

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 14/04/2026

FATTO

Il ricorrente, insoddisfatto degli esiti dell'interlocuzione intercorsa nella fase di reclamo, adiva questo Arbitro deducendo che – nonostante le segnalazioni e la denuncia sporta alle autorità per sospetta clonazione e accesso abusivo ai sistemi – l'intermediario non avesse fornito prove tangibili in relazione alle operazioni contestate.

Chiedeva, pertanto, di accertare la responsabilità della banca per chiusura ingiustificata del conto corrente; di ordinare la riattivazione immediata del conto e della carta e il riaccredito immediato di "tutte le somme indebitamente addebitate e non autorizzate" (somme che, tuttavia, non sono in alcun modo individuate/quantificate), con richiesta di consegna di Log/tracciature; il tutto oltre al risarcimento dei danni patrimoniali e non patrimoniali subiti e all'inibitoria di ulteriori richieste di pagamento / segnalazioni in CRIF da parte della banca.

Si costituiva ritualmente l'intermediario convenuto, il quale eccepiva preliminarmente l'inammissibilità della domanda volta ad ottenere la riattivazione immediata del rapporto, che implica una decisione costitutiva.

Nel merito, osservava che il proprio recesso dal rapporto fosse avvenuto nel rispetto delle Condizioni Generali di Contratto, che, in presenza di giustificato motivo, legittimano il preavviso di 1 giorno; precisava di aver esercitato il diritto di recesso mediante l'invio di apposita lettera raccomandata a.r.

del 4 agosto 2025, regolarmente ricevuta in data 8 agosto 2025, nella quale veniva evidenziato che la decisione di recedere dal rapporto fosse stata assunta “in considerazione di giustificati motivi attinenti alla sicurezza” e veniva concesso al cliente un termine di preavviso conforme a quanto previsto dalle condizioni contrattuali.

Evidenziava che la prospettazione del cliente contenuta nella “Denuncia Via PEC per Clonazione carta ed accesso abusivo informatico” del 29 settembre 2025 apparisse, sotto molteplici profili, lacunosa e contraddittoria, tanto da sollevare legittimi dubbi circa la reale dinamica dei fatti.

Con riferimento al furto della carta, avvenuto il 21 marzo 2025 in circostanze non meglio precisate, osservava che il cliente non avesse mai contestato, prima dell’odierno ricorso, la transazione effettuata in data 22 marzo 2025 di € 5,22; sottolineava, in ogni caso, che la transazione in parola fosse stata disposta tramite la funzione contactless della carta prima dell’orario in cui il cliente aveva richiesto il blocco dello strumento di pagamento in questione (ore 9:10 del giorno 22 marzo 2025).

Con riferimento alle transazioni declinate per motivi di sicurezza, evidenziava una rilevante incoerenza tra quanto dichiarato dal ricorrente nella denuncia e il reclamo dallo stesso presentato nel mese di giugno 2025; con comunicazione del 13 giugno 2025 questi aveva segnalato che la carta fosse stata rifiutata per sospetta frode ed in tale occasione dichiarava espressamente di essere l’unico utilizzatore della carta e che l’utilizzo fosse pienamente legittimo, mentre con il reclamo contestava il mancato perfezionamento di alcuni pagamenti effettuati tramite tale carta e la mancata disposizione di un bonifico istantaneo. Soggiungeva di aver fornito riscontro informando che le transazioni risultassero prive dell’autenticazione.

Faceva poi presente che nella denuncia il ricorrente avesse disconosciuto, peraltro in termini del tutto generici, diverse operazioni, che neppure si era premurato di individuare in modo completo.

Nonostante la genericità e la contraddittorietà delle contestazioni, riteneva che il cliente avesse inteso disconoscere l’importo di € 1.543,28, che corrisponde all’ammontare delle spese effettuate nel mese di agosto 2025 tramite la carta.

A tale riguardo, affermava che le operazioni in contestazione fossero state tutte regolarmente autorizzate; rappresentava, peraltro, che nella denuncia il ricorrente non avesse dichiarato di essere stato vittima di furto o sottrazione indebita della Carta, la quale era quindi nella sua disponibilità.

Dichiarava, inoltre, che numerose transazioni risultassero effettuate presso esercenti abitualmente frequentati dal cliente nei mesi precedenti, senza che ne fosse mai stata contestata la paternità, e che con la medesima carta fossero stati eseguiti due prelievi Bancomat, che non risultavano essere stati disconosciuti.

Riferiva di aver segnalato al ricorrente lo sconfinamento dovuto alla registrazione del saldo negativo sul conto conseguente all’addebito oggetto di contestazione.

Segnalava, infine, che l’addebito di € 1.412,81 del 5 agosto 2025 a titolo “Estratto Conto al 30/06/25 Carta di Credito di ... Posizione N° 4030*****9387” derivante dal doppio addebito delle spese effettuate nel mese di giugno 2025 con la Carta, frutto di un’anomalia operativa, fosse stato tempestivamente e correttamente stornato, con giusta valuta.

Circa il lamentato utilizzo indebito e la falsificazione degli strumenti di pagamento, nonché la frode informatica, rilevava che il ricorrente non avesse chiarito le modalità con cui le sue credenziali di accesso sarebbero state eventualmente compromesse, né avesse fornito alcuna spiegazione su come l'“accesso abusivo ai sistemi informatici” si sarebbe concretamente realizzato; segnalava pure che egli avesse ommesso di riferire se avesse provveduto ad effettuare le necessarie verifiche sui dispositivi utilizzati (smartphone, PC, tablet) per accertare l'eventuale presenza di malware o altri strumenti di compromissione.

Precisava, ad ogni modo, che le verifiche tecniche eseguite non avessero rilevato alcun accesso abusivo alla posizione del cliente e che non avesse effettuato alcuna iscrizione pregiudizievole presso le banche dati preposte ad eccezione di un'informazione di tipo positivo, relativa alla carta di credito accordata in fase di apertura del conto corrente.

Da ultimo, contestava la fondatezza della richiesta risarcitoria, sprovvista di qualsiasi allegazione documentale e supporto probatorio.

Chiedeva, pertanto, di dichiarare l'inammissibilità della domanda di riattivazione immediata del conto e di rigettare il ricorso per il resto.

DIRITTO

Dall'esame dei reclami che hanno preceduto il ricorso, l'oggetto del ricorso attiene alla presunta illegittimità del recesso dal rapporto di conto corrente e da tutti i servizi a esso collegati, comunicato dall'intermediario a mezzo raccomandata con un preavviso di un solo giorno dal ricevimento, senza alcuna preventiva segnalazione e con la generica motivazione di “violazione della sicurezza”, nonché la natura fraudolenta di una serie di operazioni asseritamente non autorizzate; in relazione a tali contestazioni, le domande proposte dal ricorrente riguardano l'accertamento di tale illegittimo esercizio del recesso, con conseguente obbligo di riattivazione del conto e della carta, oltre al rimborso del controvalore dei pagamenti contestati e al risarcimento dei danni asseritamente subiti e alla inibitoria di ulteriori richieste di pagamento.

Ciò chiarito in premessa, il Collegio deve rilevare che l'odierno resistente abbia eccepito l'inammissibilità del ricorso, con riferimento alla domanda volta ad ottenere l'immediata riattivazione del conto corrente, la quale solleciterebbe una decisione di natura costitutiva, preclusa a questo Arbitro. L'eccezione è infondata e non merita accoglimento.

In applicazione dei poteri di interpretazione della domanda pure riconosciuti al Collegio, infatti, essa può considerarsi alla stregua di una domanda di accertamento della inefficacia del recesso esercitato dall'intermediario, con la conseguenza che il rapporto contrattuale non potrebbe essere considerato unilateralmente risolto.

Con riguardo al merito, emerge documentalmente che l'intermediario abbia ritualmente comunicato (a mezzo raccomandata con avviso di ricevimento) il recesso dal rapporto di conto corrente, secondo quanto previsto dall'art. 26 delle condizioni generali, che attribuisce alla banca la facoltà di recedere dal contratto con preavviso di un giorno, al ricorrere delle fattispecie espressamente indicate o, comunque, “in presenza di ... giustificato motivo”. Sul punto, mette conto rilevare che parte resistente

abbia prodotto esclusivamente un estratto delle condizioni generali di contratto, dal quale non è possibile evincere se queste siano state sottoscritte dal ricorrente. In ogni caso, il cliente non ha contestato specificamente tale produzione documentale, dovendosi di conseguenza ritenere che dette condizioni siano quelle effettivamente applicabili al rapporto dedotto.

Con riguardo all'esercizio del recesso, giova rammentare che – in base al disposto degli artt. 1373 e 1855 cod. civ. – sia riconosciuto agli intermediari il diritto potestativo di recedere unilateralmente da un contratto a tempo indeterminato, a condizione che ne venga dato idoneo preavviso all'altro contraente e sempre che il concreto esercizio del recesso non si sostanzi in una condotta contraria alla buona fede, ex art. 1375 cod. civ.

In relazione al richiamato quadro normativo, il consolidato orientamento dei Collegi territoriali di questo Arbitro ha pure riconosciuto la legittimità della scelta degli intermediari di sciogliersi *ad nutum* dal vincolo contrattuale e senza bisogno di alcuna motivazione specifica, fatto salvo l'onere di preavviso “nel termine stabilito dagli usi o, in mancanza, entro quindici giorni”. Pertanto, ancorché vada riconosciuta alla banca la facoltà di procedere allo scioglimento unilaterale di un rapporto contrattuale a tempo indeterminato, senza alcun obbligo di esplicitarne le ragioni, deve pure affermarsi che – se il recesso è esercitato in assenza del preavviso d'uso, invocando un giustificato motivo – sussiste in capo alla stessa un onere di esplicitare in maniera adeguata le motivazioni del recesso.

Nel caso di specie, la legittimità del recesso intimato in forza dell'apposita previsione contrattuale non potrebbe che derivare dalla rispondenza della situazione concreta a quelle espressamente previste dalle condizioni generali o, in mancanza, alla sussistenza di un “giustificato motivo” non tipizzato, che richiederebbe comunque un'adeguata motivazione al riguardo da parte della banca.

Da quanto risulta *per tabulas*, l'odierno resistente ha comunicato il recesso per giustificato motivo con il preavviso contrattuale di un giorno, certamente inferiore ai termini d'uso, in conformità alle previsioni contrattuali; nella comunicazione ci si è limitati a richiamare a fondamento del recesso, “giustificati motivi attinenti alla sicurezza”, senza altro specificare.

Per quanto, *prima facie*, tale motivazione appaia del tutto generica ed arbitraria, in quanto tale inidonea a giustificare lo scioglimento unilaterale del rapporto, sono proprio le circostanze del caso concreto (ed in particolare le risultanze documentali relative alle operazioni in contestazioni, che farebbero emergere un fondato sospetto di frode) a legittimare l'esercizio del diritto potestativo da parte della banca.

Pertanto, alcuna censura può essere mossa con riguardo al recesso dell'intermediario dal rapporto di conto corrente in esame e da quelli ad esso collegati.

Quanto alla domanda di rimborso delle operazioni di pagamento contestate, mette conto rilevare in premessa che nella denuncia rilasciata alle autorità il ricorrente abbia dichiarato il furto della propria carta, che sarebbe avvenuto in circostanze non meglio precisate, in seguito al quale sarebbe stata eseguita un'operazione contactless da € 5,22 (che tuttavia non risulta formare oggetto di formale disconoscimento), oltre a “movimenti e addebiti anomali sul conto e sulla carta di credito collegata, relativi a prelievi da ATM e pagamenti per somme piccole presso diversi esercizi commerciali per una vastissima quantità di piccole somme”, per un totale di € 1.543,28; operazioni che vengono formalmente contestate.

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 sconosciute.

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; inerenza; 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.

Nel caso di specie, da quanto emerge documentalmente, deve osservarsi che i pagamenti contestati sono stati effettuati con diverse modalità di autenticazione: alcuni di questi risultano autorizzate mediante utilizzo della carta dotata di microchip (elemento di possesso) e corretto inserimento del PIN (elemento di conoscenza); altri, avvenuti in modalità contactless, risultano autorizzati mediante utilizzo della carta, senza inserimento del PIN, trattandosi di operazioni di importo modesto, inferiori alla soglia di € 50,00 per singolo pagamento in relazione alla quale l'art. 11 del Regolamento Delegato (UE) 2018/389 ("Pagamenti senza contatto fisico al punto vendita") prevede apposita esenzione dall'autenticazione forte; due ulteriori transazioni risultano eseguite tramite utilizzo del "Mobile code" (servizio dell'App associato al dispositivo indicato dal cliente, che consente di autorizzare il pagamento in alternativa al PIN) ed autorizzate mediante ricorso a un fattore di inerenza (il Mobile code biometrico) e a un fattore di possesso (il device del cliente sul quale è stata inviata la push).

Dall'esame delle tracciature informatiche versate in atti risulta, dunque, che dette operazioni siano state eseguite in modalità conforme a SCA.

A fronte di tali pagamenti, ve ne sono altri per i quali – di contro – la documentazione versata in atti non consente di ritenere provata l'autenticazione forte. In particolare, emerge una transazione eseguita tramite un account in uso al cliente, a fronte della memorizzazione delle credenziali della propria carta presso il commerciante (cd. "credential on file") in occasione di una transazione precedentemente effettuata, che deve essere fatta rientrare tra le cc.dd. "operazioni ricorrenti" per le quali il Regolamento Delegato (Ue) 2018/389 dispone che un pagatore può creare, modificare o disporre operazioni ricorrenti dello stesso importo e a favore dello stesso beneficiario per le quali è prevista l'applicazione della SCA del cliente da parte del PSP la prima volta che avviene la creazione, modifica o disposizione della serie di operazioni ricorrenti mentre per quelle successive, con stesso importo e a favore del medesimo beneficiario, i PSP sono autorizzati a non applicare la SCA, pur rimanendo onerati del rispetto degli obblighi generali di autenticazione. Nel caso di specie non vi è prova che la prima operazione (peraltro neppure individuata) sia stata autentica mediante SCA.

Accanto a tale transazione, risulta poi un pagamento effettuato con inserimento dei dati della carta; in relazione a tale ipotesi, va rammentato che l'EBA – nella "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2" – ha sottolineato che l'inserimento dei dati statici stampati sulla carta, ivi incluso il CVV, non costituisce un elemento riconducibile alla categoria della conoscenza o del possesso, e quindi utile per l'autenticazione forte; anche il consolidato orientamento dei Collegi territoriali ha evidenziato che l'autenticazione avvenuta con i dati statici della carta, pure incautamente forniti dall'utilizzatore al truffatore, non può essere considerata una procedura sicura di autorizzazione dell'operazione, in mancanza di ulteriori elementi di carattere dinamico.

Risulta, infine, un'ulteriore operazione che – per quanto l'intermediario non abbia descritto le modalità di autenticazione – risulta avvenuta in modalità M.O.T.O. ("mail order/telephone order") mediante la fornitura dei dati della carta di pagamento al telefono o per posta. Con riferimento a dette operazioni, questo Collegio ha già avuto modo di affermare che il regime di responsabilità tra le parti è regolato dalle norme di diritto comune, per cui l'intermediario è tenuto a dimostrare di aver verificato la provenienza dell'ordine dal pagatore con la diligenza professionale qualificata di cui all'art. 1176 comma 2 cod. civ.; in caso contrario, risponde per intero dell'operazione fraudolenta (Collegio di Milano, decisione n. 7847 del 20 agosto 2025). Nel caso di specie, l'intermediario non ha dimostrato alcunché (né le modalità di una eventuale transazione M.O.T.O., né fattori di autenticazione ove l'operazione fosse stata altrimenti autenticata).

Indipendentemente dalla prova relativa all'autenticazione forte, che – secondo il principio di diritto affermato dal Collegio di coordinamento – rappresenta un *prius* logico, in aderenza al dato normativo (cfr. Coll. coord., dec. n. 22745/2019), la condotta del cliente (per quanto emerge dalle allegazioni delle parti e dalla documentazione versata in atti) assume un decisivo rilievo.

Deve, infatti, tenersi conto che – come dedotto dall'intermediario – nell'arco temporale interessato nel quale le operazioni contestate sono state eseguite (30/07 – 20/08) – il ricorrente ha eseguito molteplici operazioni genuine con il medesimo strumento di pagamento asseritamente utilizzato anche per le operazioni oggi contestate; in particolare, nella giornata dell'08.08.2025 risultano prelievi a uno sportello ATM non sconosciuti e, quindi, pacificamente riferibili al cliente.

Allo stesso tempo, la documentazione in atti evidenzia che quasi tutti i pagamenti disconosciuti si riferiscono ad esercenti abitualmente frequentati ovvero a servizi fruiti nei mesi precedenti dal cliente, in maniera legittima e in assenza di qualsivoglia disconoscimento.

L'insieme delle riferite evidenze documentali appare idoneo a fondare la presunzione di una condotta fraudolenta posta in essere direttamente dal pagatore, tanto più se tiene conto del fatto che la asserita truffa non è in alcun modo circostanziata, sicché nessun elemento utile è fornito che possa fondare una diversa ricostruzione dell'accaduto (cfr. Coll. Milano, dec. nn. 8463, 8464 e 8465/2025; n. 8393/2025).

A tale riguardo, va ricordato che l'art. 12 del D.lgs. n. 11/2010 tiene indenne il cliente dalle perdite derivanti dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente "salvo il caso in cui abbia agito in modo fraudolento". Coerentemente, la Comunicazione di Banca d'Italia del 30 ottobre 2023 chiarisce: "Un'eccezione all'obbligo di rimborso opera nel caso in cui il PSP abbia il motivato sospetto che l'operazione non autorizzata derivi da un comportamento fraudolento posto in essere dall'utente dei servizi di pagamento, come indicato dalla direttiva 2015/2366/UE - PSD2 (art. 11, comma 2, del d. lgs. n. 11/2010)" (cfr. Coll. Milano, dec. n. 2371/2026).

Pertanto alcun rimborso può essere riconosciuto in favore del ricorrente.

Alle medesime conclusioni deve pervenirsi con riguardo alla domanda risarcitoria, per la quale manca qualsivoglia elemento di prova sia con riguardo all'illecito contestato, sia con riguardo ai danni asseritamente subiti.

Al tale ultimo riguardo, appare sufficiente richiamare il principio di diritto espresso dal Collegio di coordinamento, che ha avuto modo di precisare che "spetta al cliente il risarcimento del danno patrimoniale, la cui sussistenza ed entità egli sia in grado di dimostrare, nonché del danno non patrimoniale, la cui sussistenza non è in re ipsa, ma deve essere provata anche facendo ricorso a presunzioni semplici e a nozioni di comune esperienza; in tal caso si potrà ricorrere alla liquidazione equitativa ma rimane onere della parte ricorrente indicare al Collegio idonei elementi di valutazione" (cfr. dec. n. 1642/2019).

Residuano le ulteriori domande avanzate dal ricorrente in ordine all'inibitoria delle intimazioni di pagamento del saldo di conto e delle iscrizioni nei sistemi di informazione creditizia.

Quanto alla prima, il Collegio si limita a rilevare che, dal momento in cui gli addebiti oggetto di odierna contestazione hanno comportato la registrazione di un saldo negativo sul conto corrente, pari all'importo del debito, l'intermediario abbia correttamente segnalato al cliente lo sconfinamento. Tuttavia, non risultando ad oggi esperite azioni di recupero del credito null'altro può essere disposto in via inibitoria dall'Arbitro.

Quanto alla seconda, l'odierno resistente ha chiarito che, ad oggi, non è stata effettuata alcuna iscrizione pregiudizievole presso le banche dati preposte a carico del cliente; pertanto, non risultando neppure in via documentale che alcuna intimazione sia stata trasmessa a tale riguardo, la richiesta sembra riferirsi ad una situazione meramente ipotetica in relazione alla quale non può essere riconosciuto alcun interesse ad agire.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE