

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore MARCO CORRADI

Seduta del 31/03/2026

FATTO

La parte ricorrente deduce:

- di aver notato, all'incirca in data 15 agosto 2025, durante una vacanza all'estero, tramite APP un pagamento pari ad € 325,40 eseguito con la sua carta di credito.
- Che il pagamento di BRL 2.000,00 (valuta estera), corrispondenti a € 325,40, era avvenuto in data 17 agosto 2025 presso un negozio di telefonia sito nella città in cui si trovava in vacanza.
- Di non essersi mai recato presso il negozio in cui era stato eseguito il pagamento in quanto molto distante dal luogo in cui alloggiava.
- Che i suoi familiari non avevano effettuato il pagamento presso tale negozio né lui aveva prestato la carta a terzi.

- Di non aver mai effettuato o autorizzato l'operazione e che la carta è sempre stata nella sua esclusiva disponibilità.
- Di aver, accortosi dell'addebito, contattato la banca e annullato la carta temendo una truffa o la clonazione del mezzo di pagamento.

Parte resistente, nel controdedurre, eccepisce:

- che, nella denuncia e nel modulo di disconoscimento, il ricorrente non ha dichiarato il furto o lo smarrimento della carta, bensì ha affermato di non averne mai perso il possesso.
- Di aver inizialmente accreditato l'importo dell'operazione sul conto del ricorrente e, alla luce degli accertamenti svolti, di aver provveduto al riaddebito, dandone comunicazione al cliente in data 18 settembre 2025.
- Che l'operazione contestata risulta autorizzata, alle ore 19:47 del 17 agosto 2025, mediante lettura del microchip della carta fisica e inserimento del codice PIN, in assenza di anomalie.
- Che l'operazione di pagamento è stata correttamente autenticata, registrata e contabilizzata.
- Che il ricorrente non aveva, quindi, osservato gli obblighi di custodia e protezione della carta e del relativo PIN, il quale è unico e irriproducibile.
- Che il cliente avrebbe dovuto custodire con cura, segretamente e separatamente, la carta e il relativo numero personale segreto.
- Che l'autore dell'operazione disconosciuta deve, invece, aver avuto la disponibilità della carta originale e del PIN, il quale ultimo, quindi, deve essere stato conservato congiuntamente allo strumento di pagamento.
- Che sussiste la colpa grave e la grave negligenza del ricorrente, il quale aveva reso direttamente possibile l'esecuzione dell'operazione fraudolenta.
- Che il cliente non ha fornito minimi elementi utili alla ricostruzione della vicenda, limitandosi a disconoscere l'operazione.
- Che, a tutto voler concedere, si può presumere che il ricorrente avesse concesso ad altri la disponibilità della carta e del relativo PIN oppure che ignoti li avessero temporaneamente sottratti, a sua insaputa, per poi ricollocarli nel luogo in cui erano custoditi.
- Che il ricorrente conferma la disponibilità della carta da parte degli altri membri della sua famiglia.

DIRITTO

L'operazione contestata è stata posta in essere sotto il vigore del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2).

L'operazione consiste in un pagamento POS internazionale di € 325,40 eseguito con carta alle ore 19:47 del 17 agosto 2025 presso un negozio di telefonia sito nella città estera in cui il ricorrente si trovava in vacanza.

Dall'evidenza documentale prodotta dall'intermediario risulta che l'operazione contestata sia stata eseguita mediante lettura del microchip della carta fisica (Pos entry mode = 05) e inserimento del codice PIN (Uso PIN = 1), in assenza di anomalie tecniche registrate dal sistema.

La disciplina applicabile alla fattispecie si rinviene nel D.lgs. 27 gennaio 2010, n. 11, il quale reca l'attuazione della direttiva 2007/64/CE, successivamente modificata dalla direttiva (UE) 2015/2366 (cosiddetta PSD2), relativa ai servizi di pagamento nel mercato interno. Il decreto legislativo citato stabilisce specifici obblighi a carico sia degli utenti di servizi di pagamento sia dei prestatori di tali servizi, e definisce altresì il riparto dell'onere della prova nelle controversie aventi ad oggetto operazioni contestate.

In particolare, l'art. 7 del decreto impone all'utente abilitato all'utilizzo di uno strumento di pagamento l'obbligo di utilizzare tale strumento in conformità con i termini che ne regolano l'emissione e l'uso, di comunicare senza indugio al prestatore di servizi di pagamento lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza e, soprattutto, di adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate, quali il codice PIN.

Specularmente, l'art. 8 pone a carico del prestatore di servizi di pagamento che emette uno strumento di pagamento una serie di obblighi di sicurezza, tra cui quello di assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato, di garantire strumenti adeguati affinché l'utente possa comunicare tempestivamente la perdita della disponibilità dello strumento e di impedire qualsiasi utilizzo successivo a tale comunicazione.

Sul piano probatorio, l'art. 10, comma 1 del D.lgs. n. 11/2010 stabilisce che, qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento 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.

Il successivo comma 2 della medesima norma puntualizza in modo inequivoco che, quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7. È onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente.

Questa disciplina trova conferma e specificazione nella giurisprudenza di legittimità e negli orientamenti di questo Arbitro, secondo cui, in tema di responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema, è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di

accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo. Ne consegue che la banca, cui è richiesta una diligenza di natura tecnica da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente.

Quanto al concetto di colpa grave, la giurisprudenza di legittimità ha chiarito che essa si configura quando il comportamento è talmente incauto da non poter essere fronteggiato in anticipo dal prestatore di servizi di pagamento e si manifesta attraverso l'omissione non solo della diligenza media del buon padre di famiglia, ma anche di quel grado minimo ed elementare di diligenza generalmente osservato da tutti. L'istituto bancario che eccepisce la colpa concorrente del titolare della carta per custodia difettosa del codice personale ha l'onere di provare concretamente tale negligenza, la quale non può ritenersi in *re ipsa* per il solo fatto che una tessera bancomat, dopo il furto, sia stata utilizzata illecitamente.

Nel caso concreto, il ricorrente ha fornito una ricostruzione dei fatti estremamente lacunosa e priva di specifiche allegazioni idonee a chiarire le circostanze in cui si sarebbe verificato l'utilizzo fraudolento dello strumento di pagamento. Egli si è limitato a dichiarare di aver notato l'operazione contestata mentre si trovava all'estero, di non essersi mai recato presso il negozio in cui è stata effettuata, di non aver prestato la carta ad alcuno e di averla sempre mantenuta nella propria esclusiva disponibilità. Tuttavia, il ricorrente non ha fornito alcuna allegazione in merito alle modalità concrete di custodia dello strumento di pagamento e del relativo codice PIN, non ha indicato in quale luogo o con quali cautele conservasse la carta e il codice segreto, non ha specificato se il PIN fosse memorizzato o annotato in qualche forma, non ha illustrato le circostanze che avrebbero potuto consentire a terzi di entrare in possesso sia della carta fisica che del codice di accesso.

Tale carenza di allegazioni risulta particolarmente significativa ove si consideri che l'operazione è stata eseguita mediante l'abbinamento corretto di due elementi distinti: il possesso della carta fisica dotata di microchip e la conoscenza del codice PIN. In assenza di qualsivoglia ipotesi ricostruttiva da parte del ricorrente, diviene estremamente difficile, se non impossibile, individuare una dinamica alternativa rispetto a quella prospettata dall'intermediario, secondo cui il ricorrente avrebbe custodito congiuntamente la carta e il relativo codice segreto, ovvero avrebbe comunque adottato modalità di custodia che hanno consentito a terzi l'accesso simultaneo ad entrambi gli elementi necessari per l'esecuzione dell'operazione.

Giova rammentare che i Collegi arbitrali sono soliti valutare negativamente la reticenza del ricorrente in merito alla dinamica dei fatti, in quanto tale atteggiamento processuale impedisce la ricostruzione delle circostanze effettive e ostacola l'accertamento della verità dei fatti (v., *ex multis*, Collegio di Bologna, decisione n. 3888 del 2023; Collegio di Bologna, decisione n. 6676 del 2024).

Nel caso di specie, la scarsa contestualizzazione dei fatti, in presenza della prova della corretta autenticazione delle operazioni mediante tecnologia CHIP e PIN, costituisce indice di colpa grave dell'utente, in quanto lascia presuntivamente ritenere che il ricorrente abbia concesso ad altri la disponibilità della carta e del relativo PIN, oppure che ignoti abbiano avuto tale disponibilità a sua insaputa in ragione di una custodia non diligente.

Come correttamente evidenziato dall'intermediario, è plausibile che ignoti abbiano temporaneamente sottratto la carta e il PIN, per poi ricollocarli, una volta effettuata l'operazione, nel luogo in cui erano custoditi, al fine di non destare sospetti.

Tuttavia, tale evenienza, lungi dall'escludere la responsabilità del ricorrente, ne conferma la colpa grave, in quanto dimostra che lo stesso aveva adottato modalità di custodia tali da consentire la sottrazione temporanea e il successivo ricollocamento di entrambi gli elementi necessari per l'utilizzo dello strumento di pagamento, senza che tale sottrazione venisse immediatamente percepita.

Quanto alla prospettata ipotesi di clonazione della carta, tale circostanza deve essere esclusa alla luce delle evidenze tecniche disponibili. Come affermato dal Collegio di Coordinamento nella decisione n. 897 del 2014, l'impiego della tecnologia a microchip rende l'ipotesi della clonazione, se non di impossibile evenienza, almeno altamente improbabile, facendo dunque ritenere che l'operazione disconosciuta non possa che essere ricondotta ad una conservazione molto distratta della carta e del PIN, salvo che l'utente non fornisca la prova di circostanze tali da far ritenere quanto meno plausibile l'ipotesi della clonazione.

Nel caso di specie, il ricorrente non ha fornito alcun elemento utile a supportare l'ipotesi della clonazione, né ha indicato in quale occasione e con quali modalità tale clonazione sarebbe potuta avvenire. Peraltro, dall'evidenza documentale risulta che l'operazione è stata eseguita mediante lettura del *microchip* della carta fisica e non mediante banda magnetica, il che esclude le modalità di clonazione più comuni basate su dispositivi di *skimming* applicati agli sportelli automatici o ai terminali POS. La clonazione delle carte con *microchip* mediante procedure *hardware*, ossia con l'ausilio di macchinari sofisticati quali microscopi elettronici che consentano di superare i contatti elettrici che coprono il *microchip* e leggere i dati memorizzati al suo interno, richiede competenze tecniche elevate, strumentazioni particolari e tempi di lavorazione incompatibili con la dinamica di un utilizzo fraudolento occasionale durante un soggiorno turistico all'estero.

Considerato, pertanto, che il ricorrente ha negato di aver subito il furto della carta e ha dichiarato di averne mantenuto costantemente il possesso, e considerato che l'operazione in questione è stata effettuata mediante corretto abbinamento di CHIP e PIN, la mancata autorizzazione dell'operazione contestata non può essere presunta bensì deve essere provata dalla parte che chiede la restituzione.

In presenza dell'evidenza documentale della corretta autenticazione dell'operazione e in assenza di qualsivoglia elemento probatorio o anche solo indiziario circa le modalità con cui terzi avrebbero potuto entrare in possesso sia della carta fisica che del codice PIN, deve ritenersi che il ricorrente non abbia assolto all'onere di fornire elementi minimi di ricostruzione della vicenda, e che l'intermediario abbia invece fornito la prova presuntiva della colpa grave del ricorrente nella custodia dello strumento di pagamento e delle relative credenziali di sicurezza personalizzate.

Alla luce di quanto sopra esposto, il Collegio ritiene pertanto che, con riferimento all'operazione contestata, nella condotta dell'utilizzatore dello strumento di pagamento siano ravvisabili gli estremi della colpa grave ai sensi degli artt. 7, comma 2, e 12, comma 4, del D.lgs. n. 11 del 2010, per non avere parte ricorrente custodito con le dovute cautele né lo strumento di pagamento, né il codice PIN, ovvero per averli custoditi in modo tale da consentire a terzi l'accesso simultaneo ad entrambi gli

elementi necessari per l'esecuzione dell'operazione fraudolenta. Tale colpa grave esclude la responsabilità dell'intermediario ai sensi della disciplina applicabile e comporta che il ricorrente sopporti tutte le perdite derivanti dall'operazione di pagamento non autorizzata.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE