

COLLEGIO DI BARI

composto dai signori:

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

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 12/01/2026

FATTO

La ricorrente riferisce di essere stata vittima di una truffa “*di tipo phishing*”, a seguito della quale ha subito la sottrazione della somma complessiva di € 2.630,00.

Lamenta il diniego opposto dall'intermediario resistente alla propria richiesta di rimborso.

Costituitosi, l'intermediario resistente afferma che la ricorrente è titolare di carta di debito n. ***303 e richiede nel presente procedimento il rimborso della somma pari ad € 2.630,00, in seguito ad un'operazione di pagamento autorizzata online il 28 luglio 2025 tramite App.

Precisa che l'operazione è stata eseguita solo in seguito alla “*autenticazione forte del cliente*”, considerato che risultano regolarmente avvenute:

- la fase di *enrollment* della carta di pagamento al sistema autorizzativo di tipo dinamico, avvenuta il 28 maggio 2025;
- la fase di *login* all'home banking mediante inserimento del codice *****ID in App;
- la fase dispositiva dell'operazione oggetto di ricorso, per la quale fornisce evidenza informatica attestante la modalità autorizzativa conforme alla SCA.

Precisa, altresì, che la fase di *login* non è in alcun modo collegabile a quella dispositiva, in quanto l'operazione in esame è stata autorizzata su un sito di e-commerce. In particolare, per tali operazioni, il cliente accede sul sito del merchant attraverso il quale vuole effettuare l'acquisto e, dopo aver inserito i dati dello strumento di pagamento e la propria password, per autorizzare l'operazione può ricevere una notifica in app e inserire come mezzo autorizzativo il codice ***id.

Ribadisce, pertanto, che, per questo tipo di operazioni, non è necessario effettuare log-in né in app né sul sito dell'intermediario.

In relazione alla previsione di un generale obbligo di monitoraggio in capo all'intermediario, richiama l'orientamento secondo cui “[i]mporre agli Intermediari di intervenire ogni qualvolta un’operazione superi, per importo o frequenza, uno schema di comportamento storico, comporterebbe una discrezionalità difficilmente compatibile con la ratio del sistema normativo” (Trib. Ancona, sentenza n. 338/2024).

Con riguardo ai principi fissati dall'art. 8 del D.M. n. 112/2007, richiama ABF Collegio di Torino, decisione n. 5576/2025, secondo cui “[a]llo stato non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all'intermediario, il quale non può evitare che i propri clienti dispongano liberamente delle somme di cui hanno la disponibilità sul presupposto – indimostrato ed indimostrabile – che ogni operazione anomala sarebbe di per sé truffaldina” (richiama, altresì, Collegio di Milano, decisione n. 6732/2025).

Rappresenta che le procedure di autenticazione forte adottate possono essere: la procedura “*primaria*” mediante notifica *push* in App ed inserimento del codice *****ID (formato da 6 caratteri e scelto dall'utente in fase di abilitazione dei prodotti finanziari in App); la procedura “*secondaria*” mediante OTP ricevuto a mezzo SMS e Password. Precisa che nel caso in esame è stata attivata la procedura “*primaria*” e che, per l'utilizzo di tale procedura, è necessario in via preventiva installare l'App sul device, associando lo strumento di pagamento e configurando il codice *****ID mediante inserimento delle credenziali di accesso (username e password), dei dati dalla carta prepagata (PAN, CVV2 e data di scadenza) e della password dinamica “*usa e getta*” inviata via SMS sull'utenza mobile fornita dalla cliente e associata allo strumento di pagamento.

Dopo aver ricostruito il funzionamento del codice *****ID, precisa che, qualora il cliente sbaglia l'inserimento del codice alfanumerico per più di 5 volte, è previsto il blocco del codice stesso.

Rappresenta, altresì, che non si è verificata alcuna modifica del device “*precedentemente enrollato*” o cambio dell'utenza telefonica in concomitanza con l'evento denunciato.

Ritiene, pertanto, di aver implementato un sistema conforme al dettato normativo, garantendo la sicurezza dei propri servizi, senza alcuna anomalia o malfunzionamento delle relative procedure (cita Collegio di Bologna, decisione n. 8345/2023, Collegio di Napoli, decisione n. 4824/2022, Collegio di Palermo, decisione n. 8442/2021).

Fa presente che, a fronte di un rischio di frode “*potenziale o accertato*”, è prevista l'attivazione di contromisure che hanno la finalità di tutelare il cliente, le quali consistono nell'inibizione dell'operatività della carta di pagamento; precisa che, nel caso in esame, il blocco della carta è avvenuto il 28 luglio 2025, alle ore 15:10, quindi successivamente rispetto all'operazione contestata.

Evidenzia, altresì, di mettere a disposizione della propria clientela il servizio di SMS Alert, il quale può essere attivato gratuitamente e offre la possibilità di controllare i movimenti relativi alla carta. Precisa che l'invio dell'informativa al cliente sulle operazioni in uscita/entrata viene trasmesso tramite SMS *Alert*, ovvero tramite notifica *push* in App come nel caso in esame.

Sostiene che il comportamento negligente della cliente si è manifestato nella modifica dei limiti di spesa della carta di pagamento, utili per l'esecuzione dell'operazione oggetto di ricorso.

Ritiene che la truffa subita dalla ricorrente sia inquadrabile nella fattispecie della “*manipolazione del pagatore*”, che si verifica qualora sia lo stesso titolare dello strumento di pagamento ad eseguire l’operazione contestata “*sotto la guida di un abile frodatore*” (cita Collegio di Coordinamento, decisione n. 5304/2013, Collegio di Roma, decisione n. 1851/2021).

Con riguardo alla nozione di colpa grave, sostiene che la stessa è da intendersi come una “*inescusabile imprudenza, negligenza o imperizia*” che si verifica in seguito alla violazione di quel “*grado minimo ed elementare di diligenza generalmente osservato da tutti*” (cita Collegio di coordinamento, decisioni n. 5304/2013 e 6168/2013, Collegio di Milano, decisioni n. 40/2012 e 2310/2011, Collegio di Roma, decisioni n. 1851/2024, 2157/2011 e 712/2010). Richiama la decisione n. 24366/2019 del Collegio di Coordinamento, secondo cui la valutazione della colpa grave dell’utente “*deve essere compiuta alla luce di tutte le circostanze di fatto che, di volta in volta, caratterizzano il caso di specie*”.

Richiama, altresì, l’orientamento assunto dai Collegi ABF secondo cui, nei casi di utilizzi fraudolenti online dello strumento di pagamento, qualora il cliente non abbia allegato le circostanze di fatto della frode e a fronte della prova di autenticazione e in assenza di indici di anomalia, la colpa grave del cliente si presume (cita Collegio di Bologna, decisione n. 4895/2024, Collegio di Bari, decisione n. 1998/2024, Collegio di Napoli, decisione n. 4789/2024, Collegio di Milano, decisione n. 13496/2021).

Saggiunge che, ai sensi dell’art. 8 del D.lgs. n. 11/2010, sono stati predisposti alcuni presidi, consistenti nella trasmissione con cadenza periodica di appositi avvisi, con cui sono resi edotti i clienti di eventuali comportamenti anomali che dovrebbero essere considerati come *alert*, e nella predisposizione di apposite pagine web in cui risulta presente un manuale di ausilio all’utente su come difendersi dalle truffe.

Conclude affermando che la condotta della ricorrente è stata connotata da una “*colpevole credulità*”, considerato che l’operazione in esame è stata autorizzata dalla stessa nel rispetto dei requisiti previsti dalla SCA.

In sede di repliche, la ricorrente allega copia di una comunicazione inviata a mezzo e-mail il 29 luglio 2025 alle competenti forze dell’ordine.

In sede di controrepliche, l’intermediario resistente conferma quanto già esposto in sede di controdeduzioni, insistendo per l’accoglimento delle conclusioni ivi formulate

DIRITTO

La domanda proposta dalla ricorrente è relativa all’accertamento del proprio diritto alla restituzione del controvalore di un’operazione di pagamento di € 2.630,00, effettuata online su un sito di e-commerce il 28 luglio 2025 tramite la carta di debito n. ***303 intestata alla stessa ed emessa dall’intermediario resistente. Tale operazione è stata successivamente disconosciuta.

In sede di denuncia, presentata alle competenti autorità in data 29 luglio 2025, la ricorrente ha ricostruito i fatti oggetto di controversia dichiarando di aver ricevuto sul suo cellulare – in data 28 luglio 2025, alle ore 13:28 – una chiamata dall’utenza n. ***79, riconducibile all’intermediario; l’interlocutore si è presentato come un operatore dell’intermediario, informandola che dal suo conto erano in corso dei tentativi di pagamento “*indirizzati*” verso uno stato estero. Il sedicente operatore le ha consigliato di “*congelare il saldo attuale*” presente sul suo conto, pari ad € 2.634,97, al fine di evitare che “*qualcuno potesse prelevare*”.

Ha dichiarato di aver seguito “*tutte*” le indicazioni fornite dal sedicente operatore, con particolare riguardo alla modifica dei massimali della carta al fine di aumentare l’importo dei pagamenti tramite

POS; a seguito di tale modifica, ha ricevuto sul suo smartphone una notifica di un movimento in uscita di € 2.630,00, senza aver avuto la possibilità di autorizzare o negare tale operazione che “*si completava*”.

Il predetto pagamento avveniva mentre era in linea con il presunto operatore, il quale l'ha rassicurata invitandola a presentarsi in filiale all'orario “*prestabilito*” e a comunicare il codice alfanumerico relativo alla sua pratica; non ha accettato la proposta del sedicente operatore volta a trasferire “*gli ulteriori fondi presenti in altri miei conti*”, chiudendo pertanto la conversazione e recandosi in filiale. In tale occasione, ha appreso dal Direttore della filiale che era stata vittima di truffa e ha provveduto a richiedere telefonicamente il blocco della carta di debito.

Tanto premesso, in via preliminare, il Collegio rileva che l'operazione di bonifico è stata eseguita 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, l'operazione contestata dalla ricorrente è stata eseguita 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 carpito 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).

Fatte queste premesse, venendo all’operazione in esame, il Collegio rileva che, come dichiarato da entrambe le parti, l’operazione contestata è stata preceduta dalla modifica dei massimali della carta di debito, finalizzata ad aumentare l’importo dei pagamenti tramite POS. In particolare, la stessa ricorrente dichiara di aver personalmente effettuato e autorizzato tale variazione, seguendo le indicazioni del sedicente operatore e l’intermediario, al riguardo, ha prodotto in atti la documentazione attestante la modifica dei limiti di spesa della carta in data 28 luglio 2025, poco prima dell’operazione contestata, allegando i relativi *log*, da cui si evince l’esecuzione con SCA di tale variazione.

Inoltre, si osserva che, ai fini dell’accertamento dell’autenticazione forte (SCA) dell’operazione di pagamento contestata, risulta determinante l’insieme delle prove prodotte in atti dall’intermediario. Difatti, quest’ultimo ha prodotto alcuni stralci dei *log*, corredati della relativa legenda esplicativa, in relazione all’operazione di pagamento contestata, eseguita online in data 28 luglio 2025 alle ore 13:39 tramite la modalità di pagamento “*primaria*”, la quale prevede l’invio di una notifica *push* in App e l’inserimento del codice ***id (formato da sei caratteri e scelto dall’utente in fase di abilitazione dei prodotti finanziari in App). Nella menzionata legenda sono riportati i codici utilizzati nei *log*. In particolare, è specificato che il “*deviceID*” rappresenta l’identificativo del telefono utilizzato dalla cliente

per apporre la firma con il codice *****ID, che la voce “*appID*” corrisponde all’identificativo dell’App utilizzata dalla cliente per apporre la firma con il codice *****ID e che la descrizione “*transaction-challenge*” rappresenta la richiesta di autorizzazione disposta dalla cliente sul canale e firmata in formato *jwt* dal canale stesso e autorizzata dal cliente con il proprio codice *****ID. L’intermediario ha, altresì, allegato documentazione attestante sia l’utilizzo del protocollo 3D Secure per l’operazione in esame ed il relativo metodo autorizzativo, sia l’inserimento del codice *****ID in seguito alla ricezione di specifica notifica in App. Risulta, altresì, che, nel caso di specie, non sia avvenuto l’enrollment dell’app sul dispositivo del truffatore.

Pertanto, il Collegio ritiene di poter valutare gli elementi forniti dall’intermediario come complessivamente idonei a provare il corretto svolgimento delle procedure di autenticazione, registrazione e contabilizzazione dell’operazione contestata, in continuità con precedenti decisioni assunte in casi simili (cfr. Collegio di Bari, decisione n. 224/2025).

Invero, sulla base dei principi elaborati dal Collegio di Coordinamento, l’accertamento della conformità della procedura di autenticazione alla definizione di SCA contenuta nel d.lgs. n. 11/2010 non è di per sé dirimente per escludere la responsabilità del cliente. In particolare, «la previsione di cui all’art. 10, comma 2, del d. lgs. n. 11/2010 in ordine all’onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell’utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l’“autenticazione” e la formale regolarità dell’operazione contestata non soddisfa, di per sé, l’onere probatorio, essendo necessario che l’intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell’operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell’utente» (decisione n. 22745/19).

Pertanto, il Collegio passa a valutare i profili di dolo o colpa grave dell’utente. A tale riguardo, è innegabile che la ricorrente versò in colpa grave, essendosi fidata di chi l’ha contattata telefonicamente al punto di aver seguito “*tutte*” le indicazioni fornite dal sedicente operatore, con particolare riguardo alla modifica dei massimali della carta al fine di aumentare l’importo dei pagamenti tramite POS. Rileva, tuttavia, altresì la circostanza che la telefonata ricevuta dalla ricorrente sembrava provenire da un numero coincidente con quello di una delle filiali dell’intermediario, in quanto i criminali avevano posto in essere una truffa telefonica con falso numero chiamante, nota come “call ID spoofing”.

Alla luce del quadro complessivo delle circostanze, il Collegio ritiene che se, per un verso, risulta la colpa grave della ricorrente per le ragioni sopra indicate, per altro verso, va considerato che la stessa sia stata vittima di una truffa piuttosto insidiosa che fa presumere un difetto nell’organizzazione del servizio offerto dall’intermediario, in quanto il numero dal quale è partita la telefonata dei truffatori era comunque riconducibile all’intermediario, sebbene debba riconoscersi che questa modalità di realizzazione delle truffe finanziarie sia negli ultimi anni molto diffusa per la disponibilità di mezzi tecnologici sempre più sofisticati.

Pertanto, il Collegio reputa che la domanda di rimborso della ricorrente possa trovare parziale accoglimento, nella misura ritenuta equa di € 800,00.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l’intermediario corrisponda al ricorrente la somma di € 800,00.

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