

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) FELICETTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) FELICETTI

Seduta del 14/04/2026

FATTO

La società ricorrente riferisce di essere titolare di un conto corrente presso l'intermediario resistente, con limite di operatività da remoto pari a € 50.000,00. Oltre tale soglia, le parti hanno pattuito che le operazioni di pagamento possano essere svolte via email o tramite sportello. Riferisce di aver corrisposto un acconto a un fornitore, tramite bonifico presso un IBAN belga già noto alla banca resistente. Deduce che ignoti truffatori si inserivano nella corrispondenza del fornitore e inviavano, tramite un dominio email contraffatto, una mail corredata da fattura per il saldo della fornitura. In tale fattura e in un successivo messaggio veniva esplicitata la modifica dei precedenti recapiti per il pagamento con un nuovo IBAN portoghese. Ricevuta la fattura in data 21.06.2024, il giorno successivo la ricorrente chiedeva alla banca di disporre presso il nuovo IBAN un bonifico da oltre € 100.000,00. La banca eseguiva il pagamento in data 24.06.2024 e, lo stesso giorno, la cliente si avvedeva della truffa. La ricorrente lamenta che la banca avrebbe attivato il *recall* solo il 25.06, quando ormai i truffatori avevano già distratto l'importo. Deduce anche che il Pubblico Ministero incaricato dell'indagine penale sulla vicenda ne ha ormai richiesto l'archiviazione, data l'impossibilità di rintracciare i responsabili all'estero. Lamenta, infine, che il sistema previsto dalla banca per le operazioni da remoto superiori a

€ 50.000,00 non garantisce sufficienti presidi di sicurezza. Tanto premesso, con l'odierno ricorso la ricorrente chiede all'ABF di riconoscere la responsabilità della banca, con conseguente risarcimento dell'importo dell'operazione di € 102.242,19 *“(o della maggiore o minore somma ritenuta di giustizia), dedotta la franchigia di € 150,00 come previsto, oltre ad € 4,00 a titolo di commissioni applicate dal PSP per il trasferimento e agli interessi dal 21.06.2024”*.

La banca riferisce di aver ricevuto via mail in data 21.06.2024 dalla cliente, come contrattualmente previsto per i pagamenti sopra la soglia di € 50.000,00, l'ordine di impartire il bonifico oggetto della presente vicenda. Deduce di aver eseguito l'operazione conformemente all'identificativo IBAN fornito dalla cliente e di aver attivato la procedura di recall il 24.06, non appena avvisata dalla cliente. Riferisce che tuttavia già in quella data l'importo era stato accreditato al beneficiario e trasferito altrove. Eccepisce che non possano esserle imputati profili di responsabilità, che invece gravano sui truffatori. Evidenzia altresì un profilo di negligenza della ricorrente, la quale non si è avveduta di aver ricevuto la fattura da un indirizzo email contraffatto. Tanto premesso chiede *“dichiarare l'inammissibilità del ricorso per carenza di legittimazione passiva della banca”* e di *“rigettare integralmente il ricorso presentato dalla società, in quanto manifestamente infondato in fatto e in diritto, e per l'effetto dichiarare che nessun addebito può essere mosso alla banca resistente, la quale ha agito in piena conformità alla legge e agli obblighi contrattuali, e che la perdita subita dalla ricorrente è conseguenza esclusiva della frode dalla stessa patita e della propria grave negligenza”*.

Le parti si sono scambiate atti di repliche e controrepliche in cui hanno meglio argomentato quanto già dedotto negli atti introduttivi in fatto e in diritto. In particolare, la ricorrente ha invocato il nuovo obbligo, introdotto dal diritto europeo, per i prestatori di servizi di pagamento di svolgere un controllo incrociato tra IBAN e nominativo del beneficiario. La banca eccepisce l'inapplicabilità *ratione temporis* della predetta normativa.

DIRITTO

L'odierno ricorso riguarda un'operazione di pagamento truffaldina per € 102.242,19 eseguita in data 21.06.2024 all'esito di uno schema di frode che sembra poter essere ricondotto al c.d. *business email compromised*. Dall'ampia documentazione versata in atti e dalla denuncia presentata dalla ricorrente all'Autorità competente, risulta che la società ricorrente inviava il bonifico urgente ad un IBAN diverso da quello comunicato originariamente dal fornitore D*, dopo aver ricevuto delle mail truffaldine apparentemente inviate dal fornitore stesso.

In particolare, risulta che in data 20.06.2024, alle ore 11:30 circa, la segreteria della società ricorrente inviava una mail alla ditta D* per chiedere informazioni sullo stato di avanzamento di un ordine, al fine di effettuarne il pagamento della seconda rata. Poco più tardi, alle ore 17:10 la ditta D* inviava attraverso il dominio mail genuino (@D*.com) la fattura per effettuare il pagamento (relativo al secondo acconto citato) pari a € 102.242,19, con indicato l'IBAN beneficiario radicato in Belgio. Tuttavia, alle ore 23:43 dello stesso giorno, veniva inviata alla cliente un'altra mail, da un dominio fasullo ma a prima lettura confondibile con quello genuino (@D*o*.com). Questo messaggio recava come allegato un'altra fattura di pagamento identica alla prima ricevuta alle ore 17:10, ma con un nuovo IBAN, basato in Portogallo. Inoltre, alle ore 00:10 giungeva un'ulteriore mail, sempre da una casella di posta fasulla, in cui venivano ribaditi i nuovi dati per il pagamento. Il giorno seguente, 21.06.2025, la società ricorrente

conferiva via mail all'intermediario resistente mandato di pagamento, secondo la modalità pattuita tra le parti per le operazioni oltre il massimale di € 50.000,00. La società allegava al mandato di pagamento la seconda fattura, ricevuta dai truffatori. Sempre in data 21.06.2025 la ricorrente informava la ditta D* dell'esecuzione del bonifico alla mail fasulla, ricevendo riscontro positivo alle ore 16:49. Il 24.06.2025, la ricorrente si avvedeva dell'anomalia nella casella mail del sedicente fornitore e contattava telefonicamente e via mail la banca per chiedere di bloccare il bonifico.

È pacifico tra le parti che l'operazione disconosciuta sia stata eseguita dalla cliente, la quale, in conseguenza del raggio di cui è stata vittima, ha seguito le indicazioni dei truffatori. Nel ricorso in esame non è in contestazione né l'effettiva esecuzione del bonifico, né il successivo disconoscimento e risultano pertanto incoerenti le deduzioni offerte dalle parti circa la sottoscrizione della distinta. Conseguentemente alla vicenda non si applica la disciplina di cui al d.lgs. n. 11 del 2010 in tema di operazione di pagamento non autorizzate. Tuttavia, in casi analoghi a quello di specie, l'ABF ha ritenuto di poter rilevare secondo le norme di diritto comune un eventuale responsabilità concorrente del prestatore dei servizi di pagamento, qualora emerga dagli atti un apporto causale dell'intermediario alla frode.

Venendo ai potenziali profili di responsabilità della banca nella vicenda descritta, la ricorrente contesta alla banca la mancata rilevazione dell'incongruità del beneficiario dell'operazione di pagamento e la mancata verifica della corrispondenza tra nominativo del beneficiario indicato ed effettivo titolare dell'IBAN.

Riguardo al secondo profilo, osserva il Collegio che la disposizione di pagamento oggetto del presente ricorso è stata posta in essere il 21.06.2025. La vicenda rimane pertanto fuori dall'ambito temporale di applicazione dell'obbligo introdotto dal Regolamento UE n. 886 del 2024 che, con efficacia a partire dal 9.10.2025, impone alle banche il c.d. "*Verification of Payee*", ossia la verifica della corrispondenza tra titolarità dell'IBAN e nome (o identificativo) del beneficiario.

Sotto il primo profilo, invece, viene in rilievo la disciplina prevista dall'art. 24 del d.lgs. 11 del 2010, laddove prescrive che *"1. Se un ordine di pagamento è eseguito conformemente all'identificativo unico, esso si ritiene eseguito correttamente per quanto concerne il beneficiario e/o il conto indicato dall'identificativo unico. 2. Se l'identificativo unico fornito dall'utente è inesatto, il prestatore di servizi di pagamento non è responsabile, ai sensi dell'articolo 25, della mancata o inesatta esecuzione dell'operazione di pagamento. Il prestatore di servizi di pagamento del pagatore compie tuttavia sforzi ragionevoli per recuperare i fondi oggetto dell'operazione di pagamento. [...]"*. La norma, per come costantemente interpretata dalla giurisprudenza dei collegi ABF, esenta il prestatore del servizio di pagamento da responsabilità nei casi in cui abbia eseguito un ordine di pagamento presso l'IBAN errato indicato dal disponente (cfr. Collegio di Coordinamento n. 162 del 2017). Nel caso di specie, inoltre, la ricorrente non offre elementi atti a dimostrare che la banca avrebbe potuto rendersi conto dell'errore contenuto nelle informazioni di pagamento fornitele e quindi abbia violato i propri doveri di diligenza e buona fede. Infatti, l'attività truffaldina di terzi ignoti ha interessato le comunicazioni di posta elettronica tra la società ricorrente e il proprio fornitore e non il servizio di pagamento della banca. A tal riguardo la ricorrente solleva un'ulteriore contestazione riguardo al livello di sicurezza garantito dalle modalità pattuite tra le parti per l'invio di disposizioni superiori a una certa soglia di valore. Non è chiaro, tuttavia, come una diversa modalità avrebbe potuto influire sulla vicenda in oggetto.

La ricorrente contesta, infine, la tardività del tentativo di *recall* della disposizione di pagamento posto in essere dalla banca. Sul punto, l'intermediario fornisce prova di aver avviato la procedura di richiamo per "frode" già in data 24.06.2025 (cfr. all. 2 e 4 alle controdeduzioni) e che questa ha dato esito negativo, poiché i fondi erano già stati distratti dai truffatori il giorno stesso.

Alla luce di quanto precede, la domanda della società ricorrente non merita accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE