

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) SIVIGLIA	Membro di designazione rappresentativa dei clienti

Relatore NICOLA CIPRIANI

Seduta del 18/02/2026

FATTO

A. Il ricorrente, titolare della carta di debito collegata al conto corrente incardinato presso la convenuta, si rivolge all'Arbitro al fine di disconoscere alcuni prelievi e chiede il rimborso della complessiva somma di € 4.480,00.

B. Costitutosi, l'intermediario evidenzia che il ricorrente, ad ottobre 2025, ha disconosciuto n. 11 operazioni di prelievo, compiute sia con la propria carta di debito, sia in modalità "cardless". Sennonché, l'intermediario rileva che tali operazioni sono avvenute tra il 07/11/2024 e il 26/06/2025 e contesta il mancato rispetto dei doveri di custodia degli strumenti di pagamento da parte del ricorrente in quanto, sulla base delle evidenze allegate, le operazioni con la carta di debito sono state autorizzate con corretta lettura del chip della carta e immediata digitazione del PIN, senza errori. Quanto ai prelevamenti cardless, l'intermediario ne illustra dettagliatamente il funzionamento astratto, per poi sottolineare che nella specie anche essi sono stati effettuati in maniera regolare. Pertanto, l'intermediario conclude per il rigetto del ricorso.

DIRITTO

1. La controversia concerne una vicenda di utilizzo non autorizzato di strumenti di pagamento (artt. 9 ss. d.lgs. 27 gennaio 2010, n. 11), nella specie consistente in 11 prelevamenti eseguiti fra il 07/11/2024 e 26/06/2025, dei quali 4 avvenuti in modalità "cardless" (per € 1.820,00) e 7 con utilizzo della carta fisica (per € 2.480,00)

2. Orbene, il Collegio rileva innanzi tutto che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, 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 13.1.2018. Inoltre, le operazioni contestate sono state eseguite successivamente all'entrata in vigore delle nuove disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).

3. La disciplina appena richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore (artt. 7 e 12, co. 4, d.lgs. n. 11/2010).

In particolare, "qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente 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" (ai sensi dell'art. 10, d.lgs. n. 11/2010). Inoltre, ove l'utente neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi 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" (art. 10 comma 2, d.lgs. cit.).

Ai sensi del successivo art. 12, co. 2 bis, d.lgs. cit., "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (art. 1, lett. q-bis, d.lgs. 11/2010).

I prestatori di servizi di pagamento sono tenuti a utilizzare l'autenticazione forte "quando l'utente:

- a) accede al suo conto di pagamento on-line;
- b) dispone un'operazione di pagamento elettronico;
- c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi" (art. 97, comma 1, direttiva UE 2015/2366; art. 10-bis, comma 1, d.lgs. 11/2010).

In relazione alla disciplina richiamata, il Collegio di Coordinamento ha in più occasioni precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo

ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014. Più di recente, cfr. Coll. Coord., decisione n. 22745/2019, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).

4. Fatte queste premesse, venendo al caso di specie, le operazioni contestate consistono essenzialmente in operazioni di prelievo, 4 in modalità cardless e 7 con utilizzo della carta fisica.

Con riferimento alle transazioni cardless, l'intermediario afferma che è stato utilizzato un sistema di autenticazione forte, riconducibile alla procedura primaria, attraverso l'inserimento del codice *****ID al ricevimento della notifica in App. Secondo l'intermediario, tale processo di autenticazione garantirebbe la compliance con la normativa in materia di SCA grazie all'utilizzo di due fattori: il codice *****ID (fattore di conoscenza) e l'app installata sul device del cliente (fattore di possesso). In particolare, il resistente chiarisce che, ai fini dell'utilizzo del *****ID, è necessario preliminarmente installare l'app sul device, per poi procedere con l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e con la configurazione del codice "*****ID" tramite l'inserimento dei seguenti fattori:

- 1) le credenziali di accesso ai servizi di internet banking (username e password);
- 2) i dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (nel caso della carta PAN, CVV2 e data di scadenza);
- 3) la password dinamica "usa e getta" (c.d. "OTP") inviata via SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento.

Più in dettaglio, per i prelievi cardless, l'intermediario rileva che è necessario indicare la sezione "Prelievo senza carta" dall'APP e successivamente recarsi presso un Atm Postale, dove deve essere selezionato il pulsante dedicato; all'esito, l'interessato deve inquadrare il codice QR mostrato sullo schermo dell'ATM, inserire l'importo che desidera prelevare e confermare cliccando su "Procedi"; infine, è necessario confermare l'operazione inserendo il codice *****ID e digitare il tasto "Conferma". Sul punto, l'intermediario sostiene che, in considerazione delle modalità con cui sono state autorizzate, le operazioni disconosciute potevano essere eseguite soltanto dal titolare dello strumento di pagamento, che è in possesso del device sul quale è installata l'APP. Inoltre, nelle date relative ai prelievi cardless, risulta l'autenticazione nella home banking del ricorrente con l'inserimento del codice di sicurezza "*****ID".

Senonché, per quanto specificamente riguarda la fase dispositiva, la documentazione prodotta dall'intermediario risulta lacunosa e non idonea a provare la SCA. In particolare, se risulta dimostrato l'utilizzo del dispositivo del ricorrente (fattore di possesso), in ordine al secondo fattore di autenticazione l'intermediario non chiarisce il significato del codice "NSC" in corrispondenza della colonna MOD. DISP, né fa cenno ad un possibile riutilizzo del fattore di conoscenza *****ID.

Pertanto, questo Collegio – uniformandosi a quanto deciso dai Collegi territoriali relativi a casi analoghi (cfr. in particolare Collegio di Milano, decisione n. 1099/2026; decisione n. 1446/2025) – ritiene non provata la SCA relativamente alle 4 operazioni in modalità cardless, rammentando che la mancanza, anche parziale, della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

5. Con riferimento alle 7 operazioni di prelievo tramite carta fisica, l'intermediario deduce che le stesse sono state effettuate senza errori di digitazione del PIN. A sostegno di quanto affermato, il resistente produce idonea evidenza, corredata di legenda esplicativa delle voci indicate.

Pertanto, in base alle risultanze documentali presenti in atti, deve ritenersi che parte resistente abbia fornito la prova dell'autenticazione e della formale regolarità delle operazioni di prelievo con carta fisica (da ultimo, Collegio di Bari, decisione n. 279/2026).

6. Passando all'esame della condotta del ricorrente, nel modulo di disconoscimento quest'ultimo ha dichiarato che custodiva abitualmente la carta in auto nonché di aver ceduto, "anche temporaneamente", la carta a terzi, di aver rivelato le credenziali di sicurezza per l'accesso in app o alla piattaforma online e di aver subito il furto del dispositivo mobile su cui riceveva i codici non riutilizzabili ai fini dell'autenticazione. Il ricorrente precisa che il furto, lo smarrimento, l'uso non autorizzato o sospetto delle credenziali non sono mai stati comunicati all'intermediario. Inoltre, il ricorrente non ha depositato in atti alcuna denuncia ma, in sede di repliche, ha dichiarato di aver conservato il PIN unitamente alla carta.

Per di più, dalla documentazione prodotta dall'intermediario in sede di controdeduzioni emerge che le operazioni disconosciute sono intervallate da operazioni genuine, alcune delle quali riconducibili alla medesima tipologia dei pagamenti asseritamente non autorizzati.

Orbene, il consolidato orientamento di questo Arbitro ha più volte osservato che rileva, ai fini della configurazione della colpa grave, anche l'omesso controllo del conto corrente cui è associata la carta per un notevole lasso di tempo, poiché il monitoraggio dell'andamento del conto di appoggio consente al titolare dello strumento di pagamento di avere contezza delle operazioni effettuate tramite la carta e di intercettare eventuali utilizzi non autorizzati (cfr. Collegio di Bari, decisione n. 7364/2024; Collegio di Bologna, decisione n. 15175/2022).

Deve quindi ritenersi sussistente la colpa grave del ricorrente, il che comporta la non rimborsabilità delle 7 operazioni di prelievo effettuato con carta fisica di cui l'intermediario ha fornito idonea prova della SCA.

7. Alla luce delle considerazioni svolte, la domanda del ricorrente può trovare parziale accoglimento in relazione alle sole operazioni di prelievo cardless, relativamente alle quali risulta non provata la SCA.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 1.820,00.

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