

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore STEFANO TRAVERSI

Seduta del 13/01/2026

FATTO

Con ricorso ritualmente presentato in data 08 settembre 2025, la parte ricorrente espone quanto segue.

In data 26 agosto 2024, riceveva un messaggio SMS relativo a due transazioni di importo esiguo, ritenute sospette, che provvedeva a disconoscere, richiedendo il blocco della carta di pagamento. Successivamente, in data 19 maggio 2025, riceveva un ulteriore SMS concernente tre transazioni (due autorizzate e una negata), anch'esse ritenute fraudolente, procedendo nuovamente al blocco dello strumento e all'annullamento della carta.

In data 29 maggio 2025, il ricorrente provvedeva alla registrazione di una nuova carta di credito.

In data 05 giugno 2025, riceveva una comunicazione e-mail, graficamente analoga a quelle dell'intermediario ma recante un dominio ".org" anziché ".it", con la quale veniva invitato ad aggiornare il limite di spesa della carta; ritenendo la comunicazione autentica, forniva le informazioni richieste.

Nella medesima data del 05 giugno 2025, veniva eseguita un'operazione di pagamento e-commerce dell'importo di € 746,00, cui faceva seguito, in data 08 giugno 2025, una seconda operazione per € 316,99, entrambe a favore del medesimo esercente.

In data 09 giugno 2025, il ricorrente prendeva casualmente cognizione delle suddette operazioni e provvedeva immediatamente al blocco del rapporto nonché al disconoscimento degli addebiti. L'intermediario, dopo un iniziale riaccredito, procedeva al successivo riaddebito delle somme, richiedendo la produzione di formale denuncia all'Autorità giudiziaria, che il ricorrente sporgeva in data 03 luglio 2025.

Il ricorrente deduce, in particolare, la mancata ricezione di SMS di notifica per operazioni di importo superiore a € 250, asseritamente previsti dal contratto, l'eccessiva semplicità delle procedure di associazione di un nuovo dispositivo e un comportamento contraddittorio dell'intermediario, che avrebbe in passato bloccato operazioni di importo modesto, consentendo tuttavia il buon fine di pagamenti di maggiore entità.

L'intermediario resistente contesta integralmente la domanda, deducendo che le operazioni risultano regolarmente autorizzate mediante Strong Customer Authentication, resa possibile dalla condotta gravemente negligente del ricorrente, il quale avrebbe comunicato a terzi le proprie credenziali di accesso e i codici dispositivi in risposta a un tentativo di phishing.

DIRITTO

Le operazioni contestate sono state poste in essere 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 (PSD2).

L'intermediario ha fornito idonea prova dell'avvenuta autenticazione, registrazione e contabilizzazione delle operazioni disconosciute, in conformità all'art. 10 del d.lgs. 11/2010.

Dalla documentazione versata in atti risulta che l'enrollment dell'applicazione su un nuovo dispositivo è avvenuto mediante inserimento delle credenziali di accesso e tramite codici OTP inviati via SMS e via e-mail, con successiva abilitazione della modalità di autenticazione biometrica. Le operazioni contestate sono state quindi autorizzate mediante riconoscimento biometrico su dispositivo abilitato, secondo modalità conformi ai requisiti della Strong Customer Authentication.

Quanto alla condotta del ricorrente, dagli atti emerge che la comunicazione e-mail cui egli ha risposto presentava evidenti profili di anomalia, quali l'utilizzo di un mittente estraneo all'intermediario (noreply@m*****-lrc.org) e la presenza di una dicitura testuale errata ("...US" in luogo di "...i"). Tali elementi avrebbero dovuto indurre il destinatario ad adottare un comportamento improntato a prudente verifica, evitando l'inserimento di credenziali e codici dispositivi al di fuori dei canali ufficiali.

Secondo il consolidato orientamento dei Collegi ABF, nei casi di phishing tradizionale l'attenzione ordinariamente esigibile in capo al titolare dello strumento di pagamento è idonea a prevenire la frode; la comunicazione volontaria a terzi delle credenziali personalizzate integra pertanto un comportamento censurabile ai sensi dell'art. 12, comma 4, del d.lgs. 11/2010: l'utilizzatore è tenuto a non inserire le proprie credenziali al di fuori dei canali ufficiali dell'intermediario; la comunicazione di tali dati costituisce elemento rilevante nella valutazione della responsabilità dell'utilizzatore (cfr. Collegio di Bologna n. 14643/2019).

Quanto alla dedotta mancata ricezione degli SMS alert, il ricorrente non ha prodotto documentazione contrattuale idonea a dimostrare il contenuto specifico del servizio. In ogni caso, secondo i principi affermati dal Collegio di Coordinamento (decisione n. 8853/2019), la mancata ricezione degli alert non assume rilievo decisivo in presenza di un numero limitato di operazioni e in un arco temporale contenuto e al contesto già compromesso dalla previa certificazione del dispositivo fraudolento.

Alla luce di quanto precede, deve escludersi ogni profilo di responsabilità in capo all'intermediario.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE