Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore ALBERTO MARIA BENEDETTI

Seduta del 24/02/2026

FATTO

Parte ricorrente si duole di aver subito una truffa realizzata con invio SMS che si ha determinato un trasferimento non autorizzato di un importo pari a euro 750,00 verso un servizio di money transfer. Insoddisfatta degli esiti del reclamo, si rivolge all'Arbitro per domandare il rimborso della somma illegittimamente sottrattale.
L'intermediario, regolarmente costituitosi, esclude la propria responsabilità per l'operazione di pagamento in contestazione, risultando la stessa approvata correttamente tramite un sistema di autenticazione forte e senza alcuna anomalia, nel rispetto dei requisiti SCA di cui allega in atti apposita documentazione.
Osserva che l'operazione è stata eseguita in conformità art. 10-bis del D.lgs n.11/2010, ovvero solo in seguito alla corretta e regolare "autenticazione forte del cliente" mediante "autenticazione a due fattori" appartenenti rispettivamente alle categorie della conoscenza.
Domanda, pertanto, il rigetto del ricorso.

DIRITTO

L'operazione contestata è stata eseguita sotto il vigore del D. Lgs. 27 gennaio 2010 n. 11, come modificato dal D. Lgs. 15 dicembre 2017 n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2) entrato in vigore il 13/01/2018.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

In particolare, le fonti normative che regolano la strong customer authentication (SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del D. Lgs. n. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EB.
Va altresì richiamata la previsione dell'art. 10, comma 1, d.lgs. n. 11/2010 [così come introdotto dall'art. 2, comma 10, lettera c) d.lgs n. 218/2017], in relazione alla prova di autenticazione ed esecuzione delle operazioni di pagamento: "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 comma secondo della medesima norma precisa che: "Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".
Ciò premesso, nel caso di specie l'intermediario dimostra di avere implementato procedure di autenticazione forte del cliente attive in fase di accesso al conto di pagamento online, in fase dispositiva di un'operazione di pagamento elettronico o in occasione di qualsiasi altra azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti. Le procedure di autenticazione forte adottate dall'intermediario sono la Procedura "primaria", che consta di Push notification in APP e Codice ***ID; nonché la Procedura "secondaria", costituita da One Time Password (OTP) via SMS e Password.
Nel caso di specie, l'intermediario chiarisce che per le operazioni contestate è stata attivata la "procedura secondaria" mediante digitazione delle credenziali (userid e password) e successivo inserimento del codice OTP necessario per accedere alla propria area personale; produce altresì la tracciatura informatica dalla quale si desume l'inserimento della password (elemento di conoscenza) e del codice OTP inviato via SMS all'utenza certificata della ricorrente (fattore di possesso). Dunque la SCA risulta conforme e regolare.
Nel caso di specie, il cliente è stato vittima di phishing "tradizionale"; secondo l'orientamento condiviso dai Collegi ABF la diffusione del fenomeno è tale che i Collegi ormai ritengono da tempo che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa di talchè deve ritenersi che la truffa sia stata possibile in ragione della colpa grave del cliente che, cadendo nella trama ordita dai truffatori, ha loro fornito le proprie credenziali. Va peraltro aggiunto che, trattandosi di un'unica operazione, anche l'attivazione del servizio di alert sarebbe stata, comunque, irrilevante.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE