

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

La ricorrente afferma che in data 25 luglio 2025, alle ore 17:37, aveva ricevuto una comunicazione “*apparentemente*” proveniente dalla banca resistente, che l’avvisava che il suo profilo cliente era stato “*disabilitato*”; risultava pertanto necessario inserire i suoi dati tramite il link allegato. Precisa di aver seguito il predetto link e di aver ricevuto il “*codice di sicurezza*” sulla chat utilizzata dalla banca per comunicare i “*vari accessi, prelievi*”.

Fa presente di aver inserito tale codice nell’App della banca, e che “[n]ell’arco di qualche minuto” si è resa conto che erano stati effettuati due pagamenti di € 489,99 (ore 18:38) e di € 19,54 (ore 18:40). Precisa di aver provveduto “*immediatamente a bloccare ogni movimentazione sul conto*”, e di essersi recata presso le competenti autorità al fine di presentare formale querela, anche se veniva “*rinviata al giorno dopo*”.

Soggiunge che, in data 17 febbraio 2025, aveva presentato formale reclamo, poi riscontrato negativamente dalla banca il 5 marzo 2025.

Evidenzia che il sistema informatico della banca presenta una “*falla*”, in quanto il messaggio contenente il codice di sicurezza era pervenuto sull’utenza telefonica della cliente nella medesima chat utilizzata dalla banca per confermare le operazioni effettuate. Ritene che, anche utilizzando la normale diligenza richiesta per il consumatore, tali circostanze avrebbero indotto in errore chiunque, mentre al PSP è imposta una diligenza qualificata nell’adempimento dei propri obblighi ai sensi dell’art. 1176, comma 2°, c.c. (cita Cass. civ., sentenza n. 9158/2018).

Chiede, pertanto, il rimborso della somma di € 509,53.

Costituitosi, l'intermediario rappresenta preliminarmente che la ricorrente è titolare della carta di debito n. 5167.****.****.9600, abilitata al servizio di Internet Banking, e che in data 27 febbraio 2025 ella aveva disconosciuto due operazioni di pagamento di € 489,99 ed € 19,54, eseguite il 25 luglio 2024.

Eccepisce che tali operazioni erano state eseguite mediante un *digital wallet*, così come risulta dai tracciati della carta di debito. In particolare, osserva che: la cliente (codice utente 08935367) si connetteva prevalentemente usando lo smartphone identificato con il codice univoco "b3723255952d09b8"; il 25 luglio 2025, alle ore 17:37:12, era stata rilevata un'attività di *enrollment* che si era conclusa alle successive ore 17:38:09 su altro *device* identificato dal codice "0c2f33454361fad3"; tale *enrollment* era stato autorizzato attraverso il corretto inserimento del codice OTS, trasmesso a mezzo SMS alle ore 17:37:20 al numero di cellulare certificato della cliente; alle ore 17:38:39 veniva abilitato da App il servizio di pagamento S***** P**, autorizzato con il codice OTP generato in seguito alla ricezione della notifica *push* in App e previo inserimento del codice Pin; alle ore 18:38:23 era stata disposta la prima operazione di pagamento di € 488,99 mediante la carta di debito n. 5167.****.****.9600, a cui corrisponde la "carta virtuale" n. 5372.****.****0106, con contestuale invio sul cellulare della cliente di specifico SMS *Alert*.

Ritiene, pertanto, che tali circostanze siano "*determinanti*" nel dimostrare che alcuna responsabilità possa esserle addebitata e che le operazioni disconosciute erano state rese possibili esclusivamente a causa dell'inosservanza degli obblighi di custodia della carta e delle credenziali di sicurezza da parte della ricorrente.

Evidenzia che la colpa grave della cliente emergerebbe dalle seguenti circostanze: la comunicazione che aveva dato inizio alla truffa era stata trasmessa da un indirizzo PEC in alcun modo riconducibile alla banca ed il suo contenuto non aveva "*capacità decettiva*"; in sede di denuncia la ricorrente aveva dichiarato di aver seguito il link riportato nella predetta comunicazione, e di aver inserito il proprio codice cliente e PIN, consentendo al truffatore di accedere al servizio di Internet banking e avviare la procedura necessaria per l'*enrollment* del nuovo *device*; risulta allegato il messaggio ricevuto in occasione dell'*enrollment* del nuovo *device*, il quale recita testualmente "*NON CEDERE IL CODICE. Se qualcuno te lo chiede E' UNA FRODE!*" (cita Collegio di Palermo, decisione n. 307/2025, Collegio di Bari, decisione n. 5893/2023, Collegio di Torino, decisione n. 1344/2023); il codice necessario per l'*enrollment* del nuovo *device* era stato inviato all'utenza mobile n. 0039**8906, coincidente con quella riportata in sede di denuncia; tra la fase di *enrollment* e l'esecuzione della prima operazione di pagamento era "*passata un'ora*", avendo avuto la possibilità la ricorrente di interrompere l'operatività fraudolenta; si era trattato non di una truffa particolarmente sofisticata, bensì di un'ipotesi di *phishing* tradizionale (cita Collegio di Bologna, decisione n. 6703/2024, Collegio di Torino, decisione n. 3397/2024). Richiama un orientamento dell'ABF che ha riconosciuto in capo ai ricorrenti "*auto-responsabilità per l'operazione disconosciuta*", rigettando i relativi ricorsi (cita Collegio di Bologna, decisione n. 7698/2025, Collegio di Palermo, decisione n. 7765/2025, Collegio di Roma, decisione n. 7601/2025). Chiede, pertanto, di rigettare il ricorso, in quanto infondato in fatto ed in diritto.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di due operazioni di pagamento effettuate tramite S***** P** (*digital wallet*) il 25 luglio 2024 – rispettivamente alle ore 18:38:23 (€ 489,99) e 18:40:14 (€ 19,54), per un importo complessivo pari ad € 509,53 –, successivamente disconosciute.

Il Collegio rileva preliminarmente che le operazioni contestate 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, tali operazioni 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 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).

Tratteggiato il quadro normativo di riferimento, occorre premettere che, nel caso di specie, dalla documentazione in atti si evince che:

- la cliente (codice utente 08935367) si connetteva prevalentemente usando lo smartphone identificato con il codice univoco "b3723255952d09b8", e che l'operatività disconosciuta era, invece, riconducibile ad un differente dispositivo, avente codice univoco "0c2f33454361fad3";
- il 25 luglio 2025, alle ore 17:37:12, era stata rilevata un'attività di *enrollment* che era iniziata mediante l'inserimento del Pin (fattore di conoscenza) e si era conclusa alle successive ore 17:38:09 su altro *device* identificato dal codice "0c2f33454361fad3";
- tale *enrollment* era stato autorizzato attraverso il corretto inserimento del codice OTS (fattore di possesso), trasmesso a mezzo SMS alle ore 17:37:20 al numero di cellulare certificato della cliente, coincidente con quello indicato dalla cliente in sede di denuncia;
- alle ore 17:38:39 veniva abilitato da App il servizio di pagamento S***** P** (*digital wallet*), autorizzato con il codice OTP (fattore di possesso) generato in seguito alla ricezione della notifica *push* in App e previo inserimento del codice Pin (fattore di conoscenza);
- alle ore 18:38:23 era stata disposta la prima operazione di pagamento di € 488,99 mediante la carta di debito n. 5167.****.****.9600, a cui corrispondeva la "carta virtuale" n. 5372.****.****0106, mentre alle successive ore 18:40:14 era stata disposta la seconda operazione di pagamento di € 19,54.

Ciò premesso, tuttavia, il Collegio rileva che la banca non ha specificato quali fattori di autenticazione sono stati utilizzati per entrambe le operazioni contestate. Sul punto, si richiama il principio di diritto affermato dal Collegio di Coordinamento nella decisione n. 21285/2021, secondo il quale "*L'utilizzo di un wallet affidato a un terzo gestore per l'esecuzione di operazioni di pagamento non esime l'intermediario, in qualità di prestatore di servizi di pagamento, dall'onere di fornire prova dell'autenticazione forte delle operazioni compiute. La prova non può limitarsi alla fase di c.d. tokenizzazione della carta nel wallet, ma deve riguardare anche la fase esecutiva delle singole operazioni, non potendosi ritenere implicito che le transazioni siano state correttamente autenticate dal fatto che le stesse risultino autorizzate o comunque dalla sola evidenza che siano state effettuate in modalità contactless*".

Pertanto, non è stato assolto l'onere probatorio relativo all'autenticazione.

Secondo l'orientamento consolidato dell'Arbitro, la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta, infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

Ne consegue il riconoscimento del diritto della ricorrente al rimborso dell'importo oggetto delle operazioni di pagamento contestate.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 509,53.

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