

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) BARTOLOMUCCI

Seduta del 01/09/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che, in seguito ad un attacco hacker subito alla fine di dicembre 2025, fosse stato contattato da un numero che non proveniva dall'utenza ufficiale dell'intermediario.

Faceva presente che, nonostante ciò, la circostanza che i truffatori conoscessero il suo luogo di lavoro, il nome del titolare e l'avvenuto cambio di numero di telefono in tempi recenti avesse creato in lui un falso senso di sicurezza; soggiungeva tuttavia che, dopo un controllo online dell'estratto conto, si avvedeva dell'esecuzione di un bonifico istantaneo per € 650,00 a favore di un conto estero.

Sebbene riconoscesse che l'operazione contestata fosse stata confermata tramite notifica *push*, sosteneva che l'intermediario non fosse esente da responsabilità poiché il sistema di sicurezza complessivo non era stato in grado di prevenire tecniche di manipolazione così avanzate e mirate di "Vishing" e "Social Engineering".

Affermava di aver anche sporto denuncia presso le Autorità.

Chiedeva, pertanto, il rimborso dell'importo di € 650,00 oltre agli interessi legali.

Si costituiva l'odierno resistente, il quale evidenziava che lo stesso ricorrente avesse ammesso pacificamente, sia nel reclamo che nel ricorso, di aver autorizzato l'operazione contestata confermando la notifica *push* ricevuta.

Precisava che il bonifico fosse stato eseguito in conseguenza di una corretta procedura di autenticazione forte; di contro, evidenziava la manifesta colpa grave del cliente per la sua condotta palesemente avventata, avendo seguito le istruzioni operative fornitegli da ignoti malfattori.

Osservava che, come indicato sul proprio sito internet e in più campagne informative, non chiede alla propria clientela di inserire credenziali e/o fornire informazioni e/o dati riservati e/o svolgere operazioni, attraverso SMS, e-mail, telefonate, ecc.; peraltro, sottolineava che il recapito da cui era partita la truffa non fosse in alcun modo a sé riconducibile.

Rappresentava, da ultimo, il cliente fosse solito utilizzare lo strumento del bonifico istantaneo, e che nel corso del 2025 avesse già eseguito bonifici esteri di importo simile a quello oggetto di contestazione.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale contestava la sussistenza della sua colpa grave, in quanto l'autorizzazione all'operazione di bonifico istantaneo tramite notifica *push* era stata carpita con l'inganno tramite un raggirio mirato e straordinariamente credibile.

Soggiungeva che la chiamata iniziale al datore di lavoro, seguita da quella truffaldina, avesse contribuito a costruire un contesto credibile tale per cui l'usuale prudenza era venuta meno e a non considerare sufficienti i *pop-up* e le informative antifrode ricevute, in quanto la loro natura di messaggi generici e ripetitivi sviluppa assuefazione nell'utente.

Deduceva che i log tecnici provassero la regolarità "formale" della procedura SCA, ma non l'assenza di frode né l'adeguatezza dei presidi di sicurezza che avrebbero dovuto rilevare la natura fraudolenta del bonifico istantaneo verso beneficiario/IBAN non ordinario, con dinamica temporale compatibile con *social engineering*. Soggiungeva che i versamenti di analoga entità effettuati in passato fossero disposizioni ricorrenti verso un beneficiario estero noto e abituale, quindi non comparabili al bonifico oggetto di contestazione.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale sottolineava che il ricorrente non avesse prodotto alcuno *screenshot* da cui risulterebbe che il truffatore lo avrebbe chiamato prima al numero di telefono del suo datore di lavoro.

Ribadiva che il cliente fosse solito utilizzare lo strumento del bonifico istantaneo e lo avesse già utilizzato verso diversi beneficiari.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di pagamento, successivamente disconosciuta.

La materia, come noto, è regolata dal D. lgs. n. 11/2010 come modificato dal D. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/UE (c.d. PSD2 - Payment Services Directive 2).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici

personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *Strong Customer Authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA gli artt. 97 e 98 della direttiva PSD2, nonché l'articolo 10 bis del D. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; inerenza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che l'operazione disconosciuta consista in un bonifico istantaneo, effettuato in data 27.01.2026, per un importo di euro 650,00.

L'intermediario afferma che essa sia stata eseguita personalmente dal ricorrente; invero, con riferimento a fattispecie analoghe l'orientamento uniforme dei Collegi ha chiarito che se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il prestatore dei servizi di pagamento.

Laddove, invece, l'operazione di pagamento *online* sia stata preparata dal truffatore che ha a disposizione i codici dispositivi del cliente, questa non può ritenersi eseguita per intero dal pagatore, e quindi non può considerarsi sussistente il requisito necessario per escludere il regime di responsabilità previsto dalla PSD2.

Nel caso di specie, il ricorrente – pur non avendo fornito indicazioni utili ad individuare l'autore della disposizione di bonifico – ha comunque ammesso di aver autorizzato l'operazione tramite notifica push. Ciò rilevato, l'intermediario premette che le modalità di accesso e disposizione *online* sono subordinate all'attivazione del sistema di autenticazione "Token" nell'App V* per smartphone, regolarmente avvenuto nel caso di specie nel mese di aprile 2023; quanto all'accesso al servizio di *direct banking*, parte resistente afferma in generale che, dopo l'inserimento delle credenziali (utente e password), il cliente riceve una notifica *push* nello smartphone sul quale è attivato il *token* e, aprendo la notifica con

V*-Code (ovvero, un codice di sicurezza personale di cinque cifre definito dallo stesso cliente) o con sblocco biometrico (se previamente attivato nell'App), può autorizzare l'accesso con il suo smartphone. Nel caso di specie, deduce che alle ore 14:29 del 27/01/2026 vi sia stato l'accesso (login) al *direct banking* da parte del cliente con l'inserimento delle credenziali (utente e password - fattore di conoscenza) e con la conferma della notifica push arrivata sul cellulare del Cliente tramite biometria (fattore di inerenza).

Dall'esame delle tracciate informatiche versate in atti emerge che alle ore 14:29:30 siano state inserite le credenziali di accesso (fattore di conoscenza): alle ore 14:29:42 è stato poi inserito il fattore biometrico; tuttavia, i log prodotti non evidenziano – con riguardo all'elemento di conoscenza – la parola "password", limitandosi ad indicare la dicitura "validazione del fattore di conoscenza (credenziali)"; quanto alla conferma della *push*, invece, essi non specificano quale sia il fattore biometrico utilizzato (cfr. al riguardo, Coll. Milano, dec. n. 11273/2025; n. 964/2026).

La mancanza anche parziale della prova del rispetto dei presidi di sicurezza in tutte le fasi dell'operazione di pagamento, e quindi sin da quella di accesso al sistema, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, costituendo, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Coll. coord., dec. n. 22745/2019).

Deve, pertanto essere riconosciuto il diritto del ricorrente ad ottenere la ripetizione del controvalore dell'operazione contestata.

Il Collegio dispone che sulla somma così riconosciuta vadano computati gli interessi al tasso legale, a far data dal reclamo.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 650,00, 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