

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) VITERBO	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 17/12/2025

FATTO

La ricorrente, titolare di una carta prepagata (n. *6534) e di una carta libretto (n.*221, collegata al conto deposito n. *889) rilasciate dall'intermediario convenuto, chiede il rimborso della somma fraudolentemente sottratta da terzi (pari a € 9.960,00), a seguito del furto della borsa in cui erano custoditi i predetti strumenti di pagamento con l'uso dei quali ignoti malfattori hanno eseguito operazioni di ricarica e prelievi cardless, successivamente disconosciuti.

Al riguardo la ricorrente afferma: che il furto della borsa contenente i suoi effetti personali, il proprio smartphone e le carte è avvenuto in un fast food ubicato all'interno della stazione ferroviaria di una città italiana, tra le ore 19.10 e 20.30 del 08/05/2025; di aver riscontrato, poco dopo il furto, la presenza di molteplici prelievi non autorizzati per un ammontare complessivo di € 10.355,00; di aver tentato di contattare l'intermediario senza successo (alle ore 20:59); che il giorno seguente, alle ore 10:00 circa, suo padre si è recato presso gli uffici della convenuta per chiedere il blocco del conto e delle carte di pagamento collegate; di aver sporto denuncia presso le autorità competenti, disconosciuto le operazioni di pagamento e chiesto il rimborso all'intermediario ricevendo solo il rimborso di € 413,00, corrispondente a n. 5 pagamenti wallet.

Ciò premesso in fatto, la ricorrente esclude profili di colpa a sé ascrivibili, ritenendo l'intermediario responsabile della perdita subita per non avere correttamente monitorato i movimenti registrati sul conto, in modo da cogliere gli evidenti indici di anomalia delle transazioni compiute con i dispositivi trafugati (richiama sul punto l'art. 8 del D.M. n. 112/2007) e disporre il blocco automatico delle stesse, a fronte di comportamenti non in linea con l'operatività pregressa (cita ABF, Coll. Bologna, dec. n. 23419/2019). Sostiene che, ai sensi dell'art. 10 del d. lgs. n. 11/2010, gravi sull'intermediario l'onere di

provare che le operazioni in questione siano state autenticate, correttamente registrate e contabilizzate, sottolineando che in sede di riscontro al reclamo la convenuta avrebbe mancato di fornire chiarimenti in tal senso. Sostiene che l'intermediario non abbia altresì osservato l'obbligo di diligenza professionale posto a suo carico dall'art. 1176, co. 2, cod. civ., alla stregua del quale gli istituti di credito devono munirsi di strumenti idonei a evitare accessi ad opera di terzi non autorizzati sui conti della propria clientela (cita ABF Coll. Palermo, dec. n. 3164/2022). Pertanto, insoddisfatta dell'esito del reclamo, la ricorrente invoca la tutela dell'Arbitro affinché accerti il proprio diritto al rimborso della somma sottratta, quantificata in € 9.960,00, oltre agli interessi legali.

Instaurato il contraddittorio, l'intermediario si oppone alla domanda della ricorrente rilevando che le operazioni di pagamento oggetto di vertenza sono state procedute da movimenti in accredito sulla carta prepagata (n. *6534) trafugata, attingendo le sostanze dal libretto n. *889, parimenti intestato alla ricorrente, onde preconstituire la provvista necessaria per l'esecuzione delle successive transazioni sconosciute. Con particolare riguardo alla fase di creazione della provvista, la resistente deduce che le relative operazioni non costituiscono fonte diretta e immediata di perdite patrimoniali per la cliente (cita ABF Coll. Coord., dec. n. 8671/2024) in quanto effettuate da e verso rapporti alla medesima intestati e intrattenuti presso lo stesso istituto. Precisa che la ricorrente ha eseguito l'*enrollment* per entrambi i rapporti a settembre 2023, che i trasferimenti di denaro sono avvenuti utilizzando il *mobile device* in uso alla cliente, "mai bloccato", e che gli accrediti anzidetti, per un ammontare complessivo di € 8.052,00, sono stati autorizzati mediante inserimento, tra l'altro, del codice "*****ID".

In generale, con riguardo al sistema di autenticazione in uso alla clientela, l'intermediario fa presente che sono previste due procedure: quella "*primaria*" che contempla 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); quella "*secondaria*" che prevede l'inserimento di un codice dinamico OTP (ricevuto a mezzo sms) e di una Password. Precisa che nel caso in esame è stata attivata la procedura "*primaria*", il cui utilizzo presuppone, in via preventiva, l'installazione dell'App sul device del cliente 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 inviata via sms. Con specifico riferimento ai prelievi "*cardless*", l'intermediario sottolinea che per la relativa autenticazione è necessario: accedere dall'App alla sezione "*Prelievo senza carta*"; recarsi presso un suo sportello ATM e premere il pulsante dedicato; inquadrare il QR Code mostrato sullo schermo dell'ATM; inserire l'importo che si desidera prelevare e confermare la scelta selezionando "*Procedi*"; inserire il codice "*****ID" nella schermata successiva di riepilogo dell'operazione e premere il pulsante "*Conferma*". L'intermediario soggiunge che qualora il cliente digiti un codice alfanumerico errato per più di 5 volte, il sistema ne dispone automaticamente il blocco. Evidenzia di aver messo a disposizione della propria clientela il servizio di *sms alert*, che può essere attivato gratuitamente ed offre la possibilità di controllare i movimenti relativi alla carta. Precisa che l'invio dell'informativa al cliente sulle operazioni in uscita e in entrata viene effettuato tramite *sms alert*, ovvero tramite notifica *push* in App, come avvenuto nel caso in discorso.

Ciò posto, nella fattispecie in esame, la resistente allega che, sulla scorta delle evidenze in suo possesso, le operazioni P2P e i prelievi *cardless* addebitati sulla carta prepagata (n. *6534) risultano perfezionati in regime di autenticazione forte - previo *login* all'area riservata di home banking del cliente con inserimento del codice *****ID in App - mediante digitazione del codice "*****ID" da App, senza che gli apparati abbiano registrato anomalie o malfunzionamenti delle procedure (cita ABF Coll. Bologna, dec. n. 8345/2023, Coll. Napoli, dec. n. 4824/2022, Coll. Palermo, dec. n. 8442/2021).

Alla stregua delle risultanze in atti, la resistente ritiene di aver dimostrato, da un lato, l'adozione di un sistema di autenticazione conforme al dettato normativo che regola la materia, idoneo a garantire la sicurezza dei propri servizi; dall'altro, la colpa grave della cliente anzitutto per non avere osservato la diligenza minima nella custodia degli strumenti di pagamento e dei codici abbinati in suo possesso, evidenziando come nel caso in esame le operazioni contestate sono state effettuate il medesimo giorno

del furto del mobile device (cita Coll. Bologna, dec. n. 1900/2024). Sostiene che la ricorrente non avrebbe altresì adempiuto ai propri obblighi di tempestiva informativa, così agevolando il perfezionamento della frode.

Escludendo, dunque, profili di responsabilità riconducibili al suo operato, l'intermediario rassegna le proprie conclusioni chiedendo il rigetto del ricorso in quanto infondato.

Entrambe le parti hanno rassegnato memorie di replica e controreplica insistendo per le rispettive conclusioni.

DIRITTO

La ricorrente invoca l'accertamento del proprio diritto al rimborso della somma complessivamente sottratta da terzi, dalla medesima quantificata in € 9.960,00, a fronte di operazioni di pagamento (disconosciute) eseguite da malfattori a seguito del furto della carta prepagata, della carta libretto e del proprio smartphone su cui era configurata l'App dell'intermediario.

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 la ricorrente domanda il rimborso del controvalore di: dieci operazioni di ricarica della sua carta prepagata, per complessivi € 8.052,00 (oltre € 10,00 di commissioni) effettuate mediante addebito sulla carta libretto intestata alla stessa ricorrente; tre prelievi cardless di € 600,00 ciascuno eseguiti in data 8, 9 e 10 maggio 2025 a valere sulla carta libretto (per complessivi € 1.800,00); un pagamento di € 79,00 effettuato il 12 maggio 2025 (oltre € 1,00 a titolo di commissione), seppure dalla documentazione versata in atti tale operazione non risulta addebitata, né riportata nel modulo di disconoscimento.

Le parti concordano sull'avvenuto rimborso (€ 413,55) imputabile – secondo quanto precisato dall'intermediario – alla sommatoria di ulteriori cinque pagamenti wallet parimenti disconosciuti.

Orbene, quanto alle dieci operazioni di ricarica della carta prepagata, non è revocabile in dubbio che le

stesse abbiano costituito la provvista necessaria per la successiva esecuzione dei ventidue pagamenti P2P, sedici dei quali effettuati in favore dei terzi frodatori e disconosciuti dalla ricorrente.

Con riferimento alla fase prodromica di costituzione della provvista, è stato chiarito che “i pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente” (cfr. ABF Coll. Coord., Dec. n. 8671/2024). Resta comunque la possibilità di configurare una responsabilità dell'intermediario, ai sensi dell'art. 11 del d.lgs. n. 11/2010, qualora le operazioni di acquisizione della provvista, pur realizzate in esenzione da SCA, costituiscano incontrovertibilmente fonte diretta e immediata di perdite patrimoniali, ossia qualora sussista un nesso causale immediato e diretto fra l'assenza della SCA e il pregiudizio finale subito dal cliente, che non sia interrotto da atti riconducibili al danneggiato (cfr. ABF Coll. Milano, Dec. n. 8604/2025).

Nella fattispecie in esame l'intermediario ha documentato che i trasferimenti interni di denaro sulla carta prepagata – mediante operazioni di ricarica eseguite online in data 09/05/2025, a partire dalle ore 16:14 – sono stati autorizzati con l'inserimento del codice *****ID in App installata sul dispositivo mobile in uso alla ricorrente, secondo quanto evincibile dai log procurati, corredati dalla relativa legenda esplicativa. Nella menzionata legenda, in cui sono riportati i codici utilizzati nei tracciati elettronici, è specificato che il “deviceID” rappresenta l'identificativo del telefono utilizzato dal cliente (n. ***18B) per apporre la firma con il codice *****ID, mentre la voce “appID” corrisponde all'identificativo dell'app (***ede) utilizzata dal cliente per apporre la firma con il codice *****ID; la stringa “transaction-challenge” rappresenta la richiesta di autorizzazione disposta dal cliente sul canale, firmata in formato jwt, e da questi autorizzata con il proprio codice *****ID. Si soggiunge che l'intermediario ha, tra l'altro, allegato una schermata da cui si evince che il device (n. ***18B) e l'app (***ede) impiegati per l'autorizzazione delle operazioni che occupano risultano registrati il 19/11/2022; tale circostanza fa verosimilmente ritenere che trattasi dei dispositivi della ricorrente oggetto di furto.

Alla stregua dei principi di diritto innanzi richiamati, con riguardo alle operazioni di costituzione della provvista - prodromiche ai successivi pagamenti nei confronti dei terzi frodatori - effettuate, come nella specie, da e verso lo stesso utente titolare di diversi rapporti accesi presso il medesimo intermediario, come detto non sottoposte all'obbligo di autenticazione qualificata, le evidenze in atti inducono ad escludere qualsivoglia profilo di negligenza ascrivibile alla resistente, che ha invero dimostrato di avere adottato (anche) in relazione alla fase in commento un procedimento di autenticazione multifattoriale conforme ai requisiti di SCA.

Passando ad esaminare le operazioni che hanno determinato in concreto un ammanco patrimoniale in danno della ricorrente, giova premettere che rispetto ai ventidue pagamenti P2P, la ricorrente ne ha disconosciuti sedici; segnatamente: un pagamento di € 90,00 eseguito il 10/05/2025; cinque (dei dieci) pagamenti, di € 200,00 ciascuno, compiuti il 10/05/2025; dieci pagamenti, di € 200,00 ciascuno, disposti l'11/05/2025. Pertanto, quanto ai pagamenti P2P, l'importo complessivo oggetto di disconoscimento ammonta a € 3.090,00, che sommato alle tre operazioni di prelievo cardless di € 600,00 ciascuna (effettuate in data 8, 9 e 10 maggio 2025 a valere sulla carta libretto) fuoriuscite direttamente dalla disponibilità della ricorrente, consente di ragguagliare globalmente il quantum oggetto del contendere, astrattamente ripetibile, a € 4.890,00.

Appurato quanto sopra, in ordine alle modalità di autenticazione delle operazioni P2P disconosciute, l'intermediario allega e documenta che per autorizzare simili pagamenti è necessario l'inserimento del certificato *****ID direttamente in app. All'uopo produce i tracciati elettronici estratti dai propri sistemi informatici, corredati da legenda esplicativa, in cui sono riportati i codici utilizzati nei log, i quali dimostrano che i pagamenti in discorso sono stati disposti e autorizzati attraverso una procedura a doppio fattore di autenticazione conforme a SCA (cfr. ABF Coll. Bari, Dec. n. 224/2025) basata sulla digitazione del codice *****id (fattore di conoscenza) negli appositi campi dell'app previamente associata al device della cliente (fattore di possesso).

A non diversa conclusione deve addivenirsi anche con riferimento alle tre operazioni di prelievo cardless da ATM (senza carta) disconosciute. In proposito l'intermediario afferma che per i prelievi "cardless" è necessario: accedere da App alla sezione "Prelievo senza carta"; recarsi presso un suo ATM e premere il pulsante dedicato; inquadrare il QR Code mostrato sullo schermo dell'ATM; inserire l'importo che si desidera prelevare e confermare la scelta selezionando "Procedi"; inserire il codice *****ID nella schermata successiva di riepilogo dell'operazione e premere il pulsante "Conferma". Allega, a sostegno, talune schermate da cui si evincono gli accessi effettuati da App, in data 8, 9 e 10 maggio 2025, in corrispondenza dei prelievi senza carta perfezionati in regime di autenticazione forte mediante digitazione del codice *****ID (cfr. ABF Coll. Bari, Dec. n. 4839/2025).

Sulla scorta delle risultanze in atti può dunque affermarsi che l'intermediario resistente abbia assolto l'onere probatorio sul medesimo gravante (ex art. 10, d.lgs. n. 11/2010, cit.) fornendo adeguata evidenza dell'autenticazione e della formale regolarità delle operazioni disconosciute con i relativi chiarimenti. Tale accertamento, in aderenza al dato normativo, costituisce un *prius* logico giuridico che consente al Collegio di sindacare i possibili profili di colpa grave eventualmente ravvisabili nella condotta dell'utente in relazione al fatto occorso (cfr. ABF Coll. Coord. Dec. n. 22745/2019). Sul punto, la sussistenza di elementi concludenti - quali il breve lasso temporale intercorso tra il furto e la prima operazione di pagamento, l'assenza di anomalie nell'effettuazione delle transazioni compiute con l'uso degli strumenti trafugati, attraverso la corretta digitazione del codice segreto abbinato - induce a ritenere che i dispositivi e i relativi codici fossero conservati congiuntamente nella borsa rubata e che l'autore del furto abbia potuto agevolmente associarli (cfr. ABF Coll. Roma, Dec. n. 15913/2019); queste circostanze integrano, in applicazione degli artt. 7, comma 1, lett. a), e 12, comma 4, d.lgs. n. 11/2010, una tipica ipotesi di colpa grave dell'utilizzatore (cfr. ABF Coll. Coordinamento, Dec. n. 5304/2013).

Pur tuttavia, sebbene in questi casi non sia configurabile una responsabilità oggettiva del PSP, a diverso esito può giungersi allorquando, sulla base delle evidenze disponibili e secondo le norme di diritto comune, emerga in concreto un apporto causale dell'intermediario all'evento dannoso tale da comportare una sua colpevolezza (cfr. Coll. Bari, Dec. n. 9279/2024; Coll. Bologna, Dec. n. 9454/2024). Ciò può accadere, tra l'altro, nei casi di fallace monitoraggio, ovvero di mancato rilievo di indizi di frode, come riscontrato nel caso in esame. Deve infatti rilevarsi che tra il 10 e l'11 maggio 2025, con la carta della ricorrente sono state portate a segno venti operazioni di pagamento in favore dello stesso beneficiario senza che le procedure approntate dall'intermediario abbiano riscontrato segnali di allerta in ordine all'eventualità che fosse in atto una frode. Come questo Collegio ha avuto modo di sottolineare in precedenti analoghi, è ragionevole attendersi che gli intermediari operanti nel settore si dotino di sistemi di osservazione capaci di intercettare indizi sintomatici di un illecito rispetto a operazioni inusuali, secondo le "indicazioni contenute nel d.m. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante 'Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento')". In particolare, ai sensi dell'art. 8, 1° comma, lett. b), n. 1) del citato d.m., si configura un rischio di frode quando si verificano, tra l'altro, "sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento" ovvero "tre o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento, presso un medesimo punto vendita". In simili contesti assumono importanza gli Orientamenti finali sulla sicurezza dei pagamenti via internet - adottati il 19 dicembre 2014 dall'Autorità Bancaria Europea e recepiti in Italia a maggio 2016, ad opera del 16° aggiornamento alla Circolare n. 285/2013, nella parte prima, IV.4.24 - ove si raccomanda l'adozione di sistemi efficaci di monitoraggio delle operazioni in grado di rilevare modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente. Ivi si afferma che: "I meccanismi per il monitoraggio delle operazioni volti a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti dovrebbero essere attivati prima dell'autorizzazione finale del prestatore di servizi di pagamento; le operazioni sospette o ad alto rischio dovrebbero essere oggetto di una specifica analisi e procedura di valutazione (...). Detti sistemi dovrebbero essere basati, per esempio,

su regole parametrizzate (come le “Black-list” dei dati relativi alle carte compromesse o rubate) e monitorare i modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente” (cfr. anche l’art. 2 del Regolamento EBA n. 2018/389).

Nel caso in esame non sembra che l’intermediario abbia fatto buon governo delle predette raccomandazioni se si considera che nell’arco di 24 ore, in data 10 e 11 maggio 2025, con la carta (n. *6534) della ricorrente risultano compiute, per ciascun giorno, dieci operazioni di pagamento in favore di uno stesso beneficiario, senza che i sistemi di sicurezza abbiano rilevato anomalie né operato cautelativamente un blocco automatico a fronte di operazioni reiterate dal carattere eminentemente sospetto (cfr. ABF Coll. Bari, Dec. nn. 6494/2024, 10175/2023, 2334/2023). Il richiamo, in particolare nei confronti dell’imprenditore bancario, all’obbligo di adottare tutte le misure di carattere tecnico ed organizzativo idonee a conferire il massimo grado di sicurezza ai servizi offerti, appare ulteriormente confermato dalle prescrizioni in tema di assetti organizzativi societari nell’ambito della disciplina generale (artt. 2381 e 2403, c.c.).

Di conseguenza, alla stregua delle normative e dei principi innanzi richiamati, ritiene questo giudicante che le operazioni controverse siano un effetto di una verosimile disfunzione organizzativa sul quale si innesta il comportamento gravemente negligente della cliente, che però non assorbe completamente il nesso di causalità con l’evento lesivo ma concorre con esso. Pertanto il Collegio dispone che l’intermediario corrisponda alla ricorrente l’importo di euro 2.600,00 liquidato in via equitativa.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l’intermediario corrisponda al ricorrente la somma di € 2.600,00.

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