Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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

Relatore (MI) BARTOLOMUCCI

Seduta del 31/03/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che, in data 17/08/2025, dopo aver riscontrato le prime operazioni anomale sull'app del proprio conto corrente, avesse perso il controllo dell'accesso alla stessa a seguito del furto delle credenziali.
Faceva presente di essere venuto a conoscenza dell'esecuzione di numerose operazioni non autorizzate effettuate mediante le proprie carte di credito, di debito e prepagata, per un importo complessivo pari ad € 5.545,17, con contestuale perdita di accesso all'app bancaria; precisava che, non potendo contattare immediatamente il servizio clienti in quanto giornata festiva, avesse provveduto tempestivamente a bloccare le carte e a presentare denuncia alle competenti Autorità.
Affermava di essere stato rimesso in condizione di accedere al conto in data 28/08/2025 e di aver formalmente disconosciuto le operazioni, ottenendone inizialmente l'integrale rimborso; soggiungeva, tuttavia, che dopo circa due mesi e mezzo, l'intermediario avesse riaddebitato integralmente l'importo precedentemente rimborsato, motivando genericamente tale decisione con una presunta "criticità nella custodia delle credenziali utilizzate per l'autorizzazione di alcune delle transazioni con carta", senza fornire ulteriori chiarimenti.
Chiedeva, pertanto, il rimborso dell'importo complessivo di € 5.545,17.

Si costituiva l'odierno resistente il quale rilevava che i log informatici prodotti in atti attestassero la corretta autenticazione, contabilizzazione e registrazione delle operazioni contestate, nonché la regolare installazione dell'App su un nuovo dispositivo nel rispetto della Strong Customer Authentication, articolato nell'inserimento di credenziali di conoscenza (codice cliente, data di nascita e PIN), nell'utilizzo di un elemento di possesso (OTP inviato via SMS al numero di telefono registrato) e nella successiva autorizzazione tramite Smart Code dal medesimo dispositivo su cui era stata installata l'App.

Riteneva che il cliente fosse caduto vittima, se del caso, di una frode realizzatasi comunque con la cooperazione dello stesso, il quale avrebbe necessariamente comunicato a terzi credenziali personali riservate (codice cliente, data di nascita, PIN e codice OTP), consentendo così l'installazione della nuova App su un nuovo dispositivo in data 15/08/ 2025 alle ore 22:57.

Considerava sussistente la colpa grave del cliente in quanto l'installazione dell'App su un nuovo dispositivo non avrebbe potuto avvenire senza la comunicazione a terzi di codici personali e dell'OTP ricevuto sul proprio numero di telefono, nonché in quanto il cliente, pur avendo ricevuto una notifica e-mail di alert relativa all'installazione dell'App su un nuovo device, non avrebbe contattato tempestivamente il servizio clienti per bloccare gli strumenti di pagamento, consentendo così il perfezionarsi delle operazioni effettuate alcune ore dopo l'enrollment.

Evidenziava, peraltro, che non fossero stati riscontrati malfunzionamenti, anomalie o intrusioni nei sistemi informatici dell'intermediario, risultando dai log una procedura regolare di associazione del dispositivo e di autorizzazione delle disposizioni di pagamento.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale affermava che controparte non avesse assolto al proprio onere probatorio, avendo fornito una mera descrizione astratta del sistema di autenticazione SCA senza dimostrare in concreto la sussistenza di frode, dolo o colpa grave a suo carico.

Evidenziava che la frode si fosse consumata in luoghi (Austria e Spagna) diversi da quello in cui egli si trovava (Sardegna), con modalità a lui ignote e non percepibili tempestivamente, senza alcuna sua cooperazione o negligenza, non avendo mai comunicato credenziali né lasciato incustoditi i propri dispositivi; soggiungeva, peraltro, che la ricezione, in orario notturno e in giorni festivi, di OTP ed e-mail di configurazione dell'App su nuovo dispositivo e di modifica dell'indirizzo e-mail dimostrerebbe non già una sua colpa, ma la sofisticazione della frode e l'impossibilità di un intervento tempestivo, anche in ragione dell'assenza del servizio clienti nel fine settimana.

Sottolineava che alcune operazioni fossero state bloccate dallo stesso intermediario nella medesima giornata del 17 agosto, circostanza che dimostrerebbe la rilevabilità dell'anomalia da parte della banca e l'incongruenza della tesi secondo cui per alcune operazioni sussistevano anomalie e indici di frode e per altre no.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale ribadiva che l'App fosse stata installata il 15/08/2025 alle ore 22:57 su nuovo dispositivo mediante inserimento di Codice Cliente,

data di nascita, PIN e OTP inviato al numero di telefono del cliente, previa notifica e-mail di alert, circostanza che confermerebbe la cooperazione colposa del medesimo.

Quanto alla dedotta assenza del servizio clienti nel fine settimana, precisava che il blocco delle carte è garantito 24/7 tramite numeri dedicati e che è altresì possibile procedere autonomamente al blocco tramite Area Riservata, escludendo quindi l'impossibilità di un intervento tempestivo.

DIRITTO

La domanda proposta dal 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; 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.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Risulta documentalmente che le operazioni in parola consistono in n. 11 pagamenti effettuati in parte con carta di debito, in parte con carta di credito e in parte con carta prepagata, tutte intestate al ricorrente ed eseguite in data 17/08/2025, per il complessivo importo di € 5.545,17.

Quanto al processo di autenticazione, l'odierno convenuto chiarisce che le operazioni contestate sono state precedute, alle ore 22.57.21 del 15/08/2025, dall'installazione dell'APP della banca su un nuovo device, descrivendo i singoli passaggi dell'*iter*: In particolare afferma che alle ore 22.55.49 il truffatore ha digitato il Codice Cliente e la propria data di nascita e conferma cliccando sul bottone "Continua", per poi digitare (alle ore 22.55.51) le tre cifre del PIN richieste e confermare cliccando sul bottone "Continua".

Ottenuto riscontro positivo dal sistema, alle ore 22.56.39, è stato scelto il codice segreto (Smart Code) ed è stata effettuata la scelta se utilizzare o meno i propri dati biometrici per accedere all'app e autorizzare le operazioni. Alle ore 22.56.58 la banca ha inviato un sms OTP al numero di telefono che corrisponde a quello dichiarato dal cliente in sede di denuncia; risulta pure in atti il testo di un ulteriore sms ricevuto dalla ricorrente, che potrebbe coincidere con l'OTP a lei richiesto per l'enrollment su altro dispositivo.

Da ultimo, è stato inserito il Codice OTP ricevuto via SMS che ha ottenuto la validazione della banca alle ore 22.57.20. All'esito di tali passaggi, alle ore 22.57.21 la banca ha completato l'attivazione dell'APP sul nuovo dispositivo ed ha inviato la relativa e-mail di notifica.

Sulla scorta di tali risultanze documentali, deve ritenersi che l'accesso all'area riservata sia avvenuto in modalità conforme a SCA, mediante l'utilizzo dei due fattori di autenticazioni: il PIN (fattore di conoscenza) e l'SMS OTP (fattore di possesso).

Emerge altresì dall'analisi delle tracciature informatiche che le operazioni di carattere dispositivo siano state precedute dai rispetti accessi all'App scaricata sul nuovo device precedentemente enrollato; tali accessi risultano eseguiti in modalità conforme a SCA, tramite l'applicazione (fattore di possesso) e la digitazione dello Smart Code (fattore di conoscenza).

Con riferimento alla fase dispositiva, l'intermediario non ha fornito i log relativi ad una delle operazioni effettuate tramite carta prepagata e a quelle eseguite tramite carta di credito e carta di debito, tutte intestate al ricorrente (per un totale di cinque delle undici operazioni contestate).

Rispetto ad esse, dunque, la mancata produzione delle tracciature informatiche deve essere considerata alla stregua della mancata prova di conformità a SCA, il cui onere grava sull'intermediario, con la conseguenza che debba essere riconosciuto il diritto della ricorrente ad ottenerne l'integrale restituzione.

Con riguardo alle operazioni residue, i log prodotti evidenziano che esse siano state tutte autenticate mediante la ricezione della notifica push sul device precedentemente enrollato (fattore di possesso) e con la conseguente validazione della push con inserimento PIN, mediante Smart Code (fattore di conoscenza).

Attesa la conformità a SCA dell'operazione contestata, non resta che verificare se – dalla condotta tenuta dalla ricorrente – siano evidenziabili profili di colpa grave, rispetto alla quale la prova di

autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

A tale proposito, il cliente non ha riferito nulla in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento; nella denuncia e nel ricorso infatti rappresenta solo di aver subito il blocco dell'accesso all'app dell'intermediario e di aver ricevuto diverse e-mail riguardo all'avvenuto cambio dei dati legati alla sua applicazione, e altre notifiche di autorizzazione di pagamenti.

Tali circostanze appaiono pure confermate dalle risultanze documentali; per un verso, infatti, emerge che tra le ore 4.20 e le ore 4.23 del 17.08.25 – nel mentre venivano eseguite le operazioni fraudolente – il ricorrente riceveva diverse e-mail che lo avvisavano dell'avvenuta modifica dei dati associati al suo account nell'app dell'intermediario; per altro verso, risultano alcune notifiche push con richiesta di autorizzazione delle rispettive operazioni, successive al blocco, che non è chiaro come abbia fatto a ricevere.

Le risultanze documentali appaiono, dunque, idonee a fondare la presunzione per cui sia stato lo stesso cliente a fornire i codici dispositivi ai truffatori, onde consentire loro di disporre l'enrollment del dispositivo e, successivamente, di eseguire i pagamenti contestati.

Pertanto, attesa la conformità a SCA delle rispettive operazioni ed in considerazione della colpa grave del ricorrente, alcun ulteriore rimborso può essere disposto in favore di quest'ultimo, ad eccezione di quello relativo ai pagamenti per i quali l'intermediario non ha inteso produrre le rispettive tracciature informatiche.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.596,00.
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