

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 18/02/2026

FATTO

Con ricorso del 25.8.2025, parte attrice lamenta la sottrazione di € 4.623,72, avvenuta tra il 19.7.2025 e il 18.8.2025, tramite l'utilizzo della sua carta di credito da parte di suo figlio minore, a mezzo di pagamenti *online*. Dichiara di aver dato ai suoi due figli, residenti a Singapore, le credenziali della sua carta di credito per provvedere ai loro bisogni; da circa tre mesi, uno dei suoi due figli esegue operazioni con la sua carta di credito, senza autorizzazione, mentre i minori non erano in possesso del PIN, in quanto le operazioni dovevano essere preventivamente autorizzate e controllate dal ricorrente. Il ricorrente ha avuto contezza delle operazioni sconosciute solo a seguito della consultazione dell'estratto conto mensile, in quanto impossibilitato a contattare i figli o a interloquire con la ex moglie,

con la quale ha interrotto ogni tipo di comunicazione. Afferma che la carta è sempre rimasta in suo possesso.

In sede di controdeduzioni, la banca eccepisce la mancanza di anomalie e malfunzionamenti durante l'esecuzione delle operazioni, le quali risultano eseguite con l'utilizzo dei codici associati alla carta e affidati alla esclusiva custodia del ricorrente; viene, inoltre, esclusa, la clonazione: infatti, il ricorrente stesso ha dato le credenziali della sua carta di credito ai suoi due figli, e quindi le operazioni non possono considerarsi non autorizzate. Il rendiconto della carta di credito relativo al mese di luglio è stato regolarmente inviato e ricevuto dal cliente, il quale, quindi, poteva consultare ed eventualmente procedere con il blocco della carta; egli ha quindi omesso di controllare la movimentazione della sua carta di credito. Tra le numerose operazioni di pagamento disconosciute nel periodo interessato, ve ne sono altre che il cliente non disconosce, effettuate sempre presso *merchant* ove sono state eseguite alcune delle operazioni, poi disconosciute. Inoltre, anche nel periodo antecedente a quello oggetto di disconoscimento, sono presenti operazioni della medesima tipologia di quelle oggetto del presente ricorso, non disconosciute dal ricorrente. Secondo l'intermediario, l'episodio fraudolento si è realizzato esclusivamente a causa della negligente condotta del ricorrente in relazione alla cattiva custodia dello strumento di pagamento.

In relazione alle rispettive argomentazioni, il ricorrente chiede il rimborso delle operazioni fraudolentemente eseguite da parte di suo figlio minore, in quanto non autorizzate. Dal canto suo, l'intermediario chiede al Collegio di: «a) dichiarare inaccoglibile in quanto immotivata ed infondata la richiesta oggetto del ricorso presentato dal [ricorrente]; b) nella denegata ipotesi che il Collegio ritenga di poter ravvisare profili di responsabilità nell'accaduto in capo [alla banca], definire la ripartizione fra le parti del danno in esame, in misura proporzionale alle rispettive effettive responsabilità ed in particolare ai sensi dell'art. 1227, commi 1 e 2 c.c. con l'applicazione della franchigia di € 50,00 contemplata dalla normativa in materia di servizi di pagamento».

DIRITTO

1. Parte ricorrente richiede la restituzione di € 4.623,72 corrispondenti a 19 pagamenti *online* disconosciuti, avvenuti tra il 23.7.2025 e il 18.8.2025. Dal modulo di disconoscimento risulta che le operazioni disconosciute sono 21, tuttavia l'operazione di € 115,78 addebitata in data 19.7.2025 risulta riaccreditata il 21.7.2025; senza considerare tale operazione, l'importo disconosciuto corrisponde a quanto richiesto dal ricorrente.

Si rileva la corrispondenza nell'importo solo di alcune operazioni tra quelle indicate dalla banca nei *log* e quelle riportate dal ricorrente nel modulo di disconoscimento, e in particolare:

1. pagamento *on line* del 23.7.2025 di € 132,78;
2. pagamento *on line* del 25.7.2025 di € 201,98;
3. pagamento *on line* dell'8.8.2025 di € 177,91;
4. pagamento *on line* del 15.8.2025 di € 221,09.

In merito alle altre operazioni, vi è corrispondenza tra la data e il *merchant*, mentre gli importi sono differenti (non è noto se per un errore imputabile al ricorrente nella individuazione delle operazioni in sede di disconoscimento): le parti sul punto non forniscono precisazioni.

Assumendo a riferimento l'ammontare che risulta dai soli *log* prodotti, l'importo delle operazioni non autorizzate ammonta a € 4.547,48, importo minore rispetto a quanto dichiarato dal ricorrente, ossia € 4.623,72.

2. L'intermediario afferma che tutte le operazioni disconosciute sono state autenticate, correttamente registrate e contabilizzate, ed esclude ogni tipo di malfunzionamento o anomalia durante l'esecuzione; produce le registrazioni elettroniche per l'intero periodo relativo all'operatività disconosciuta dal cliente.

I pagamenti MO/TO (*Mail Order/Telephone Order*) sono transazioni senza presentazione di carta. Il cliente può fornire i dati della carta per telefono o via *mail* all'esercente ed effettuare un ordine. Una volta comunicati i dati della carta, l'esercente esegue - tramite POS virtuale o fisico - la transazione per la quale è stato ricevuto l'ordine, con inserimento manuale dei dati della carta, senza che sia richiesta l'adozione di un sistema di autenticazione forte, opzione non compatibile con la dinamica delle operazioni ed espressamente esclusa dal legislatore: rappresentano, ad esempio, transazioni MO/TO i pagamenti effettuati a seguito di prenotazioni telefoniche di hotel e B&B nell'ambito delle quali vengono comunicati i dati della carta. Tali operazioni sono al di fuori dell'ambito di applicazione dell'obbligo di adozione di un sistema di autenticazione forte, sia per la modalità di conferimento del mandato, che può avvenire direttamente dal pagatore al *merchant*, senza alcun coinvolgimento del prestatore di servizi di pagamento, sia in quanto operazioni disposte direttamente dal beneficiario del pagamento (appunto il *merchant*).

Ciò viene chiarito espressamente dal "considerando" 95 della direttiva PSD 2, ai sensi del quale non è stata ravvisata la necessità di garantire alle transazioni MO/TO lo stesso livello di protezione offerto per i pagamenti disposti ed eseguiti con l'uso di piattaforme o dispositivi elettronici. L'EBA (cfr. Q&A 2018_4031) ha chiarito che il mandato dal pagatore al beneficiario per l'esecuzione di operazioni MO/TO può essere soggetto a SCA, ma solo se emerge che il mandato è stato conferito attraverso la banca - e quindi che non sia stato direttamente conferito dal pagatore al beneficiario del pagamento - e da canale remoto (dal momento che tale modalità implica un rischio di frode ai sensi dell'art. 97, comma 1, lett. c) della direttiva PSD2). L'art. 97, comma 1, della direttiva PSD2 prevede che «gli Stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando il pagatore: a) accede al suo conto di pagamento *on line*; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi». Dalla lettura del menzionato "considerando" 95 della PSD 2, emerge che per canale a distanza si intende una modalità di disporre le operazioni diversa rispetto all'uso di piattaforme o dispositivi elettronici e il cui funzionamento non dipende dal luogo fisico in cui sono situati il dispositivo per disporre l'operazione di pagamento o lo strumento di pagamento. Inoltre, l'art. 4, comma 6 della PSD 2 definisce "operazione di pagamento a distanza" un'operazione di pagamento iniziata tramite *internet* o tramite un dispositivo che può essere utilizzato per comunicare a distanza. Per completezza, va aggiunto che:

- l'EBA (cfr. Q&A 2018_4359 relativa agli addebiti diretti SEPA) ha confermato che le operazioni disposte su iniziativa del beneficiario fuoriescono dal perimetro applicativo dell'autenticazione forte previsto dalla PSD2, e che (soltanto) l'operazione con cui si conferisce il mandato è soggetta ad autenticazione forte se il mandato è conferito tramite canale a distanza;
- sempre l'EBA ha ulteriormente chiarito (cfr. Q&A_4664) che l'obbligo di SCA si applica solo se un PSP è direttamente coinvolto nel conferimento del mandato. Qualora, invece, il mandato sia stato

conferito direttamente dal pagatore al beneficiario, quindi senza coinvolgimento dell'intermediario, tale mandato non è soggetto a SCA (che d'altronde l'intermediario non potrebbe predisporre, non essendo coinvolto).

Conclusivamente, il mandato è soggetto a SCA solo se è stato conferito (cumulativamente): 1) con il coinvolgimento dell'intermediario e quindi non in via diretta dal pagatore al beneficiario; 2) tramite canale a distanza. Viceversa, laddove non si abbia evidenza del coinvolgimento dell'intermediario nella predisposizione del mandato, il conferimento dello stesso non è soggetto a SCA e non occorre verificare la sussistenza di eventuali meccanismi di autenticazione in fase di mandato.

Nel caso di specie, non risulta che il mandato per la MO/TO sia stato conferito tramite canale a distanza né che sia stato conferito con il coinvolgimento della banca. In ogni caso, il ricorrente non ha sollevato contestazioni sul punto.

Le considerazioni fin qui svolte sono state già esposte nella decisione n. 5076/2023, con la quale il Collegio di Roma ha affermato quanto segue: «con riguardo all'applicabilità della SCA a questo tipo di operazioni, mentre le singole transazioni disposte dal beneficiario non sono soggette ad autenticazione forte, lo è invece l'autorizzazione iniziale all'addebito quando sia prestata attraverso un canale a distanza: secondo l'EBA, tale modalità implica un rischio di frode ai sensi dell'art. 97, comma 1, lett. c) della direttiva PSD2 (cfr. "Q&A" dell'EBA – *Question* ID EB 2018_4031). (...) Nella casistica già sottoposta all'ABF si è accertato che "MO/TO" è l'acronimo di *Mail Order/Telephone Order* (ovvero *Ordine via e-mail/Ordine telefonico*). Si tratta di un tipo di pagamento senza presentazione di carta, con il quale il cliente può telefonare o scrivere un'e-mail all'esercente, effettuare un ordine e pagare fornendo i dati della carta di pagamento per telefono o via e-mail. Tali operazioni non sono soggette a SCA (cfr. Collegio di Roma, decisione n. 9382/2021). Con riguardo all'applicabilità della SCA a questo tipo di operazioni, mentre le singole transazioni disposte dal beneficiario non sono soggette ad autenticazione forte, lo è invece l'autorizzazione iniziale all'addebito quando sia prestata attraverso un canale a distanza: secondo l'EBA, tale modalità implica un rischio di frode ai sensi dell'art. 97, comma 1, lett. c) della direttiva PSD2 (cfr. "Q&A" dell'EBA – *Question* ID EB 2018_4031)».

3. Accertata la sussistenza della corretta autenticazione, registrazione e contabilizzazione per le operazioni disconosciute e chiarite le caratteristiche procedurali dell'operazione MO/TO, resta da esaminare il comportamento delle parti in relazione all'evento truffaldino.

Parte ricorrente ammette che i pagamenti sono stati effettuati da uno dei due figli minorenni ai quali aveva fornito le credenziali della carta di credito, in violazione del principio della custodia personale delle credenziali da parte del titolare; inoltre non ha presentato denuncia all'autorità. In casi simili il Collegio di Roma, a fronte del disconoscimento di operazioni eseguite dal figlio minore del ricorrente, ha rilevato la violazione degli obblighi di custodia della carta e delle credenziali di sicurezza, posti in carico al cliente, ponendo in luce due profili: (i) la responsabilità del cliente per fatto del figlio minore, ai sensi dell'art. 2048 c.c.; (ii) la mancata presentazione della denuncia (mancante anche nel caso di specie), considerato documento rilevante per la decisione arbitrale; dalla ricorrenza di tali profili emerge una condotta gravemente colposa di parte ricorrente: cfr. decisioni n. 13500/2022; n. 14279/2021, n. 22461/2021 (secondo cui, nella fattispecie del tutto analoga a quella qui in discussione, va «rilevata la violazione, da parte del cliente-genitore, degli obblighi di custodia della carta e delle credenziali di sicurezza posti a suo carico (...). Tale violazione non può che ravvisarsi anche nel caso in esame. L'art. 3.2 del Regolamento Generale della Carta prevede espressamente che, "al fine di evitare usi indebiti della Carta, il Titolare e gli eventuali Titolari di Carte Supplementari devono: (i) firmare la Carta con

inchiostro indelebile non appena ricevuta; (ii) custodire diligentemente la Carta in qualsiasi momento; (iii) controllare periodicamente che la Carta sia in loro possesso; (iv) assicurarsi che altri soggetti terzi non autorizzati non usino la Carta; (v) assicurarsi di ritirare la Carta dopo ogni operazione; (vi) evitare di rivelare a terzi i dati della Carta se non in conformità al Regolamento”. Appare pertanto evidente, sotto questo profilo, la violazione dei summenzionati obblighi posti in capo al cliente. Il Collegio ravvisa, altresì, nel caso di specie, la responsabilità del cliente per fatto illecito del figlio minore non emancipato ai sensi dell’art. 2048 c.c., nonché la violazione, da parte dello stesso, dell’art. 24 del Regolamento Generale della Carta, il quale prevede, nel caso in cui “la carta sia stata utilizzata per operazioni non autorizzate”, l’obbligo del titolare “di presentare denuncia alle competenti autorità”, denuncia che nel caso di specie è assente. Come noto, la denuncia va presentata in ogni ipotesi di operazioni non riconosciute, in quanto contenente informazioni utili sulle circostanze in cui sono state eseguite le operazioni di pagamento contestate dai clienti (cfr. Collegio di Roma, decisione n. 418/2019)».

4. Raggiunta la valutazione circa la sussistenza della colpa grave del ricorrente, occorre aggiungere che non viene fornita evidenza dell’invio di *sms alert* da parte dell’intermediario. È noto che, secondo il consolidato orientamento dell’Arbitro, sulla scorta della decisione del Collegio di coordinamento n. 8553/2019, tra 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. In questa prospettiva, la mancata attivazione del servizio costituirebbe una carenza organizzativa imputabile all’intermediario resistente, con conseguente responsabilità, eventualmente in concorso con il comportamento gravemente negligente del cliente, per le operazioni non autorizzate.

Tuttavia, va del pari rammentato che, per contro e con notazione parimenti negativa (che tendenzialmente esclude quella a carico dell’intermediario), nel periodo in cui sono state eseguite le operazioni non autorizzate sono state disposte anche operazioni autorizzate e che l’operatività contestata ha riguardato un periodo considerevole di tempo (dal 23.7.2025 al 18.8.2025). Tra gli elementi valorizzati dal Collegio ai fini della valutazione della colpa grave del ricorrente rientra anche l’omesso controllo, per un periodo di tempo significativo, della movimentazione del conto corrente in relazione al quale risultano compiute le operazioni di pagamento disconosciute (Collegio di Roma, decisione n. 1849 del 2025). Infine, si richiama, per completezza, l’orientamento dell’Arbitro che, in presenza di operazioni disconosciute intervallate da operazioni autorizzate (come nel caso che qui ci occupa), ritiene la prospettazione del ricorrente, che impugni selettivamente solo alcune operazioni, foriera di un quadro presuntivo, incerto e contraddittorio, incompatibile con una presunta frode (si rammenta che nel caso di specie è pacifico che non ci sia stata una frode).

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE