

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 31/03/2026

FATTO

Con ricorso pervenuto il 5.12.2025 il ricorrente riferisce che l'intermediario convenuto aveva emesso una nuova carta di debito a suo nome, mai consegnata, né attivata, e rimasta pertanto nella piena custodia dell'intermediario stesso. In data 27.11.2025 venivano eseguiti quattro prelievi fraudolenti sul proprio conto corrente, per complessivi € 3.000,00, mediante l'utilizzo materiale della carta e del relativo PIN, che il ricorrente dichiara di non avere mai avuto nella propria disponibilità. Precisa che, a seguito dell'accaduto, provvedeva al blocco immediato dello strumento di pagamento, presentava denuncia alle autorità competenti e trasmetteva all'intermediario una formale contestazione via PEC. Successivamente, la banca rimborsava le somme sottratte, così riconoscendo la propria responsabilità e l'estraneità del cliente ai fatti.

Riferisce inoltre che soggetti terzi, verosimilmente in possesso di informazioni a lui riferibili, avevano tentato di indurlo ad apporre una firma digitale per autorizzare un'operazione potenzialmente idonea a svuotare il conto corrente. Tale circostanza avrebbe determinato, secondo quanto dedotto, un significativo pregiudizio psicologico e l'esposizione a un rischio non prevedibile né evitabile, con compromissione della propria sicurezza finanziaria e personale.

Sotto il profilo giuridico, il ricorrente richiama gli artt. 10 e 12 della direttiva PSD2 e il D.Lgs. 11/2010, evidenziando che la responsabilità per l'utilizzo dello strumento di pagamento grava sull'intermediario fino alla sua effettiva consegna al cliente. Rappresenta che la mancata consegna della carta, il successivo utilizzo fraudolento e la disponibilità indebita di dati da parte dei truffatori configurano una possibile violazione delle misure di sicurezza connesse al processo di gestione e consegna del mezzo di pagamento, rilevante ai fini dell'eventuale qualificazione dell'evento come *data breach* ai sensi degli artt. 33 e 34 del GDPR, con conseguente applicabilità dell'art. 82 del medesimo regolamento.

Chiede all'Arbitro di:

1. accertare la responsabilità dell'intermediario per mancata consegna dello strumento di pagamento e sottrazione nella filiera.
2. accertare la vulnerazione delle misure di sicurezza relative al processo di consegna e gestione dello strumento di pagamento, con riferimento anche ai profili di possibile *data breach* ai sensi del GDPR.
3. condannare l'intermediario al pagamento di € 7.500,00 a titolo di risarcimento del danno non patrimoniale.
4. porre le spese della procedura a carico dell'intermediario.

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso. Afferma che la domanda del ricorrente è connessa a quattro prelievi in contanti eseguiti il 27.11.2025, per complessivi € 3.000,00, mediante la carta di debito collegata al conto corrente intestato allo stesso. Premette che il cliente aveva ricevuto nella medesima giornata del 27.11.2025 una telefonata da un soggetto, qualificatosi come dipendente dell'istituto, il quale lo aveva indotto ad accedere all'area riservata dell'*internet banking* e a compiere alcune operazioni, riferite dal ricorrente in sede di denuncia. Successivamente il cliente constatava l'esecuzione delle quattro operazioni di prelievo, presentava denuncia e, in data 2.12.2025, sottoscriveva il modulo di disconoscimento. La banca, svolti gli accertamenti del caso, rimborsava al cliente la somma di € 1.500, pari al 50% dell'importo disconosciuto, ritenendo sussistente la colpa grave dello stesso ai sensi della normativa sui servizi di pagamento. Le operazioni conosciute come fraudolente risultano, infatti, in base ai log e alla documentazione prodotta, regolarmente autenticate, correttamente registrate e prive di anomalie, con utilizzo della carta originale e del PIN, nel rispetto delle regole di sicurezza e del sistema di autenticazione forte previsto dalla PSD2. Evidenzia che l'attivazione della carta e la richiesta del PIN sono state effettuate tramite l'applicazione mobile del cliente e che le operazioni contestate sono riconducibili a un fenomeno di *boxing* conseguente a intercettazione del plico contenente la carta, accompagnato da condotte di *vishing*, che avrebbero indotto il ricorrente a comunicare le proprie credenziali. La resistente richiama gli obblighi imposti all'utente dagli artt. 7, 10 e 12 del D.Lgs. 11/2010, sostenendo che il cliente avrebbe violato con colpa grave i propri doveri di custodia e di protezione delle credenziali, come desumibile anche dalla ricostruzione dei fatti riportata nella denuncia e dalle incongruenze rilevate circa la telefonata ricevuta, della cui provenienza non è fornita prova. Richiama inoltre la giurisprudenza dell'Arbitro che, in casi come quello in esame, riconosce l'incidenza del concorso di colpa per la rivelazione delle credenziali personali a terzi, evidenziando che, nel caso di specie, il rimborso del 50% dell'importo sottratto è un'applicazione coerente degli orientamenti giurisprudenziali consolidati.

Eccepisce l'infondatezza della domanda di risarcimento del danno non patrimoniale, richiamando le decisioni dell'ABF e della giurisprudenza di legittimità che escludono la configurabilità di un danno "*in re ipsa*" e richiedono una puntuale allegazione e prova del pregiudizio subito, onere che, secondo la resistente, il ricorrente non avrebbe assolto. L'intermediario conclude sostenendo la correttezza del proprio operato, chiedendo in via principale che sia dichiarata cessata la materia del contendere in ragione del rimborso già effettuato; in via alternativa, che il ricorso sia dichiarato inaccoglibile; e, in subordine, che, ove ritenuti concorrenti profili di responsabilità, il danno sia ripartito tra le parti ai sensi

dell'art. 1227 c.c., considerando le somme già restituite e la franchigia prevista dalla normativa sui servizi di pagamento.

Con la replica, oltre a ribadire sostanzialmente le proprie ragioni, il ricorrente ha rilevato che, in sede di apertura della pratica di disconoscimento, l'intermediario aveva integralmente rimborsato l'importo di € 3.000,00 salvo poi operare una decurtazione di € 1.500,00 sulla base di una successiva rivalutazione unilaterale non assistita da una puntuale ricostruzione causale. Alla luce di tali elementi, il ricorrente chiede al Collegio, quanto al danno patrimoniale, di riconoscere una "responsabilità concorrente" dell'intermediario e di disporre la restituzione integrale delle somme oggetto di disconoscimento; quanto al danno non patrimoniale, di valutarne l'eventuale riconoscimento in via subordinata e nella misura ritenuta equa, avuto riguardo alla gestione complessiva della vicenda. L'intermediario ha controreplicato, ribadendo le proprie conclusioni.

DIRITTO

La controversia attiene ad una richiesta di rimborso di somme che sono state fraudolentemente sottratte al ricorrente, attraverso una serie di bonifici da lui non autorizzati.

Si deve preliminarmente valutare come ammissibile l'ampliamento della domanda da parte del ricorrente in sede di repliche, in quanto solo successivamente alla presentazione del ricorso egli ha appreso che l'intermediario – come del resto da questo affermato con le controdeduzioni – ha deciso di limitare il rimborso alla metà delle somme prelevate. L'argomento è condivisibile e si può, dunque, procedere a valutare la fondatezza nel merito anche della richiesta di rimborso integrale delle somme prelevate.

Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. Ai sensi dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare:

- l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

In sintesi, secondo gli orientamenti condivisi dei Collegi (cfr. Collegio di Coordinamento, dec. n. 22745/2019), la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente.

Le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del dlgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).

Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Parte ricorrente lamenta l'esecuzione fraudolenta di 4 operazioni di prelievo, eseguite, tutte il 27.11.2025, tramite una nuova carta di credito a lui intestata, speditagli via posta e mai pervenutagli.

Si tratta di tre operazioni da € 950,00 ciascuna e di una operazione da € 150,00, per un totale di € 3.000,00.

Da quanto rappresentato dalle parti, emerge che le quattro operazioni di prelievo sconosciute siano state effettuate presso due ATM dello stesso istituto convenuto, dopo che sono state eseguite da APP di *mobile banking*, installata su dispositivo mobile della Cliente, le seguenti operazioni:

- attivazione della nuova carta di debito,
- richiesta di "PIN carta a video",
- variazione dei limiti operativi.

Al riguardo, si ribadisce che, per giurisprudenza consolidata dei Collegi ABF (cfr. Collegio di coordinamento, dec. n. 21285/2021) devono essere presidiati dalla autenticazione forte a due fattori non solo le singole operazioni dispositive ma anche tutte le operazioni idonee a incidere sulla sicurezza dello strumento e dei pagamenti con questo effettuati. E, sulla base delle evidenze documentali prodotte dall'intermediario e sopra richiamate, risulta che le operazioni prodromiche all'esecuzione dei prelievi contestati - segnatamente l'attivazione della carta, la definizione del PIN e la variazione del limite operativo di prelievo - sono state effettuate mediante l'impiego di un sistema di autenticazione forte a due fattori: un fattore di possesso, rappresentato dal dispositivo del ricorrente che ha generato l'OTP dispositivo, e un fattore d'inerenza, probabilmente l'impronta digitale ("TOUCH"), acquisita per la validazione dell'OTP. Secondo le indicazioni dello stesso intermediario resistente, l'evidenza del processo di autenticazione descritto risiederebbe nel campo MSG_INPUT del foglio tracciature, allegato alle controdeduzioni, dove è possibile trovare le registrazioni. In esse viene indicato l'identificativo del dispositivo utilizzato ("deviceId":"***52E"), riconducibile direttamente all'attuale ricorrente, e la tipologia del fattore d'inerenza ("authType":"TOUCH"). La riconducibilità del dispositivo usato al ricorrente è accertata, e in quanto il relativo identificativo (**52E) risulta più volte associato al codice del ricorrente (4***509), anche per più operazioni compiute in date diverse da quelle delle operazioni contestate. Analogamente, anche i prelievi oggetto di contestazione risultano autorizzati mediante autenticazione a doppio fattore, attraverso l'utilizzo fisico della carta di debito (con lettura del relativo chip integrato) quale elemento di possesso, e l'inserimento del PIN quale elemento di conoscenza. In questo caso, le evidenze del processo di autorizzazione emergono dai log riportati negli allegati giornale di fondo dell'ATM e "Tracciati N***".

Dal giornale di fondo si evince, oltre l'effettiva esecuzione delle operazioni di prelievo, l'utilizzo fisico della carta, identificata dal relativo numero e PAN.

Dai "Tracciati N***" si evincono sia la lettura del chip, sia la digitazione del PIN.

In conclusione, sul punto, si può ritenere provata la SCA per tutte le fasi che hanno condotto al compimento delle operazioni sconosciute. Si può, dunque, procedere a valutare la sussistenza di eventuali profili di colpa grave del ricorrente e di un eventuale concorso di colpa dell'intermediario.

Nella denuncia presentata all'Arma dei Carabinieri, parte ricorrente espone pochi elementi inerenti ai fatti oggetto del ricorso: in particolare, dichiara che in data 27.11.2025, alle ore 19:27 (prima dell'esecuzione delle operazioni contestate), ha ricevuto una telefonata da un sedicente operatore della banca convenuta e riferisce che il proprio interlocutore lo invitava ad entrare nell'"internet banking" della propria banca per aggiornare il proprio indirizzo, eseguendo le istruzioni che gli avrebbe fornito. Dichiara di aver ricevuto dei codici "PIN" e di avere scoperto più tardi, tramite APP, l'addebito delle 4 operazioni di prelievo di contante di € 3.000,00.

Si osserva che, nonostante il ricorrente riferisca pochi elementi in merito alla dinamica degli eventi, comunque riporta un numero telefonico sconosciuto (non riferibile alla banca convenuta), dal quale

avrebbe ricevuto la telefonata truffaldina e, inoltre, suggerisce di essersi collegato al sito di *internet banking* per eseguire le operazioni richieste e, in conseguenza di ciò, di avere ricevuto dei codici. Non precisa di aver riferito tali codici al proprio interlocutore, ma nel modulo disconoscimento delle operazioni oggetto del ricorso afferma (anche se poco prima aveva negato di essere stato contattato da presunti operatori bancari) che i truffatori sono entrati in possesso dei “dati” della carta “per un *vishing* telefonico”.

Nelle repliche, afferma che la comunicazione delle credenziali è avvenuta nell’ambito di una truffa telefonica, in un contesto “confidenziale e credibile” del quale non avrebbe potuto dubitare per la mancanza di informazioni sul mancato recapito della carta.

Inoltre, il ricorrente non fornisce copia degli sms ricevuti dal ricorrente, né il registro delle chiamate con l’evidenza della telefonata ricevuta, né indicazioni sull’attività compiuta da parte del ricorrente con l’APP di *mobile banking*, si osserva che, secondo l’orientamento condiviso dai Collegi territoriali, nel caso in cui:

- i. l’intermediario ha offerto la prova dell’autenticazione delle transazioni disconosciute,
- ii. il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA),
- iii. non risultano indici di anomalia delle operazioni e/o ulteriori elementi,

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo.

Nel caso di specie, il convincimento che il ricorrente abbia agito con colpa grave è rafforzato dalle sostanziali ammissioni di un contatto con un soggetto che lo ha indotto ad entrare nell’*home banking*. Ritiene il Collegio che sia verosimile che gli stessi soggetti che hanno intercettato la carta spedita al ricorrente (circostanza ammessa dall’intermediario), siano risaliti a lui e lo abbiano indotto a comunicare i codici per attivare la carta e operare con essa. Si consideri che, sulla base di quanto dedotto e documentato dall’intermediario, e corrispondente ad una prassi consolidata nel settore, la spedizione della carta non includeva alcun codice necessario al suo funzionamento. Al contrario, la carta risulta essere stata originariamente inattiva e, pertanto, inutilizzabile sino al completamento di una specifica procedura di attivazione tramite il servizio di *internet banking*, nonché fino all’acquisizione del relativo codice PIN mediante distinta e separata operazione, anch’essa da effettuarsi *online*.

Parte ricorrente chiede, però, di accertare la responsabilità dell’intermediario per la “mancata consegna dello strumento di pagamento”.

Sul punto, giova preliminarmente richiamare l’art. 8, comma 1, lett. b), del d.lgs. n. 11/2010, ai sensi del quale l’intermediario è tenuto ad astenersi dall’inviare strumenti di pagamento non richiesti dall’utente, salvo il caso in cui lo strumento già in possesso di quest’ultimo debba essere sostituito. Circostanza che, secondo quanto dichiarato dal ricorrente nella denuncia presentata presso l’Arma dei Carabinieri, ricorreva proprio nel periodo in cui sono state eseguite le operazioni contestate. Peraltro, l’art. 39 del contratto prodotto dall’intermediario resistente – la cui validità non è stata contestata dal ricorrente – prevede, al comma 4, che “la Carta in scadenza viene sostituita a iniziativa della Banca”. Legittimo, dunque, l’invio per posta della carta, occorre, tuttavia, richiamare l’orientamento costante dei Collegi territoriali dell’ABF, secondo cui, in caso di disconoscimento di operazioni di prelievo presso ATM eseguite mediante l’utilizzo fraudolento di una carta di debito, qualora la fattispecie presenti i connotati dell’intercettazione dello strumento nel corso della spedizione (c.d. *boxing*) e risulti accertata la rivelazione del codice PIN da parte dell’intestatario della carta attraverso tecniche di ingegneria sociale, deve ritenersi configurabile un concorso di colpa tra le parti. L’intermediario risponde, infatti, in parte del pregiudizio economico subito dal titolare dello strumento di pagamento in ragione del rischio di impresa connesso alla spedizione di questo, ai sensi dell’art. 8, comma 2, del d.lgs.

n. 11/2010, mentre l'utente risponde per la violazione gravemente colposa degli obblighi di custodia delle credenziali di sicurezza personalizzate. Da ciò, viene fatta discendere una ripartizione equitativa della perdita, ordinariamente determinata nella misura del 50 per cento o in misura maggiore, qualora emergano significativi indici di anomalia nell'esecuzione delle operazioni ovvero si rilevino particolari carenze di tipo tecnico (si vedano, ad es., Collegio di Palermo, dec. n. 4131/2025 e n. 7182/2025; Collegio di Bologna, dec. n. 5810/2025).

Nel caso di specie, l'intermediario resistente, conformandosi al richiamato orientamento consolidato dei Collegi, ha dichiarato di avere già corrisposto al ricorrente – che ha confermato la circostanza - la somma di € 1.500,00, pari alla metà dell'importo complessivamente sottratto.

Con il rimborso di tale somma, il ricorrente deve, dunque, ritenersi soddisfatto e nessuna ulteriore somma spetta al ricorrente, neppure a titolo risarcitorio (per la considerazione del quale, peraltro, manca ogni supporto probatorio).

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE