoscimento dei pagamenti presso il portale antifrode dell'intermediario che rispondeva in maniera negativa, rigettando la richiesta. Nello stesso giorno effettuava reclamo tramite pec ricevendo nuovamente in maniera negativa, a causa della sua asserita colpa grave.
- La ricorrente domanda il rimborso nella misura almeno del 70% dell'importo sottratto fraudolentemente, atteso il concorso di colpa della Banca, che ha reso possibile il trafugamento di dati e non ha adottato i necessari presidi antifrode in presenza di movimentazione anomala, pur essendo a conoscenza delle attività di spoofing compiute sulle loro linee telefoniche e messaggistiche.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite il 19 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)"*.

4.- La ricorrente lamenta di essere stata vittima di frode in relazione a cinque operazioni di bonifico on line, per un importo complessivo di 2.445,00 euro, asseritamente compiute il 19.5.2025.

Non produce evidenza del compimento di tali operazioni, limitandosi a depositare la denuncia nella quale il loro compimento viene riferito.

La ricorrente riferisce di aver compiuto personalmente e per intero le operazioni oggetto di disconoscimento, seguendo le indicazioni telefoniche impartite dal frodatore, il quale avrebbe contattato la ricorrente da un numero di telefono riconducibile all'intermediario a seguito della ricezione di alcuni messaggi decettivi inseritisi nella corrispondenza sms intrattenuta con l'intermediario.

Non risulta prodotta evidenza di telefonata e messaggi in discorso, benché di questi si faccia menzione nella denuncia depositata.

La fattispecie fraudolenta descritta dalla parte ricorrente parrebbe inquadrabile nello schema del c.d. social hacking.

D'altro canto, l'intermediario ha ritenuto di rimanere assente nel presente procedimento non avendo depositato le controdeduzioni.

5.- Nella riunione del 20 novembre 2025 il Collegio ha richiesto "copia della documentazione comprovante le operazioni disconosciute e il loro ammontare, nonché copia delle schermate integrali del cellulare relative ai messaggi e alle chiamate ricevuti il giorno della truffa istruttoria".

Con comunicazione del 25 novembre 2025 la ricorrente ha prodotto la seguente documentazione: copia delle contabili delle 5 operazioni di pagamento disconosciute; copia della schermata relativa alla telefonata decettiva (si osserva che la data, l'orario e il numero di telefono corrispondono a quanto riferito nella denuncia; il numero di telefono corrisponde a quello reperibile su internet come appartenente all'intermediario); copia delle schermate del telefono relative ai messaggi decettivi (si osserva che le operazioni sono state compiute in un breve lasso di tempo, 19.26 – 21.05, compatibile con quello della telefonata decettiva sopra richiamata iniziata alle 19.12 e durata 54 minuti).

L'intermediario, tuttavia, è rimasto assente e, quindi, non ha prodotto evidenze relative alle modalità di autenticazione delle operazioni.

5.- In ordine alla prova di autenticazione forte in capo all'intermediario, si rammenta che i Collegi sono unanimi nel ritenere che in caso anche di parziale mancanza della prova della SCA il ricorso debba essere accolto integralmente, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova di colpa grave dell'utente (Collegio di Roma, decisione n. 26738/19).
Alla luce di quanto esposto, il Collegio ritiene che il ricorso debba essere accolto.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 2.445,00.

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