

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) DELL'ANNA MISURALE

Seduta del 20/01/2026

FATTO

La cliente, con ricorso del 2 ottobre 2025 espone quanto segue:

- ha subito una frode informatica, in data 27/08/2025, per l'importo di € 181,49;
- ha tempestivamente segnalato l'operazione disconosciuta, presentato denuncia alle Autorità competenti e inviato reclamo scritto alla banca;
- l'intermediario convenuto ha tuttavia respinto la richiesta di rimborso, sostenendo che l'operazione era stata autorizzata correttamente;
- non ha mai autorizzato l'operazione o comunicato a terzi i suoi dati.

Chiede, pertanto, il rimborso dell'importo di € 181,49 oltre al contributo di 20 euro versato per il deposito del ricorso.

L'intermediario, riportato il fatto, afferma quanto segue:

- l'operazione è stata impartita con il corretto inserimento di tutte le credenziali possedute dal cliente e la banca ha dovuto darne esecuzione in adempimento degli obblighi assunti contrattualmente nei confronti del cliente;

- la procedura di autenticazione adottata nel caso di specie è conforme ai requisiti della SCA;
- sia con la denuncia, sia con il reclamo, sia con il deposito del ricorso, il ricorrente non ha fornito elementi utili alla ricostruzione dell'accaduto;
- è dunque presumibile che al cliente siano state carpite le proprie credenziali, anche se nulla dichiara in proposito;
- la banca ha allertato il cliente inoltrando al medesimo, al momento dell'inserimento dell'operazione, la push e, dopo l'inserimento dell'operazione, un sms;
- il contenuto di tali messaggi è stato del tutto ignorato con la conseguenza che la banca non ha avuto alcun dubbio circa la riconducibilità dell'operazione al cliente.

Chiede, pertanto, il rigetto del ricorso o, in subordine, tenersi conto della responsabilità concorrente del cliente ai sensi dell'art. 1227 c.c.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di n. 1 operazione di pagamento e-commerce effettuata il 27/08/2025 alle ore 12:24, di € 181,49.

È in atti la denuncia presentata dalla cliente in data 28/08/2025.

Viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate.

Deve, dunque, procedersi ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010. Più in generale, 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, vale a dire l'onere di provare la SCA, l'intermediario afferma che l'operazione è stata autenticata attraverso la validazione dell'OTP generato tramite APP sul cellulare abitualmente in uso al cliente e previa digitazione del PIN. Dalle evidenze prodotte al riguardo detta versione è confermata perché risulta che:

- il dispositivo abitualmente impiegato dal ricorrente ha un codice univoco;
- l'operazione è stata autorizzata mediante validazione dell'OTP generato dall'APP installata sul dispositivo abitualmente utilizzato dal cliente;
- la generazione dell'OTP è avvenuta previa digitazione del PIN.

Dunque, l'operazione è stata autenticata mediante i fattori di conoscenza (del PIN) e possesso (dello smartphone su cui è stato generato il codice OTP)

È necessario, quindi, passare all'esame del profilo soggettivo, per verificare se, allo stesso modo, risulta provata la colpa grave del cliente.

Il cliente non ha riferito nulla in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento: nella denuncia si limita a riferire di essersi accorto dell'utilizzo fraudolento ricevendo una notifica sul proprio cellulare dall'APP della banca.

Secondo l'orientamento condiviso tra i Collegi, in aderenza al dato normativo (art. 10 del D.lgs. 11/20105) se ai fini dell'applicazione della PSD2 è necessario, ma anche sufficiente, che il cliente neghi di aver autorizzato la transazione, il Collegio una volta verificata la SCA può però valutare la mancata allegazione dei fatti, tra i vari elementi, per formare il proprio convincimento circa la colpa grave del ricorrente.

Fermo quanto sopra, secondo l'orientamento dei Collegi nelle contestazioni di utilizzi fraudolenti on line di strumenti di pagamento in cui, come nel caso di specie, l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute; il sistema di pagamento

risulta conforme alla Strong Customer Authentication (SCA); 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 circa la colpa grave del cliente medesimo.

Solo per completezza si rileva che è stato inviato l'SMS alert al corretto numero telefonico del ricorrente e la notifica push al device che risulta abitualmente utilizzato dallo stesso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE