

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) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CAPIZZI

Seduta del 01/09/2026

FATTO

Con ricorso del 25 febbraio 2026, la ricorrente riferisce di avere denunciato, in data 4 dicembre 2025, di essere stata oggetto di frode informatica – asseritamente riconducibile al fenomeno c.d. phishing tramite invio di sms (smishing) e successive telefonate truffaldine (vishing) – che si sarebbe concretizzata nell'esecuzione di n. 2 (due) pagamenti fraudolenti e, in particolare, di:

- n. 1 (un) bonifico online di importo pari a € 4.656,64, disposto in data 3 dicembre 2025 tramite accesso all'area riservata dei servizi di home banking dell'intermediario convenuto;
- n. 1 (un) bonifico ordinario, di importo pari a € 19.900,00, eseguito in data 4 dicembre 2025 direttamente dalla cliente presso la filiale del convenuto in cui è radicato il conto corrente intestato alla medesima.

Di conseguenza, disconoscendo gli addebiti registrati sul proprio conto corrente sopra evidenziati, la ricorrente ha chiesto il rimborso dell'importo di € 24.556,65 relativo alla somma delle due menzionate operazioni di pagamento contestate e disconosciute, 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. Chiede altresì il riconoscimento degli interessi legali dalla data dei singoli addebiti sino al saldo effettivo.

L'intermediario convenuto, con le controdeduzioni, sostiene la regolare contabilizzazione, autenticazione e registrazione delle operazioni in oggetto, evidenziando inoltre la colpa grave della

cliente, che, per sua stessa ammissione, ha cooperato attivamente all'esecuzione dei pagamenti contestati, seguendo le indicazioni ricevute telefonicamente dai truffatori e consentendo il controllo da remoto del proprio computer. Segnala inoltre di avere esperito un tentativo di recall dei bonifici controversi, che tuttavia non ha avuto esito positivo. Chiede dunque il rigetto del ricorso.

DIRITTO

La questione sottoposta al Collegio concerne la rimborsabilità o meno in favore di parte ricorrente della somma fraudolentemente sottratta mediante svolgimento di operazioni sconosciute. Si tratta, in particolare, di un bonifico online, di importo pari a € 4.656,64, disposto alle ore 14:16 del 3 dicembre 2025 tramite accesso all'area riservata dei servizi di internet banking dell'intermediario convenuto, e di un bonifico ordinario di importo pari a € 19.900,00, eseguito in data 4 dicembre 2025 direttamente dalla cliente presso la filiale del convenuto in cui è radicato il conto corrente intestato alla medesima. 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).

Il Collegio rileva innanzitutto come, dall'analisi della documentazione versata in atti, con riferimento alla dinamica della truffa di cui è ricorso, non è contestata la circostanza che la ricorrente dichiarò chiaramente di aver dato seguito, almeno parzialmente, alle indicazioni ricevute telefonicamente da un sedicente operatore del servizio antifrode dell'intermediario convenuto, collaborando dunque con il truffatore per l'esecuzione del pagamento di cui è ricorso. Senonché, dalla documentazione versata in atti e dai log prodotti, è pacifico rilevare che: a) la ricorrente, tratta in inganno da quanto riferito dal sedicente operatore della banca, ha fornito le "credenziali d'accesso" al suo conto online; b) successivamente, seguendo le istruzioni impartite nel corso di una seconda telefonata, questa volta da parte di un sedicente carabiniere, ha scaricato un'applicazione utile a consentire al truffatore il controllo da remoto del suo pc; c) la prima operazione di pagamento contestata è stata disposta dal truffatore e autorizzata dalla cliente confermando la notifica push in App (sistema SmartOTP) sul proprio device certificato, credendo di eseguire una procedura strumentale a bloccare un tentativo di bonifico fraudolento in corso di pari ammontare; d) infine, il truffatore anticipava una successiva chiamata per il giorno successivo allo scopo di completare le presunte operazioni di messa in sicurezza dei risparmi della cliente (telefonata che poi avverrà, con l'effetto di indurre la medesima a disporre la seconda operazione contestata direttamente presso la filiale di riferimento del convenuto). In proposito, si ritiene che se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad esempio con l'inserimento, come nel caso di specie, di uno solo dei fattori di autenticazione), l'operazione contestata non deve intendersi, per ciò solo, autorizzata (cfr. Collegio di Milano, Decisione n. 4601/2024). Ne consegue che, in relazione alla data di effettuazione della prima operazione contestata, la sussistenza delle responsabilità che le parti della controversia odierna vicendevolmente si addebitano dovrà essere valutata in base a quanto previsto dal vigente 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) 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 abus"*. 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 la cliente sia caduta vittima del noto fenomeno del c.d. "phishing attraverso smishing misto a vishing",

realizzato mediante iniziale sms contenente un numero telefonico da chiamare allo scopo di impedire l'esecuzione di una o più operazioni di pagamento disposte attraverso accesso fraudolento alla propria area riservata dei servizi di internet banking del convenuto. Successivamente, gli ignoti truffatori contattati telefonicamente chiedevano alla vittima di fornire le credenziali e i codici necessari a consentire loro di accedere tramite web all'area riservata dei servizi di internet banking dell'intermediario, anche per il tramite di un'apposita App, che ha consentito di assumere da remoto il controllo del pc della cliente. In tal modo i malfattori sono stati in grado di poter autorizzare, almeno parzialmente, la prima transazione fraudolenta al centro della presente controversia. L'intermediario, in effetti, attraverso le evidenze versate in atti e i log prodotti, ricostruisce i singoli passaggi sia dell'esecuzione delle operazioni prodromiche alla menzionata transazione fraudolenta, sia dell'esecuzione di quest'ultima e dimostra che il sopra menzionato bonifico online è stato disposto attraverso il sistema autorizzativo di tipo dinamico funzionante mediante notifica push generata dall'App dei servizi di internet banking installata sul cellulare registrato dell'utilizzatore, previo accesso tramite PC all'area riservata dei servizi di internet banking tramite inserimento di credenziali statiche e dinamiche. In particolare, l'autenticazione forte a due fattori (SCA) sarebbe provata dal fatto che, con riferimento alla fase prodromica (accesso alla pagina web dell'area riservata dei servizi di internet banking), sarebbe stato richiesto all'utilizzatore la conferma della notifica push generata in App sullo smartphone della ricorrente (fattore di possesso), previo inserimento di userid e password (fattore della conoscenza); similmente, l'operazione risulta essere stata autenticata tramite l'inserimento di userid e password (fattore della conoscenza) e successiva conferma in App della notifica push generata sul device certificato della cliente (fattore di possesso). Alla luce delle evidenze in atti, anche tenendo in considerazione le dichiarazioni confessorie di parte ricorrente, 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 il proprio orientamento consolidato, induce a ritenere, in assenza di ulteriori indizi di anomalia delle operazioni, 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. 5321/2025 e n. 9002/2024).

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 con riferimento alla prima delle due operazioni contestate. Sul punto, dalla ricostruzione dei fatti così come evincibile dalla documentazione versata in atti dalle parti, pare sia da escludersi, nella vicenda in oggetto, la possibilità di desumere in capo all'utilizzatore un comportamento gravemente colposo, non essendo presente una serie di elementi di fatto particolarmente univoca e convergente, al punto che possa ragionevolmente ritenersi che l'utilizzo fraudolento sia effettivamente riconducibile sul piano causale alla condotta dell'utilizzatore (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 della cliente sia temperata dalla natura particolarmente insidiosa e sofisticata della truffa di cui è ricorso, realizzatasi attraverso "ID caller spoofing". In effetti, come risultante dalla denuncia e dal registro chiamate prodotto in atti, il numero telefonico utilizzato per la prima chiamata effettuata dai truffatori in data 3 dicembre 2025 ai fini della perpetrazione della truffa al centro della presente controversia corrisponde al numero verde dell'intermediario: e ciò non può essere senza conseguenze in quanto l'apparente provenienza da un canale ufficiale della banca può senz'altro attenuare il livello di attenzione e di sospetto da parte della cliente (cfr. ex multis Collegio di Milano, Decisione n. 4033/2021). E così pure, dalle allegazioni documentali, è agevole rilevare come il numero telefonico utilizzato dal sedicente carabiniere per le telefonate fraudolente successive alla prima e strumentali all'esecuzione delle operazioni di pagamento disconosciute e contestate è riconducibile alla Stazione dei Carabinieri ubicata presso la città di residenza della cliente. Pertanto, con riferimento alla prima delle due operazioni di pagamento di cui è ricorso – il bonifico online di importo pari a € 4.656,64 – il Collegio, in conformità all'orientamento consolidato dell'Arbitro, da cui non c'è ragione di discostarsi, valutata la gravità delle colpe a carico di entrambe le parti in relazione ai fatti illustrati e documentati, ritiene di doverle ripartire in misura di metà a carico della parte ricorrente e di metà a carico della parte resistente, con la conseguenza che l'intermediario dovrà provvedere a corrispondere alla cliente la somma di € 2.328,00, pari al 50% della somma fraudolentemente sottratta (cfr. ex multis Collegio di Milano, Decisioni n. 8435/2023, n. 3819/2023 e n. 2184/2023). Con riferimento, invece, alla seconda operazione contestata – il bonifico ordinario di importo pari a € 19.900,00 - dall'analisi della documentazione versata in atti, con riferimento alla dinamica della truffa di cui è ricorso, non è contestata la circostanza che la ricorrente dichiarò chiaramente di aver dato seguito alle indicazioni ricevute telefonicamente da un sedicente carabiniere, effettuando personalmente l'operazione di pagamento di cui è ricorso, nella convinzione di eseguire una procedura finalizzata a stornare un bonifico di pari importo, precedentemente disposto da ignoti truffatori che erano riusciti ad accedere all'area riservata dei servizi di internet banking del convenuto. Parte ricorrente, se pur in buona fede, ha, quindi, personalmente eseguito le istruzioni date dal truffatore che hanno portato al perfezionamento della menzionata operazione di bonifico, successivamente contestata. Orbene, in casi simili, in modo assorbente, i Collegi territoriali hanno statuito che le operazioni effettuate dall'utilizzatore dei servizi di pagamento, seppure sulla base di un consenso viziato dal raggirio subito dal terzo ignoto, non possono configurarsi come non autorizzate, ex art. 10 D. Lgs. n. 11/2010, dovendo, piuttosto, essere inquadrate nel contesto delle operazioni autorizzate dall'utilizzatore (cfr. ex multis Collegio di Milano, Decisioni n. 2419/2025, n. 432/2023 e n. 12726/2022; Collegio di Roma, Decisione n. 8538/2021). Pertanto, in caso di operazioni compiute direttamente dall'utilizzatore dei servizi di pagamento, l'intermediario è esonerato dalla prova di autenticazione e non è configurabile una responsabilità oggettiva a suo carico, non sussistendo i presupposti previsti dalla PSD II per il rimborso della somma richiesta da parte ricorrente (cfr. ex multis Collegio di Milano, Decisioni n. 638/2025, n. 13472/2023 e n. 15827/2022; Collegio di Bari, Decisione n. 6757/2025).

Ciò non toglie che il Collegio non possa rilevare una responsabilità concorrente del prestatore di servizi

di pagamento secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode. Tale responsabilità può configurarsi nei casi di mancata disponibilità del numero verde del prestatore, di mancata identificazione del tentativo di frode in corso da parte del dipendente cui il pagatore si sia rivolto, ovvero di mancato rilievo di indizi di frode quando il blocco delle transazioni avrebbe reso il cliente consapevole dell'effettiva natura delle operazioni (cfr. ex multis Collegio di Milano, decisione n. 9261/2025). Nel caso di specie, esclusa pacificamente la sussistenza dell'ipotesi che l'unica operazione contestata eseguita personalmente allo sportello possa integrare gli indizi di frode di cui al D.M. 112/2007, è agevole rilevare il mancato rilievo delle altre ipotesi sopra richiamate. In particolare, dall'analisi della documentazione versata in atti, la ricorrente non ha fornito alcun elemento idoneo a dimostrare che l'operazione contestata non fosse in linea con la propria normale operatività, anche considerata la causale del bonifico ("*prestito familiare infruttifero*") e l'irremovibilità manifestata dalla cliente nell'esecuzione del bonifico a fronte delle domande di verifica poste dal personale della filiale. Né sono stati fornite da parte ricorrente adeguate evidenze probatorie in merito al suo comportamento e allo stato emotivo durante l'interazione con l'operatore di sportello, per il quale non vi sono elementi idonei a provare un comportamento non conforme al livello di diligenza dovuta. Sul punto, nonostante la cliente abbia dichiarato che durante l'esecuzione dell'operazione sarebbe stata in contatto telefonico con il truffatore – come dimostrato dal registro chiamate versato in atti – non è tuttavia chiaro se tale chiamata fosse in concreto percepibile dal personale di filiale; circostanza questa, che avrebbe dovuto mettere in allerta l'operatore di sportello. Inoltre, la ricorrente ha ammesso di essere rientrata nella filiale subito dopo essersi accorta della truffa e di avere chiesto al personale della filiale di attivare la procedura di recall del bonifico, la quale tuttavia ha avuto esito negativo. In effetti, in relazione alla natura della truffa di cui è ricorso, secondo la consolidata giurisprudenza dell'Arbitro, l'unico obbligo che grava sull'intermediario è solo quello di eseguire gli ordini di pagamento impartiti (e quindi appositamente autorizzati) dall'utilizzatore dello strumento di pagamento, con la conseguenza che i profili imputabili alla sua responsabilità sono solo quelli relativi all'eventuale inadempimento o inesatto adempimento di detto obbligo (cfr. ex multis Collegio di Milano, Decisioni n. 6732/2025, n. 14351/2022 e n. 24573/2019; Collegio di Roma, Decisione n. 6531/2016; Collegio di Coordinamento, Decisioni n. 1260/2014 e n. 1259/2014).

In conclusione, la domanda di rimborso della seconda operazione contestata deve essere rigettata, essendo stata personalmente eseguita dalla ricorrente, ancorché sulla base di un consenso viziato dal raggirio subito, e non sussiste alcuna responsabilità concorrente dell'intermediario convenuto (cfr. ex multis Collegio di Milano, Decisioni n. 2890/2025 e n. 12409/2023).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.328,00 oltre interessi legali dal reclamo al saldo.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE