

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

Relatore (MI) BARTOLOMUCCI

Seduta del 23/06/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che, in data 08.10.2025, controllando l'estratto conto della sua carta di debito, avesse riscontrato la presenza di due operazioni da lei non autorizzate per un importo complessivo di € 1.498,00.

Faceva presente di aver bloccato immediatamente la carta di pagamento, precisando di non aver mai comunicato le sue credenziali a soggetti terzi né autorizzato le operazioni tramite OTP.

Chiedeva, pertanto, il rimborso della somma fraudolentemente sottratta, oltre alla corresponsione degli interessi legali.

Si costituiva l'odierno resistente, il quale rilevava che le operazioni contestate fossero state correttamente autenticate, registrate e contabilizzate senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Sosteneva, inoltre, che le operazioni fossero state eseguite personalmente dalla cliente che non aveva mai segnalato il furto o lo smarrimento della carta di debito e, anzi, avesse dichiarato di non averne mai perso il possesso né averla ceduta a terzi.

Osservava che la ricorrente avesse fatto accesso dal proprio abituale *smartphone* e avesse personalmente generato i CVV dinamici propedeutici alle operazioni oggetto di contestazione; di contro, ella non aveva esposto alcun elemento utile a ricostruire una eventuale truffa.

Riteneva quindi evidente la sua colpa grave per non essersi accorta che il suo dispositivo fosse utilizzato da altri o per aver condiviso dati e codici bancari personali con terzi per la corretta esecuzione dei pagamenti.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale sottolineava che la mera generazione o trasmissione di un codice OTP non costituisse di per sé prova di una volontà dispositiva consapevole, né equivallesse ad autorizzazione valida ai sensi del D. lgs. 11/2010, soprattutto in presenza di un contesto chiaramente fraudolento.

Soggiungeva che fosse l'intermediario a dover dimostrare non solo la correttezza tecnica dell'autenticazione, ma anche l'assenza di vulnerabilità del sistema e l'effettiva riconducibilità dell'operazione alla volontà del cliente.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale ribadiva che la cliente non avesse offerto alcun elemento utile a ricostruire una eventuale truffa, né che fosse stata indotta a condividere involontariamente le OTP con terzi.

Rammentava che gli ordini di pagamento non possono essere revocati dopo essere stati ricevuti dal PSP anche poiché la carta di debito è una "tessera di pagamento o di prelievo con addebito immediato sul proprio conto".

Evidenziava che la ricorrente si fosse accorta e avesse contestato detti pagamenti solo 13 giorni dopo la loro esecuzione, incorrendo in colpa grave anche per omesso controllo del proprio conto corrente. Sottolineava che non vi fosse mai stato alcun malfunzionamento nei sistemi di sicurezza della banca né alcun apporto causale da parte della stessa.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni di pagamento, successivamente disconosciute.

La materia, come noto, è regolata dal D. lgs. n. 11/2010 come modificato dal D. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/UE (c.d. PSD2 - *Payment Services Directive 2*).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d.

strong customer authentication - SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA, gli artt. 97 e 98 della direttiva PDS2, nonché l'articolo 10-*bis* del D. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa 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.

In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; ineranza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che le operazioni in parola consistano in due pagamenti online effettuati l'08/10/2025, per l'importo complessivo di € 1.498,00.

L'intermediario afferma che le operazioni siano stata eseguite personalmente dalla ricorrente e che, pertanto, non dovrebbe trovare applicazione la disciplina di cui all'art. 11 D. lgs. 11/2010. Invero, dalle deduzioni e allegazioni delle parti risulterebbe che la cliente abbia autorizzato le operazioni predisposte dal truffatore.

Con riferimento a fattispecie analoghe l'orientamento uniforme dei Collegi ha chiarito che se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il prestatore dei servizi di pagamento.

Laddove, invece, l'operazione di pagamento online sia stata preparata dal truffatore che ha a disposizione i codici dispositivi del cliente, questa non può ritenersi eseguita per intero dal pagatore, e quindi non può considerarsi sussistente il requisito necessario per escludere il regime di responsabilità previsto dalla PSD2.

Ciò rilevato, le tracciate informatiche versate in atti mostrano un accesso effettuato tramite l'utilizzo del riconoscimento biometrico alle ore 13:11; rispetto a tale accesso, tuttavia, l'intermediario non fornisce evidenze tese a dimostrare che il *device* indicato nei log corrisponda a quello certificato della cliente, sebbene dai log lo stesso risulterebbe associato all'*username* che riporta il nome della ricorrente. Non risultano neppure prodotti log relativi ad accessi antecedenti a quello delle 13:11 in esame, effettuati con medesimo *device*, onde verificare la riferibilità all'utenza della cliente. Sul punto, l'odierno resistente si limita ad affermare che il *device* indicato è quello usualmente utilizzato dalla stessa.

La mancanza anche parziale della prova del rispetto dei presidi di sicurezza in tutte le fasi dell'operazione di pagamento, e quindi sin da quella di accesso al sistema, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili alla cliente, costituendo, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Coll. coord., dec. n. 22745/2019).

Deve, pertanto essere riconosciuto il diritto della ricorrente ad ottenere il rimborso del controvalore delle operazioni contestate.

Il Collegio dispone che sulle somme così riconosciute vadano computati gli interessi al tasso legale, a far data dal reclamo.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.498,00, oltre interessi legali dal reclamo al saldo.

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