

## 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) SCARANO      | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) FORMAGGIA

Seduta del 14/04/2026

## FATTO

Il ricorrente, nel ricorso presentato, afferma che in data 15/12/2025 aveva ricevuto una notifica dall'app dell'intermediario circa un pagamento in dollari a favore di un e-commerce, da lui non eseguita; di aver ricevuto una seconda notifica che lo informava dello storno di questa prima operazione; che pochi minuti dopo veniva contattato da un numero di telefono mobile con prefisso 350 dal quale un sedicente operatore dell'intermediario gli comunicava che l'operazione era stata intercettata dai sistemi di sicurezza e probabilmente la sua app o la sua carta erano state hackerate; che dopo aver verificato una serie di dati personali, il sedicente operatore informava il cliente che sarebbe stato contattato da un numero di telefono con prefisso 02 per effettuare ulteriori verifiche col servizio clienti dell'intermediario; che avendo verificato dai motori di ricerca che il numero corrispondeva effettivamente a un numero dell'intermediario, si sentiva rassicurato e rispondeva a questa seconda chiamata; che in questa seconda chiamata, dopo un'ulteriore verifica sui dati personali e sugli strumenti di pagamento in possesso del cliente, gli veniva prospettato un possibile bonifico di € 10.000,00 in uscita non disposto dal cliente e che per poter bloccare questa operazione avrebbe dovuto eseguire un "bonifico di storno" a suo nome verso un IBAN fornitogli telefonicamente dall'interlocutore; che, rassicurato del fatto che al termine avrebbe ricevuto una notifica a conferma del blocco dell'operazione, disponeva personalmente il bonifico, senza però ricevere notifiche; che gli veniva chiesto, inoltre, di aggiornare l'app di internet banking e di provvedere ad un secondo bonifico di storno per annullare una operazione di € 990,00 in favore di un presunto operatore di criptovalute; che dopo aver eseguito questo secondo bonifico senza ricevere alcuna notifica, insospettitosi, aveva bloccato gli strumenti di

pagamento e ridotto i massimali di bonifico; di aver quindi contattato il vero servizio clienti dell'intermediario dal quale apprendeva di essere stato truffato; di aver presentato denuncia alla Polizia Postale in data 22/12/2025 e reclamo all'intermediario, da questi riscontrato negativamente. Chiede che venga dichiarata l'illegittimità del diniego di rimborso opposto dall'intermediario, per violazione degli artt.10,11 e 12 del D.Lgs.n.11/2010 e dei principi di correttezza e buona fede professionale; che venga accertato che le operazioni erano state dal ricorrente autorizzate in un contesto di errore indotto da artifici fraudolenti senza dolo o colpa grave del cliente, che l'intermediario non aveva assolto l'onere di provare un uso fraudolento imputabile esclusivamente al cliente, che è mancata la comunicazione tempestiva delle procedure di recupero con riduzione della possibilità di contenere il danno; che l'intermediario venisse condannato al rimborso di € 10.990,00 oltre al contributo ABF di € 20,00, o, in subordine, a un rimborso equamente determinato.

L'intermediario, nelle controdeduzioni depositate, rileva che la denuncia presentata dal cliente contiene la dichiarazione, di natura confessoria, per cui era stato lo stesso cliente ad effettuare le operazioni seguendo le istruzioni del frodatore; che, di conseguenza, non era applicabile la disciplina di cui alla PSD2 e al D. Lgs n. 11 del 27/01/2010; che l'operazione è stata comunque correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali.

Ha concluso chiedendo il rigetto *in toto* del ricorso in quanto infondato in fatto e in diritto.

Il ricorrente, nelle repliche, ha sottolineato che la semplice autenticazione delle operazioni in app tramite SCA non implica che il cliente le abbia autorizzate o che abbia agito con colpa grave; che la manipolazione telefonica subita era articolata, mentre la colpa grave richiede una negligenza macroscopica; che la richiesta di recall del bonifico era stata fatta solo in data 23/12/2025, otto giorni dopo che si era consumata la truffa, mentre avrebbe dovuto avvenire tempestivamente, dato che si trattava di un bonifico istantaneo.

Insiste per l'accoglimento del ricorso anche in via equitativa.

L'intermediario, nelle controrepliche, ribadisce che le operazioni risultavano correttamente autenticate, registrate e contabilizzate in assenza di malfunzionamenti o intrusioni nei sistemi bancari; che la condotta del cliente è stata caratterizzata da colpa grave per aver assecondato pedissequamente le istruzioni del frodatore, aver disposto le operazioni mediante l'applicazione della SCA e non aver tenuto un comportamento conforme ai doveri di ordinaria diligenza; che l'operazione è da considerarsi autorizzata in quanto si è perfezionata con l'impiego dei fattori di autenticazione a disposizione del cliente. Insiste sulla colpa grave del cliente, il quale ha personalmente disposto operazioni di pagamento su dettatura di un soggetto sconosciuto verso un IBAN sconosciuto e autorizzando una seconda operazione verso una piattaforma di criptovalute, il tutto dalla propria app. Rileva di essersi prontamente attivato per il recall del bonifico a seguito della ricezione del reclamo del cliente, pur in assenza di uno specifico obbligo; che però il recall non è stato possibile in quanto il conto corrente di destinazione del bonifico, radicato su un diverso intermediario, risultava chiuso; che i presidi di sicurezza dell'intermediario risultano conformi alla normativa vigente e correttamente applicati al caso concreto.

Insiste per il rigetto del ricorso.

## **DIRITTO**

Si osserva, in fatto, che le operazioni disconosciute sono 2, assommano all'Importo complessivo di €10.990,00, sono state effettuate il 15/12/2025 dalle 16:34 alle 16:47 (nell'arco cioè di 13 minuti).

È in atti la denuncia del cliente presentata in data 22/12/2025.

Secondo la descrizione fatta della frode subita, essa sarebbe partita da una notifica in app, seguita da una prima chiamata da un numero di telefono cellulare che ha rimandato il cliente ad una seconda chiamata in arrivo da un numero di telefono fisso, nella quale il frodatore lo ha indotto ad effettuare due operazioni con le quali avrebbe asseritamente stornato altre due operazioni da lui non autorizzate.

Si osserva, in diritto, che alla data dell'operazione contestata trovava applicazione il D.Lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018; tale disciplina deve ritenersi integrata con le novità sui bonifici istantanei introdotte dal Regolamento 2024/886, in vigore dal 9-10-2025, con particolare riguardo all'obbligo di prevedere il servizio gratuito di verifica del beneficiario (cd. *Verification of Payee - VoP*). Più precisamente, in relazione all'esecuzione dei bonifici (ordinari e istantanei), il Regolamento (UE) 2024/886 del Parlamento europeo e del Consiglio ha disposto, con efficacia a partire dal 9 ottobre 2025, l'obbligo della c.d. "*Verification of Payee*", un sistema che verifica la corrispondenza tra IBAN e nome (o identificativo) del beneficiario. Tale meccanismo è stato introdotto al fine di ridurre frodi ed errori, restituendo un esito in tempo reale (corrispondenza, mancata corrispondenza, corrispondenza parziale o impossibilità di verifica) e permettendo a chi effettui un bonifico di confermare il pagamento dopo aver visto il risultato.

Le fonti normative regolanti la materia sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).

La prova di autenticazione delle operazioni, a carico dell'intermediario, rappresenta, in aderenza al dato normativo, un *prius* logico rispetto ad ogni ulteriore accertamento, compreso quello sulla colpa grave del cliente.

Secondo il consolidato orientamento dei collegi, nel caso in cui risulti pacifico o dimostrato che le operazioni contestate siano state compiute direttamente e interamente dal cliente (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'operazione 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. Rientrano in questa fattispecie, in particolare, le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, pur senza la consapevolezza di disporre una transazione (ad esempio, le operazioni "sotto dettatura"). Mentre in tali ipotesi l'intermediario è esonerato dalla prova di autenticazione, diversamente, ove vi siano operazioni non compiute interamente dal cliente, occorre l'accertamento della sussistenza della SCA (*Strong Customer Authentication*), con riferimento alle singole operazioni e ad ogni fase attraverso cui si sono realizzate, con onere della prova a carico dell'intermediario.

È pacifico, come dichiarato dal ricorrente con valenza confessoria, che le operazioni oggetto del ricorso sono state eseguite direttamente dal cliente, il quale – cadendo vittima di un raggiro – ha personalmente disposto il pagamento, seguendo le istruzioni impartite dal frodatore. Più precisamente il ricorrente, a seguito di notifiche e due interlocuzioni telefoniche, ha personalmente disposto un

bonifico e un'operazione tramite carta di pagamento, nella convinzione di bloccare dei movimenti in uscita di importo analogo da lui non autorizzati.

Nella fattispecie in esame, dunque, il Collegio non procede alla verifica della corretta esecuzione e autenticazione delle operazioni contestate ai sensi degli artt. 10 ss. del decreto citato.

Inoltre, non rilevano neppure profili di sofisticatezza o meno della forma di truffa perpetrata via sms/telefonica [*attuata con strumenti atti a camuffare il messaggio/la chiamata facendoli apparire provenienti dall'intermediario*], posto che le operazioni che vi hanno fatto seguito sono state poste in essere personalmente dal cliente e pertanto non è necessario il vaglio di colpa grave dello stesso.

L'esame deve invece concentrarsi sulla condotta dell'intermediario, al fine di verificare la sussistenza di eventuali profili di responsabilità a suo carico. Esclusa la configurabilità di una sua responsabilità oggettiva, spetta al Collegio valutare se, in concreto, vi sia stata una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode (quali ad esempio, la mancanza o temporanea indisponibilità del numero verde del PSP, o il mancato rilievo di indici di frode).

L'intermediario fornisce LOG ed altre evidenze e, negli atti, si riporta al loro contenuto, dandone in sostanza una spiegazione.

A questo proposito si rammentano i principi generali espressi dai collegi in merito alla valenza da attribuire alle informazioni presenti nei *log* prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento disconosciute (artt. 10, comma 1 e 10-*bis* del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza). Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, i collegi ritengono che, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP (Prestatore dei Servizi di Pagamento) nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione.

I collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c..

Sulla base di tali principi consolidati nell'orientamento dei collegi, vanno dunque esaminate le evidenze emergenti dai LOG, gli argomenti esplicativi forniti dall'intermediario e le dichiarazioni del ricorrente.

Il complesso di tali elementi consente un confronto delle condotte delle parti.

Si rileva, innanzitutto, che la vicenda descritta non evidenzia peculiarità indicative di una frode particolarmente sofisticata, trattandosi di una fattispecie piuttosto frequente e ormai nota.

Si rileva poi, da un lato, che il cliente, nella denuncia, afferma di aver bloccato autonomamente dall'app le carte di pagamento durante la telefonata col frodatore e di aver ridotto a € 1 il massimale dei bonifici; trattasi di circostanza non contestata dall'intermediario. D'altro canto si rileva che l'intermediario ha documentato di aver tentato il *recall* del bonifico istantaneo in data 23/12/2025 a seguito del reclamo del cliente; il *recall* non è andato a buon fine in quanto il conto corrente del beneficiario, radicato su altro intermediario (riscontrato dallo stesso in data 16/01/2025), risultava chiuso (all. 9). La fattispecie non evidenzia indici di anomalie o di frode che avrebbero dovuto sollecitare l'intermediario a riconoscere nell'immediatezza dei fatti che il cliente agiva in conseguenza di un raggirio; peraltro si

tratta di due operazioni effettuate nell'arco di pochi minuti, sicché non si imponeva neppure l'invio di *alert*. Si condivide infatti l'interpretazione sostanzialistica del servizio di *sms-alert*, secondo cui, considerata la sua natura di presidio di sicurezza ex post, la mancata attivazione ovvero il mancato funzionamento di tale servizio (o di servizio assimilabile) sono irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'*alert* non avrebbe potuto in concreto limitare il pregiudizio dell'utente.

Per tutto quanto osservato la domanda del ricorrente è infondata e il suo ricorso va respinto.

### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE