

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) RUGGIERO	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore ALBERTO MARIA BENEDETTI

Seduta del 27/01/2026

FATTO

Parte ricorrente, titolare di una carta di credito emessa dall'intermediario resistente e cointestatario del rapporto insieme alla moglie, si rivolge all'Arbitro, insoddisfatta degli esiti del reclamo, lamentando l'esecuzione di un pagamento non autorizzato effettuato in data 21 agosto 2025, per l'importo di € 450,08, nell'ambito di una truffa realizzata attraverso una piattaforma online di compravendita di beni usati.

In particolare, il ricorrente espone che la moglie, cointestataria del rapporto, stava procedendo alla creazione di un account sulla piattaforma di vendita, la quale avrebbe richiesto l'inserimento dei dati di una carta di credito a fini di verifica. Dopo aver inserito tali dati, la cliente riceveva sul proprio dispositivo mobile una richiesta di autorizzazione, che veniva confermata. Successivamente, tuttavia, la piattaforma non restituiva l'importo asseritamente bloccato e segnalava, tramite un collegamento esterno, la possibile natura fraudolenta dell'operazione. Il giorno successivo il ricorrente si avvedeva della presenza di addebiti a favore di un esercente non riconducibile alla piattaforma di vendita. Provvedeva quindi a bloccare la carta e a presentare reclamo all'intermediario, senza ottenere il rimborso richiesto. Domanda, pertanto, il rimborso della predetta somma.

L'intermediario, regolarmente costituitosi, ricostruisce l'episodio come una classica truffa di phishing posta in essere al di fuori dei canali ufficiali della banca e della piattaforma di compravendita. In particolare, deduce che il cliente, seguendo le istruzioni di un sedicente servizio di supporto, avrebbe inserito i dati della carta su una pagina esterna e successivamente autorizzato il pagamento mediante notifica push, confermando consapevolmente l'operazione. Evidenzia inoltre che il sistema di

autenticazione adottato è conforme alla strong customer authentication (SCA) prevista dalla PSD2; la notifica push riportava in modo chiaro l'importo e il beneficiario dell'operazione; non risultano anomalie, malfunzionamenti o compromissioni dei sistemi; il ricorrente non ha bloccato tempestivamente la carta né ha contattato il servizio clienti prima di autorizzare l'operazione; la condotta del ricorrente integra, a suo avviso, una colpa grave, avendo egli fornito e confermato le credenziali necessarie all'esecuzione del pagamento.

Domanda, pertanto, il rigetto del ricorso.

DIRITTO

L'operazione ricade 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.

In particolare, le fonti normative che regolano la *strong customer authentication* (cd. 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".

La controversia ha ad oggetto l'utilizzo non autorizzato di strumenti di pagamento ed è disciplinata dal D. Lgs. n. 11/2010, come modificato dal D. Lgs. n. 218/2017, di recepimento della direttiva (UE) 2015/2366 (PSD2).

Ai sensi dell'art. 10 del citato decreto, qualora l'utente neghi di aver autorizzato un'operazione di pagamento, grava sull'intermediario l'onere di provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata, nonché di dimostrare l'eventuale sussistenza del dolo o della colpa grave dell'utente. L'utilizzo delle credenziali di sicurezza non è di per sé sufficiente a dimostrare l'autorizzazione dell'operazione né la colpa grave del cliente.

Nel caso di specie, l'intermediario ha assolto all'onere della prova dimostrando la regolarità della SCA; dalla documentazione prodotta dall'intermediario risulta che l'operazione contestata è stata autorizzata mediante una procedura conforme ai requisiti richiesti e, in particolare, il pagamento è stato preceduto dall'invio di una notifica push sull'applicazione mobile associata al profilo del cliente; la notifica riportava in modo chiaro e comprensibile l'importo e il beneficiario dell'operazione, consentendo all'utente di verificare ex ante il contenuto della disposizione; l'autorizzazione è avvenuta tramite interazione attiva dell'utente, mediante inserimento del PIN o conferma biometrica (impronta digitale o riconoscimento

facciale), integrando così almeno due fattori di autenticazione riconducibili alle categorie della conoscenza e dell'inerenza, unitamente al fattore del possesso rappresentato dal device previamente associato.

La circostanza che l'autorizzazione sia avvenuta tramite SCA "silente", con generazione automatica di una OTP transazionale non visibile all'utente ma strettamente collegata alla singola operazione, non incide sulla validità dell'autenticazione, trattandosi di una modalità espressamente prevista e consentita dalla disciplina PSD2, purché l'utente sia messo in condizione di comprendere quale operazione stia autorizzando. Condizione che, nel caso di specie, risulta soddisfatta dalla presenza di una notifica push "parlante".

Secondo il consolidato orientamento dei Collegi ABF, in presenza di una SCA regolarmente applicata e di un'autorizzazione prestata direttamente dal cliente secondo le modalità contrattualmente previste, l'operazione deve considerarsi correttamente autenticata, restando irrilevante, ai fini della responsabilità dell'intermediario, il successivo accertamento che il consenso dell'utente sia stato viziato da artifici o raggiri posti in essere da terzi estranei al rapporto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE