Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 10/02/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 28/10/2024 alle ore 14:28, un sms apparentemente proveniente dall'intermediario convenuto, con cui veniva informata di un pagamento di euro 3.950,00 e veniva invitata a chiamare il numero ivi indicato per assistenza.

Faceva presente di aver chiamato il numero indicato, al quale rispondeva un soggetto che si qualificava come operatore dell'ufficio antifrode della banca che riferiva di un accesso illecito al conto corrente e le suggeriva di rivolgersi alla propria filiale e a sporgere denuncia, indicandogli anche il soggetto cui rivolgersi.

Soggiungeva di essere stata nuovamente contattata, alle ore 18:11, dal medesimo soggetto che la induceva ad effettuare un'operazione di storno, per la quale riceveva anche un sms di conferma. Precisava, però, di ave ricevuto solo il giorno successivo il messaggio autentico della banca relativo all'avvenuta esecuzione del bonifico di euro 3.950,00.

Riteneva che la frode fosse stata perpetrata mediante la sofisticata combinazione di tecniche fraudolente utilizzate dai malfattori, per cui doveva essere esclusa la sua colpa grave in considerazione del fatto che i messaggi e la telefonata ricevuti fossero tali da suscitare il suo legittimo affidamento circa la loro genuinità nonché il fatto che i truffatori fossero già in possesso del pin e di altri codici di sicurezza; inoltre, considerava che l'accesso reiterato al canale ufficiale della banca da parte dei truffatori fosse tale da provare l'esistenza di un grave malfunzionamento del sistema e della negligenza dell'intermediario.

Contestava, inoltre, che la banca non avesse recepito le importanti novità sui bonifici istantanei introdotte dal Regolamento UE 2024/886 e che, solo in seguito ai fatti occorsi, avesse informato i clienti circa le nuove tecniche fraudolente.

Chiedeva, pertanto, il rimborso dell'importo di euro 3.950,00, oltre agli interessi legali.

Costituitosi ritualmente, l'intermediario convenuto rilevava che la ricorrente fosse stata guidata in una falsa operazione di storno, senza rendersi conto che stava autorizzando un bonifico; questa, infatti, aveva dichiarato di aver eseguito l'operazione che gli veniva comunicata, nonostante l'iban beneficiario fosse di un diverso istituto bancario e intestato ad una sconosciuta.

Evidenziava che, in una prima denuncia, la cliente avesse affermato che il bonifico risultasse eseguito alle ore 14:30, contestando la ricezione del messaggio autorizzativo alle ore 18:22, salvo poi dichiarare in una successiva denuncia che il bonifico risultasse effettuato alle 18:22, all'orario della ricezione della notifica; sottolineava, quindi, che la dinamica apparisse confusa e incompleta: in una prima denuncia, la cliente aveva attestato un addebito non autorizzato, mentre, in una seconda denuncia integrativa, richiamava un presunto data breach per dati anagrafici, sostenendo che la frode fosse imputabile alla presunta inadeguatezza dei sistemi di sicurezza della banca.

Osservava che il richiamo al data breach fosse irrilevante ai fini del procedimento, atteso che tali dati non consentono di accedere ai sistemi di pagamento o ai codici dispositivi, mentre la contestazione della cliente riguarda un'operazione eseguita su disposizione della cliente stessa, autenticata tramite procedura SCA dall'app installata sul suo dispositivo e senza alcuna anomalia riscontrata dalla banca.

Sosteneva di essersi attivato tramite circuiti telematici interbancari per il richiamo del bonifico, tuttavia con esito negativo per assenza di fondi; precisava che la frode in questione viene perpetrata tramite alcuni tool facilmente reperibili tramite web, senza bisogno di violare la sicurezza della banca, osservando che se il truffatore fosse stato realmente in grado di violare la sicurezza della banca, non vi sarebbe stata nemmeno ragione di dover contattare il cliente.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Affermava, quindi, che la truffa fosse avvenuta con un diretto coinvolgimento della ricorrente, posto che era stata quest'ultima ad effettuare e autorizzare il bonifico, sottolineando che questa tipologia di truffa è stata oggetto di numerose informative periodiche indirizzate alla cliente, anche prima della truffa.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale evidenziava che il messaggio civetta fosse apparso nella chat genuina della banca, così come il messaggio di storno ricevuto dopo l'operazione.
Ribadiva che fossero stati i truffatori a fornirle un codice di sicurezza, verosimilmente dopo aver avuto accesso al sistema dati.
Rilevava che la documentazione prodotta dalla banca dimostrasse che il telefono cui era stato inviato il PIN fosse un device che non era mai stato in suo possesso; riteneva, quindi, che fossero venuti meno i requisiti del possesso e della conoscenza.
Le repliche della ricorrente venivano riscontate dall'intermediario, il quale rilevava che l'accesso e le disposizioni fossero avvenuti con corretto riconoscimento delle credenziali e delle password dispositive, senza forzature e violazione dei sistemi e che le attività dispositive risultassero correttamente autorizzate, inserite e finalizzate direttamente dall'app della cliente, attiva sul telefono da novembre 2020.
Osservava pure che, decodificando il modello di cellulare segnalato nella scheda tecnica, questo corrispondesse a quello in possesso della cliente e da lei stessa dichiarato.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del diritto alla restituzione del controvalore di un'operazione, successivamente disconosciuta.
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 l'operazione contestata consiste in un bonifico eseguito il 28/10/2024, per un importo di euro 3.950,00.

Contrariamente a quanto rappresentato nel ricorso, la ricorrente rettifica l'orario di autenticazione dell'operazione contestata comunicato nella prima denuncia e riferisce di avere effettuato detta operazione nel corso della telefonata ricevuta alle ore 18:11. Nella seconda denuncia confermerebbe altresì di aver preso visione solo la mattina successiva del messaggio alert autentico della banca.

Dalle dichiarazioni rese non è neppure chiaro se la ricorrente abbia effettuato autonomamente il bonifico, seppure cadendo vittima dell'inganno del frodatore, ovvero se abbia contribuito con quest'ultimo a portare a termine la truffa ai propri danni; in relazione al quadro complessivamente delineato dalle allegazioni delle parti, il Collegio ritiene preferibile concludere che l'apporto causale dell'utente sia stato parziale.

Con riferimento a fattispecie analoghe l'orientamento uniforme dei Collegi ha chiarito che 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 on-line 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. Nel caso di specie, dunque, può escludersi che le operazioni possano considerarsi eseguite personalmente dalla ricorrente.

Ciò chiarito in premessa, con riferimento alla fase di accesso all'home banking effettuato in app, risulta documentalmente che siano stati utilizzati entrambi i fattori di autenticazione: l'impronta digitale (fattore di inerenza) ed il PIN (fattore di conoscenza).

La cliente, tuttavia, contesta che il dispositivo sia ad essa riconducibile: dalle evidenze in atti, invero, pur rilevandosi che il modello utilizzato sia lo stesso, emerge pure che esso sia di una versione più recente di quella in possesso della ricorrente. A giustificazione di tale apparente incongruenza l'intermediario rappresenta che l'app dalla quale è stata autorizzata l'operazione è attiva sul telefono della cliente da novembre 2020 e che il codice risultante dal log, pur non corrispondente al modello ma va decodificato secondo una tabella che è stata versata in atti.

In ogni caso, appaiono risolutive le dichiarazioni rilasciate dalla ricorrente in entrambe le denunce, nelle quali – pur non affermando espressamente di aver effettuato l'accesso in app – conferma tuttavia di aver dato seguito alle istruzioni "attraverso l'app" della banca.

Quanto alla fase dispositiva del bonifico oggi contestato, le tracciature informatiche evidenziano che l'autorizzazione sia avvenuta mediante riutilizzo del fattore di inerenza impiegato in fase di accesso, avvenuta pochi minuti prima l'esecuzione dell'operazione contestata, e mediante l'inserimento del mPIN (fattore di conoscenza).

Questo Collegio ha avuto modo in molteplici occasioni di ricordare che la European Banking Authority ha riconosciuto la conformità a SCA delle operazioni che avvengano mediante il riutilizzo di un fattore di autenticazione, purché ciò avvenga nella medesima sessione (cfr. Q&A 2018_4141 e pure Q&A 2020_5516).

Attesa la conformità a SCA dei pagamenti contestati, non resta che verificare se – dalla condotta tenuta dalla ricorrente – non 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).

La ricorrente ha affermato di aver ricevuto un sms apparentemente riconducibile all'intermediario; le risultanze documentali evidenziano che la denominazione della chat in cui è inserito il messaggio è

riferibile all'intermediario e che in essa siano presenti messaggi genuini dell'intermediario, antecedenti e successivi a quello civetta.

Quanto a quest'ultimo, esso contiene un numero che la cliente afferma di aver chiamato immediatamente, che tuttavia non è riconducibile all'odierno resistente ed è inoltre diverso da quello risultante dai precedenti messaggi autentici ricevuti; il messaggio, peraltro, non contiene errori grammaticali, o lessicali ma l'impostazione del testo è diversa dai messaggi autentici antecedenti. Da ultimo, deve pure osservarsi che, in coda al messaggio civetta, è presente un messaggio alert autentico delle ore 18:22 relativo all'operazione contestata e un messaggio truffaldino che ne indica lo storno.

Con riferimento all'orario di esecuzione dell'operazione, è stato già osservata la diversa ricostruzione della cliente nella seconda denuncia, rispetto alla prima: nella prima denuncia, infatti, la cliente riferisce di aver eseguito l'operazione nel primo pomeriggio e lamenta la mancata ricezione del messaggio alert se non dopo diverse ore; nella seconda denuncia, invece, riferisce di una telefonata ricevuta alle ore 18:11 dallo stesso sedicente operatore della banca con cui aveva parlato nel primo pomeriggio e colloca l'esecuzione dell'operazione (avvenuta effettivamente alle ore 18:22) nel corso della citata telefonata. Anche in questo, tuttavia, lamenta di non aver ricevuto il messaggio alert della banca e di averne preso visione solo la mattina successiva.

Dall'insieme di tutti questi elementi deve concludersi che la fattispecie in esame sia riconducibile allo spoofing misto a vishing.

Al riguardo si ha presente che secondo l'orientamento condiviso dei Collegi, deve ritenersi che allo stato, nonostante la maggiore diffusione di campagne informative sul tema, lo spoofing conservi ancora il carattere di insidiosità.

Rispetto ad esso non mancano, tuttavia, elementi riconducibili alla colpa grave della ricorrente; se, infatti, da un lato deve ritenersi che l'inserimento del messaggio truffaldino nella chat in uso dall'intermediario abbia indotto la stessa ad abbassare la sua soglia di attenzione, al tempo stesso la presenza di una evidente differenza della impostazione sintattica dei messaggi genuini da quello civetta e la non riconducibilità del numero di telefono ad una utenza dell'intermediario costituiscono ulteriori aspetti che lasciano emergere la colpa grave della cliente.

Ne deriva che il Collegio ritiene sussistente un concorso di colpa tra le parti nella determinazione dell'evento dannoso, *ex* art. 1227 cod. civ., che deve essere imputato nella misura di 2/3 a carico della ricorrente ed 1/3 a carico dell'intermediario.

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

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.317,00, 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