

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 - ANDREA NERVI

Seduta del 28/04/2026

FATTO E DIRITTO

Parte ricorrente premette di essere correntista dell'odierno resistente, nonché titolare di una carta di pagamento. La ricorrente espone di aver ricevuto, in data 14 novembre 2024 sul proprio cellulare, alcune telefonate e poi un messaggio sms, contenente l'invito a cliccare su un *link* ivi evidenziato per attivare la nuova carta mediante la comunicazione delle credenziali di sicurezza.

Nei giorni immediatamente successivi il ricorrente constatava l'esistenza di sette operazioni fraudolente (prelievo e pagamento), per un importo pari ad euro 4.420/00, che ella disconosce. Chiede pertanto il rimborso della predetta somma.

L'intermediario resiste alla domanda. Sostiene che le operazioni contestate sono sei per un importo pari ad euro 4.170/00 e si dichiara disponibile a rimborsare alla parte ricorrente l'importo pari alla metà della somma frodata (ossia euro 2.085/00). Per il resto, chiede il rigetto del ricorso, sostenendo che le operazioni contestate risultano correttamente autenticate in conformità alla normativa vigente. Aggiunge che la cliente versa in colpa grave per non essersi accorta del fatto che il messaggio ricevuto presentava alcune anomalie, e ciò consentiva di escludere la sua provenienza dall'intermediario. Entrambe le parti depositano repliche e controrepliche con cui insistono nelle rispettive domande ed argomentazioni.

In punto di fatto, il Collegio precisa che, alla luce della documentazione versata in atti, le operazioni contestate dalla parte ricorrente sono sei ed ammontano a complessivi euro 4.170/00. Esse consistono in una operazione di prelievo ATM, di importo pari ad euro 250/00, ed in cinque operazioni di pagamento effettuate mediante l'utilizzo "fisico" della carta di pagamento; le operazioni di pagamento

ammontano ad euro 920/00; euro 600/00; euro 600/00; euro 910/00; euro 890/00. Tutte le operazioni sono state compiute il giorno 14 novembre 2024; quelle di pagamento, inoltre, risultano effettuate presso il medesimo punto vendita, a breve distanza temporale l'una dall'altra.

Secondo parte ricorrente vi sarebbe un'ulteriore operazione di prelievo ATM, compiuta sempre il medesimo giorno per l'importo di euro 250/00. Tale operazione, tuttavia, fa parte dei c.d. *declinati*, con codice KO e, pertanto, risulta non eseguita. Essa non può quindi essere computata ai fini della presente decisione.

Ciò premesso, il Collegio prende atto della proposta di rimborso formulata dall'intermediario, pari al 50% dell'importo frodato, come ora determinato.

Ad avviso del Collegio, tale proposta è in linea con il consolidato orientamento dell'Arbitro in tema di c.d. *boxing* (ex multis decisioni n. 6395/2024 e n. 3784/24), che identifica le controversie occasionate dall'invio alla clientela – da parte degli intermediari – di carte di pagamento destinate a sostituire quelle in scadenza.

Sul piano normativo, il Collegio ricorda che, ai sensi dell'art. 8, comma 2, del d. lgs. 11/2010, *“i rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento”*.

Tale ultima previsione è stata integrata dal regolamento della Banca d'Italia del 5 luglio 2011 (attuativo del Titolo II del d.lgs. n. 11/2010), a norma del quale *“i prestatori di servizi di pagamento pongono altresì la massima attenzione nella scelta del mezzo di spedizione di uno strumento di pagamento e/o dei relativi codici di sicurezza, in considerazione del rischio di accesso non autorizzato a detti strumenti e codici; per questo motivo, il legislatore pone interamente a carico del prestatore di servizi di pagamento detto rischio”*.

Si veda anche l'art. 22 RTS, che prevede l'obbligo dell'intermediario di assicurare *“la riservatezza e l'integrità delle credenziali di sicurezza personalizzate dell'utente dei servizi di pagamento, compresi i codici di autenticazione, durante tutte le fasi del processo di autenticazione l'autenticazione”*.

Fermo quanto precede, il Collegio rileva la sussistenza di profili di negligenza nell'operato della cliente. Infatti, le evidenze fornite dall'intermediario attestano la corretta autenticazione delle operazioni contestate. Per altro verso, parte ricorrente dichiara di essere stata contattata da un numero telefonico, a suo dire riconducibile al servizio clienti dell'intermediario e, poi, di aver cliccato su un link contenuto in un Sms ricevuto e di aver interloquito con un sedicente operatore; deduce che l'interlocutore era già a conoscenza di tutti i suoi dati, compreso il Pin.

Ne deriva che, nell'ambito delle interlocuzioni intercorse, la ricorrente ha fornito le credenziali di sicurezza, mediante le quali sono state compiute le predette operazioni.

In conclusione, dunque, la controversia può considerarsi definita, previa esecuzione – da parte dell'intermediario – della proposta di rimborso già formulata.

P.Q.M.

Respinta ogni altra domanda, il Collegio dichiara la cessazione della materia del contendere.

IL PRESIDENTE