

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) DELL'ANNA MISURALE

Seduta del 28/04/2026

FATTO

Il cliente, con ricorso del 22 dicembre 2025, espone quanto segue:

- è titolare del conto corrente a cui è collegata la carta di debito, della carta prepagata e di un libretto di deposito;
- in data 06/08/2025, riceveva un sms riconducibile all'intermediario che lo avvisava di una operazione sospetta;
- successivamente, nel corso di un colloquio telefonico con un sedicente operatore dell'ufficio antifrode, veniva rassicurato circa il blocco dell'operazione sospetta e che nei successivi minuti avrebbe ricevuto le informazioni necessarie circa l'avvio dell'operazione di blocco del conto corrente;
- al fine di procedere con il blocco del proprio conto coinvolto nella presunta operazione truffaldina, forniva il suo indirizzo e-mail e il suo codice fiscale e poi terminava la telefonata;
- successivamente il ricorrente accedeva alla propria app di home banking del conto n. *272 e riscontrava un trasferimento dell'importo di € 1.900,00, a lui intestato proveniente dal libretto postale al conto corrente e quattro bonifici, non da lui autorizzati, del valore rispettivamente di € 498,00; € 499,50, € 495,80 e € 404,00 per un totale complessivo di € 1.897,30, in favore del medesimo beneficiario;
- accedeva poi al proprio conto n. **001 e riscontrava un'ulteriore operazione truffaldina in uscita dal suo conto, del valore di € 580,00;

- contattava l'intermediario e apprendeva di essere stato truffato;
- procedeva al disconoscimento delle operazioni e, in data 08/08/2025, sporgeva denuncia alle Autorità competenti;
- sussiste la responsabilità dell'intermediario per non aver predisposto le misure e gli accorgimenti atti a prevenire un illecito accesso ai dati sensibili dei propri clienti e per non aver bloccato le operazioni fraudolente nonostante l'evidente anomalia delle stesse e la sua segnalazione;
- le operazioni disconosciute erano sospette per gli importi elevati rispetto alle operazioni normalmente disposte dal ricorrente, e per il destinatario in favore del quale non era mai in precedenza disposto alcun bonifico.

Chiede, pertanto il rimborso della somma di € 2.477,30.

L'intermediario, intervenuto nel procedimento in luogo dell'intermediario convenuto, riportato il fatto, afferma quanto segue:

- il cliente, titolare di una carta prepagata, di una carta di debito collegata al conto corrente e di una carta libretto collegata a un libretto, chiede il rimborso di € 2.477,30 relativo a 5 operazioni eseguite in data 06/08/2025;
- il cliente contesta altresì una transazione in addebito sul libretto di risparmio utilizzata per costituire la provvista sulla carta prepagata che non costituisce fonte diretta e immediata di perdite patrimoniali;
- alla luce di quanto rappresentato e da quanto si evince dalle allegazioni portate agli atti, il cliente è caduto vittima di "Card Relay Attack" e il primo contatto è avvenuto attraverso un sistema di phishing tradizionale;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi, in quanto realizzate in modalità contactless con successivo inserimento del PIN;
- nella data in cui sono state autorizzate le operazioni contestate, la parte ricorrente ha provveduto al recupero del PIN in app;
- sussiste la colpa grave del cliente che, seguendo pedissequamente le istruzioni impartite dal truffatore, ha provveduto ad installare sul proprio dispositivo un'APP non riconducibile all'intermediario;
- è presumibile, inoltre, che il cliente abbia anche comunicato il codice segreto PIN, consentendo così il verificarsi delle operazioni in contestazione e partecipando, pur inconsapevolmente, alla truffa a suo danno, violando il minimo grado di diligenza e di accortezza consistenti nel non condividere in alcun modo con terzi le proprie credenziali o qualsiasi altro codice personale;
- entrambe le carte sono state bloccate successivamente alle operazioni per cui è controversia;
- l'informativa delle operazioni è stata trasmessa al cliente tramite notifiche push;
- da tempo svolge campagne informative per la prevenzione delle truffe.

Chiede, pertanto, il rigetto del ricorso.

Il cliente replica che:

- non sussiste la sua colpa grave;

- il numero da cui proveniva l'SMS civetta era riconducibile all'intermediario e l'SMS si è incanalato nella chat utilizzata per l'interlocuzione con l'intermediario;
- verosimilmente il codice PIN è stato ricavato dai truffatori inserendosi nel dispositivo nonché nell'Area Personale; di certo non è stato da lui comunicato;
- la documentazione prodotta dall'intermediario per provare la SCA è costituita da meri file Word convertiti in PDF sicuramente modificati, dato che contengono dei commenti esogeni al documento stesso e apposti in epoca successiva;
- non ha ricevuto alcun SMS alert relativo alle operazioni contestate, altrimenti si sarebbe tempestivamente attivato per porre rimedio alla truffa in corso;
- è evidente l'anomalia delle operazioni;
- ricorre dunque la responsabilità dell'intermediario che non ha rilevato l'anomalia delle operazioni né predisposto adeguati presidi di sorveglianza e non ha provato che le campagne informative lo abbiano raggiunto.

Con le controrepliche l'intermediario si riporta a tutto quanto già eccepito e contro-dedotto e insiste nel richiedere il rigetto del ricorso in quanto infondato in fatto ed in diritto.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di n. 5 operazioni. Segnatamente, si tratta di quattro pagamenti *online* con carta prepagata effettuati il 6 agosto 2025, tra le ore 16:23 e le 16:24 di € 498,00; € 499,50; € 495,80 e € 404,00, nonché un'operazione di pagamento effettuata lo stesso giorno, con carta di debito di € 580,00. Il tutto per complessive € 2.477,30.

È in atti la denuncia presentata l'08/08/2025.

Stante il disconoscimento delle operazioni da parte del ricorrente, viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate ed in proposito, va innanzi tutto rilevato che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, n. 11.

Le fonti normative applicabili alla fattispecie sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, 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 è richiesta l'autenticazione forte (SCA) 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.

Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Ciò premesso, per quanto attiene al primo profilo sopra individuato, l'intermediario ricostruisce i singoli passaggi della esecuzione delle operazioni fraudolente, fornendo la prova della SCA per ciascuno di essi.

Secondo la ricostruzione fornita dall'intermediario le operazioni contestate sono state precedute:

- a) dall'enrollment della carta di debito e della carta libretto al sistema autorizzativo di tipo dinamico funzionante mediante invio con SMS della password dinamica sul numero di cellulare;
- b) da una operazione di creazione della provvista dal libretto di risparmio alla carta prepagata;
- c) dal recupero del PIN in app.

Con riferimento all'enrollment delle carte di pagamento dalle evidenze prodotte dall'intermediario si ricava che:

- le carte n. ***272 e **001 risultano inserite e attive;
- il numero associato è lo stesso indicato nella denuncia dal titolare (***158);
- l'enrollment è avvenuto in data 17/06/2025 per la carta n. **272 e in data 03/01/2025 per la carta **001, ossia in date ampiamente anteriori ai fatti controversi.

Con riferimento alle operazioni di creazione della provvista, entrambe le parti deducono che, in data 06/08/2025 dalla carta n. **317 collegata al libretto di risparmio è stata disposta una ricarica di € 1.900,00 verso la carta n. **272 come creazione di provvista.

L'intermediario dichiara che l'operazione è stata autorizzata con codice OTP inviato sul numero di telefono certificato.

In considerazione della circostanza che tale operazione, che non è oggetto di disconoscimento, non ha determinato alcun pregiudizio per il cliente, il Collegio non reputa di dovere verificare la SCA. Al riguardo, si richiama quanto affermato dal Collegio di coordinamento (decisione n. 8671 del 23 luglio 2024) sulla questione relativa all'applicabilità dell'art. 10-bis del D. Lgs. n. 11/2010, relativo all'autenticazione forte delle operazioni (SCA), a fronte di "operazioni di costituzione della provvista", prodromiche ai pagamenti nei confronti dei terzi frodatori. Il Collegio di Coordinamento ha enunciato il principio di diritto secondo cui *"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"*.

Con riferimento al recupero del PIN da APP, l'intermediario rappresenta che, nella data in cui sono state autorizzate le operazioni contestate, la parte ricorrente ha provveduto al recupero del PIN in APP.

In proposito allega evidenze attestanti che il detto recupero è avvenuto dall'APP che rappresenta il fattore di possesso, attraverso l'inserimento del Codice P***ID (fattore di conoscenza) alle ore 14:10 del 06/08/2025.

Infine, con riguardo all'esecuzione delle singole operazioni contestate, l'intermediario produce evidenze dalle quali si ricava che i pagamenti sono stati autorizzati tramite:

- lettura della carta in modalità contactless (fattore di possesso), come indicato dalla dicitura "C" nella colonna "Input Mode";
- inserimento corretto del PIN (fattore di conoscenza), come indicato dalla dicitura "PIN" indicata nella colonna "Dati Autenticazione".

In linea con quanto già da questo Collegio affermato a fronte di analoghe evidenze, deve reputarsi provata la SCA.

Le modalità di autenticazione delle operazioni contestate sono conformi a SCA e appaiono coerenti con la natura della truffa subita dal cliente che va ricompresa nel genere "Card Relay Attack", come di seguito si evidenzierà.

Considerate, dunque, le operazioni regolarmente autenticate, deve verificarsi la sussistenza di eventuali profili di colpa grave in capo al cliente.

Il cliente riferisce di aver ricevuto in data 06/08/2025 un sms proveniente dall'intermediario che lo informava che tramite il suo conto era stata commessa una truffa per € 450,00 e gli forniva un numero di telefono per chiarire la situazione.

In merito all'SMS il cliente ha prodotto evidenza dalla quale tuttavia risulta che il messaggio è stato ricevuto in data 29/09/2025 e quindi in data successiva alla truffa, senza contare che non è possibile determinare da quale numero di telefono provenga.

Il cliente in denuncia aggiunge che chiamava il numero di telefono presente nel suddetto sms e il sedicente operatore dell'ufficio antifrode lo informava che c'era stato un tentativo di trasferire i soldi del suo conto corrente in Spagna bloccato dall'ufficio antifrode.

Tuttavia, il cliente non ha prodotto alcuna evidenza della chiamata truffaldina. Il numero indicato, da una ricerca on-line, non risulta riconducibile all'intermediario, bensì segnalato come truffaldino.

Aggiunge che subito dopo veniva contattato dall'operatore tramite whatsapp e scaricava sul suo cellulare l'app Supercard e forniva la sua e-mail e il suo codice fiscale.

Interrotta la conversazione si accorgeva che il sedicente operatore aveva trasferito a sua insaputa € 1.900,00 dal libretto postale alla carta di pagamento con cui erano state effettuate n. 4 operazioni e che era stata eseguita una operazione con un'altra carta.

Il cliente sembrerebbe dunque essere caduto vittima di card relay attack: avrebbe cioè subito un attacco con l'invio di un SMS apparentemente proveniente dall'intermediario che comunica un'attività sospetta sul conto corrente e invita a chiamare un numero per risolvere la situazione. Quando il cliente effettua la telefonata entra in contatto con un finto operatore bancario che lo induce a fornire dati sensibili (nel caso di specie la mail e il codice fiscale) e lo convince ad installare un'applicazione che contiene il malware "SuperCard X".

Una volta che l'app viene installata, il truffatore convince l'utente ad appoggiare la propria carta di pagamento sullo smartphone allo scopo di eseguire una presunta verifica: in questo modo il malware legge i dati della carta dal chip NFC della stessa, inviandoli in tempo reale ai truffatori. I dati della carta di credito inviati agli attaccanti vengono usati per emulare una carta virtuale che, grazie ad una serie di accorgimenti che coinvolgono i messaggi ATR (Answer To Reset), viene riconosciuta come autentica dai terminali POS e dagli sportelli ATM consentendo l'esecuzione di pagamenti contactless e prelievi di denaro.

In un caso analogo il Collegio di Milano (decisione n. 1982/26 del 05/03/2026) si è così pronunciato: *“Dalle stesse ammissioni della ricorrente, contenute nel ricorso e nella denuncia sporta, emerge un comportamento connotato da straordinaria e inescusabile negligenza. La cliente ha infatti: a) dato seguito a un SMS palesemente sospetto, proveniente da un'utenza di telefonia mobile e non da un canale ufficiale dell'intermediario; b) contattato telefonicamente un numero privato indicato nel messaggio; c) installato sul proprio smartphone un'applicazione sconosciuta tramite un link non riconducibile in alcun modo al dominio dell'intermediario”*.

In linea con l'orientamento dei Collegi deve dunque concludersi per la colpa grave del cliente. Vi è, tuttavia, un profilo di responsabilità ascrivibile all'intermediario, perché nel caso di specie risultano integrati gli indici di rischio frode previsti dall'art. 8, punto 2, lett. a, del D.M. 112/2007: “tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita”.

La norma citata identifica i casi di frode che, ai fini della normativa stessa, vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze, per consentire un monitoraggio del mercato delle carte di pagamento. Seppure tali previsioni (sinora mai modificate, anche a fronte della significativa evoluzione degli strumenti di pagamento) non abbiano un valore precettivo diretto, esse cionondimeno rappresentano utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. Anche la mancata attivazione, da parte dell'intermediario, in occasione delle quattro operazioni disposte tra le ore 16:23 e le 16:24 di vari importi, rileva quindi – nella fattispecie concreta – come comportamento gravemente negligente dell'intermediario, che ha colpevolmente ignorato l'indicatore di anomalia, che invece avrebbe dovuto indurlo al blocco della carta o, quanto meno, a segnalare la circostanza al titolare della carta richiedendo una immediata verifica e la conferma dell'operazione.

Questo Collegio ritiene, in conformità peraltro all'orientamento anche degli altri Collegi ABF, che la mancata attivazione dell'intermediario in ipotesi che configurano un rischio di frode secondo l'art. 8 del D.M. n. 112/2007 costituisce una disfunzione organizzativa che implica l'addebito della responsabilità per le operazioni non autorizzate: deve essere quindi dichiarata la responsabilità dell'intermediario per non avere attivato, in presenza dell'indice di rischio, i dovuti presidi di sicurezza che la frequenza e la peculiarità dei prelievi avrebbe imposto di immediatamente attivare.

In definitiva, quindi, in forza di tutto quanto sopra osservato devono rimborsarsi le ultime due operazioni effettuate con la stessa carta (n. 272*) nelle 24 ore presso uno stesso punto vendita

per un importo complessivo di € 900,00 (in virtù dell'arrotondamento previsto dalle disposizioni ABF).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 900,00.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE