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) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 14/05/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 12/07/2024, un sms da un'utenza che appariva con la denominazione "CARTA **", con il quale veniva comunicato il diniego di una transazione su un sito internet per € 1.106,00, con richiesta di contattare un'utenza mobile per informazioni e blocco.
Faceva presente che, avendo effettivamente acquistato nei giorni precedenti alcuni prodotti da tale sito web, avesse contattato il numero indicato sul messaggio, ma la linea cadeva senza risposta; soggiungeva di essere stata in seguito contattata telefonicamente da un numero riconducibile all'intermediario presso cui è radicato il conto corrente e il sedicente operatore bancario le chiedeva di collegarsi all'home banking tramite l'applicazione installata sul telefono cellulare per confermare il blocco delle transazioni sospette.
Precisava di aver eseguito l'accesso al conto corrente tramite l'app e di aver constatato la presenza di alcuni pagamenti bloccati che figuravano in attesa di autorizzazione che provvedeva ad annullare.
Rappresentava di essere stata contattata, in data 15/07/2024, dal personale della propria filiale, che le riferiva di aver bloccato alcune operazioni di bonifico estero e le chiedeva l'autorizzazione per bloccare

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

l'operatività del conto corrente; sottolineava che, in occasione della concessione di detta autorizzazione, avesse riferito quanto accaduto nei giorni precedenti al suo interlocutore che la rassicurava dell'appartenenza del numero ad uno dei loro uffici e della correttezza della procedura seguita, anche in seguito alla denuncia già sporta dalla ricorrente.
Sosteneva poi che, nel corso della medesima mattinata, fosse stata contattata nuovamente dall'utenza riconducibile all'Intermediario e avesse così provveduto ad annullare ulteriori operazioni sospette collegandosi al proprio conto corrente tramite applicazione e senza fornire alcuna credenziale di accesso.
Evidenziava che, solo in data 18/07/2024, accedendo al proprio conto, avesse constatato di avere il saldo azzerato e che risultassero pagamenti che non aveva disposto, sia tramite carta di credito che tramite bonifico e di cui non aveva ricevuto alcuna notifica e/o richiesta di autorizzazione.
Affermava di essersi attivava personalmente per il blocco della carta di credito e del conto corrente, contattando la filiale che le comunicava che aveva subito una truffa e apprendeva così che, inspiegabilmente, il conto corrente non fosse stato bloccato a seguito della telefonata del 15/07/2024.
Seguiva denuncia alle autorità e disconoscimento delle operazioni.
Riteneva sussistente una grave responsabilità a carico dell'intermediario per non aver adottato le misure idonee ad impedire l'illecito utilizzo della carta da parte dei truffatori e per non aver rispettato la corretta procedura di autenticazione ed autorizzazione delle operazioni, dal momento che non lei non aveva fornito ad alcuno le proprie credenziali, non aveva eseguito o comunque autorizzato le operazioni fraudolente e non aveva ricevuto alcuna notifica in occasione dei pagamenti.
Peraltro segnalava che le operazioni illecite, ossia due pagamenti di importo pari ad € 500,00 ciascuno eseguiti quasi contestualmente, presentassero profili di anomalia che avrebbero imposto un doveroso monitoraggio da parte dell'intermediario.
Chiedeva, pertanto, il rimborso delle somme fraudolentemente sottratte.
Si costituiva l'intermediario convenuto, il quale – dopo aver precisato che il presente ricorso avesse fatto seguito ad altro presentato dalla cliente, per la medesima vicenda, anche nei confronti di un diverso intermediario, il quale era stato rigettato per inammissibilità, essendo stato proposto cumulativamente nei confronti di distinti intermediari per transazioni di competenza esclusiva dell'uno e dell'altro – rilevava che la versione dei fatti riportata dalla ricorrente non fosse credibile, né provata, oltre che in contrasto che quanto risultante dai LOG e dalle stesse dichiarazioni rilasciate dalla cliente nella denuncia, in cui ella non aveva fatto riferimento ad alcuna telefonata del 12/07/2024, affermando anzi che tutti i fatti fossero avvenuti il 15/07/2024.
Affermava, di contro, che le transazioni fossero state consapevolmente autorizzate dalla stessa e per tale motivo, considerava inapplicabile la disciplina prevista dall'art. 10, co. 2 del D. Lgs 11/2010.
Ribadiva che, dall'analisi dei log, le transazioni contestate risultassero correttamente contabilizzate, registrate ed autenticate tramite il device della ricorrente; osservava, infatti, che la ricorrente avesse ricevuto i messaggi autorizzativi delle due transazioni che aveva autenticato tramite l'APP installata sul suo device con inserimento dei suoi dati biometrici.
Contestava la tardività del blocco della carta, richiesto solo in data 18.07.2024, ovvero tre giorni dopo le transazioni contestate, nonché l'ulteriore allegazione contenuta nel ricorso, precisando di contro che, in occasione delle due transazioni, avesse inviato al cellulare della cliente le notifiche push e 2 sms alert relative alle transazioni in corso.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Evidenziava pure che, successivamente alle due transazioni contestate, vi fossero altre transazioni effettuate con la medesima carta, dalla ricorrente, che la stessa non aveva contestato, assumendosene la paternità; circostanza, questa, che escludeva l'ipotesi di della clonazione dello strumento di pagamento.
Riteneva sussistente la colpa grave della ricorrente che, peraltro, non aveva offerto una compiuta e documentata ricostruzione dei fatti, limitandosi a riferire di aver effettuato una telefonata di cui non vi era prova verso un numero di cellulare sconosciuto e allegando solo uno dei messaggi ricevuti sulla propria utenza, il quale peraltro era facilmente rilevabile come falso, atteso che proveniva da un mittente che non corrisponde a quello originale.
Di contro, sosteneva che la ricorrente avrebbe dovuto accorgersi delle anomalie del messaggio e conseguentemente diffidare e non dar seguito alle istruzioni di uno sconosciuto truffatore, né chiamare lo sconosciuto numero di cellulare per poi lasciarsi convincere con colposa credulità.
Affermava di aver da tempo avviato una campagna di informazione finalizzata a evidenziare il fenomeno delle truffe, divulgando, costantemente, tramite i propri canali ufficiali (sito internet, e-mail, sms, push notification su APP ed estratto conto) ai clienti le indicazioni per riconoscere i tentativi di phishing/vishing, indicazioni che la cliente aveva colpevolmente ignorato.
Da ultimo, considerava irrilevanti le circostanze dedotte dalla ricorrente in ordine alle telefonate avute con l'intermediario terzo e la presunta responsabilità di quest'ultimo dato che le telefonate avevano ad oggetto i bonifici e la richiesta di blocco dell'operatività del conto corrente e non le transazioni eseguite con la carta e il blocco della carta.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale tuttavia depositava memorie relative ad un altro procedimento nei confronti dell'intermediario di radicamento del conto corrente, come pure rilevato dall'odierno resistente.

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; 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.
Risulta documentalmente che le operazioni in parola consistano in due pagamenti on line di € 500,00 ciascuno, eseguiti il 15.07.2024.
Le tracciature informatiche versate in atti evidenziano che entrambe l'operazione siano state autenticate tramite notifica push sul dispositivo in uso alla parte ricorrente (elemento di possesso) e riconoscimento biometrico (elemento di inerenza).
Attesa la conformità a SCA delle operazioni contestate, non resta che verificare se – dalla condotta tenuta dal 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, la ricorrente ricostruisce la vicenda in maniera contradditoria e lacunosa; in particolare la narrazione dei fatti, come rilevato anche dall'intermediario, presenta alcune discrepanze tra quanto dichiarato in ricorso e le dichiarazioni rese in sede di denuncia: parrebbe, infatti, che la truffa si sia articolata in più giorni, nel corso dei quali sarebbero state effettuate plurime operazioni, per quanto la ricorrente si limiti a svolgere le proprie considerazioni soltanto con riguardo ad alcune di quelle eseguite in data 15/07/2024.
Nella memoria allegata al ricorso la cliente dichiara che la truffa è iniziata in data 12/07/2024, quando ella contattava l'utenza mobile indicata nell'sms apparentemente proveniente dall'intermediario di radicamento del conto corrente. Ella afferma pure che, a seguito della truffa, si sarebbero cancellate le chiamate ed i messaggi truffaldini ricevuti; produce, tuttavia, una copia del messaggio civetta dalla quale emerge che la denominazione della chat in cui è inserito il messaggio non contiene la denominazione dell'intermediario convenuto; nella medesima chat non sono presenti messaggi genuini dell'intermediario antecedenti o successivi a quello civetta; il messaggio contiene errori lessicali ed è parzialmente privo di punteggiatura ed il numero di telefono indicato non è riconducibile all'intermediario convenuto.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Aggiunge pure di essere stata ricontattata da altro numero riferibile alla banca di radicamento del conto in data 12.07.2024, per ricevere indicazioni di collegarsi all'home banking tramite l'applicazione installata sul telefono cellulare per confermare il blocco di alcune transazioni sospette. In relazione a tale circostanza, tuttavia, ella si limita a versare in atti non già lo screenshot delle telefonate ma una schermata relativa agli esiti di una ricerca on-line.

Secondo il consolidato indirizzo di questo Collegio, la mancata allegazione, da parte del cliente, del registro delle chiamate non consente di verificare se il numero da cui la telefonata truffaldina sarebbe partita possa essere riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la sua genuinità.

A ciò si aggiunga che, per quanto ella affermi (senza fornire alcuna prova) di aver ricevuto rassicurazioni sulla genuinità del numero dal quale sarebbe stata contattata, la ricostruzione fornita in occasione della denuncia alle autorità sia del tutto difforme, non facendo riferimento alla telefonata del 12/07/2024, né all'utenza apparentemente riconducibile all'intermediario di radicamento del conto corrente, e collocando l'intera vicenda nella giornata del 15/07/2024, sia per le interlocuzioni genuine con l'intermediario di radicamento del conto corrente sia per le interlocuzioni (via sms e via telefono) con i truffatori.

Parimenti smentita per tabulas l'ulteriore contestazione secondo la quale la ricorrente non avrebbe ricevuto alcun messaggio di allerta al momento della esecuzione delle operazioni fraudolente; l'intermediario ha infatti versato in atti evidenze di messaggi di alert inviati tramite sms al numero riconducibile alla cliente.

L'insieme delle riferite circostanze induce il Collegio a ritenere che la condotta della ricorrente sia stata contraddistinta da colpa grave. Non vi sono, pertanto, elementi che consentano di accogliere il ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE