

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 06/05/2026

FATTO

Il ricorrente espone di aver messo in vendita uno smartphone su una nota piattaforma di e-commerce in data 12/12/2025 al prezzo di € 580,00. In pari data, riceveva una e-mail che gli confermava l'avvenuto acquisto e lo invitava a cliccare su un link per incassare il corrispettivo. Seguendo le istruzioni fornitegli, il cliente veniva indotto a confermare, per tre volte e con codici diversi, delle operazioni tramite l'app del proprio istituto di credito, nella convinzione di finalizzare una transazione in entrata. Solo alla richiesta di un quarto codice, si avvedeva che dal suo conto erano stati eseguiti tre prelievi per importi di € 700,00, € 281,00 e € 319,00, per un totale di € 1.300,00. Procedeva quindi a bloccare la carta e a sporgere denuncia presso le Autorità competenti. In data 17/12/2025, presentava reclamo all'intermediario, che forniva riscontro negativo. Il ricorrente chiede la restituzione dell'importo fraudolentemente sottratto, sostenendo di non aver mai avuto la consapevolezza di disporre operazioni di pagamento in uscita. A suo dire, la mera esecuzione materiale, seppur autenticata, non integra il consenso, poiché tratto in inganno da un raggirò non immediatamente riconoscibile. Contesta inoltre che le notifiche PUSH ricevute avessero un contenuto idoneo a renderlo edotto della natura dispositiva delle operazioni.

L'intermediario resiste al ricorso, eccependo in via preliminare il valore confessorio delle dichiarazioni rese dal cliente in sede di denuncia, dalle quali emergerebbe l'ammissione di aver inserito i propri dati su un sito truffaldino. Nel merito, sostiene che le operazioni debbano considerarsi autorizzate ai sensi del D.Lgs. 11/2010. In subordine, evidenzia la sussistenza della colpa grave del cliente, il quale

sarebbe caduto vittima di una truffa semplice e non scusabile, seguendo pedissequamente le istruzioni di uno sconosciuto per una procedura palesemente anomala rispetto all'incasso di una somma di denaro. L'intermediario asserisce che le operazioni sono state correttamente autenticate mediante sistema di autenticazione forte (SCA), con notifica PUSH sul dispositivo certificato del cliente (fattore di possesso) e successiva validazione tramite codice PIN (fattore di conoscenza). Aggiunge di fornire ampia informativa alla clientela sui rischi di frode e che la notorietà di tali fenomeni impone un onere di diligenza minima in capo all'utente.

Nelle proprie repliche, il ricorrente ribadisce l'assenza di consapevolezza nel disporre i pagamenti e contesta la sussistenza di una colpa grave a suo carico, operando egli in un contesto apparentemente coerente con una vendita online.

L'intermediario, in controreplica, insiste per il rigetto del ricorso, sottolineando come il raggiro sia totalmente estraneo alla sua sfera di controllo e si sia perfezionato unicamente a causa della condotta negligente del cliente.

DIRITTO

La questione sottoposta all'esame del Collegio attiene alla richiesta di rimborso di somme addebitate sul conto del ricorrente a seguito di operazioni di pagamento sconosciute, perfezionatesi nell'ambito di una frode informatica nota come "phishing".

La disciplina di riferimento è contenuta nel D.Lgs. 27 gennaio 2010, n. 11, che recepisce la Direttiva europea sui servizi di pagamento (PSD2). Ai sensi dell'art. 10 di tale decreto, in caso di operazione di pagamento non autorizzata, grava sul prestatore di servizi di pagamento (PSP) l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze di malfunzionamenti o altri inconvenienti.

Il comma 2 del medesimo articolo precisa, inoltre, che l'utilizzo di uno strumento di pagamento non è di per sé sufficiente a dimostrare che l'operazione sia stata autorizzata, né che l'utente abbia agito in modo fraudolento o con dolo o colpa grave, la cui prova è sempre a carico del PSP.

Nel caso di specie, l'intermediario ha fornito evidenza documentale (log informatici) attestante che le operazioni contestate sono state autorizzate mediante un sistema di autenticazione forte (SCA), in conformità con quanto previsto dall'art. 10-bis del D.Lgs. 11/2010.

Dagli atti risulta che le disposizioni sono state validate tramite l'invio di una notifica PUSH sul dispositivo mobile del ricorrente, censito e certificato dall'intermediario (elemento di "possesso"), e la successiva autorizzazione mediante l'inserimento del codice PIN personale del cliente (elemento di "conoscenza"). Il Collegio ritiene, pertanto, che l'intermediario abbia assolto all'onere probatorio relativo alla corretta autenticazione delle operazioni.

Ciò posto, occorre valutare se la condotta del ricorrente integri gli estremi della colpa grave, idonea a escludere il diritto al rimborso. Secondo l'orientamento consolidato di questo Arbitro, la colpa grave dell'utente non può desumersi dalla mera allegazione della corretta autenticazione dell'operazione, ma deve essere provata dall'intermediario sulla base di elementi specifici e concreti che dimostrino una palese e macroscopica violazione degli obblighi di diligenza e custodia delle credenziali personalizzate. Dalla ricostruzione dei fatti, emerge che il ricorrente, al fine di incassare il prezzo di una vendita online, ha seguito un link contenuto in una e-mail sospetta e ha eseguito una procedura che lo ha portato ad

autorizzare, tramite l'app della banca, tre distinte operazioni di pagamento in uscita. La condotta del cliente appare connotata da un'evidente e non scusabile negligenza. L'idea di dover autorizzare operazioni dispositive sul proprio conto per ricevere un pagamento è intrinsecamente contraddittoria e contraria alle più elementari regole di prudenza che si richiedono a un utente di servizi di home banking. Il fenomeno del phishing è, inoltre, talmente diffuso e noto al pubblico, anche grazie alle campagne informative condotte dagli stessi istituti di credito, che ci si può attendere da un consumatore mediamente avveduto la capacità di riconoscere i tentativi di frode più comuni, quale quello in esame. Il ricorrente ha attivamente cooperato con i truffatori, autorizzando egli stesso le transazioni mediante l'inserimento del proprio PIN, seppur nella convinzione errata di ricevere denaro. Tale errore, tuttavia, non può essere considerato scusabile, in quanto frutto di una grave disattenzione e dell'inosservanza di quel livello minimo di diligenza che avrebbe dovuto indurlo a diffidare di una procedura così palesemente anomala e a non inserire le proprie credenziali di sicurezza a seguito di istruzioni ricevute da sconosciuti tramite e-mail.

Le argomentazioni del ricorrente circa la presunta non chiarezza delle notifiche PUSH non appaiono idonee a scalfire il quadro di grave negligenza delineato. Indipendentemente dal dettaglio testuale della notifica, l'atto stesso di confermare un'operazione tramite l'app bancaria, inserendo un codice personale segreto, costituisce un'azione dispositiva che richiede la massima cautela. Il fatto che il ricorrente abbia ripetuto tale operazione per ben tre volte in un breve lasso di tempo, senza insospettirsi, rafforza la valutazione di una condotta gravemente imprudente.

Alla luce delle suesposte considerazioni, il Collegio ritiene che l'intermediario abbia fornito prova sufficiente della colpa grave del ricorrente, la quale si configura come causa esclusiva del danno patito. Tale circostanza, ai sensi della normativa vigente, esclude il diritto del cliente a ottenere il rimborso delle somme oggetto di contestazione.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE