

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 una carta di debito rilasciata dall'intermediario convenuto, rivendica il diritto al rimborso della somma fraudolentemente sottratta da terzi (€ 1.630,00) a seguito del furto del portafoglio in cui era riposto lo strumento di pagamento. In particolare, in sede di denuncia sporta presso le autorità competenti, la ricorrente ha dichiarato: che in data 19/09/2025, mentre effettuava acquisti in un supermercato riponeva la borsa contenente il portafoglio all'interno del carrello della spesa; che giunta presso la propria autovettura, si accorgeva che ignoti avevano sottratto il portafoglio dalla borsa. A quel punto, effettuato l'accesso all'app dell'intermediario, la ricorrente riscontrava l'addebito di n. 3 operazioni di pagamento, non autorizzate, effettuate dopo il furto e prima del blocco della carta disposto alle ore 11:56 dello stesso giorno; segnatamente un prelievo da sportello ATM di € 500,00 eseguito alle ore 10:24 e due pagamenti POS di € 500,00 ed € 630,00, autorizzati, rispettivamente, alle ore 10:48 e 11:07. Nel modulo di disconoscimento la ricorrente ha dichiarato, diversamente dal ricorso, di essersi avveduta del furto della carta tra le 9.30 e le 10.00. Ciò premesso, la ricorrente afferma di aver chiesto il rimborso all'intermediario ricevendo riscontro negativo. Insoddisfatta dell'esito del reclamo, pertanto la ricorrente invoca la tutela dell'Arbitro affinché accerti il proprio diritto al rimborso della somma sottratta (€ 1.630,00).

Instaurato il contraddittorio, l'intermediario si oppone alla domanda della ricorrente affermando che alla luce dei tracciati informatici estratti dai propri sistemi informatici, le operazioni controverse sono risultate tutte autorizzate, tra le ore 10:24 e le ore 11:07 del 19/09/2025, con la regolare lettura del microchip di cui è dotato lo strumento e il corretto inserimento del PIN associato, al primo tentativo,

senza alcuna anomalia riscontrata nella digitazione delle credenziali. All'uopo la resistente produce talune evidenze tecniche onde dimostrare la regolare autenticazione delle operazioni disconosciute, conformemente alle previsioni dell'art. 10, comma 1, d.lgs. n. 11/2010. Evidenza che la prima operazione di prelievo è stata portata a termine in un breve lasso temporale intercorso tra il momento del furto e la sua esecuzione, per cui esclude che la carta possa essere stata clonata. A tale ultimo riguardo, l'intermediario cita uno studio condotto dall'istituto Politecnico di Torino, secondo cui la clonazione del chip richiederebbe tempi e costi molto elevati, incompatibili con la dinamica della vicenda che occupa. La resistente inoltre nega che la ricorrente sia rimasta vittima di furto perpetrato "con destrezza", giacché la sottrazione del portafoglio è avvenuta in un supermercato, ossia in un luogo aperto al pubblico ove è richiesto un grado di attenzione maggiore nella custodia dei propri effetti personali. Saggiunge che è attivo di default il servizio di *push notification* in APP per le operazioni di pagamento. Sulla scorta degli elementi acquisiti, la resistente deduce pertanto la colpa grave della titolare della carta, ritenendo plausibile che il PIN fosse conservato unitamente allo strumento di pagamento. Conclude chiedendo al Collegio la declaratoria di rigetto del ricorso; in subordine chiede l'applicazione della franchigia prevista dalla legge.

DIRITTO

La ricorrente invoca l'accertamento del proprio diritto al rimborso della somma complessivamente sottratta da ignoti (€ 1.630,00), a seguito del furto della carta di debito a sé intestata, corrispondente al controvalore di tre operazioni di pagamento eseguite in data in data 19/09/2025, successivamente disconosciute. Trattasi, in particolare, di un prelievo da ATM per l'importo di € 500,00, compiuto alle ore 10:24, e due pagamenti POS di € 500,00 ed € 630,00 perfezionati alle ore 10:48 e 11:07.

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 con la corretta validazione del PIN associato alla carta

intestata alla ricorrente, munita di microchip, prima del blocco operativo intervenuto alle ore 11:56 del 19/09/2025. A sostegno della regolarità formale delle transazioni, l'intermediario produce talune evidenze estratte dai propri sistemi informatici dalle quali emerge: (i) l'uso della carta con la lettura del Chip (*fattore di possesso* rilevante secondo le regole di *Strong customer authentication*), attestato dal valore "M" (riportato in corrispondenza del prelievo da ATM) e dal valore "C" (in corrispondenza dei due pagamenti POS eseguiti in modalità *contactless*) all'interno della colonna "INPUT MODE"; (ii) la digitazione del PIN (stringa "PIN" in corrispondenza della colonna "MOD DISP) quale *fattore di conoscenza*. Alla stregua delle risultanze in atti, può affermarsi 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. Bari, Dec. n. 177/2025). 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 della ricorrente in relazione al fatto occorso (cfr. ABF Coll. Coord. Dec. n. 22745/2019). Sul punto, la riscontrata assenza di anomalie nell'effettuazione delle operazioni compiute con la carta dotata di microchip, attraverso la corretta digitazione/lettura del PIN abbinato, induce a ritenere che il dispositivo e il relativo PIN fossero conservati congiuntamente nel portafoglio trafugato e che l'autore del furto, commesso in luogo ad alta densità di frequentazione liberamente accessibile al pubblico (ove è ragionevole attendersi una soglia di attenzione rafforzata da parte dell'utilizzatore) abbia potuto agevolmente associarli (cfr. ABF Coll. Roma, Dec. n. 573/2026; Coll. Bari, Dec. 4848/2025).

Queste circostanze integrano, in applicazione degli artt. 7, comma 1, lett. a), e 12, co. 4, d.lgs. n. 11/2010, una tipica ipotesi di colpa grave dell'utilizzatore (cfr. ABF Coll. Coord., Dec. n. 897/2014; Dec. n. 5304/2013). Nondimeno va precisato che sebbene in questi casi non sia configurabile una responsabilità oggettiva del PSP, a diverso esito può giungersi allorquando, sulla base delle evidenze disponibili, emerga in concreto un apporto causale dell'intermediario all'evento dannoso tale da comportare una sua colpevolezza. In questa prospettiva è stato affermato che "fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto" (cfr. ABF Coll. Coord., Dec. n. 24366/2019). Nel caso in esame, l'intermediario ha allegato l'estratto delle notifiche di alert, recanti orari compatibili con quelli delle operazioni contestate, da cui si evince la presenza di movimenti in uscita sul conto. Al riguardo la ricorrente, in sede di denuncia, ha affermato di essersi avveduta delle operazioni "accedendo all'applicativo" dell'intermediario sul quale, secondo quanto affermato dalla resistente, è attivo di default il servizio di push notification in APP per le operazioni di pagamento (circostanza sulla quale non vi è contestazione). Di conseguenza, alla stregua delle normative e dei principi innanzi richiamati, il ricorso non può trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE