

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) NUZZO	Membro designato dalla Banca d'Italia
(BA) BUSSOLI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 09/02/2026

FATTO

Parte ricorrente, titolare di conto corrente presso la banca resistente, afferma che in data 23 maggio 2025, controllando il proprio estratto conto, si era accorta della presenza di n. 14 disposizioni di pagamento in favore di soggetti terzi a lei sconosciuti ed eseguite senza la sua autorizzazione, per un ammontare complessivo di € 2.185,06.

Reclama di non aver ricevuto alcun sms di avviso, né alcuna notifica dall'App della Banca per nessuna delle predette operazioni, nonostante l'istituto bancario fosse a conoscenza del suo recapito telefonico. Fa presente di essersi recata in filiale per effettuare il disconoscimento delle operazioni e che, in data 29 maggio 2025, si era rivolta alle competenti autorità per presentare denuncia.

Ritiene la banca responsabile del danno economico subito, in quanto la normativa di settore impone agli operatori bancari e finanziari di adeguare i propri sistemi di protezione all'evoluzione delle tecniche di frode, al fine di tutelare la propria clientela da accessi non autorizzati ai conti correnti, ai sensi dell'art. 11 del D.Lgs. n. 11/2010.

Precisa di non aver fornito a nessuno i dati di accesso al predetto conto corrente e nega di aver mai ricevuto alcun OTP, necessario per “finalizzare” le disposizioni di pagamento, ai sensi dell'art. 10-bis del D.Lgs. n. 11/2010.

Chiede, pertanto, il rimborso della complessiva somma di € 2.185,06, oltre interessi legali.

Costitutosi, l'intermediario contesta alla cliente le precedenti dichiarazioni da lei rese, con le quali sosteneva di *"non voler intraprendere alcuna azione nei confronti dei presunti responsabili dell'accaduto"*, essendo sua intenzione avviare solo una *"pratica di rimborso"* nei confronti dell'Istituto bancario. Contesta, inoltre, il mancato avvio di tale procedura secondo le modalità previste contrattualmente.

Sostiene che, mentre la ricorrente dichiara di essersi avveduta delle operazioni fraudolente solo a distanza di circa due mesi dall'ultima operazione compiuta, dalle verifiche tecniche effettuate emerge che dal medesimo device, nel periodo compreso tra il 12 ottobre 2024 e il 7 marzo 2025, erano stati registrati 127 accessi al servizio di home banking, 13 dei quali riferibili alle operazioni poi disconosciute. Precisa che tale device è quello certificato e in uso alla ricorrente, e che lo stesso è tutt'ora utilizzato *"regolarmente"* per accedere ai servizi di *home banking*.

Contesta alla ricorrente di essersi accorta delle presunte operazioni fraudolente il 25 maggio 2025 mentre la comunicazione all'intermediario è avvenuta il 5 giugno 2025, anche in merito ad operazioni risalenti ad ottobre 2024.

Dichiara che, dall'analisi della movimentazione complessiva del periodo in esame, emerge che la ricorrente ha ricevuto plurimi bonifici in entrata dall'estero, di *"modesto importo"*, provenienti da soggetti e istituti di diversa nazionalità, con causali eterogenee (*"lavoro"*, *"pagamento"*, *"amico"*) e da lei non disconosciuti. Precisa che tali accrediti avevano costituito la provvista dei successivi bonifici in uscita, questi ultimi disconosciuti.

Inoltre, sottolinea che la ricorrente avrebbe disconosciuto un bonifico in uscita (14 novembre 2024), ma *"riconosciuto"* un bonifico in entrata da parte dello stesso soggetto: tale circostanza lascerebbe presumere l'esistenza di *"rapporti economici bilaterali"* tra lei e i terzi ordinanti.

Sempre dall'analisi della movimentazione, emergerebbe che tutti i bonifici in uscita erano stati disposti non già utilizzando una *"provvista preesistente"* sul conto, bensì a seguito di versamenti o accrediti specificamente effettuati per costituirla, in gran parte coincidenti per importo e tempistica con le operazioni disconosciute. In particolare, le operazioni in entrata ammontano complessivamente a circa € 2.316,00, importo sostanzialmente coincidente con la somma dei bonifici oggi disconosciuti.

Ritiene, pertanto, che o la cliente era vittima di una truffa finanziaria, in ragione della quale avrebbe effettuato versamenti connessi a presunti investimenti e/o opportunità economiche (ciò spiegherebbe i versamenti eseguiti in prossimità dei bonifici in uscita), oppure che la stessa avesse aderito inconsapevolmente a un'offerta lavorativa fraudolenta, divenendo parte di uno schema di trasferimento di fondi riconducibile a un fenomeno di *"money mule"* (a tal proposito richiama la propria campagna di sensibilizzazione sul tema). In ogni caso, fa presente che entrambe le ipotesi escludono l'estraneità della ricorrente alle operazioni e fanno emergere un comportamento *"imprudente e reticente"*, tale da non poter giustificare la pretesa restitutoria avanzata.

Evidenzia, altresì, che sia l'art. 8 del D.Lgs. n. 11/2010, sia l'art. 70 della Direttiva (UE) 2015/2366, non impongono al PSP un obbligo di monitoraggio preventivo o di blocco delle operazioni in presenza di importi o frequenze considerate *"anomale"*.

Conclude sostenendo che tutte le disposizioni di pagamento impartite dalla cliente risultano conformi rispetto alla Strong Customer Authentication (S.C.A.), poiché eseguite attraverso: il dispositivo personale certificato (elemento di possesso); l'autenticazione biometrica (elemento di inerenza) non riproducibile da terzi; in un caso, anche mediante OTP inviato al numero di telefono personale della ricorrente. Alla luce di ciò, ritiene assente qualsiasi elemento che potesse indurre la banca a rilevare

come anomale o fraudolente le operazioni contestate, risultando piuttosto *“perfettamente”* compatibili con il comportamento abituale della cliente.

Chiede, pertanto, di respingere il ricorso, in quanto infondato.

In sede di repliche, la ricorrente ritiene *“giuridicamente infondata”* l'affermazione di controparte secondo cui avrebbe *“limitato la portata”* della denuncia, ovvero omesso di avviare formalmente la procedura di rimborso. Richiama quanto disciplinato dagli artt. 10 e 11 del d. lgs. n. 11/2010, secondo cui l'obbligo di rimborso non può essere subordinato a formalismi estranei alla normativa né alla scelta dell'utente di adire o meno l'autorità giudiziaria in sede penale nei confronti degli autori della frode. Sostiene che la denuncia in questione ha valore meramente dichiarativo della *“non riconducibilità soggettiva delle operazioni”*, ma non riguarda il suo diritto alla restituzione delle relative somme.

Quanto all'assunto della banca secondo cui avrebbe *“verificato tardivamente”* i movimenti del conto corrente, fa presente che la disciplina PSD2 non impone controlli giornalieri né attribuisce alcun rilievo alla maggiore o minore frequenza delle verifiche compiute dall'utente, il quale è tenuto unicamente a notificare il disconoscimento, come peraltro avvenuto nel caso in esame.

Eccepisce che l'imputabilità delle operazioni alla ricorrente, desumibile dalla provenienza delle stesse dal suo device, sarebbe carente sotto il profilo tecnico e giuridico. In particolare, contesta che: manchi la prova della corretta esecuzione della S.C.A. relativa a ciascun pagamento contestato; l'utilizzo del *“medesimo smartphone”* non integra prova dell'autorizzazione dell'operazione viste le tecniche fraudolente di *“compromissione”* dei dispositivi; la banca non produce alcun *log* attestante l'invio, la ricezione e l'utilizzo dei codici dispositivi né prova l'assenza di anomalie.

Ritiene *“del tutto priva di fondamento”* la tesi avversa secondo cui vi sarebbe una presunta *“coerenza”* tra gli accrediti ricevuti e le successive operazioni disconosciute, in quanto: gli accrediti esteri in entrata hanno natura eterogenea, importi contenuti e causali generiche che non consentono alcuna correlazione logica; le causali dei bonifici disconosciuti ricalcano quelle frequentemente utilizzate nelle frodi; la ricostruzione proposta dalla banca è fondata su un'argomentazione priva di riscontro probatorio.

Richiama il principio elaborato dall'ABF secondo cui, in presenza di operazioni disconosciute, spetta alla banca dimostrare che esse siano state autorizzate dall'utente, o che quest'ultimo abbia agito con dolo o colpa grave. Eccepisce che, in questo caso, non è stata dimostrata l'autenticazione delle operazioni, non è stato provato l'utilizzo consapevole dei codici dispositivi e non è stato dimostrato alcun comportamento gravemente negligente della cliente, né documentata l'assenza di possibili compromissioni del sistema.

Conclude insistendo nell'accoglimento delle domande formulate in sede di ricorso.

In sede di controrepliche, la banca resistente afferma che la ricorrente non esclude che, sotto il profilo oggettivo, le operazioni fossero state eseguite dalla stessa, considerato che in sede di repliche afferma che la denuncia avrebbe valore meramente dichiarativo della presunta non riconducibilità *“soggettiva”* delle operazioni alla ricorrente. Sottolinea che, alla luce dell'ammissione di *“oggettiva riconducibilità”*, è introdotto un ulteriore profilo di criticità rappresentato dalla contraddittorietà dell'atteggiamento tenuto dalla ricorrente che, da un lato riconosce oggettivamente le operazioni riportate in estratto conto, ma dall'altro ne nega la paternità soggettiva. Ritiene che la ricorrente sia consapevole della perfetta rispondenza tra operazioni in entrata e in uscita, e proprio per questo ritiene abbia rielaborato gli estratti conto prodotti dalla banca, selezionando solo le operazioni disconosciute, limitando il suo diritto di difesa.

Eccepisce che non sono stati prodotti elementi idonei a qualificare l'accaduto come frode.

Contesta le dichiarazioni della ricorrente sull'assenza di procedure da seguire per il disconoscimento delle operazioni richiamando, invece, l'art. 7, comma 1, lett. b) del d.lgs. 11/2010 che prevede l'obbligo per l'utilizzatore di comunicare senza indugio, secondo le modalità indicate nel contratto, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento di pagamento, non appena ne venga a conoscenza. Precisa che la ricorrente non avrebbe avviato le procedure formali di disconoscimento delle operazioni, ritenendo di disattendere i termini contrattuali che prevedono il coinvolgimento di altra società.

Chiarisce che la ricorrente aveva fatto ampiamente uso dei servizi di Digital Banking, senza mai sollevare alcuna contestazione in merito alle operazioni eseguite. Precisa che la ricorrente non era venuta a conoscenza delle operazioni disconosciute in data 23 maggio 2025, bensì le aveva eseguite "*consapevolmente*".

Evidenzia che la cliente non aveva mai segnalato un malfunzionamento del proprio smartphone sia nel periodo in esame, sia successivamente. Inoltre, esclude che nell'ipotesi di "*Remote Device Takeover*" possano essere superati i presidi previsti dalla SCA, e che dall'esame dei log non è rilevabile alcun tentativo di "*push bombing*".

Ribadisce, inoltre, che il comportamento "*selettivo e incoerente*" della ricorrente, che ha riconosciuto i bonifici in entrata provenienti dai medesimi soggetti ai quali, successivamente, aveva trasferito le somme poi disconosciute, sia riconducibile agli eventi di *Money Mule*. Sottolinea poi che la ricorrente non nega in alcun modo l'utilizzo del proprio smartphone, limitandosi a invocare ipotesi di frode non dimostrate, non dimostrabili e, soprattutto, incompatibili con l'effettivo andamento delle operazioni.

Conclude insistendo per l'accoglimento delle conclusioni formulate in sede di controdeduzioni.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto al rimborso dell'importo di € 2.185,06 corrispondente al controvalore della somma di n. 14 operazioni di pagamento, eseguite nel periodo tra il 12 ottobre 2024 e il 7 marzo 2025 e successivamente disconosciute.

In via preliminare, il Collegio rileva che tali operazioni 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 gennaio 2018. Inoltre, le operazioni contestate dalla ricorrente sono state eseguite successivamente all'entrata in vigore delle 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).

La disciplina 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, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento della Banca d'Italia del 5 luglio 2011.

In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore 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". Il comma 2 del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore 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'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" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è, altresì, precisato che "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".

Ai sensi del successivo art. 12, comma 2 bis, "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). Deve, inoltre, ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpirlo via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione.

Si deve, altresì, rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente 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".

Al riguardo, 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). 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. Coordinamento, decisioni n. 3947/2014 e, da ultimo, 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, comma 2, d.lgs. n. 11/2010).

Tratteggiato il quadro normativo di riferimento, venendo al caso di specie, ritiene il Collegio che il ricorso possa trovare parziale accoglimento, nei termini qui di seguito specificati.

In primo luogo, va rilevato che l'intermediario ha fornito adeguata prova del corretto svolgimento delle procedure di autenticazione, registrazione e contabilizzazione di tutte le operazioni contestate, tranne la prima di € 54,05.

Difatti, la banca non ha prodotto in atti i log relativi all'operazione di € 54,05 effettuata *“in modalità internet”* mediante la carta di debito collegata al conto corrente; mentre, con riferimento alle altre operazioni contestate, la banca ha prodotto evidenze dalle quali si evince che le stesse sono state eseguite mediante l'utilizzo dei seguenti fattori: il dispositivo personale certificato (fattore di possesso); autenticazione biometrica (fattore di inerenza); in un caso, anche mediante il *“criterio aggiuntivo di sicurezza”*, cioè l'OTP inviato al numero di telefono personale della ricorrente (fattore di conoscenza). Segnatamente, l'intermediario ha prodotto le schermate con i log relativi alla corretta autenticazione sia della fase di accesso all'app (precisando che: il *“Tipo Browser”* riportava il dispositivo del Cliente; la voce *“App_Enroll”* indicava che il Login era avvenuto attraverso il dispositivo certificato; la voce *“MT_BIOMETRICO”* indicava che l'accesso era avvenuto tramite l'elemento di inerenza; il brevissimo intervallo temporale tra invio e conferma della notifica push in app dimostrava che l'autorizzazione era stata rilasciata in tempo reale dal titolare del dispositivo); sia della fase autorizzativa di ciascuna operazione.

Inoltre, deve ritenersi sussistente la colpa grave della ricorrente, la quale non ha fornito elementi idonei a comprovare la dinamica della truffa. Secondo l'orientamento dell'Arbitro, nelle contestazioni di utilizzi fraudolenti online di strumenti di pagamento in cui, come nel caso di specie:

- i. l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute;
- ii. il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA);
- iii. non risultano indici di anomalia delle operazioni e/o ulteriori elementi;

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo (cfr. Collegio di Bari, decisioni n. n. 8247/2024; e n. 7144/2023).

Ciò premesso, il Collegio rileva che, nel caso di specie, appare comunque censurabile la condotta della banca resistente, sotto il profilo della mancata attivazione del sistema di alert. Difatti, dalla documentazione in atti, non risultano notifiche ricevute dalla ricorrente sulla base dell'attivazione del servizio di alert. Orbene, fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene (Collegio di Coordinamento, decisione n. 24366/2019). Inoltre, secondo le posizioni condivise dai Collegi, la mancata attivazione ovvero il mancato funzionamento del servizio di alert (o di servizio assimilabile) sono ritenuti irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'alert non potrebbe in concreto limitare il pregiudizio dell'utente. Tali esenzioni non riguardano il caso di specie in cui le 14 operazioni disconosciute sono state eseguite tra il 12 ottobre 2024 ed il 7 marzo 2025 e la banca, sul punto, non ha preso posizione.

D'altra parte, va osservato che gli effetti della mancata adozione del servizio di alert devono essere valutati alla stregua delle circostanze di fatto del caso concreto. In tale ottica, va evidenziato che la ricorrente si è limitata a produrre le parti di estratto conto relative ad operazioni dalla stessa disconosciute, omettendo invece una serie di altre operazioni in entrata provenienti dall'estero, non disconosciute. In particolare, dalla lista movimenti allegata dalla banca, si nota che, in taluni casi, la ricorrente ha disconosciuto il bonifico disposto in favore di un certo beneficiario, ma ha ommesso di disconoscere il bonifico in entrata proveniente dalla stessa persona. Inoltre, la ricorrente ha dichiarato di essersi accorta delle operazioni in esame il 23 maggio 2025, mentre la comunicazione alla banca è avvenuta solo in data 5 giugno 2025, a fronte di operazioni risalenti anche al mese di ottobre 2024. Tale condotta sembra censurabile per violazione del principio, affermato recentemente dalla Corte di Giustizia UE, secondo il quale *"l'utente di servizi di pagamento è privato, in linea di principio, del diritto di ottenere la rettifica di un'operazione se non ha informato senza indugio il suo prestatore di servizi di pagamento di essere venuto a conoscenza di un'operazione di pagamento non autorizzata, sebbene lo abbia informato riguardo alla medesima nei tredici mesi successivi alla data di addebito"* (Corte di Giustizia UE, 1° agosto 2025, causa C-665/23).

Alla luce di tali considerazioni, ritiene il Collegio che la domanda di rimborso della ricorrente possa trovare parziale accoglimento nella misura, ritenuta equa, di € 1.000,00 comprensivi degli interessi legali.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 1.000,00.

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