

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	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 20/01/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto – in data 08.08.2025 – una telefonata da parte di un sedicente operatore della sicurezza bancaria, il quale sosteneva che fosse in corso un bonifico di € 940,00 sul conto, invitandola a chiamare il relativo numero telefonico per bloccare l'operazione. Precisava di aver effettuato una videochiamata in cui mostrava il proprio bancomat e comunicava i dati di accesso al proprio conto.

Faceva presente di essere una signora anziana di 74 anni, che si era fatta intimorire dal truffatore, il quale aveva effettuato le operazioni tramite chip della carta, utilizzando un POS in un negozio di Napoli. Riteneva che l'app dell'intermediario, che utilizza la geolocalizzazione, avrebbe dovuto bloccare le operazioni poiché il proprio telefono si trovava a Vicenza; soggiungeva che l'intermediario avrebbe dovuto attuare sistemi di blocco dell'operatività anche in virtù delle modalità anomale di utilizzo della carta, cioè una rapida successione di importi tutti uguali.

Contestava, da ultimo, di non aver ricevuto alcuna notifica sms in merito alle operazioni.

Chiedeva, pertanto, il rimborso delle somme fraudolentemente sottratte.

Costituitosi ritualmente, l'intermediario convenuto rilevava che la cliente fosse stata vittima di "Card Relay Attack".

Sottolineava che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; considerava, quindi, sussistente la colpa grave della ricorrente, in quanto era caduta in una truffa all'interno di uno schema di raggio non complesso (phishing tradizionale) ed colpevolmente aveva reso possibile il compimento della frode comunicando i dati e assecondando il truffatore.

Osservava che non fossero stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici. Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale precisava di non aver mai comunicato il PIN della carta, avendo solo mostrato il frontespizio della carta una volta che – ricevuta la chiamata – era apparsa una foto della Polizia.

Ribadiva che, nonostante le anomalie, l'intermediario non avesse provveduto al blocco della carta e non avesse mai realizzato alcuna campagna informativa nei confronti della signora.

Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale si riportava ai propri scritti difensivi.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla ripetizione del controvalore di alcune operazioni 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 PSD2, 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 disconosciute consistono in dieci pagamenti tramite POS effettuati in data 08.08.2025, tra le ore 19.23 e le ore 19.34, per il complessivo importo di € 4.667,80. Con riferimento alla fase preliminare all'operatività contestata, l'intermediario ha fornito evidenze alla luce delle quali è possibile concludere che lo strumento di pagamento utilizzato fosse una carta "inserita e attiva", collegata all'utenza telefonica della cliente, enrollata il 18/03/2024, quindi in epoca di molto antecedente l'operatività fraudolenta, senza aver subito successive modifiche.

Emerge, altresì, *per tabulas* che in data 19.09.2024 la carta è stata associata all'app, scaricata sul device della cliente, tramite inserimento di username, password e OTP.

Riguardo alla fase dispositiva, le tracciatore informatiche prodotte in atti evidenziano che le operazioni contestate siano state effettuate mediante lettura della carta in modalità contactless (fattore di possesso), come indicato dalla dicitura "C" nella colonna "Input Mode", ed inserimento corretto del PIN (fattore di conoscenza), come indicato dalla dicitura "PIN" indicata nella colonna "Dati Autenticazione". Attesa la conformità a SCA del pagamento contestato, 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).

La cliente nella denuncia e nel ricorso riferisce di aver ricevuto un messaggio in data 07.08.2025 alle ore 19:11, contenente un finto alert dell'intermediario, nel quale si riferiva di un trasferimento sul conto e di chiamare un'altra utenza telefonica per bloccarlo.

Essendosi avveduta del messaggio solo il giorno seguente, la ricorrente ha contattato il numero fornitole, entrando in contatto con il truffatore (identificatosi come un agente della polizia postale), il quale l'ha invitata a seguire le sue indicazioni per risolvere il problema.

Questi ha quindi avviato una videochiamata, senza mostrarsi in video, nel corso della quale le ha chiesto di condividere lo schermo mentre accedeva all'app dell'intermediario e di inquadrare la carta fisica; la ricorrente ha pure precisato che, non essendo riuscita autonomamente a svolgere le operazioni, ha comunicato al truffatore i dati di accesso al profilo.

Dall'esame del messaggio civetta ricevuto dalla ricorrente, non risulta il mittente, anche se compare la denominazione dell'intermediario; non è neppure chiaro se esso si ponga in coda o sia seguito da altri messaggi genuini. Il testo presenta un errore grammaticale e riporta (quale utenza da contattare) non un numero verde ma un cellulare.

L'insieme di tali risultanze lascerebbe deporre per la colpa grave della ricorrente, la quale è caduta vittima di una truffa riconducibile allo schema del "card relay attack".

Secondo la descrizione fornita dall'intermediario, lo scenario si concretizza con l'installazione - mediante tecniche di social engineering - di un app malevola sul device del cliente, che consente ai truffatori di veicolare il flusso di una transazione contactless verso un dispositivo mobile in loro possesso che a sua volta dialoga con un terminale POS o ATM permettendo di finalizzare l'operazione di pagamento.

In tale contesto, l'intermediario spiega che l'operazione verrebbe inizializzata mediante l'avvicinamento della carta del cliente al proprio dispositivo che, "tramite tecnologia NCF, comunica con il malware precedentemente installato". I frodatori verrebbero in possesso del PIN tramite tali tecniche combinate (ma con modalità non meglio specificate).

Tuttavia, nel caso di specie, risulta solo una parziale corrispondenza tra la ricostruzione della truffa fornita dall'intermediario e gli avvenimenti rappresentati.

Se è vero che la cliente ha allegato di aver avvicinato la carta allo schermo del suo device durante una video call con il truffatore, la stessa cliente non ha mai riferito di aver scaricato un'App (potenzialmente un malware); neppure dal messaggio truffaldino è possibile scorgere link che astrattamente avrebbero potuto consentire di raggiungere detto scopo.

Al contrario, ella ha specificato di aver fornito al truffatore le credenziali per accedere all'APP dell'intermediario – su cui aveva precedentemente enrollato la carta – pur avendo negato di aver

comunicato il PIN della carta stessa. Pertanto, anche le modalità con cui il PIN è stato carpito non sono del tutto chiare.

Non va neppure sottaciuto che, come risulta dalle allegazioni delle parti e dalle risultanze documentali, la carta è sempre rimasta in possesso della ricorrente, residente a Vicenza, mentre le operazioni sono state autorizzate tramite POS a Napoli in modalità contactless.

Inoltre, emergono alcune specifiche circostanze di fatto che assumono rilievo quali indici di una frode (ai sensi delle disposizioni di cui al D. M. n. 112/2007) che avrebbe potuto essere rilevata da parte dell'intermediario; infatti, secondo la posizione più recente condivisa dai Collegi territoriali di questo Arbitro, i principi del suddetto D. M. n. 112/2017 – pur non avendo un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario – possono comunque rappresentare elementi utili per valutare la condotta dell'intermediario, in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.

In particolare, l'art. 8 del menzionato D.M. prevede che si configura il rischio di frode nel caso di “tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita” e di “sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento”. Nel caso di specie, risulta che nel giro di pochi minuti siano eseguite/tentate 8 operazioni presso un merchant e 4 verso altro merchant. Risultano, pertanto, integrati gli indici di frode previsti dalla normativa ministeriale, con conseguente riconoscimento del diritto della ricorrente ad ottenere la ripetizione del controvalore di tutti i pagamenti effettuati a partire dal terzo.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.698,00.

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