Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 06/02/2026

FATTO

La parte ricorrente espone quanto segue.
• In data 24/03/2025, il ricorrente ha ricevuto una telefonata da un numero apparentemente riconducibile all'intermediario. L'interlocutore ha dichiarato che erano in corso attacchi informatici era necessaria l'installazione di un antivirus sul telefono del ricorrente per garantire la sicurezza del suo conto bancario.
• Il ricorrente, persuaso della veridicità delle affermazioni del truffatore, ha seguito le sue istruzioni e installato sul proprio smartphone l'applicazione indicata dall'interlocutore. Le operazioni hanno richiesto circa mezz'ora.
• Conclusa la telefonata, il ricorrente si è reso conto che era stata disinstallata l'app dell'intermediario e ha telefonato al numero verde per chiedere spiegazioni. Ha così appreso di essere stato vittima di una truffa, nell'ambito della quale era stato disposto un bonifico da 23.900,00 €.
Ciò posto, il ricorrente osserva quanto segue.
• La telefonata truffaldina ha tratto in inganno il ricorrente perché proveniva dal numero verde dell'intermediario.
• Nel corso della truffa il ricorrente non ha comunicato alcun codice al truffatore.
• L'operazione non è stata seguita da alcun SMS alert.
• In ogni caso, l'intermediario avrebbe dovuto bloccare preventivamente l'operazione, in quanto anomala rispetto al proprio profilo di spesa.
Tanto premesso, si chiede la retrocessione dell'importo relativo alle operazioni contestate.
L'intermediario resiste al ricorso ed eccepisce quanto segue.
• Il ricorso è inammissibile per carenza di preventivo reclamo.

• Le operazioni disconosciute sono state precedute dall'accesso all'home banking via app – tramite inserimento delle credenziali statiche (numero cliente e PIN) all'interno nell'app token – ed eseguite sempre tramite la digitazione del PIN in ambiente app.
• Quanto alla colpa grave dell'utente, egli ha seguito in modo pedissequo e acritico le istruzioni ricevute al telefono da persona sconosciuta che l'ha guidato nel download di un'applicazione non collegata alla banca resistente sul proprio smartphone.
• Peraltro, parte ricorrente non produce evidenze relative al contatto telefonico ricevuto.
• A seguito dell'operazione è stato regolarmente trasmesso un SMS alert al numero di telefono del ricorrente.

Tanto premesso, la banca chiede il rigetto del ricorso.

Nelle repliche, oltre a ribadire quanto già allegato, la parte ricorrente sostiene quanto segue.

• Il reclamo è stato presentato con PEC del 29/03/2025, trasmessa alla casella dell'intermediario.
• La frode è avvenuta tramite tecniche informatiche sofisticate, tramite l'intromissione nei sistemi dell'intermediario resistente, il che esclude la colpa grave in capo al ricorrente.
• Quanto all'autenticazione, le tecniche utilizzate dall'intermediario si sono rivelate insufficienti a prevenire la frode, tenuto anche conto della natura sospetta delle operazioni.
• L'SMS alert cui fa riferimento l'intermediario non è mai arrivato.

Nelle controrepliche l'intermediario ha ribadito quanto già dedotto.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 24 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 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)*".
4.- Il ricorrente chiede la restituzione della somma di 23.900,00 €, corrispondente a un bonifico eseguito il 24/03/2025 a valere sul suo conto corrente, nell'ambito di una truffa di tipo SMS spoofing + vishing.
L'intermediario ha eccepito la carenza di preventivo reclamo, tuttavia il ricorrente produce una PEC di reclamo del 29/03/2025.
Secondo la ricostruzione dell'intermediario, il truffatore ha anzitutto effettuato l'accesso all'home banking tramite lo smartphone del ricorrente, digitando il numero cliente e il PIN (elemento di conoscenza) all'interno nell'app token (elemento di possesso).
Il resistente produce il log, da cui risulta l'accesso mediante credenziali statiche in ambiente Android, via smartphone.
Successivamente, il bonifico sarebbe stato autenticato sempre tramite la digitazione del PIN (elemento di conoscenza) nell'app token (elemento di possesso).
Dai log prodotti risulta la digitazione del PIN in ambiente Android, via smartphone.
5.- In base alla denuncia, il ricorrente è stato contattato telefonicamente da un sedicente operatore dell'intermediario che – con il pretesto di un attacco informatico in corso – l'ha convinto a installare un presunto antivirus sul suo smartphone.
Quanto alla data della frode, nella denuncia è indicato il 23/03/2025, tuttavia dalle concordi dichiarazioni delle parti dalle risultanze informatiche in atti, risulta che sia avvenuta il 24/03/2025.
Nell'ambito della frode, è stato disposto un bonifico da 23.900,00 € a valere sul conto corrente del ricorrente ed è stata poi disinstallata l'app bancaria dal suo smartphone.
Il ricorrente non ha prodotto l'evidenza del registro delle chiamate.
Il Collegio, nella riunione del 7/11/2025, ha deliberato quanto segue: "Il Collegio, ritenuto necessario acquisire ulteriori elementi ai fini della decisione, invita la parte ricorrente a produrre, entro 15 giorni dalla ricezione del presente provvedimento, le schermate del telefono relative al registro chiamate del giorno della truffa. Proroga di 90 giorni il termine per l'assunzione della decisione".
Con nota del 25/11/2025 i ricorrenti hanno riscontrato la richiesta d'integrazione istruttoria, comunicando che non hanno disponibilità del richiesto registro chiamate perché, a seguito della frode, il ricorrente ha resettato il proprio smartphone alle impostazioni di fabbrica.
Affermano di aver interessato la propria compagnia telefonica per ottenere i tabulati telefonici, ma che glie ne è stata comunicata la cancellazione, per decorso del termine massimo di conservazione di sei mesi, come da lettera che si riporta di seguito.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Pertanto, all'esito della ricostruzione in sede istruttoria, sembra possibile che il ricorrente sia stato vittima di una truffa di tipo vishing, nel corso della quale ha scaricato un'applicazione di controllo remoto sul proprio smartphone, tramite la quale il truffatore ha in primo luogo oscurato lo schermo del dispositivo, per poi effettuare le operazioni tramite smartphone.
Il Collegio è solito riconoscere la colpa grave dell'utente che, su indicazione del frodatore, installi un software "la cui funzionalità risiede (…) nel permettere l'accesso ed il controllo di pc e smartphone da remoto", consentendo in tal modo al frodatore di agire indisturbato e disporre i pagamenti (Collegio di Roma, decisione n. 4317/2024; Collegio di Roma, decisione n. 2856 del 22/03/2023).
D'altro canto, il ricorrente lamenta la mancata attivazione del sistema di SMS alert, che avrebbe, a suo avviso, potuto mitigare il danno economico subito. In realtà, l'intermediario documenta l'invio dell'alert al numero di telefono indicato dallo stesso ricorrente come proprio recapito del ricorso. Il ricorrente nega di aver ricevuto tale messaggio.
6.- La procedura di autenticazione sopra descritta risponde ai requisiti previsti dalla normativa vigente per potersi qualificare come di autenticazione forte (*Strong Customer Authentication*), possedendo almeno (i necessari) due dei tre elementi previsti in materia, secondo quanto specificato dalla "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*".
7.- Tanto osservato in ordine alla SCA, laddove il ricorrente ammetta di aver dato seguito a una comunicazione di *phishing* (via email, sms o chiamata vocale), fornendo le proprie credenziali, i Collegi, in linea con la decisione n. 3498/2012 del Collegio di Coordinamento, ritengono che il cliente sia vittima di colpevole credulità, risultando "tali forme di accalappiamento" "ormai note al pur non espertissimo navigatore di internet".
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