

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) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 10/03/2026

FATTO

Il ricorrente, insoddisfatto degli esiti dell'interlocuzione nella fase di reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 04.11.2025, un sms apparentemente proveniente dal servizio postale (a cui era riferito il link ivi contenuto), riguardante la consegna di un pacco realmente atteso quello stesso giorno, che indicava che la spedizione fosse in attesa di aggiornamento per mancanza del numero civico.

Faceva presente di aver ingenuamente inserito i dati della carta di credito per il pagamento simbolico richiesto (€ 0,27), convinto della genuinità del messaggio, e di essere stato immediatamente indirizzato all'app della banca, ove completava l'accesso tramite riconoscimento facciale (Face ID), senza ricevere però uno specifico codice o notifica di conferma.

Subito dopo, riceveva ricevuto un altro sms che lo informava dell'addebito immediato di € 394,59; resosi conto di essere caduto vittima di un attacco fraudolento, provvedeva a bloccare immediatamente la carta contattando il servizio clienti della banca.

Precisava che il sistema di sicurezza normalmente prevede l'invio di un codice di verifica (OTP) prima di autorizzare un pagamento, mentre nel caso dell'operazione fraudolenta da € 394,59 tale passaggio non fosse avvenuto.

Chiedeva, pertanto, il rimborso della somma fraudolentemente sottratta, oltre alla verifica tecnica sulla mancata attivazione del secondo fattore di autenticazione e ad una relazione scritta sulla tempistica e sull'esito del rimborso.

Si costituiva l'odierno resistente il quale rilevava che la denuncia contenesse la dichiarazione, di natura confessoria, per cui era stato lo stesso cliente ad inserire ad autorizzare l'operazione tramite il proprio device; riteneva, pertanto, inapplicabile la disciplina di cui alla PSD2 e al D. Lgs n. 11 del 27/01/2010.

Osservava, in ogni caso, che l'operazione fosse stata comunque correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali.

Soggiungeva, peraltro, che sussistesse la colpa grave del cliente, il quale – come pure accertato in fattispecie analoghe da questo Arbitro – aveva seguito le istruzioni ricevute tramite una mail/sms in cui si affermava che la consegna di un pacco non fosse andata a buon fine e veniva chiesto di effettuare un pagamento di un importo di pochi centesimi di euro tramite un link, per vedersi poi invece addebitare un importo superiore, dando seguito a un tentativo di phishing.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale negava di aver mai visualizzato, prima dell'addebito, una notifica o una schermata di autorizzazione riportante l'importo di € 394,59 e il nominativo del beneficiario; di contro sosteneva di aver ricevuto un ulteriore sms inerente l'autorizzazione di € 0,00.

Ribadiva che il tentativo di phishing cui era rimasto vittima prevedesse il pagamento di una somma forfettaria minima pari ad € 0,27, come chiaramente indicato nella pagina fraudolenta riproducente il sito dell'operatore postale, il quale non coincideva con l'importo effettivamente addebitato, con conseguente assenza di una preventiva e consapevole autorizzazione dell'importo di € 394,59.

Sottolineava che la truffa si fosse inserita in un contesto oggettivamente plausibile, essendo presente una reale spedizione in consegna nello stesso giorno, circostanza che esclude una valutazione automatica di colpa grave.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale rappresentava come dalle evidenze informatiche si evincesse che l'operazione contestata fosse stata autorizzata dal device del ricorrente per l'importo di € 394,59, e non di € 0,27, in favore di un esercente diverso dall'operatore postale.

In merito all'SMS inerente all'autorizzazione di un addebito di € 0,00, specificava che si trattasse di operazione automatica eseguita dal merchant per accertare che la carta fosse attiva e non prevedesse quindi l'invio al titolare carta di una notifica push di autorizzazione; di contro, rilevava che in denuncia il cliente avesse affermato espressamente di aver autorizzato la notifica push per l'autorizzazione del pagamento di € 394,59.

Pur comprendendo che sulla pagina apparentemente riconducibile all'operatore postale il ricorrente potesse aver visualizzato l'importo di € 0,27, richiamava - per evitare di incorrere in frodi - la necessità di leggere con attenzione anche la notifica push di autorizzazione al pagamento ricevuta dalla banca, controllando che vi sia corrispondenza nei dati relativi ad esercente ed importo, come la Banca da tempo consiglia di fare mediante apposite campagne informative.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di pagamento, 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 consista in un pagamento effettuato il 04.11.2025 alle ore 08.41, per l'importo di € 394,59.

Circa le modalità con le quali la truffa è stata portata a termine, con particolare riguardo al contributo causale del cliente, l'intermediario ritiene che – dalle stesse dichiarazioni da questi rilasciate nella denuncia sporta alle autorità – l'operazione sia stata posta in essere personalmente dal ricorrente; circostanza, questa, che (per costante e consolidato orientamento dell'Arbitro) escluderebbe l'applicabilità della richiamata disciplina normativa.

Invero, dall'esame delle allegazioni delle parti e dei riscontri documentali fornite, il Collegio ritiene che il quadro così delineato evidenzia, invece, un concorso del comportamento del cliente con la condotta dei truffatori.

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 online 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 l'operazione possa considerarsi eseguita personalmente dal ricorrente.

Dall'esame delle tracciature informatiche versati in atti emerge, invero, che l'operazione *de qua* sia stata correttamente autorizzata mediante notifica push inviata sul dispositivo del cliente (fattore di possesso) e successiva conferma tramite riconoscimento biometrico (fattore di inerenza).

Proprio in relazione a ciò, e tenuto conto di quanto affermato in precedenza, va osservato che l'autenticazione mediante fattore biometrico parrebbe peraltro in linea con le dichiarazioni dello stesso cliente, che ha pacificamente ammesso di aver utilizzato il proprio "Face ID", ancorché lo stesso precisi che è solito autenticare i pagamenti mediante codice OTP che riceve sul proprio device.

Attesa la conformità a SCA dell'operazione contestata, 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, il ricorrente ha dichiarato di avere ricevuto un sms apparentemente proveniente da intermediario che cura anche i servizi di spedizione e, poiché in quella giornata era effettivamente in attesa di un pacco dalla Spagna, di aver cliccato sul link inserendo le proprie credenziali per eseguire un pagamento che era stato indicato per € 0,27.

Risulta *per tabulas* che il messaggio civetta, peraltro proveniente da un'utenza mobile, non è neppure in apparenza riferibile alla banca, essendo relativo alla spedizione di un pacco che il cliente era in attesa di ricevere, e che la schermata apparsa dopo aver cliccato sul link fraudolento, è riferibile all'operatore postale e non all'odierno convenuto. Peraltro, emerge pure documentalmente che nella chat della banca sono presenti unicamente messaggi relativi ad OTP per perfezionare una transazione di € 413,49 (che tuttavia non risulta eseguita e non forma oggetto del presente ricorso).

In considerazione di tali evidenze documentali, il Collegio ritiene che la truffa è stata perpetrata tramite canali in alcun modo riferibili all'intermediario, posto che sia l' sms fraudolento, sia il link truffaldino ivi contenuto non sono neppure in apparenza ricondotti alla banca. Ne consegue che (come pure è stato rilevato in fattispecie analoghe) "le modalità della truffa non possono considerarsi tali da giustificare la

condotta della cliente la quale, ove avesse rispettato l'obbligo di prudente custodia delle proprie credenziali, avrebbe certamente potuto impedire il perfezionamento dell'operazione fraudolenta" (cfr. Coll. Milano, dec. n. 5390/2025).

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE