

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) CAPIZZI

Seduta del 10/02/2026

FATTO

Con ricorso del 26 settembre 2025, il ricorrente riferisce di avere denunciato, in data 11 aprile 2025, di essere stato oggetto di frode informatica – asseritamente riconducibile al fenomeno c.d. phishing tramite ricezione di telefonata truffaldina (vishing) – che si sarebbe concretizzata nell'esecuzione, il

giorno precedente, di un bonifico istantaneo di importo pari a € 49.499,00. La suddetta transazione è stata realizzata tramite accesso all'area riservata dei servizi di mobile banking dell'intermediario previo enrollment dell'App dedicata sul device dei truffatori. Di conseguenza, disconoscendo l'addebito registrato sul proprio conto corrente sopra evidenziato, il ricorrente ha chiesto il rimborso della somma di € 49.499,00 relativa all'operazione di pagamento contestata e disconosciuta, in quanto frutto di frode informatica la cui responsabilità è asseritamente da imputare all'intermediario convenuto, che non avrebbe saputo impedire una violazione al proprio sistema informatico da parte dei truffatori.

L'intermediario convenuto, con le controdeduzioni, sostiene la regolare contabilizzazione, autenticazione e registrazione dell'operazione in oggetto, evidenziando inoltre la colpa grave del cliente, che ha collaborato, sia pure inconsapevolmente, all'esecuzione del pagamento contestato consentendo l'installazione dell'App di mobile banking dell'intermediario sul device dei truffatori. Chiede dunque il rigetto del ricorso in quanto infondato in fatto e in diritto.

DIRITTO

La questione sottoposta al Collegio concerne la rimborsabilità o meno in favore di parte ricorrente della somma fraudolentemente sottratta mediante svolgimento di un'operazione disconosciuta. Si tratta, in particolare, di un bonifico istantaneo, di importo pari a € 49.499,00, eseguito alle ore 09:31 del 10 aprile 2025. La suddetta operazione è stata eseguita tramite accesso in App, su device precedentemente registrato dai truffatori, all'area riservata dei servizi di mobile banking dell'intermediario.

Alla data di effettuazione delle operazioni contestate era vigente il D. Lgs. n. 11/2010, modificato a seguito dell'entrata in vigore del D. Lgs. n. 218/2017 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD II). Pertanto, la sussistenza delle responsabilità che le parti della controversia odierna vicendevolmente si addebitano dovrà essere valutata in base a quanto previsto da tale decreto con riferimento a entrambi i profili caratterizzanti l'onere probatorio, ossia l'accertamento della regolare autenticazione ed esecuzione delle operazioni di pagamento, nonché l'accertamento dell'eventuale colpa grave dell'utilizzatore dei servizi di pagamento. Con riferimento al primo profilo, il Collegio osserva che l'art. 8, comma 1, lett. a) del D. Lgs. 11/2010, come novellato dal D. Lgs. 218/2017, prevede che *“il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7 [...]”*. L'art. 10, comma 1, del medesimo Decreto prescrive che *“qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti”*. L'art. 10, comma 2, prevede che *“quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, [...] è onere del prestatore di servizi di pagamento [...] fornire la prova della frode, del dolo o della colpa grave dell'utente”*. Inoltre,

con riferimento alle modalità di autenticazione di una operazione di pagamento, ai sensi dell'art. 10 bis, comma 1, *"i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi"*. L'art. 1, comma 1, lett. q-bis, del summenzionato testo normativo definisce l' "autenticazione forte del cliente" quale *"basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione"*. Vale comunque la pena ribadire che, già prima dell'entrata in vigore delle citate modifiche normative, l'orientamento consolidato dei Collegi ABF era nel senso di richiedere all'intermediario la prova dell'avvenuta autenticazione delle operazioni tramite sistema a due o più fattori (cfr. ex multis Collegio di Milano, Decisioni n. 6936/2016 e n. 7131/2017). Quanto al secondo profilo dell'onere probatorio, l'orientamento consolidato dell'Arbitro è nel senso conformarsi al principio interpretativo statuito dal Collegio di Coordinamento (Decisione n. 22745/2019), secondo cui *"la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente"*. Tuttavia, il Collegio di Coordinamento ha al contempo evidenziato che, anche *"nel caso in cui l'intermediario si sia costituito nel procedimento, fornendo prova dell'autenticazione e della regolarità formale dell'operazione, ma nulla abbia dedotto in merito alla colpa grave dell'utente, il Collegio [può] comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso"*.

Venendo ora al caso di specie, si rileva, innanzitutto, che dalla ricostruzione dei fatti parrebbe che il cliente sia caduto vittima di phishing, realizzato mediante smishing misto a vishing. Al riguardo, il ricorrente afferma che la truffa sarebbe stata eseguita mediante iniziale telefonata truffaldina ricevuta in data 8 aprile 2025 da parte di un soggetto che si qualificava come un operatore della banca convenuta, il quale lo induceva a disinstallare e reinstallare l'App dei servizi di mobile banking per motivi di sicurezza; in tal modo, i truffatori riuscivano a carpire le informazioni necessarie a registrare l'App anche su altro device, da cui, in data 10 aprile 2025 è stata effettuata un'operazione di costituzione della provvista – in particolare, un giroconto dal conto di deposito al conto corrente di corrispondenza del cliente per l'importo di € 46.999,00 – strumentale all'esecuzione del bonifico istantaneo di cui è ricorso, di importo pari a € 49.499,00. Il cliente è venuto a conoscenza dell'esecuzione del bonifico contestato attraverso un sms-alert ricevuto nella chat riferibile alla banca.

L'intermediario convenuto, attraverso le evidenze versate in atti e i log prodotti, ricostruisce i singoli passaggi dell'esecuzione del bonifici istantaneo di cui è ricorso e dimostra che la fase di enrollment dell'App sul device riconducibile ai truffatori è stata autenticata attraverso il sistema autorizzativo di tipo dinamico funzionante mediante digitazione del codice PIN (fattore della conoscenza) e del codice

monouso OTP inviato tramite sms sul device certificato del cliente (fattore del possesso). L'intermediario produce in atti evidenza anche della fase di accesso all'App dei servizi di mobile banking da parte dei truffatori sul nuovo smartphone registrato, che è avvenuta previa digitazione del codice segreto (fattore della conoscenza) e validazione del token (Mobile App Id) associato univocamente al device (fattore del possesso).

Una ulteriore attività prodromica all'esecuzione del pagamento di cui è ricorso è consistita nell'effettuazione di un giroconto di importo pari a € 46.999.00 dal conto deposito al conto corrente intestato al cliente. Tuttavia, trattandosi di una operazione strumentale alla costituzione della provvista, in conformità a quanto stabilito dal Collegio di Coordinamento con Decisione n. 8671/2024, la medesima è sottratta dall'obbligo della prova di autenticazione forte a due fattori (Strong Customer Authentication – SCA). Con riferimento, infine, all'esecuzione del pagamento online contestato, il convenuto produce evidenza dell'inserimento dello Smart Code (fattore della conoscenza) e della conferma della notifica push generata in App sul device certificato dell'utilizzatore (fattore del possesso). Alla luce delle evidenze in atti, questo Collegio conclude che il sistema predisposto dall'intermediario è conforme ai criteri previsti per l'autenticazione forte a "due fattori", il che, in conformità con l'orientamento consolidato dell'Arbitro, induce a ritenere, in assenza di ulteriori indici di anomalia delle operazioni contestate, che parte resistente abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del D. Lgs. n. 11/2010, (cfr. ex multis Collegio di Milano, Decisioni n. 10279/2024, n. 8996/2024 e n. 7703/2024).

È ora possibile passare alla disamina circa l'assolvimento da parte del convenuto dell'onere probatorio in merito alla colpa grave dell'utente del servizio di pagamento. Sul punto, dalla ricostruzione dei fatti così come evincibile dalla documentazione versata in atti dalle parti, emerge chiaramente la possibilità di desumere in capo all'utilizzatore un comportamento gravemente colposo nella vicenda in oggetto, essendo presente una serie di elementi di fatto particolarmente univoca e convergente, al punto che possa ragionevolmente ritenersi che l'operazione fraudolenta sia effettivamente riconducibile sul piano causale alla condotta del ricorrente (cfr. ex multis Collegio di Roma, Decisione n. 6770/2022; Collegio di Milano, Decisioni n. 7844/2021 e n. 1828/20). Al proposito, occorre ricordare che, secondo quanto indicato dalla giurisprudenza di legittimità (cfr. Cass. civ., 19 novembre 2001, n. 14456) e dal Collegio di Coordinamento (Decisione n. 5304/2013), la colpa grave consiste in *"un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti"*. Invero, nella vicenda al centro della presente controversia, il Collegio ritiene che la responsabilità del cliente non possa essere temperata dalla natura della truffa di cui è ricorso ("phishing attraverso vishing"), alla quale, nel caso di specie, non si possono associare quegli elementi di sofisticatezza e insidiosità che la giurisprudenza dell'Arbitro normalmente attribuisce viceversa alla fattispecie nota come "ID caller spoofing". Con riferimento, infatti, alla telefonata truffaldina ricevuta, il ricorrente non produce evidenza della chiamata truffaldina, allegando solo degli screenshot relativi ad alcune chiamate in entrata, dai quali non è tuttavia possibile evincere il numero chiamante. Non è pertanto

possibile presumere un legittimo affidamento dell'utente circa la genuinità del contenuto della telefonata truffaldina alla base dell'operazione di pagamento disconosciuta, non potendo la medesima essere ricondotta alla più insidiosa fattispecie qualificabile come "ID caller spoofing". Il comportamento tenuto dal ricorrente integra, pertanto, una condotta gravemente colposa, con la conseguenza che il ricorso non può essere accolto (cfr. ex multis Collegio di Milano, Decisioni n. 7641/2024, n. 10876/2023 e n. 114/2023).

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE