

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) MAFFEO	Membro di designazione rappresentativa dei clienti

Relatore ALBERTO MARIA BENEDETTI

Seduta del 10/03/2026

FATTO

Parte ricorrente espone di essere titolare di un conto corrente con carta di debito collegata, sul quale, in data 27 maggio 2024, venivano eseguite quattro operazioni di pagamento e-commerce da lui non autorizzate per un importo complessivo di € 1.317,00, di cui ha appreso tramite notifica su dispositivo mobile; proposta regolare denuncia, l'intermediario procedeva al riaccredito "salvo buon fine" della somma richiesta; tuttavia successivamente la banca disponeva lo storno del rimborso sostenendo che le operazioni risultavano autorizzate tramite l'utilizzo delle credenziali di sicurezza a lui assegnate. Insoddisfatto degli esiti del reclamo, si rivolge all'Arbitro domandando la restituzione della predetta somma, oltre alle spese.

L'intermediario, regolarmente costituitosi, contesta la ricostruzione di controparte, specie per quel che riguarda la possibile truffa subita dal cliente; osserva che le operazioni sono avvenute regolarmente e fa presente che un blocco tempestivo della carta avrebbe potuto evitare almeno tre delle quattro operazioni disconosciute.

Osserva inoltre che tutte le operazioni risultano correttamente autenticate e autorizzate tramite notifica push e fattore biometrico (face-ID, impronta digitale o codice di sblocco), con utilizzo del dispositivo e delle credenziali nella disponibilità del ricorrente.

Osserva infine che la dinamica emersa indica, invece, una custodia negligente degli strumenti di pagamento e delle credenziali da parte del ricorrente, invocando la sussistenza della colpa grava e 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.

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'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".

Ciò precisato, dalla documentazione allegata in atti da parte resistente risulta che le operazioni appaiono autorizzate mediante l'utilizzo di un doppio fattore (SCA); in particolare in relazione alla cd. "push based authentication", in cui l'utente autorizza la transazione tramite l'utilizzo di un PIN o di un'impronta digitale a seguito della ricezione di notifica push sul proprio dispositivo, si ritiene che la notifica push possa essere utilizzata alla stregua di un elemento di possesso a condizione che il PSP rispetti i requisiti di cui all'art. 7 del Regolamento delegato (UE) n. 2018/389 il quale prevede che "i prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come possesso siano utilizzati da soggetti non autorizzati". Nel caso di specie, l'intermediario ha prodotto evidenza delle notifiche push inviate al cliente con il relativo testo.

Nel caso di specie, date le modalità temporali di realizzazione delle operazioni non autorizzate (avvenute tre il 27 maggio alle ore 13:14, 13:38 e 14:00 e il 28 maggio), ha rilevanza l'invio dell'SMS alert: il Collegio di Coordinamento, con la decisione n. 24366/19 e con la decisione n. 8672/2024, ha affermato che "fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto".

Nel caso di specie, l'intermediario non ha provato di aver inviato detti SMS perché, pur producendo un elenco di SMS asseritamente spediti al cliente, non è dato sapere se si tratti di SMS alert spediti successivamente al compimento dell'operazione, né se ne allega il testo e, soprattutto, il numero di cellulare cui si affermano siano stati diretti. Se il cliente avesse ricevuto un SMS alert dopo la prima operazione, avrebbe certamente potuto bloccare lo strumento di pagamento impedendo la realizzazione delle operazioni successiva (dalla seconda alla quarta) che, pertanto, debbono essere

rimborsate a parte ricorrente come da dispositivo.

In aggiunta, vanno valorizzati anche gli indici di frode, sebbene ulteriori a quelli di cui al DM 112/2007, che il Collegio può apprezzare in presenza di un'operatività anomala rispetto alle movimentazioni storiche del cliente; nel caso di specie, l'operazione di € 368,00 del 28/5/2024 risulta autorizzata dopo che nella giornata precedente (in seguito al compimento della terza operazione contestata) erano state annullate cinque operazioni per sospetta frode (cfr. codice 102, "Suspected fraud").

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente alla restituzione dell'importo di € 1.236,00, 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