

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) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) GILIBERTI

Seduta del 29/01/2026

FATTO

Parte ricorrente, nel proprio ricorso, afferma che:

- sono state effettuate 12 operazioni non autorizzate dal suo conto;
- il giorno seguente alla scoperta delle operazioni riceveva una notifica da Google che lo informava di una violazione delle password;
- non ha mai condiviso con nessuno i codici del conto;
- non ha ricevuto alcun alert SMS riguardo tali transazioni;

- ha agito in maniera tempestiva.

Pertanto, chiede il rimborso delle operazioni contestate.

L'intermediario resistente, nel chiedere il rigetto della avversa pretesa, sostiene che:

- il cliente è stato probabilmente vittima di *phishing*;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- il cliente non fornisce alcun elemento utile che possa contribuire a ricostruire le circostanze dalle quali è scaturito l'evento criminoso;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

In sede di replica il ricorrente ha chiarito che:

- La tokenizzazione A* Pay richiede una consapevole iniziativa dell'utente, mai avvenuta.

DIRITTO

Alla data delle operazioni trovava applicazione il D. lgs. 27 gennaio 2010, n. 11 come modificato dal D. lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

Il ricorso ha ad oggetto n. 12 operazioni eseguite con pagamento POS per un ammontare complessivo di € 10.440,00 tutte contestate dal ricorrente ed eseguite tra il 4.10.2025 ed il 13.10.2025.

Il cliente non ha prodotto evidenza della presentazione della denuncia, e non ne viene fatta menzione nella rappresentazione dei fatti, né nella documentazione in atti.

Ciò posto, nel caso di specie, attesa la contestata esecuzione delle operazioni di pagamento, viene in rilievo la verifica dell'autenticazione forte (SCA) sempre 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, come noto, 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.

In ordine alla fase di enrollment della carta di pagamento da cui risultano eseguite le operazioni contestate, l'intermediario produce evidenze atte a dimostrare che:

- la carta risulta di titolarità della cliente, nonché "inserita e attiva"
- il numero telefonico associato alla carta di pagamento in fase di enrollment corrisponde a quello indicato dal cliente nel ricorso;
- l'enrollment è avvenuto in data 11.09.2025 e pertanto in data di molto antecedente all'esecuzione delle operazioni fraudolente (avvenute nell'ottobre 2025).

Quanto all'enrollment dell'APP su un nuovo dispositivo, inoltre, da tutte le evidenze sopra prodotte emerge che:

- acceso all'app tramite password e P*ID;
- che il dispositivo associato è un iPhone;

Sui fattori di autenticazione forte relativi all'installazione dell'APP su nuovo dispositivo dalle evidenze in atti, si rinviene sia il riferimento all'OTP via sms (pure documentato nel suo invio al numero di cellulare della cliente) sia il riferimento ai dati della carta (CVV).

Al contempo, sulla fase di tokenizzazione è possibile sostenere, alla luce della documentazione in atti, che: la tokenizzazione avviene in data 13.09.2025, mentre le prima delle operazioni contestate è del 04.10.2025 (quasi un mese dopo); il log in prodromico alla creazione del token è stato autorizzato con

codice P*ID (fattore di conoscenza) dal dispositivo precedentemente enrollato (fattore di possesso); il nome del device su cui viene enrollato è "iPhone di Pellegrino"; l'autenticazione del token avviene tramite codice P*ID (fattore di conoscenza).

Alla luce della documentazione prodotta dall'intermediario, il Collegio rileva che se, per un verso, risulta adeguatamente provato l'utilizzo di un fattore di possesso, dall'altro, non risulta invece alcuna evidenza relativa all'utilizzo di un secondo fattore di autenticazione, come in ipotesi l'utilizzo di un PIN o del codice P***ID.

Pertanto, in maniera coerente con quanto assunto dal Collegio di Coordinamento citato dalla medesima parte resistente ed intervenuto in materia di SCA e utilizzo di Digital Wallet gestiti da provider terzi (com'è nel caso di specie il wallet A*P*) si tiene a chiarire che: *"La prova non può limitarsi alla fase di c.d. tokenizzazione della carta nel wallet, ma deve riguardare anche la fase esecutiva delle singole operazioni, non potendosi ritenere implicito che le transazioni siano state correttamente autenticate dal fatto che le stesse risultino autorizzate o comunque dalla sola evidenza che siano state effettuate in modalità contactless"* (cfr. decisione n. 21285/2021).

L'intermediario non riferisce neppure di un eventuale utilizzo nella fase dispositiva del fattore per lo sblocco del dispositivo sul quale era installato il wallet, rispetto al quale in ogni caso il Collegio di Coordinamento ha avuto modo di chiarire che tale elemento (sia esso un PIN di sblocco vero e proprio o un fattore biometrico) può essere usato come valido elemento della SCA durante il pagamento, solo se è stato previamente associato tramite SCA alle credenziali usate per lo sblocco del telefono (ovvero se tale associazione è avvenuta inizialmente in fase di tokenizzazione, vd. Collegio di Coordinamento, decisione n. 9559/24 del 4 settembre 2024),

In conclusione, nel caso in cui l'intermediario non risulta assolvere compiutamente al proprio onere probatorio sull'autenticazione delle operazioni di pagamento contestate dal cliente, di cui all'art. 10, comma 1 del D. lgs. 11/2010, l'orientamento costante dei Collegi prevede che il ricorso venga accolto integralmente, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario interveniente corrisponda alla parte ricorrente la somma di € 10.440,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario soccombente 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