

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 20/01/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che nel mese di febbraio 2025 fosse stato contattato, tramite sms, da un sedicente broker finanziario, che rappresentava la possibilità di effettuare investimenti in criptovalute.

Faceva presente di aver eseguito alcuni versamenti mediante l'utilizzo dell'applicativo AnyDesk, con cui il truffatore controllava remotamente il computer, utilizzando direttamente il suo conto corrente.

Precisava che tutte le operazioni fossero state effettuate a seguito di giroconto per la creazione della provvista; soggiungeva che due operazioni da euro 33.000,00 (effettuata in data 02.04.2025) e da euro 8.000,00 (effettuata in data del 10.04.2025) fosse stata eseguita direttamente allo sportello, senza che l'operatore addetto chiedesse alcuna giustificazione, né facesse firmare un modulo antiriciclaggio.

Riteneva che l'intermediario avrebbe dovuto realizzare azioni di tutela del cliente a fronte dell'operatività anomala sul conto.

Chiedeva, pertanto, la restituzione del controvalore delle operazioni disconosciute per il complessivo importo di euro 93.228,00 (o del diverso importo ritenuto di giustizia), oltre alla rifusione delle spese di assistenza difensiva.

Costituitosi ritualmente, l'intermediario evidenziava che la rappresentazione dei fatti presentata dal cliente contenesse la dichiarazione, di natura confessoria, per cui avesse effettuato personalmente le operazioni seguendo, le istruzioni del frodatore; riteneva, di conseguenza, che non fosse applicabile la disciplina di cui alla PSD2 e al D. Lgs n. 11 del 27/01/2010.

Precisava, comunque, che ciascuna operazione fosse stata comunque correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali.

Chiedeva, pertanto, il rigetto del ricorso.

Seguivano memorie di replica e controreplica, con le quali le parti reiteravano le rispettive deduzioni.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni, successivamente disconosciute.

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 le operazioni contestate consistono in sette bonifici eseguiti tra il 03.03.2025 e il 10.04.2025, per il corrispettivo importo di euro 93.228,00; di queste, due sono state eseguite allo sportello mentre le altre cinque mediante canali digitali.

Quanto alle prime, il Collegio non può mancare di rilevare la natura confessoria delle allegazioni contenute nel ricorso, dalle quali emerge che esse siano state eseguite direttamente dal cliente, il quale è caduto vittima di un raggirò ed ha impartito i rispettivi ordini di bonifico allo sportello.

In relazione ad analoghe fattispecie, invero, questo Collegio ha avuto modo di affermare che debba considerarsi esclusa l'applicabilità della disciplina prevista nelle ipotesi di utilizzi fraudolenti di strumenti di pagamento atteso che, "per quanto la volontà del cliente di effettuare tali operazioni sia stata viziata per effetto del raggirò subito dal terzo ignoto, l'intermediario non poteva che considerare autorizzati i pagamenti effettuati personalmente dal titolare dello strumento di pagamento, non avendo alcuna possibilità di accorgersi della truffa perpetrata ai danni del cliente" (cfr. Collegio di Milano, decisione n. 16551/2021).

Tanto basta perché i bonifici contestati dal ricorrente non possano considerarsi come "operazione non autorizzata" e non ricadendo quindi nell'ambito di applicazione delle norme protettive (artt. 10 e 12 del d. lgs n. 11/2010) previste per le operazioni di pagamento.

Dalle risultanze istruttorie non è dato rilevare neppure la sussistenza di ulteriori e distinti profili di responsabilità – anche concorrente – dello stesso, in applicazione delle norme di diritto comune.

Rispetto alle contestazioni del ricorrente, il quale ha affermato che l'addetto allo sportello non avrebbe chiesto alcunché rispetto alle operazioni in corso di esecuzione e non avesse neppure effettuato le verifiche antiriciclaggio, l'intermediario ha prodotto in atti alcune evidenze che riportano la dicitura "controlli antifrode", affermando di avere implementato tale ulteriore misura di sicurezza che consente

al cliente di visualizzare un messaggio univoco cui dare conferma; per entrambe le operazioni risulta inoltre compilato il questionario di adeguata verifica.

Quanto alle ulteriori operazioni, effettuate mediante canali digitali, risulta *per tabulas* che l'enrollment della carta di pagamento sul sistema autorizzativo del dispositivo mobile del ricorrente sia stato eseguito in data 06.10.2024, di molto antecedente rispetto alle operazioni disconosciute, tramite digitazione di password (fattore di conoscenza) e OTP ricevuto via sms (fattore di possesso).

Con riferimento alla fase dispositiva, le tracciate informatiche evidenziano che i log in siano avvenuti pochi minuti prima delle operazioni disconosciute e realizzati da app con il telefono precedentemente enrollato; in seguito, le operazioni sono state autorizzate tramite codice Id (fattore di conoscenza) dal device precedentemente associato (fattore di possesso).

Attesa la conformità ai requisiti di autenticazione forte richiesti dalla normativa, non resta, quindi, che verificare se – dalla condotta tenuta dalla ricorrente – siano evidenziabili profili di colpa grave, rispetto alla quale la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

Mette conto, in primo luogo, osservare che lo stesso cliente abbia riferito di essere stato vittima di una truffa articolata, iniziata con un ingaggio avvenuto con l'invio di un sms che promuoveva investimenti in criptovalute, in seguito al quale egli ha scaricato l'applicazione anydesk sul proprio dispositivo.

Con riferimento specifico a siffatte tipologie di applicazione, va rilevato che esse consentono il controllo da remoto del dispositivo su cui sono state installate, gestendo i relativi contenuti da un computer. Per acquisire il controllo da remoto è necessario e sufficiente inserire l'ID univoco fornito dall'applicazione. Il truffatore, pertanto, una volta convinto il cliente a scaricare l'applicazione, riesce ad accedere al dispositivo e ad operare direttamente in esso, visualizzando in modo automatico tutti i messaggi provenienti dall'intermediario (contenenti ad es. le notifiche push, gli OTP ovvero gli alert relativi all'avvenuta operazione di pagamento), eseguendo le operazioni fraudolente senza la necessità di contattare ulteriormente il cliente ovvero richiedere informazioni aggiuntive. Tale applicazione non reca alcuna indicazione riferibile all'intermediario ed è direttamente scaricabile da parte di ogni utente.

Appare, dunque, evidente che – al fine di consentire tale controllo da remoto – il cliente abbia dovuto scaricare la relativa applicazione e, violando gli obblighi di custodia e di segretezza delle credenziali, abbia così consentito ai truffatori di poter operare e di agire indisturbati (cfr. Coll. Milano, dec. n. 3309/2025; n. 11631/2024).

Tale circostanza, infatti, (unitamente alla mancata produzione dell'sms civetta asseritamente ricevuto dall'utenza del ricorrente) non soltanto conferma il mancato assolvimento dell'onere probatorio che la

normativa pone a carico dell'utilizzatore, ma dimostra implicitamente che la manipolazione del device sia del tutto estranea alla sfera di controllo dell'intermediario.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE