

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 ESTERNI - FABIO GIROLAMO PORTA

Seduta del 18/02/2026

FATTO

La ricorrente, titolare di un conto corrente abilitato all'operatività on line cui è associata una carta di debito rilasciata dall'intermediario convenuto, rivendica il rimborso della somma fraudolentemente sottratta da terzi (€ 431,88) a seguito di una truffa perpetrata ai suoi danni. In particolare, in sede di denuncia sporta in data 16/06/2025 presso le autorità competenti, la ricorrente dichiara che: in data 12/06/2025, durante una procedura di rinnovo del servizio di posta elettronica certificata effettuata per conto di un suo parente, veniva trasferita su un sito web, apparentemente identico a quello del gestore della PEC, dove inseriva il numero (****.****.****.2344) della carta di debito a lei intestata; di aver ricevuto, successivamente, sull'App bancaria installata sul suo cellulare, talune notifiche che segnalavano l'accesso al conto corrente e l'esecuzione di due pagamenti online, ciascuno per l'importo di € 206,94, dalla medesima non autorizzati; di aver segnalato alla banca la vicenda occorsa, disconoscendo le operazioni, in riscontro alla quale quest'ultima disponeva il blocco della carta "per movimenti sospetti".

Insoddisfatta dell'esito del reclamo, avendo la banca negato la restituzione del maltolto, la ricorrente invoca la tutela dell'Arbitro affinché disponga a carico dell'intermediario convenuto il rimborso del controvalore delle operazioni di pagamento contestate.

Instaurato il contraddittorio, l'intermediario si oppone alla domanda della ricorrente affermando che alla luce dei tracciati elettronici estratti dai sistemi informatici, le operazioni controverse sono risultate realizzate in regime di *commercio elettronico sicuro*, con inserimento del CVV della carta di pagamento intestata alla cliente, senza rilevare anomalie. Sostiene che la truffa di cui sarebbe rimasta vittima la ricorrente sia stata resa possibile per negligenza della titolare della carta, la quale ha evidentemente

comunicato al terzo il codice OTS ricevuto sul proprio device (certificato dal codice univoco "16C09D**D4A96AF3") necessario per l'*enrollment* del nuovo dispositivo, unitamente alla notifica *Push* in App contenente, altresì, il messaggio anti frode che mette in guardia il cliente nel caso in cui non sia lui ad operare sul device. Per cui la resistente afferma di non aver avuto dubbi sulla riconducibilità alla ricorrente circa la sostituzione del nuovo device. Deduce dunque la colpa grave della ricorrente nella misura in cui ha disatteso l'obbligo di custodia degli strumenti di pagamento e dei codici di accesso che consentono l'utilizzo del servizio online (cita ABF Coll. Bologna, Dec. nn. 7698/2025, 6703/2025; Coll. Torino, Dec. n. 3397/2024), nonostante sia stata posta nella condizione di interrompere sin da subito l'operatività fraudolenta.

Alla stregua delle superiori considerazioni, la resistente esclude profili di censurabilità ascrivibili al proprio operato e chiede al Collegio la declaratoria di rigetto del ricorso ritenuto infondato in fatto e in diritto.

Con memoria di replica alle controdeduzioni dell'intermediario, la ricorrente rileva che la banca avrebbe disatteso gli obblighi di monitoraggio delle transazioni sospette, sulla medesima gravanti ai sensi degli art. 2 e 18 del Regolamento Delegato UE 2018/389. La ricorrente osserva che la banca non avrebbe intercettato una serie di anomalie evidenti, tra cui: il breve lasso temporale intercorso tra il cambio del dispositivo e la prima operazione di pagamento eseguita a distanza di soli tre minuti dalla sostituzione del device, reso immediatamente operativo; la circostanza che i pagamenti fossero diretti ad un esercente noto per la vendita di "*strumenti quasi-monetari ad alto rischio di riciclaggio e frode*"; il rapido svuotamento del conto incompatibile con un comportamento consumeristico ordinario. Di conseguenza la ricorrente esclude profili di grave negligenza ascrivibili alla sua condotta, assumendo, da un lato, di essere rimasta vittima di una frode sofisticata attuata mediante S.m.s. *Spoofing*; dall'altro, che la ricezione del messaggio "*non cedere il codice... è una frode*" nella chat ufficiale intrattenuta con la Banca comporta un affidamento incolpevole del cliente, tale da degradare la colpa da "*grave*" a "*semplice*". Insiste, dunque, per l'accoglimento del ricorso.

Con memoria di controreplica, la banca rileva che le attività espletate ai fini dell'*enrollment* del nuovo device devono ritenersi coerenti con le prescrizioni dell'art. 18 del Regolamento Delegato UE 2018/389, poiché il codice OTS necessario per l'associazione del nuovo dispositivo all'utenza di Internet banking è stato inviato al cellulare certificato della ricorrente ed inserito consentendo l'abbinamento. Al riguardo la resistente rileva come tra l'*enrollment* e la prima operazione fossero passati "quasi 7 minuti", ossia un tempo sufficiente per consentire alla ricorrente di attivarsi per impedire la truffa. Ritene inoltre inconferente il rilievo della ricorrente secondo cui non avrebbe ricevuto la richiesta di autorizzazione delle singole operazioni disposte dal frodatore dopo l'*enrollment*, considerato che in seguito all'associazione del nuovo dispositivo al servizio di home banking, il frodatore ha potuto operare autonomamente nel disporre le operazioni contestate. Deduce altresì l'irrelevanza del fatto che i pagamenti oggetto del ricorso fossero diretti verso un esercente che si occupa di "beni digitali", non costituendo questo un elemento di Alert, considerata la tendenza del mercato ad operare in tali ambiti. Conclude insistendo per il rigetto del ricorso.

DIRITTO

La ricorrente rivendica il diritto al rimborso del controvalore di due operazioni di pagamento online eseguite in data 12/06/2025, ciascuna per l'importo di € 206,94, a valere sulla carta di debito a sé intestata, successivamente disconosciute.

La materia trova precipua regolamentazione nelle disposizioni del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017, che ha attuato la Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). L'operazione controversa risulta posta in essere anche sotto la vigenza del Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per

l'autenticazione forte previsti dalla direttiva. Tale disciplina prevede che il rischio di utilizzazione illecita degli strumenti di pagamento ricada in prima battuta sull'intermediario (tenuto a garantire l'affidabilità e la sicurezza complessiva del servizio offerto, in relazione al sistema informatico, organizzativo e di controllo all'uopo adottati) il quale può sottrarsi all'obbligo di rimborso delle somme trafugate fornendo la prova del dolo o della colpa grave dell'utilizzatore (tenuto alla diligente custodia dello strumento e alla segretezza delle credenziali necessarie per l'autenticazione) ai sensi del combinato disposto degli artt. 7, 10 e 12, comma 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. L'art. 10 del citato decreto legislativo n. 11/2010 stabilisce infatti: "1. 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". Inoltre "2. 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. 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".

Tracciato il quadro normativo di riferimento, nella fattispecie in esame l'intermediario afferma che le operazioni contestate sono state autorizzate in data 12/06/2025, previa sostituzione del device originariamente certificato della ricorrente, con la corretta validazione dei fattori di autenticazione previsti dal sistema adottato, in regime di SCA, prima del blocco operativo. A sostegno, la resistente allega un file di "tracce informatiche" composto da cinque fogli:

- 1) "anagrafica" (recante i dati anagrafici del cliente reperiti nell'archivio del servizio internet banking);
- 2) "accessi" (che ricostruisce gli accessi al servizio effettuati dall'utenza del cliente);
- 3) "tracciatura" (concernente i log delle operazioni disconosciute);
- 4) "sms" (recante l'elenco dei messaggi sms inviati al numero telefonico mobile del cliente in data 12/06/2025 e 14/06/2025);
- 5) "push" (avente ad oggetto l'elenco delle *push notification* inviate all'APP).

Dall'esame dei predetti log risulta che alle ore 10:29:23 del 12/06/2025 è stata avviata la procedura di sostituzione del device della ricorrente, dal dispositivo in uso alla stessa (avente codice identificativo C0B480**_****_****_****_****D4A565), conclusasi alle ore 10:30:12 sul nuovo device (16C09D**_****_****_****_****D4A96AF3). L'abbinamento è stato autorizzato mediante il corretto inserimento del PIN (fattore di conoscenza) e del codice OTS, quale fattore di inerenza (v. Foglio Tracciatura, riga 325) trasmesso via Sms alle ore 10:29:25 sul numero di cellulare certificato della cliente (+39320**377, coincidente con quello indicato nel modulo del ricorso; cfr. Foglio sms, riga 2).

Alle ore 10:30:11 l'operazione risulta comunicata sul device della ricorrente, identificato dal codice "C0B480**_****_****_****_**** D4A565" (cfr. Foglio push, riga 11, colonna "STATO", dicitura "OK"), con la seguente notifica Push in App: *"Stai attivando l'App su iPhone 13 Pro- iPhone. SE QUESTO DISPOSITIVO NON È IN TUO POSSESSO È UNA FRODE! Contatta la Filiale Digitale"*.

Con riguardo alla fase dispositiva, i log prodotti evidenziano che alle ore 10:33 e 10:35 del 12/06/2025 sono state inviate sul nuovo device collegato al servizio di Internet banking due notifiche Push in App aventi il seguente tenore letterale: *"Stai autorizzando il pagamento di 206.94 EUR presso startselect.help del 12/06/2025 [ore 10:33 e 10:35] con la carta 539768xxxxxx2344"*. Ambedue le notifiche risultano confermate (cfr. stringhe "deviceFingerprint" e "authType":"TOUCH" presenti nella colonna R, denominata "MSG INPUT", del Foglio Tracce) mediante validazione delle *push* in App (elemento di possesso) alle ore 10:34 (v. riga 385) e 10:36 (v. riga 420) con riconoscimento biometrico (elemento di inerenza).

Alla stregua delle risultanze in atti, può dunque concludersi che l'intermediario resistente abbia assolto l'onere probatorio sul medesimo gravante (ex art. 10, d.lgs. n. 11/2010, cit.) fornendo evidenza dell'autenticazione e della formale regolarità delle transazioni contestate con i relativi chiarimenti (cfr. ABF Coll. Torino, Dec. n. 4749/2025; Coll. Bologna, Dec. n. 1697/2022; Coll. Roma, Dec. n. 21308/2021). Tale accertamento, in aderenza al dato normativo, costituisce un *prius* logico giuridico che consente al Collegio di sindacare i possibili profili di colpa grave ravvisabili nella condotta dell'utilizzatore in relazione al fatto occorso (cfr. ABF Coll. Coord. Dec. n. 22745/2019). In questa prospettiva, nel caso in esame assumono rilievo, per un verso, la riscontrata assenza di anomalie nell'effettuazione delle operazioni compiute attraverso la corretta lettura delle credenziali di autenticazione conosciute dal titolare della carta, in ambiente digitale rispondente ai requisiti di strong customer authentication; per altro verso, la circostanza che la cliente non ha prestato la giusta attenzione al testo della notifica push "parlante" ricevuta sulla App installata sul device certificato in origine, nella fase cruciale di abbinamento del nuovo dispositivo all'utenza di internet banking, manifestamente esplicita nel segnalare l'operazione che si stava compiendo (cfr. ABF Coll. Bari, Dec. n. 134/2023); e viepiù, con un margine di tempo (circa sette minuti dal primo pagamento) sufficiente per inibire l'esecuzione delle transazioni ad opera dei malfattori. Si osserva inoltre che l'invio del messaggio parlante contenente il codice OTS autorizzativo, necessario per attivare il nuovo device, rende influente la mancanza di indicazioni sull'operatività di un sistema di alert ex post. Quest'ultima circostanza consente di escludere che vi sia stato un apporto causale dell'intermediario all'evento dannoso tale da comportare una sua colpevolezza (cfr. ABF Coll. Coord., Dec. n. 24366/2019) e induce a concludere che l'utilizzatrice sia incorsa in colpa grave, avendo mancato di adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate, ai sensi dell'art. 7, co. 1, 2, d.lgs. n. 11/2010 (cfr. ABF Coll. Bari, Dec. n. 7717/2022; Coll. Coord., Dec. nn. 897/2014, 5304/2013). Di conseguenza il ricorso non può trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE