

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) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 29/07/2026

FATTO

La ricorrente - titolare di conto corrente abilitato all'operatività on line acceso presso l'intermediario convenuto, cui è associata una carta di debito alla medesima intestata - chiede il rimborso della somma portata da una operazione di pagamento eseguita a mezzo bonifico istantaneo in data 21 marzo 2026, per l'importo di € 1.000,00, con l'uso non autorizzato degli strumenti in suo possesso. Afferma in particolare: di avere subito, intorno alle ore 13.30 del 21/03/2026, il furto del proprio device sul quale era installata l'App rilasciata dall'intermediario per la fruizione dei servizi di pagamento; di essersi accorta della sottrazione del device allorquando, recatasi con il marito presso un noto negozio di arredi e accessori che opera nella grande distribuzione, si avvedeva che il suo smartphone non era più riposto nella tasca del cappotto; di avere riscontrato, alcune ore dopo il furto, l'esecuzione di un bonifico di € 1.000,00 disposto da ignoti in favore di un soggetto a lei sconosciuto; di essersi resa conto dell'operazione non autorizzata consultando l'App installata sul cellulare del marito altresì collegato al conto addebitato; di non avere mai conservato sul proprio cellulare le credenziali di accesso all'App e di aver comunicato immediatamente l'accaduto all'intermediario. Ritenendo di essere rimasta vittima di un furto operato con destrezza, la ricorrente ha sporto denuncia presso le autorità competenti, disconosciuto la transazione e chiesto il rimborso all'intermediario ricevendo riscontro negativo. Insoddisfatta dell'esito del reclamo, la ricorrente invoca la tutela dell'Arbitro affinché condanni la convenuta al rimborso integrale della somma illecitamente sottratta da terzi, pari ad € 1.001,00 al lordo della commissione applicata.

Instaurato il contraddittorio, l'intermediario si oppone alla domanda della ricorrente rilevando che l'operazione di pagamento disconosciuta è risultata correttamente eseguita in data 21/03/2026, con

l'uso delle credenziali segrete in possesso della titolare, tramite app (**188aea) installata sul device in uso alla cliente (**CC654C). Rappresenta che il sistema di autenticazione adottato (c.d. procedura primaria) prevede l'invio in App (fattore di possesso) di una notifica *push* che il titolare convalida inserendo il codice alfanumerico segreto "****ID" (fattore di conoscenza). L'utilizzo della menzionata procedura di autenticazione forte presuppone, in via preventiva, l'installazione dell'app sul device, l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e la configurazione del codice "*****ID" attraverso l'inserimento: delle credenziali di accesso ai servizi di internet banking (username e password); dei dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (nel caso della carta, PAN, CVV2 e data di scadenza); della password dinamica "usa e getta" (OTP) inviata tramite SMS sul numero di cellulare certificato fornito dalla cliente e associato allo strumento di pagamento in modo sicuro. Afferma che il sistema descritto, basato su un fattore di conoscenza (il codice statico scelto dall'utente) e un fattore di possesso (l'utilizzo di una *app* previamente associata ad uno specifico dispositivo), risponde ai requisiti di autenticazione forte previsti dalla vigente normativa. Saggiunge che è possibile utilizzare il fattore di conoscenza solo sul dispositivo sul quale è stato abilitato precedentemente il prodotto finanziario e, in caso di possesso del device ma non del codice, ovvero di errato inserimento dello stesso per più di 5 volte, è prevista una procedura di blocco automatico. Sottolinea di mettere gratuitamente a disposizione dei clienti il servizio di SMS alert attivo di default all'interno dell'APP.

Nella fattispecie, l'intermediario eccepisce che dai tracciati a sua disposizione, l'operazione di bonifico disconosciuta risulta regolarmente autorizzata (alle ore 15:38:58 del 21/03/2026), mediante inserimento del codice "****ID" in app (fattore di conoscenza) sul device (fattore di possesso) in uso alla cliente (ID**CC654C), in regime di autenticazione forte, senza alcuna anomalia registrata nella digitazione dei codici segreti (codice "****ID" al ricevimento della notifica *push* in APP). Saggiunge che nel caso di specie non vi è stata alcuna modifica del numero "securizzato", rimasto invariato dall'enrollment della carta di debito collegata al conto fino al suo blocco. Sostiene inoltre che il breve lasso di tempo intercorso tra il furto del device associato all'app di internet banking e l'utilizzo contestato rappresentino circostanze indicative del fatto che la titolare conservasse le credenziali per la fruizione dei servizi di pagamento unitamente al proprio cellulare - contravvenendo agli obblighi imposti dal contratto e dall'art. 7 del d.lgs. n. 11/2010 - ovvero che i malfattori siano venuti immediatamente a conoscenza del PIN collegato allo strumento (cita ABF Coll. Bologna, Dec. n. 1900/2024); per cui deduce che il perfezionamento dell'operazione, avvenuto prima del blocco operativo intervenuto alle ore 16:19 dello stesso giorno, sia conseguenza diretta della condotta gravemente negligente della titolare del device associato alla carta di debito dotata dei più evoluti standard tecnologici per la sicurezza. Alla luce dei superiori rilievi, la resistente ritiene di aver provato sia l'adozione di un sistema di autenticazione forte, sia la colpa grave della ricorrente che non avrebbe prestato la dovuta cura nella protezione delle credenziali di sicurezza associate agli strumenti di pagamento in suo possesso. Rassegna dunque le proprie conclusioni chiedendo la declaratoria di rigetto del ricorso.

Le parti allegano memorie di replica e controreplica insistendo sulle rispettive conclusioni.

DIRITTO

La ricorrente - titolare di un conto corrente abilitato all'operatività on line intrattenuto presso l'intermediario convenuto - rivendica il diritto al rimborso dell'importo di € 1.001,00, quale controvalore di una transazione eseguita a mezzo bonifico istantaneo in data 21 marzo 2026 con l'uso non autorizzato degli strumenti di pagamento in suo possesso, a seguito del furto del device associato ai rapporti.

L'operazione contestata risulta compiuta sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di

pagamento nel mercato interno, e il Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata normativa. 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 rivendicate 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. In particolare, l'art. 10 del citato decreto legislativo n. 11/2010 stabilisce: "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".

Nel caso in esame, l'intermediario afferma che l'operazione è stata eseguita con un sistema di autenticazione forte conforme alla normativa in materia, attraverso l'inserimento del codice "*****ID" (fattore di conoscenza) al ricevimento della *push notification* sull'APP (id:*****188aea) previamente associata allo specifico dispositivo ("*device id*: *****CC654C") in uso alla ricorrente (fattore di possesso). Al riguardo, l'intermediario descrive il processo autorizzativo di una transazione tramite codice "*****ID", che prevede la firma della transazione "mediante certificato presente sul Back-End", l'inserimento di un PIN e la generazione di una OTP. Nella vicenda che occupa, l'intermediario precisa che la cliente ha operato in modalità c.d. "primaria", in virtù dell'inserimento del codice "*****ID" (elemento di conoscenza) al ricevimento della *push notification* nell'app installata sul device abilitato (elemento di possesso). Tale procedura, conforme a SCA, presuppone la preliminare installazione dell'APP sul device certificato della cliente, l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e la configurazione della chiave "****ID" tramite inserimento dei seguenti fattori: credenziali di accesso ai servizi di internet banking (username e password); dati dello strumento di pagamento utilizzato per effettuare i pagamenti (nel caso della carta PAN, CVV2 e data di scadenza); password dinamica "usa e getta" (OTP) inviata via SMS al numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento.

Nella fattispecie in esame, in ordine alla fase di autenticazione dell'operazione contestata, gli estratti informatici prodotti, unitamente alla legenda esplicativa e alle tracciatore della firma digitale applicata con il codice "*****ID", documentano che la transazione è stata effettivamente compiuta in regime di SCA, attraverso l'inserimento del codice "*****ID" in App al ricevimento della *push notification*. Depongono in questo senso le stringhe presenti nei log prodotti, dove: il codice associato alla voce "*deviceId*" rappresenta l'identificativo del telefono utilizzato (**CC654C) per apporre la firma con il codice "*****ID"; la voce "*appId*" corrisponde all'identificativo dell'App (**188aea) utilizzata per apporre la firma con il codice "*****ID"; la descrizione "*transaction-challenge*" rappresenta la richiesta di autorizzazione disposta sul canale elettronico e firmata in formato jwt dal canale stesso nonché autorizzata con il codice ****ID. L'intermediario ha inoltre procurato apposita evidenza dalla quale si evince che non vi è stato alcun cambio di utenza nel periodo intercorrente tra la fase di associazione della carta (collegata al conto) al device in uso alla ricorrente ("Data censimento" 20/09/2023) sino al

blocco del dispositivo (effettuato alle ore 16:19 del 21/03/2026), ovvero alla data di dissociazione del device ("Data ultima modifica" registrata il 24/03/2026).

Sulla scorta della documentazione esaminata può dunque affermarsi che il sistema adottato dall'intermediario soddisfa i requisiti di autenticazione forte dell'utente, secondo gli standard di sicurezza indicati dall'EBA con gli orientamenti del 21 giugno 2019 elaborati in tema di SCA (cfr. ABF Coll. Bari, Dec. nn. 1383/2026 e 5732/2026); ciò consente di ritenere raggiunta la prova in ordine alla corretta esecuzione dell'operazione in esame (ex art. 10, comma 1, del d.lgs. n. 11/2010), ovvero che la stessa non sia il frutto di malfunzionamenti delle procedure esecutive (cfr. ABF Coll. Bari, Dec. n. 224/2025; id. Dec. n. 10993/2024, Dec. n. 7434/2024).

Pur tuttavia, la dimostrazione della regolarità formale di un'operazione specificamente contestata non è di per sé sufficiente ad attribuirne le conseguenze patrimoniali in capo al titolare dello strumento ove constino elementi che permettano di escludere il dolo o la colpa grave dell'utilizzatore (cfr. ABF Coll. Coord., Dec. n. 22745/2019). In questa prospettiva, il Collegio deve valutare gli elementi ulteriori acquisiti agli atti del procedimento che consentano una plausibile ricostruzione su base indiziaria delle caratteristiche della truffa denunciata dalla ricorrente, onde formare il proprio convincimento in ordine alla sussistenza o meno di profili di negligenza inescusabile ascrivibili alla condotta della cliente nell'uso del dispositivo.

Nel caso esaminato la ricorrente non descrive in maniera specifica le modalità del furto, avvenuto in un quartiere verosimilmente affollato di una grande città italiana, né fornisce elementi precisi che consentano di collocare con esattezza, sul piano cronologico, le varie fasi dell'evento denunciato. Si soggiunge che l'operazione disconosciuta è stata eseguita alle ore 15:38 del 21/03/2026, a distanza di un breve lasso temporale dalla sottrazione del device (che l'istante dichiara essere presumibilmente avvenuta intorno alle ore 13:30), mentre la ricorrente ha bloccato la carta di debito collegata al conto alle ore 16:19 dello stesso giorno e disconosciuto l'operazione solo in data 23/03/2026 (cfr. ABF Coll. Milano, Dec. n. 3542/2025; Coll. Roma, Dec. n. 7343/2025; Coll. Torino, Dec. n. 4723/2025).

Sul punto, si osserva che nei casi di furto - avvenuto in un luogo pubblico particolarmente affollato - di un device associato a un dispositivo di pagamento utilizzato per l'esecuzione di una o più operazioni perfezionate in un breve lasso temporale intercorso tra la sottrazione e la prima transazione fraudolenta, l'orientamento dell'Arbitro è incline a "ritenere che i codici autorizzativi fossero conservati unitamente al cellulare stesso" (cfr. ABF Coll. Napoli, Dec. n. 8253/2025) e, dunque, a ravvisare uno standard di diligenza inadeguato da parte del titolare dello strumento (cfr. ABF Coll. Bari, Dec. n. 208/2026; Coll. Napoli, Dec. n. 9904/2025).

Alla luce del descritto quadro fattuale e probatorio, sussistono pertanto plurimi elementi rivelatori della colpa grave dell'utilizzatore (arg. ex artt. 7, co. 1, lett. a, 12, co. 4, d.lgs. n. 11/2010) nella custodia delle credenziali personali necessarie per l'uso a distanza del dispositivo di pagamento (cfr. ABF Coll. Coord., Dec. n. 897/2014; Dec. n. 5304/2013), sicché il ricorso non può trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE