Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) PICARO	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 RAFFAELE PICARO

Seduta del 25/03/2026

FATTO

La ricorrente chiede la restituzione della somma di euro 7.000,00, corrispondente al valore di un bonifico ordinario eseguito a seguito di una truffa di tipo *vishing* con *caller ID spoofing*, nell'ambito della quale installava un'applicazione di controllo remoto sul proprio smartphone. Più in particolare, l'istante deduce che, in data 8.7.2025, riceveva una telefonata apparentemente proveniente dall'intermediario, con cui una voce registrata la allertava di un pagamento sospetto sul suo conto, invitandola a premere un tasto per essere ricontattata a fini del blocco dell'operazione. La ricorrente premeva il tasto richiesto e veniva richiamata da un sedicente operatore, che la induceva a installare un'applicazione sul proprio *smartphone*, tramite un *link* trasmessole via SMS. Dopo l'installazione il cellulare si spegneva e, secondo le indicazioni del truffatore, sarebbe dovuto rimanere spento fino all'indomani. Il giorno successivo la ricorrente riaccendeva il telefono e si avvedeva che l'8.7.2025 era stato disposto un bonifico fraudolento di euro 7.000,00 dal suo conto corrente. L'istante contesta alla banca il mancato blocco dell'operazione evidentemente anomala e, pertanto, chiede il rimborso del controvalore del bonifico contestato.

L'intermediario, ritualmente costituitosi, eccepisce la colpa grave della ricorrente per avere assecondato le istruzioni ricevute dallo sconosciuto interlocutore, consentendo l'installazione di un'applicazione utile a favorire l'accesso al suo dispositivo da parte di un terzo. In tal guisa, segnala che l'operazione risulta correttamente autorizzata, precisando che l'accesso all'*home banking* avveniva attraverso la digitazione del codice di accesso della ricorrente, all'interno della *token app* configurata sul suo *smartphone*, ormai sotto il controllo del truffatore; mentre la disposizione dell'operazione era autenticata tramite la digitazione del PIN nel *token app*. Segnala ancora che, a fronte delle operazioni eseguite, la banca ha inviato al cellulare della cliente un SMS *alert* e una notifica *push* che avrebbero potuto consentirle di attivarsi con tempestività per evitare ogni danno a suo carico. Infine, eccepisce che il numero da cui proveniva la telefonata fraudolenta, riportato nella denuncia, non è riconducibile all'intermediario. Conclude, pertanto, per il rigetto del ricorso.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

DIRITTO

La domanda di parte ricorrente deve scrutinarsi alla luce delle disposizioni previste dal d.lgs. n. 11 del 2010 (in attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno - c.d. PSD - come aggiornate in recepimento della direttiva 2015/2366/CE - c.d. PSD2; nonché secondo le norme tecniche fornite dall'EBA recepite nel Reg. UE 2018/389, circa la *Strong Customer Authentication*, SCA) volte a disciplinare gli obblighi reciprocamente gravanti sul prestatore e sull'utilizzatore dei servizi di pagamento. Ai sensi dell'art. 8 del d.lgs. n. 11 del 2010 «*il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7*». Tale ultima disposizione prevede che «*l'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso [...] e che a tal fine adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo*». Rileva, ancora, l'art. 10, co. 1, d.lgs. n. 11 del 2010 per cui «*Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita (…), è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*».

Il mancato rispetto dei reciproci obblighi gravanti sulle parti determina, secondo i criteri fissati dagli artt. 11 e 12, d.lgs. n. 11 del 2010, la responsabilità del prestatore o dell'utilizzatore per i danni prodotti da operazioni di pagamento non autorizzate.

Se ne desume che l'intermediario possa sottrarsi alla responsabilità risarcitoria per l'uso non autorizzato dello strumento di pagamento, soltanto quando sia provata la colpa grave dell'utilizzatore. In proposito, la giurisprudenza di questo Arbitro si è consolidata nel senso di ritenere che possa ritenersi raggiunta la prova della colpa grave – e che quindi possa dirsi assolto l'onere gravante a carico dell'intermediario – quando sia dimostrato quell'elevato e abnorme grado di negligenza in capo all'utilizzatore, al ricorrere del quale possa imputarsi allo stesso la responsabilità delle conseguenze di un utilizzo fraudolento.

Il Collegio di Coordinamento, con dec. n. 22745 del 2019, ha poi chiarito che «*la previsione di cui all'art. 10, co. 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*».

Inoltre, con specifico riferimento agli oneri di allegazione a carico delle parti, il Collegio di Coordinamento ha precisato che, in applicazione del principio della domanda e del rispetto del contraddittorio, "*il ricorrente è tenuto a formulare una domanda che sia articolata nel* petitum *(il provvedimento o il bene della vita richiesto) e nella* causa petendi *(la situazione giuridica giustificatrice della domanda) e a produrre la documentazione dimostrativa. Reciprocamente, il resistente ha l'onere processuale di addurre le argomentazioni (fattuali e giuridiche) idonee a contrastare la domanda e di produrre la documentazione ritenuta idonea allo scopo […]. Il giudicante (l'arbitro come il giudice) ha il potere-dovere di stabilire la corretta qualificazione giuridica delle questioni portate alla sua cognizione, ma non quello di prendere in esame situazioni di fatto diverse da quelle rappresentate dalle parti. Ne consegue, in applicazione dei principi sopra enunciati, che, al di fuori delle ipotesi della rilevabilità d'ufficio normativamente prevista, all'arbitro non è consentito esaminare questioni su cui non abbia sollecitato il contraddittorio delle parti*" (Coll. Coord., dec. n. 10929/2016).

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Si tratta, dunque, di orientarsi nel perimetro tracciato delle allegazioni, volta per volta, sottoposte dalle parti alla cognizione dell'Arbitro, al fine di verificare se, alla luce degli elementi costituitivi della fattispecie, sia possibile desumere in capo all'utilizzatore un comportamento gravemente colposo.
Orbene, l'operazione contestata coincide con un bonifico ordinario di euro 7.000,00, a valere sul conto corrente della ricorrente.
L'intermediario produce evidenze idonee a dimostrare la corretta autenticazione dell'operazione, da cui si evince che l'accesso all'*home banking* via app è avvenuto tramite la digitazione del codice di accesso della ricorrente (elemento di conoscenza), all'interno della *token app* configurata sul suo *smartphone* (elemento di possesso).
Passando alla condotta serbata dall'istante, risulta che la stessa abbia scaricato un'applicazione di controllo remoto sul proprio *smartphone*, tramite la quale il truffatore ha effettuato l'operazione disconosciuta.
In questi casi, l'Arbitro riconosce 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).
Non può dirsi dimostrato che la truffa sia partita da un caso di *spoofing*, in quanto la ricorrente non ha prodotto il registro delle chiamate e, inoltre, il numero indicato nella denuncia non è riconducibile all'intermediario che ha espressamente contestato tale circostanza.
Sotto altro profilo, la ricorrente lamenta che l'intermediario non abbia bloccato preventivamente le operazioni di pagamento contestate, a fronte della natura anomala rispetto al proprio profilo di spesa.
Sul tema del monitoraggio preventivo delle operazioni di pagamento, l'art. 2 del Regolamento Delegato (UE) n. 2018/389 della Commissione prevede che gli intermediari predispongano meccanismi di monitoraggio in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. In base all'interpretazione fornita dall'EBA, non è necessario che questi meccanismi operino in tempo reale, potendo limitarsi a un monitoraggio delle frodi *ex post* (cfr. Collegio di Roma, decisione n. 2534 del 10.2.2022).
Nel caso di specie, non ricorrono neanche gli indici di frode previsti dall'art. 8, D.M. 30 aprile 2007, n. 112, in presenza dei quali è rinvenibile, in capo all'intermediario, un obbligo di blocco preventivo di operazioni di pagamento.
Peraltro, la ricorrente non ha allegato, prima ancora che provato, elementi utili a ritenere che l'operazione contestata possa ritenersi anomala rispetto all'operatività fisiologica del suo conto.
Alla luce di tutto quanto esposto, la domanda di rimborso è infondata e va rigettata.

PER QUESTI MOTIVI.

Il Collegio respinge il ricorso.

IL PRESIDENTE