

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) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 23/04/2026

FATTO

La ricorrente - titolare di una carta prepagata rilasciata dall'intermediario convenuto - chiede il rimborso della somma portata da n. 14 operazioni di pagamento online, disposte in data 31 luglio 2025, per l'importo complessivo di € 3.142,00, sul rilievo che le stesse siano avvenute in difetto di autorizzazione. Ritenendo di essere rimasta vittima di una frode, la ricorrente ha sporto denuncia presso le autorità competenti, disconosciuto le transazioni e chiesto il rimborso all'intermediario ricevendo riscontro negativo. Ascrivendo all'intermediario la responsabilità del danno risentito per via dell'evento criminoso, la ricorrente invoca la tutela dell'Arbitro affinché dichiari l'intermediario tenuto al rimborso dell'importo illecitamente sottratto.

Instaurato il contraddittorio, l'intermediario si oppone alla domanda della ricorrente sul rilievo che le operazioni di pagamento disconosciute sarebbero risultate correttamente, eseguite in data 31/07/2025, con l'uso della carta prepagata n. ***1739 alla medesima intestata, tramite Token G****Pay. 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 (ossia, 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 tale sistema risponde ai requisiti di autenticazione forte previsti dalla normativa vigente, in quanto basata 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). 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. 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 risultano regolarmente definite le fasi di enrollment della carta di pagamento di titolarità della ricorrente, mediante inserimento dei codici OTP SMS trasmessi al numero certificato della cliente (mai modificato), nonché di creazione del Token attraverso cui viene disposto il pagamento e di disposizione delle singole operazioni di pagamento, impartite senza alcuna anomalia registrata nella digitazione dei codici segreti avvenuta in regime di autenticazione forte.

L'intermediario sostiene, pertanto, che il perfezionamento delle operazioni sconosciute sia avvenuto a causa della condotta gravemente negligente della titolare dello strumento, la quale, senza specificare le circostanze fattuali della frode subita, è plausibile che abbia divulgato a terzi i codici OTP ricevuti, consentendo in tal modo la configurazione del certificato ****ID sul device del frodatore. Afferma che la cliente ha provveduto a bloccare la carta alle ore 14:27 del 31/07/2025, dopo l'esecuzione delle operazioni controverse. Da ultimo, fa presente di condurre da tempo campagne informative antifrode e azioni di sensibilizzazione della clientela tramite il proprio sito web, trasmettendo avvisi relativi a possibili comportamenti anomali che l'intermediario non è solito tenere.

Alla luce dei superiori rilievi, la resistente ritiene di aver provato, per un verso, l'adozione di un sistema di autenticazione forte; per altro verso, la colpa grave della ricorrente che ha violato l'obbligo di diligente custodia dello strumento di pagamento e dei codici segreti abbinati. Rassegna dunque le proprie conclusioni chiedendo la declaratoria di rigetto del ricorso.

DIRITTO

La ricorrente rivendica il proprio diritto al rimborso della somma sottratta da ignoti (complessivamente pari a euro 3.142,00), all'esito di quattordici operazioni di pagamento online effettuate tra le ore 14:12 e le ore 14:18 del 31 luglio 2025 (di cui n. 10 operazioni da € 240,00, n. 3 operazioni da € 239,00 e n. 1 operazione da € 25,00), successivamente sconosciute.

Le transazioni oggetto di vertenza risultano compiute 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 le operazioni di pagamento controverse sono state eseguite con l'intervento di un provider di servizi (terza parte) in regime di autenticazione forte, conformemente alla normativa in materia, attraverso l'inserimento del codice ***ID (fattore di conoscenza) al ricevimento della notifica sulla App previamente associata ad uno specifico dispositivo (fattore di possesso). Al riguardo, svolge alcune considerazioni di carattere tecnico per descrivere il funzionamento del processo autorizzativo di una transazione tramite "****ID", basato, in sintesi, sulla firma della transazione "*mediante certificato presente sul Back-End*", l'inserimento di un PIN e la generazione di OTP. Con specifico riferimento alla fase di configurazione dell'App sul dispositivo abbinato allo strumento di pagamento, l'intermediario riferisce che, ai fini dell'utilizzo del codice "****ID", è necessario preliminarmente installare l'App sul device, procedere con l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e configurare la chiave "****ID" tramite inserimento dei seguenti fattori: le credenziali di accesso ai servizi di internet banking (username e password); i dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (nel caso della carta PAN, CVV2 e data di scadenza); la password dinamica "usa e getta" (OTP) inviata via SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento.

Fatte queste premesse, con riguardo al caso in esame, l'intermediario riferisce che il conto del cliente è stato associato su un nuovo dispositivo. Specifica che l'attivazione dell'app presuppone che il cliente dimostri, dapprima, il possesso dei propri prodotti (dati carta, codice conto, identità privata) e successivamente confermi l'operazione, normalmente tramite un codice monouso (OTP via SMS). A sostegno, l'intermediario produce il log estratto in corrispondenza dell'attivazione dell'App che valorizza l'inserimento della password (v. stringa "grant_type. password") e della OTP alle ore 14:01 del 31/07/2025. Inoltre, le tre cifre presenti nel campo "Mobile Number" corrispondono alle ultime tre cifre del numero di telefono indicato dalla ricorrente in sede di denuncia e risultante anche dall'enrollment. Si soggiunge che il device del frodatore, evincibile alla voce "dati identificativo device mobile", risulta essere il modello 24***CY, codificato con ID 56C***D30.

I tracciati esaminati confermano, dunque, che l'enrollment della carta sul device del frodatore tramite OTP sms (fattore di possesso) e password di accesso al conto (fattore di conoscenza) si sia effettivamente perfezionato alle ore 14:01 del 31/07/2025.

Una volta eseguito l'enrollment, l'intermediario afferma che qualora il cliente decida di tokenizzare uno strumento P* su wallet G***-Pay, può farlo direttamente dall'App del PSP oppure sul sito del wallet provider terzo, sempre in regime di SCA.

Rispetto alla fase appena descritta, la schermata procurata dalla resistente documenta che il token è stato attivato alle ore 14:05 del 31/07/2025. L'intermediario allega inoltre gli estratti informatici, corredati dalla relativa legenda esplicativa: della procedura di log-in nativa in APP con ***ID, utile alla creazione del token e dell'autorizzazione del token eseguita in data 31/07/2025 alle ore 14:05. Nella menzionata legenda sono riportati i codici utilizzati. In particolare, è specificato che: il "deviceId" rappresenta l'identificativo del telefono utilizzato dalla cliente per apporre la firma con il codice *****ID; la voce "applID" corrisponde all'identificativo dell'App utilizzata dalla cliente per apporre la firma con il codice *****ID; 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.

Alla luce delle superiori evidenze, può affermarsi che la carta prepagata di titolarità della ricorrente è stata tokenizzata sul wallet G*Pay in data 31/07/25 alle 14:05, a seguito dell'accesso in app sul device del frodatore certificato secondo le modalità sopra descritte (elemento di possesso) e inserimento della firma digitale con il codice *****ID (elemento di conoscenza).

Quanto alla fase dispositiva delle operazioni oggetto di ricorso, l'intermediario allega apposita evidenza atta a dimostrare la modalità autorizzativa adottata nella fattispecie, affermando che le transazioni sarebbero state perfezionate sempre in regime di SCA.

Al riguardo deve tuttavia rilevarsi come, al netto dell'elemento di possesso, rappresentato dal "mobile wallet", non si rinviene nella documentazione prodotta la prova dell'ulteriore fattore di autenticazione utilizzato per la procedura.

In tema di onere della prova delle modalità di autenticazione delle operazioni di pagamento effettuate mediante carta digitalizzata all'interno di un wallet, mette conto richiamare il principio enunciato da questo Arbitro secondo cui: 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 la dimostrazione 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" (cfr. ABF Coll. Coord. Dec. n. 21285/2021).

Ora, alla luce delle regole che governano i servizi di pagamento innanzi richiamate, la valutazione della conformità ai requisiti di SCA rispetto ai singoli passaggi che caratterizzano la procedura di configurazione dell'APP, "tokenizzazione" della carta, autenticazione, autorizzazione e disposizione di ciascuna delle operazioni di pagamento contestate costituisce, in aderenza al dato normativo, un *prius* logico giuridico rispetto all'esame di eventuali profili di negligenza inescusabile dell'utente (cfr. ABF Coll. Coord. Dec. n. 24366/2019, cit.) nella gestione dello strumento di pagamento (cfr. ABF Coll. Bari, Dec. nn. 2912/2025; 3270/2024; 3965/2023; 3749/2023; 6257/2022; Coll. Torino, Dec. n. 4258/2022). Difettando, dunque, la prova della regolare esecuzione delle transazioni disconosciute, oltre che del dolo o colpa grave del titolare dello strumento di pagamento, la perdita procurata nella sfera patrimoniale della ricorrente deve essere sopportata dall'intermediario, tenuto al ristoro del controvalore delle transazioni non autorizzate, complessivamente pari a euro 3.142,00, secondo le risultanze della documentazione in atti.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 3.142,00.

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