

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 10 marzo 2026, la cliente riferisce di avere denunciato, in data 27 dicembre 2025, di essere stata oggetto di frode informatica – riconducibile al fenomeno c.d. phishing – che si sarebbe concretizzata nell'addebito sul proprio conto corrente di un pagamento online su un noto sito estero di e-commerce, per un importo pari a € 1.287,05, comprensivo di commissione bancarie per € 14,00. La transazione fraudolenta è stata effettuata il precedente 25 dicembre 2025 tramite carta di credito intestata alla ricorrente ed emessa dall'intermediario convenuto. Di conseguenza, disconoscendo l'addebito registrato sul proprio conto corrente sopra evidenziato, la ricorrente ha chiesto il rimborso della somma di € 1.287,05 relativa all'operazione di pagamento online contestata e disconosciuta, in quanto frutto di frode informatica la cui responsabilità è asseritamente da imputare alla banca, che non avrebbe saputo impedire una violazione al proprio sistema informatico da parte dei truffatori, non garantendo adeguata tutela alla cliente. Chiede altresì il riconoscimento degli interessi legali a decorrere dalla data di effettuazione dell'operazione fraudolenta, nonché la rifusione delle spese di lite.

L'intermediario convenuto, con le controdeduzioni, sostiene la regolare contabilizzazione, autenticazione e registrazione dell'operazione in oggetto, evidenziando inoltre la colpa grave della cliente, che, per sua stessa ammissione, ha cooperato attivamente all'esecuzione del pagamento contestato seguendo le indicazioni ricevute dai truffatori e inserendo i dati della propria carta di credito su di un link di dubbia provenienza, non riconducibile alla banca. 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 pagamento online su un noto sito estero di e-commerce, di importo pari a € 1.287,05 (comprensivo di commissioni bancarie per € 14,00), disposto alle ore 20:31 del 25 dicembre 2025 tramite carta di credito intestata alla cliente ed emessa dall'intermediario convenuto. 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 via sms da una sedicente controparte interessata all'acquisto del bene posto in vendita dalla cliente sulla menzionata piattaforma di vendita online, 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 comunicato dal sedicente acquirente, ha cliccato sul link inviato da quest'ultimo, venendo indirizzata su un sito web – clone del portale di e-commerce menzionato in fatto – che confermava il buon esito della transazione; b) successivamente, provvedeva a inserire le credenziali della propria carta di credito all'interno di tale sito, credendo di eseguire una procedura di identificazione strumentale alla ricezione dell'accredito derivante dalla vendita; c) l'operazione di pagamento contestata è stata disposta dal truffatore ed autorizzata dalla cliente tramite conferma di notifica push generata in App sul proprio device. 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 dell'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 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 documentazione versata in atti non vi sono elementi capaci di chiarire senza ombra di dubbio la dinamica della asserita truffa perpetrata ai danni della cliente, la quale, invero si limita a disconoscere genericamente l'operazione fraudolenta di cui è ricorso, ribadendo con fermezza di non aver disposto il pagamento e di essere stata vittima di una sofisticata frode informatica. L'intermediario convenuto, comunque, ritenendo di qualificare come “phishing” il fatto al centro della presente controversia, sulla base del materiale documentale e dei file di log versati in atti, ricostruisce i singoli passaggi strumentali all'esecuzione della transazione fraudolenta e dimostra che quest'ultima è stata disposta attraverso il sistema autorizzativo di tipo dinamico funzionante mediante conferma di notifica push generata a mezzo token software dall'App dei servizi di internet banking installata sul device certificato dell'utilizzatore. In particolare, l'autenticazione forte a due fattori (SCA) sarebbe provata dal fatto che, ai fini del perfezionamento del pagamento online sul portale web condiviso dal truffatore con la cliente, sarebbe stato richiesto alla medesima di confermare la notifica push generata in App a mezzo token software sul device certificato dell'utilizzatore (fattore del possesso) e, successivamente, di attivare il riconoscimento biometrico mediante impronta digitale (fattore dell'inerenza). 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 il proprio orientamento consolidato, induce a ritenere, in assenza di ulteriori indici 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. 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 di cui è ricorso sia effettivamente riconducibile sul piano causale alla condotta della 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”*. Al riguardo, con riferimento alla vicenda al centro della presente controversia, sulla base della documentazione versata in atti, il Collegio osserva che la cliente è caduta vittima di una comune forma di frode informatica perpetrata tramite inserimento delle credenziali dello strumento di pagamento su un portale web di e-commerce non riconducibile all'intermediario, come agevolmente deducibile dagli scambi di sms intercorsi tra ricorrente e truffatore. In particolare, secondo canoni di ordinaria prudenza, doveva reputarsi anomala e non plausibile la richiesta di inserire i dati della carta di pagamento e di confermare una notifica push al fine dichiarato di ricevere un accredito derivante da una vendita online, trattandosi di attività tipicamente funzionali all'esecuzione di un pagamento e non alla mera ricezione di somme. Secondo l'orientamento consolidato dell'Arbitro, le frodi basate sull'invio di link che inducono il titolare dello strumento di pagamento a inserire credenziali o dati della carta su piattaforme esterne all'intermediario rientrano in uno schema ormai tipico e noto di phishing, privo di caratteri di particolare sofisticazione ed evitabile con l'impiego di media diligenza da parte dell'utilizzatore dello strumento di pagamento (cfr. ex multis Collegio di Milano, Decisioni n. 4697/2026 e n. 5836/2025). In considerazione di quanto sopra evidenziato, rilevata, da un lato, la corretta autenticazione con sistema forte a due fattori, contabilizzazione e registrazione dell'operazione contestata da parte del convenuto e, dall'altro lato, accertata la colpa grave della cliente, in coerenza con l'orientamento consolidato dell'ABF, da cui non c'è ragione di discostarsi, la richiesta di rimborso non può essere accolta (cfr. ex multis Collegio di Milano, Decisioni n. 2036/2023, n. 10876/2022, n. 6441/2022 e n. 22528/2021).

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE