

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 si rivolge all'Arbitro, insoddisfatta degli esiti del reclamo, lamentando l'esecuzione di operazioni di pagamento fraudolente effettuate, tra il 25 e il 29/10/2024, su due carte di pagamento emesse dall'intermediario resistente, per un importo complessivo pari a € 1.425,28 (di cui € 1.335,28 riferibili a sei operazioni eseguite su una carta prepagata c.d. "evoluta" ed € 90,00 relativi a un'operazione eseguita su una carta prepagata "standard"). Riferisce di aver scoperto le operazioni solo in data 13/11/2024, allorché l'applicazione dell'intermediario risultava bloccata. Il giorno successivo, recatasi presso un ufficio postale, apprendeva dell'avvenuta esecuzione delle operazioni sospette e provvedeva a sporgere denuncia, nonché a presentare formale reclamo all'intermediario, chiedendo il rimborso delle somme indebitamente sottratte.

L'intermediario, regolarmente costituitosi, osserva che le operazioni contestate sono state eseguite a seguito di regolare autenticazione forte del cliente (SCA) e che la frode fosse riconducibile a una condotta colposa della ricorrente, la quale avrebbe comunicato a terzi i propri codici di sicurezza, consentendo l'associazione (enrollment/onboarding) di un nuovo dispositivo e la successiva esecuzione delle operazioni.

Domanda, pertanto, il rigetto del ricorso.

DIRITTO

Le operazioni contestate sono state eseguite 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'EBA.

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 prodotto evidenze tecniche dalle quali risulta che l'enrollment del nuovo dispositivo è stato completato mediante inserimento dei dati della carta e successivo OTP inviato via SMS all'utenza certificata della ricorrente; le operazioni contestate sono state autorizzate mediante combinazione di fattori riconducibili alle categorie della conoscenza (password/codice) e del possesso (device associato), in conformità alle procedure previste dal sistema dell'intermediario.

Ciò precisato, tuttavia, il Collegio reputa che l'elemento decisivo per risolvere la controversia in esame sia rappresentato dal ridottissimo lasso temporale intercorrente tra l'associazione del nuovo dispositivo (ore 14:38) e la prima operazione fraudolenta (ore 14:45).

L'associazione di un nuovo device costituisce una fase di massima criticità del processo di autenticazione, poiché abilita un nuovo strumento a operare in piena autonomia sul conto e sugli strumenti di pagamento del cliente; proprio in considerazione dell'elevato rischio connesso a tale fase,

l'European Banking Authority, nella Opinion del 29/4/2024, ha individuato, tra le misure di rafforzamento della sicurezza: la necessità di prevedere un adeguato intervallo temporale (c.d. cooling-off period) tra la registrazione di un nuovo dispositivo e la sua piena operatività; l'adozione di presidi di monitoraggio rafforzati immediatamente successivi all'enrollment.

Nel caso di specie il nuovo device è divenuto immediatamente operativo, senza alcun periodo di raffreddamento e le operazioni fraudolente sono state eseguite a distanza di pochi minuti dall'enrollment; l'intermediario non ha dedotto né dimostrato di aver attivato misure ulteriori di verifica o di blocco, nonostante la concentrazione e la rapidità dell'operatività.

Tale circostanza evidenzia un deficit dei presidi organizzativi e procedurali dell'intermediario, poiché l'assenza di uno spazio temporale minimo tra l'associazione del device e l'operatività ha reso inefficace la funzione preventiva della SCA, consentendo ai truffatori di sfruttare immediatamente il nuovo strumento. Per tali ragioni, la domanda di parte ricorrente è meritevole di accoglimento.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto della ricorrente al risarcimento del danno per l'importo di € 713,00 oltre interessi legali dalla data del reclamo nei sensi di cui in motivazione.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE