

COLLEGIO DI NAPOLI

composto dai signori:

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

Relatore FULVIO GIGLIOTTI

Seduta del 13/01/2026

FATTO

1. Con ricorso presentato in data 30.5.2025 – previo regolare reclamo del 4.2.2025, riscontrato negativamente dall'intermediario resistente – il ricorrente ha riferito che:

- lo stesso era titolare di una carta prepagata *business*, scaduta a febbraio 2024;
- dopo aver chiesto chiarimenti in filiale per la mancata sostituzione della carta, gli veniva comunicato che vi erano problemi di spedizione e che la situazione sarebbe stata risolta a breve;
- il 31/01/2025 riceveva una chiamata da un numero apparentemente riconducibile all'intermediario resistente. L'interlocutore dimostrava di conoscere i suoi dati anagrafici, lo informava del ritardo nella consegna della nuova carta, dichiarava di essere in possesso della nuova carta, a lui intestata. Richiedeva conferma dei dati e il codice di sblocco per la nuova carta, convincendolo della legittimità della chiamata;
- a seguito della interlocuzione telefonica, il 04/02/2025 venivano sottratti € 85.162,00 dalla nuova carta (mai attivata, né in possesso del ricorrente);

A seguito del riscontro negativo al reclamo, ha quindi presentato ricorso all'Arbitro, chiedendo il rimborso integrale delle somme sottratte, pari a € 85.162,00, oltre il risarcimento dei danni,

quantificandoli in una misura pari al 15% dell'importo sottratto.

2. Si è costituito l'intermediario, ipotizzando che il ricorrente sia rimasto vittima di *boxing* e *social engineering* (fattispecie in cui il titolare di uno strumento di pagamento viene contattato telefonicamente da un falso addetto dell'intermediario il quale, essendo in possesso dei suoi dati personali, si guadagna la sua fiducia estorcendogli il PIN).

Tanto premesso, ha poi dedotto e documentato che:

- la somma inizialmente sottratta a parte ricorrente era pari ad € 85.162,00, ma esso intermediario ha recuperato parzialmente i fondi trasferiti su altri strumenti di pagamento, per un totale di € 55.840,18 e ha anche provveduto a rimborsare al cliente il 50% del restante importo, per un totale di € 14.658,15 (dando evidenza che gli accrediti al ricorrente sono avvenuti sul libretto postale);
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- nei casi di *boxing*, il PIN associato alla carta in scadenza rimane invariato e quindi deve necessariamente essere utilizzato anche per l'attivazione della carta nuova, spedita per scadenza della precedente;
- non è stata generata dal sistema alcuna richiesta di un nuovo PIN fin dalla prima emissione della carta scaduta e poi rinnovata.

Su queste premesse – ritenuto che, nella specie, per consolidato orientamento, la responsabilità deve essere ripartita equamente tra intermediario e cliente – ha poi osservato che sussiste senz'altro la colpa grave del ricorrente, in quanto – oltre a lamentare una frode non altrimenti circostanziata – esso ha comunque comunicato, verosimilmente, ad un falso addetto dell'intermediario il proprio PIN (atteso che le operazioni disconosciute sono state effettuate tutte dopo lettura del *microchip* ed autenticazione del codice).

Ha anche precisato di *mettere a disposizione* il servizio di sms *alert*, il quale può essere attivato gratuitamente ed offre la possibilità di mantenere sotto controllo i movimenti relativi alla Carta; e che l'informativa al cliente sulle operazioni in uscita e in entrata viene trasmessa tramite servizio di *push notification* in App, che consente al cliente di ricevere una notifica in App per ogni operazione effettuata e ricevuta dalla propria carta (servizio attivo di *default*) ed il Servizio di SMS *alert*, per i clienti che non dispongono dell'App.

Il blocco della carta è stato richiesto soltanto dopo il compimento delle operazioni disconosciute.

Ha quindi concluso per il rigetto del ricorso (evidenziando anche, quanto alla domanda di risarcimento del danno, l'inaammissibilità della stessa per mancata preventiva proposizione nel reclamo, nonché l'assenza di prova del danno).

3. In sede di repliche, parte ricorrente – dando atto dei rimborsi intanto intervenuti – ha insistito nelle proprie richieste, limitate (in ragione di quanto già restituitogli) alla somma di euro 14.658,15, riferita al 50% di quanto non recuperato (€ 29.318,30), nonché il risarcimento di tutti i danni subiti, pari al 15% dell'importo così delimitato (*in realtà, eseguiti correttamente i conti di quanto sottratto, recuperato e rimborsato, la somma residua risulterebbe di euro 14.663,67; ma parte ricorrente ha chiesto la somma di euro 14.658,15 euro e a questa richiesta – in conformità di quanto dettato dall'art. 112 c.p.c. – il Collegio farà quindi riferimento*).

Parte resistente, controreplicando, si è riportata a tutto quanto già eccepito e controdedotto, insistendo nel richiedere il rigetto del presente ricorso, in quanto infondato in fatto ed in diritto.

DIRITTO

4. Ritiene il Collegio, per le ragioni di seguito illustrate, che il ricorso sia (parzialmente) da accogliere.
5. Preliminarmente, rileva il Collegio che, pur non risultando in atti evidenza del contratto stipulato tra le parti, è pacifico che si tratti, nella specie, di operazioni effettuate attraverso una carta prepagata “*business*”, riservata quindi, come si desume dal sito internet della resistente, ai possessori di Partita Iva e alle Ditte Individuali.

Deve quindi riqualificarsi la posizione del ricorrente come “non consumatore”.

6. 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, relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13 gennaio 2018; le fonti normative che, nel contesto considerato, regolano la c.d. “autenticazione forte” (in gergo, individuata dall’acronimo SCA: *strong customer authentication*) sono rinvenibili negli artt. 97 e 98 della PSD2, nell’articolo 10-*bis* del D. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall’EBA (*European Banking Authority*) 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 (in particolare, parere del 21 giugno 2019).

Secondo le previsioni normative sopra richiamate, la responsabilità di un Prestatore dei servizi di pagamento (PSP) è esclusa quando, *avendo esso dato prova di utilizzare meccanismi di “autenticazione forte” dell’utente*, sia anche riuscito a dimostrare una condotta dolosa o gravemente colposa dell’utente del servizio (con la precisazione che si intende per “autenticazione forte” 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).

Più in particolare, 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 non è di per sé necessariamente sufficiente a dimostrare che l’operazione sia stata autorizzata dall’utilizzatore 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 D. lgs. n. 11/2010.

Piuttosto, sarà onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell’utente: in mancanza di ciò, egli sarà tenuto responsabile dei pregiudizi subiti dall’utente, in ragione del rischio d’impresa sopportato.

Ne consegue che l’intermediario non si libera dalla responsabilità provando la mera regolarità formale delle transazioni, dovendo lo stesso, ai sensi dell’art. 10 del D. lgs. n. 11/2010, documentare elementi di fatto che caratterizzano le modalità esecutive dell’operazione dai quali possa trarsi la prova, anche in via presuntiva, della colpa grave (o del dolo) dell’utente (cfr. Collegio di Coordinamento ABF, n. 22745 del 10 ottobre 2019).

In tema di spedizione degli strumenti di pagamento, poi, viene in rilievo, il comma 2 dell’art. 8 del D.lgs 11/2020, ai sensi del quale: “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*”.

7. Nel caso di specie, per quanto emerso in atti, risulta che:

- la somma fraudolentemente sottratta era (inizialmente) pari a euro 85.162,00;
- l'intermediario ha recuperato la somma di euro € 55.840,18 e rimborsato al cliente il 50% (€ 14.658,15) del restante importo (€ 29.318,30) non recuperato;
- la perdita subita da parte ricorrente è quindi residuata nella misura di euro 14.658,15 (secondo quanto richiesto da parte ricorrente: cfr. *supra*, § 3 delle considerazioni in "fatto"), alla quale (oltre ai pretesi danni) è stata limitata la richiesta definitiva del ricorrente, come formulata in sede di repliche;
- le operazioni contestate sono state eseguite con la carta appena attivata;
- la nuova carta è stata attivata alle ore 16:34 del 31/01/2025, presso uno sportello ATM dell'intermediario (così è emerso dalla documentazione versata in atti);
- le operazioni fraudolente sono state autorizzate mediante lettura del *microchip* della carta e corretto inserimento del relativo codice PIN.

Deve quindi concludersi (come già deciso da altri Collegi: cfr. Coll. ABF Milano, nn. 3939/2024 e 10877/2024) che le operazioni in contestazione risultano correttamente autenticate mediante i fattori del possesso (la carta) e della conoscenza (il codice PIN).

Sotto altro profilo, è altresì emerso che parte resistente non ha fornito evidenza dell'avvenuta consegna della nuova carta al ricorrente; la stessa ha comunque evidenziato (con circostanza non contestata dalla ricorrente) che in tutti i casi di carta rinnovata a scadenza, il PIN rimane invariato rispetto a quello associato alla carta di prima emissione e scaduta; è anche emerso che – secondo la ricostruzione della stessa parte ricorrente – il ricorrente veniva contattato telefonicamente da parte di un sedicente operatore dell'intermediario convenuto, che lo invitava a fornire dati necessari all'attivazione della nuova carta, essendo quella attualmente in suo possesso prossima alla scadenza; e che essa parte ricorrente (per sua espressa ammissione) ha comunicato al proprio interlocutore i dati richiesti.

8. Per quanto fin qui esposto, deve allora ritenersi provata la procedura di SCA, ma anche, almeno, un concorso di colpa delle parti, in ragione della *spedizione non sicura da parte dell'intermediario* (a cui carico è, per espressa previsione normativa, il rischio della spedizione) e della incauta condotta del ricorrente, desumibile dalle circostanze di fatto sopra riferite.

In proposito, secondo un consolidato orientamento dei Collegi, in caso di truffa realizzata con il contestuale utilizzo delle tecniche del c.d. *social engineering* e del c.d. *boxing*, è possibile ravvisare un concorso di colpa; tuttavia, secondo orientamento altrettanto consolidato, la colpa del cliente rileva solo nel caso in cui l'operazione contestata sia stata autorizzata previa autenticazione forte, quindi solo nel caso in cui siano tracciati i due elementi di identificazione: nel caso di specie possesso (carta) e conoscenza (PIN).

Risultando provata, nella specie, la procedura di SCA, il concorso di colpa del ricorrente assume rilievo, e dovrebbe determinare, secondo l'orientamento consolidato, una ripartizione dell'ammanto al 50% tra le parti (così come è avvenuto).

9. Nondimeno, osserva anche il Collegio che – secondo quanto statuito da Coll. coordinamento 8853/2019 – è ravvisabile un obbligo dell'intermediario di predisporre servizio di sms *alert* (o assimilabili), attraverso il quale l'utente sia messo in grado di qualificare il pagamento registrato come non autorizzato; e che l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene, mentre gli effetti della mancata adozione del servizio di *alert* dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto.

In conformità a tale indirizzo, i Collegi territoriali ABF ritengono comunemente che la mancata

attivazione del servizio di *sms alert* (o altro assimilabile, come notifica tramite app dell'intermediario oppure *e-mail*, con una valutazione di equivalenza da condurre caso per caso) costituisca, in genere, un profilo (assorbente) di responsabilità dell'intermediario, salvo l'esplicito rifiuto dell'utente ad avvalersene (e salvo che si tratti di operazione *unica*, o di operazioni plurime poste in essere a così ravvicinata distanza di tempo l'una dall'altra (meno di cinque minuti) da non consentire, utilmente, interventi idonei ad impedire la consumazione delle ulteriori condotte fraudolente).

Nel caso di specie, dalla documentazione in atti non consta l'attivazione del servizio di *alert*, né il rifiuto dell'utente di avvalersene; mentre risulta che l'attivazione fraudolenta della nuova carta è avvenuta – peraltro, direttamente presso ATM dell'intermediario – *ben 4 giorni prima della esecuzione dei prelievi fraudolenti*, per cui, certamente, un SMS al ricorrente, avente ad oggetto l'avvenuta attivazione, avrebbe potuto scongiurare il compimento delle operazioni (consistenti, peraltro, in ben 13 operazioni concentrate in un tempo inferiore a 24 ore, con ciò concretizzandosi anche un chiaro indice di frode ai sensi del punto 1 della lett. b) dell'art. 8 d.m. n. 112/2007, che fa riferimento all'ipotesi di 7 o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento).

Ne consegue che, a giudizio del Collegio, la condotta di parte resistente è risultata tale da avere *interamente determinato* la perdita subita dal ricorrente: perdita della quale, pertanto, parte resistente dovrà farsi carico, risultando perciò tenuta a rimborsare al ricorrente (nei limiti di quanto da esso domandato) la somma di euro 14.658,15, da arrotondare a euro 14.658,00.

10. Nessuna evidenza, invece, è stata fornita in ordine al preteso danno, quantificato da parte ricorrente nella misura del 15% di quanto dovutogli a titolo di rimborso. Ne consegue che la domanda di danni non può essere accolta.

11. Per le ragioni fin qui esposte, quindi, ritiene il Collegio che parte resistente sia tenuta a corrispondere al ricorrente la somma di euro 14.658,00.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente alla restituzione dell'importo di € 14.658,00.

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