

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) ONZA	Membro di designazione rappresentativa dei clienti

Relatore MAURIZIO ONZA

Seduta del 09/12/2025

FATTO

Con ricorso presentato il 17 marzo 2025, la ricorrente T. s.r.l.s., in persona dei legali rappresentanti *pro tempore* L. C. e F. M. (la “Ricorrente”) ha domandato nei confronti della resistente N. s.p.a. (la “Resistente” e, assieme alla Ricorrente, le “Parti”) di accertare e dichiarare il proprio diritto a ottenere il riaccredito di Euro 4.634,94 da parte della Resistente e, per l’effetto, condannarla a provvedere conformemente.

La Ricorrente ha dedotto nel proprio ricorso di aver ricevuto, il 5 agosto 2024, a seguito di un acquisto *on-line*, un SMS contenente un’informativa su un supposto errore nell’indicazione dell’indirizzo di consegna dell’ordine. Adempiendo in buona fede alla richiesta di aprire un *link* volto alla soluzione del problema, la Ricorrente ha autorizzato il pagamento di un supposto onere accessorio per il trasporto, il cui ammontare sarebbe stato espresso in valuta saudita anziché in Euro. In seguito, è stata però addebitata a carico della Ricorrente la somma di Euro 4.634,94, pagamento per vero mai debitamente autorizzato.

Più precisamente, la Ricorrente si è doluta del mancato rimborso della somma pagata dalla Resistente, nonostante il proprio disconoscimento dell’operazione, in violazione dell’art. 11 d.lgs. n. 11/2010 (oltre a non aver dato riscontro al reclamo ricevuto all’uopo 27 gennaio 2025).

Costituitasi con controdeduzioni del 9 aprile 2025, la Resistente si è difesa in fatto e nel merito.

Nel dettaglio, la Resistente ha evidenziato come l’operazione controversa fosse stata autorizzata dal dispositivo, a sua volta autorizzato, del legale rappresentante della Ricorrente mediante autenticazione biometrica: ciò, senza che quest’ultima si avvedesse del proprio errore di calcolo per la determinazione del cambio tra valute nelle quali stava venendo eseguito il pagamento. Inoltre, la Ricorrente non avrebbe dato debita prova di aver ricevuto un SMS truffaldino né – nei fatti – di aver effettivamente

patito un addebito del valore dichiarato nel ricorso, puntualizzando che il valore del pagamento fosse invero inferiore a quello allegato.

Inoltre, la Resistente ha eccepito che la Ricorrente avrebbe anche regolarmente ricevuto un SMS di conferma dell'operazione in corso al proprio numero di telefono censito nell'anagrafica (come dimostrerebbero i documenti tecnici versati in atti).

La Resistente si è anche difesa affermando che la Ricorrente fosse in colpa grave, essendo incorsa in un caso di *phishing* rispetto al quale si è dichiarata estranea: a tal proposito, è stato evidenziato come nel contesto della truffa così perpetrata nessuno dei contatti coinvolti sarebbe stato riconducibile (neanche indirettamente o falsamente) all'intermediario. Neppure, sostiene la Resistente in ultimo, sarebbe possibile predicare la sua responsabilità, non essendo emersi nel caso di specie indizi di anomalia o rischio dell'operazione ex D.M. n. 112/2007.

La Resistente ha concluso, gradatamente, chiedendo: (i) di ridurre l'oggetto della contesa alla minor somma di Euro 4.583,26; (ii) di respingere il ricorso per l'esistenza di una regolare autorizzazione della Ricorrente per l'operazione contestata; (iii) di respingere il ricorso per difetto di idonee allegazioni sulla truffa asseritamente subita; e (iv) di respingere il ricorso per infondatezza e difetto di prova, nonché per colpa grave della Ricorrente o, in subordine, di ridurre la condanna a proprio carico alla luce della corresponsabilità colposa di quest'ultima.

Le Parti si sono ritualmente scambiate repliche e controrepliche.

Da un lato, la Ricorrente ha dedotto che: (i) importo del cui indebito addebito si è doluta fosse esatto, come avrebbe dimostrato il proprio estratto conto; (ii) l'SMS di convalida ricevuto dal proprio legale rappresentante riportasse la somma addebitanda soltanto in valuta estera e non in Euro; (iii) la rappresentazione della somma addebitanda in valuta locale sarebbe stata dovuta alla luce della propria qualità di microimpresa italiana, operante in Italia e in rapporto con una banca italiana, costituendo invece la dinamica per cui è procedimento una violazione dell'art. 5 Reg. (UE) 2018/839, per via dell'incapacità dell'SMS in questione di informare debitamente l'utente sulle caratteristiche dell'autorizzando pagamento; e (iv) l'operazione, in ogni caso, sarebbe stata anomala perché effettuata, come mai prima di allora, in valuta straniera; pertanto avrebbe dovuto essere bloccata dalla Resistente.

La Resistente, d'altro canto, ha replicato affermando che: (i) essa ha preso atto dell'effettivo ammontare del pagamento in contesa; (ii) il messaggio truffaldino da cui sarebbe scaturito il pagamento era riconoscibile come tale dalla Ricorrente, in quanto avente caratteristiche all'evidenza sospette; (iii) la Ricorrente non ha mai contestato di aver ricevuto il messaggio di conferma dell'operazione; (iv) la disciplina di settore non impone di dar conto, nel messaggio di conferma dell'operazione, del valore *post-cambio* delle operazioni autorizzate; e (v) l'identità del beneficiario del pagamento avrebbe dovuto allertare la Ricorrente, che è stata evidentemente incauta.

DIRITTO

Venendo alle ragioni (in fatto e) in diritto della decisione, occorre procedere con ordine.

In primo luogo, occorre circoscrivere l'oggetto della controversia con la necessaria esattezza. Sul punto, anche a seguito del contraddittorio svoltosi tra le Parti, deve ritenersi appurato che l'operazione per cui è procedimento ha un valore pari a Euro 4.634,94.

Ciò premesso, occorre verificare se l'operazione in questione, nelle sue concrete modalità realizzative, sia stata posta in essere con dinamiche tali da rendere responsabile la Resistente ovvero se sia da imputarsi, anche soltanto in parte, alla Ricorrente.

Orbene, occorre rammentare che secondo l'orientamento consolidato di questo Arbitro, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'operazione stessa deve considerarsi autorizzata: pertanto, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al d.lgs. n. 11/2010 (v. da ultimo, Collegio di Milano, decisione n. 7840/2025; Collegio di Milano, decisione n. 7833/2025).

Nel caso di specie, è dalle stesse parole della Ricorrente, impresse nel suo ricorso, che risulta come questa abbia provveduto personalmente, tramite il proprio legale rappresentante, a svolgere ogni fase del procedimento esecutivo del pagamento, confidando nella legittimità dell'SMS di richiesta di integrazione del corrispettivo ricevuta. Comunicazione, questa, evidentemente non riconducibile alla Resistente né tantomeno lontanamente – neanche in modo apparente o dubbio – ad essa connesso. Del resto, il *link* contenuto nell'SMS da cui è scaturita la truffa in danno della Ricorrente è indirizzato ad una pagina imitante il sito *web* di un noto vettore.

Vieppiù, dalla documentazione in atti – ma, prima ancora, anche dalle stesse argomentazioni della Ricorrente – risulta che non vi sia stata nessuna manomissione dei dispositivi della truffata, né alcun accesso non autorizzato alle sue utenze, né alcuna indebita intromissione nei procedimenti autorizzativi del pagamento.

La Ricorrente, in definitiva, è stata inconsapevole vittima di un *phishing*, cui ha dato seguito spontaneamente e, comunque, senza che la Resistente abbia fatto, omesso o permesso alcunché che potesse agevolare tale truffa. D'altronde, le particolari modalità con le quali la frode è stata perpetrata avrebbero dovuto, quantomeno, insospettire la Ricorrente. Si pensi al nominativo del destinatario del pagamento, a quanto risulta riferibile a una persona a lei ignota, alla valuta estera nella quale veniva richiesto il pagamento di somme connesse a una spedizione eminentemente locale (o comunque certamente non riferibile a Stati nei quali è usuale far circolare il Riyal saudita), la natura sospetta del *link* contenente la richiesta di pagamento e le anomalie nel testo del messaggio che tale *link* portava. Circostanze, queste, tali da escludere l'applicabilità dell'art. 10, co. 2, d.lgs. n. 11/2010, giacché è, sì, vero che la Ricorrente ha negato di aver autorizzato un'operazione di pagamento; ma è altrettanto vero che dalla documentazione in atti è dimostrata la colpa grave della medesima nel permettere l'operazione truffaldina (circostanza peraltro eccepita dalla Resistente), valevole a escludere l'addebitabilità dell'accaduto in capo all'intermediario. Tanto esclude ogni responsabilità della Resistente.

In casi di questa fatta, questo Collegio (decisione n. 554/2023) ha affermato, richiamando il Collegio di Coordinamento, decisione n. 22745/2019, che *«in ipotesi caratterizzate dalla presenza di artifici e raggiri della medesima tipologia di quelli di cui è rimasto vittima il ricorrente, note con l'espressione di phishing (o smishing), l'utente del servizio di pagamento che dà corso all'operazione versi in colpa grave. Si giunge a una simile conclusione sulla base della constatazione dell'ampia diffusione di tale fenomeno, quantomeno nella sua variante classica che si realizza tramite l'invio di e-mail o sms truffaldini, eventualmente accompagnato dalla telefonata di un sedicente operatore dell'intermediario,*

nonché della considerazione che l'impiego da parte dell'utente di una media diligenza risulti sufficiente a scongiurare tale pericolo e quindi a evitare la truffa".

Non vale a vincere queste considerazioni l'asserita anomalia dell'operazione per cui è procedimento, che a detta della Ricorrente avrebbe dovuto porre in debita allerta la Resistente. Invero, non ricorre in specie nessuno degli indici di anomalia indicati dal D.M. n. 112/2017. Ne essa comunque presenta quei connotati di numero, tipi ed importo dell'operazione che le pronunce dei Collegi dell'ABF ritengono rilevanti per il riconoscimento della violazione da parte dell'intermediario gli standard di diligenza del *bonus argentarius* (cfr. Collegio di Roma, decisione n. 595/2023, decisione n. 5550/2019; Collegio di Milano, decisione n. 5346/2022; Collegio di Bari, decisione n. 1690/2023). Si tratta, in specie, di una sola operazione, di importo contenuto e occasionale: dunque non v'è alcunché di sospetto, neppure per un banchiere diligente, specialmente considerando che la Ricorrente non ha prodotto documenti relativi alle proprie ordinarie attività di pagamento.

In breve, l'operazione di cui si duole la Ricorrente è regolarmente autorizzata, senza che la Resistente potesse né dovesse rilevarne la natura truffaldina.

Le doglianze della Ricorrente sono pertanto prive di fondamento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE