

COLLEGIO DI NAPOLI

composto dai signori:

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

Relatore ESTERNI - GIUSEPPE SORRENTINO

Seduta del 28/04/2026

FATTO

Il ricorrente riferisce di aver subito in data 11.04.2025, mentre si trovava al lavoro, il furto della carta di debito rilasciata dall'intermediario convenuto. Accortosi dall'accaduto accedeva alla App collegata al conto corrente e si avvedeva che nel frattempo erano state effettuate, con tale strumento, tre operazioni, per un importo totale di € 1.085,00, da lui non riconosciute. Presentata formale denuncia all'Autorità Giudiziaria, provvedeva a disconoscere formalmente all'intermediario tali operazioni che però provvedeva a rimborsarne solo una (il primo prelievo), per un importo di €700,00. Insoddisfatto di tale prodromica interlocuzione, si rivolge all'Arbitro chiedendo il rimborso delle ulteriori due operazioni, per l'importo totale di €385,00, oltre alle spese legali. L'intermediario, ritualmente costituitosi, rileva che, effettuate le dovute verifiche, provvedeva a rimborsare la prima operazione effettuata, il prelievo ATM, mentre confermava l'addebito delle ulteriori due operazioni. Analizzate le modalità dell'accaduto ritiene di non dover accogliere le richieste del ricorrente, relative al rimborso dei due pagamenti tramite POS in quanto: (i) le operazioni oggetto di ricorso sono state compiute a distanza di 36 minuti dalla prima, segnalata con sms ed alert sulla app in uso al cliente; (ii) le operazioni sono state eseguite tramite lettura del microchip e corretta digitazione del PIN elemento che lascia presumere, attesa la ridotta distanza temporale tra il furto e le operazioni, che le credenziali fossero custodite insieme alla carta trafugata. In ordine poi alla generica richiesta di rimborso delle spese legali, pure richiesta, evidenziando la mancanza di qualsiasi documentazione in merito, ricorda che le Disposizioni che disciplinano la procedura non prevedono l'obbligatorietà dell'assistenza di qualsivoglia professionista.

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 (v. in particolare il parere dell'EBA del 21 giugno 2019). Alla luce delle dette coordinate ermeneutiche la prima verifica non può che riguardare il rispetto o meno da parte dell'intermediario dei requisiti tecnico-normativi previsti per la strong customer authentication (SCA). Infatti, a fronte del disconoscimento delle operazioni di pagamento on line da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, commi 1 e 2 e dell'art. 10-bis, c. 1 del d.lgs. 11/2010. In mancanza di tale dimostrazione l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute. L'intermediario produce evidenze informatiche da cui si ricava l'idoneità a garantire la compliance con la normativa in materia di SCA, in virtù dell'inserimento dei due elementi classificati rispettivamente nelle categorie della conoscenza e del possesso. Dalla documentazione informatica depositata dall'istituto, infatti, emerge chiaro che i pagamenti tramite POS, siano stati autorizzati previa lettura contactless della carta (elemento di possesso) ed inserimento corretto del codice PIN (elemento di conoscenza). Quindi, verificata la conformità alla normativa di settore del procedimento di autenticazione e di autorizzazione del pagamento, occorre appurare in che misura vada ripartita la colpa tra le parti in ossequio a quanto prescritto dal D.lgs. 11/2010. Dalla documentazione agli atti non pare ricorrano le condizioni per qualificare in termini colposi la condotta dell'intermediario in quanto è documentato che lo stesso, per tutte le operazioni poste in essere, ha tempestivamente informato il ricorrente sia per mezzo dell'invio dell'SMS alert che di messaggi push sulla app installata sul telefonino del cliente, rimasto nella disponibilità dell'ultimo. Al pari, le modalità tramite le quali si è consumata la condotta antigiuridica del truffatore non si collocano tra le ipotesi rappresentate dall'art.8 del D.M. 112/07, il quale è finalizzato a descrivere i più significativi indici di frode atti a destare allarme e spingere l'intermediario a dubitare della genuinità dell'operazione di pagamento. Ed ancora, va rilevato che le operazioni in questa sede contestate (pagamenti tramite POS) sono state effettuate circa 36 minuti dopo il prelievo presso l'ATM, (già rimborsato dall'intermediario) di cui il consumatore era stato tempestivamente avvisato tramite SMS alert. Per tale ragione il ricorrente, avendo ricevuto debito avviso della prima operazione di prelievo illecita, era nella piena possibilità di bloccare tempestivamente la carta e di evitare, dunque, il compimento delle operazioni in questa sede denunciate. Vieppiù, il fatto che le operazioni in esame siano state realizzate mediante l'inserimento corretto del PIN associato alla carta rende plausibile che, contrariamente a quanto previsto dalla normativa di settore, il detto codice segreto fosse custodito unitamente allo strumento di pagamento. A tal proposito giova ricordare che ai sensi del comma 2 dell'art 7 del D. Lgs. 11/2010 l'utente è tenuto ad adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate. In conclusione, alla luce di quanto emerso dall'istruttoria, pare sussistere la colpa grave del ricorrente il quale, oltre a non essersi attivato tempestivamente per il blocco della carta di pagamento, ha negligenemente custodito il codice PIN, indispensabile per il suo utilizzo. Ogni altra questione è da ritenersi assorbita.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE