Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARTOLOMUCCI

Seduta del 02/12/2025

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver subito il furto delle credenziali di accesso al conto corrente online e di essersi accorto dell'esecuzione di alcune operazioni fraudolente in data 28.06.2025.
Chiedeva, pertanto, il rimborso del controvalore delle stesse.
Costituitosi ritualmente, l'intermediario rilevava che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali, sottolineando che i bonifici fossero stati eseguiti dall'abituale dispositivo in uso al cliente.
Evidenziava che il ricorrente non avesse spiegato il modo in cui si sarebbe realizzata la truffa, precisando che non fossero stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici e che non avrebbe in alcun modo potuto impedire l'esecuzione dei bonifici, eseguiti con autenticazione forte da dispositivo abitualmente in uso del cliente.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale contestava di non aver mai ricevuto gli OTP di autorizzazione, di non aver ceduto e/o comunicato a terzi le credenziali di accesso del proprio conto corrente, né di aver subito il furto o lo smarrimento della carta e/o del PIN ovvero di averne rivelato gli estremi.

Affermava che lo *user agent* del cliente è una stringa che un *client http* invia al server ed è facilmente falsificabile e che gli attacchi hacker possono inviare gli stessi valori rendendo il riconoscimento biometrico nei log somigliante se non uguale a quello legittimo.
Soggiungeva che la spunta verde in riferimento all'OTP (contenuta nelle tracciature informatiche prodotte dalla banca) attestasse esclusivamente che il sistema non avesse rilevato anomalie o irregolarità.
Le repliche della ricorrente venivano riscontrate dall'intermediario, il quale si riportava a quanto dedotto nei propri scritti difensivi, insistendo per il rigetto del ricorso.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento della responsabilità dell'intermediario e al conseguente riconoscimento 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 PDS2, 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 otto bonifici eseguiti tra il 27 e il 28.06.2025, per un importo complessivo di € 4.461,02.
Dai log informatici e dalla legenda esplicativa versati in atti emerge che tutti gli accessi alla home banking siano avvenuti per il tramite del cellulare univocamente associato al conto corrente del cliente,

mediante riconoscimento biometrico (fattore di inerenza); le tracciature informatiche, tuttavia, non rilevano la registrazione del secondo fattore di autenticazione.
Al riguardo, l'intermediario ha precisato che detti accessi siano avvenuti senza la necessità dell'inserimento di un secondo fattore di autenticazione, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/389, che autorizza i PSP a non applicare la SCA qualora non siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha effettuato un accesso con doppio fattore.
La norma appena richiamata, come modificata dal Regolamento Delegato (UE) 2022/2360, consente invero che l'accesso c.d. informativo al conto possa avvenire senza applicare la SCA, a condizione che non siano decorsi più di 180 giorni dall'ultima applicazione della SCA.
Rispetto alla richiamata disposizione normativa, si pone la questione di stabilire se, una volta avuto accesso al conto mediante ricorso a un unico fattore (in applicazione della citata esenzione dalla SCA), sia o meno possibile riutilizzare detto fattore e combinarlo con un secondo elemento di autenticazione per autorizzare un'operazione di pagamento. Sul tema si è pronunciata l'EBA (cfr. Q&A 2018_4141) la quale ha chiarito che il Regolamento delegato consente di riutilizzare uno dei fattori di autenticazione inseriti per l'accesso al conto per disporre un'operazione di pagamento online nell'ambito della medesima sessione, purché l'associazione di entrambi fattori produca il *dynamic linking* richiesto dall'art. 5 del Regolamento stesso; l'Autorità ha pure precisato (cfr. Q&A 2020_5516) che tale principio trova applicazione anche allorché l'accesso al conto non sia presidiato da SCA, in quanto riconducibile a una delle ipotesi per le quali è prevista l'esenzione ai sensi dell'art. 10 del Regolamento delegato. In tali casi, è possibile per gli intermediari riutilizzare l'(unico) elemento utilizzato per l'accesso al conto ai sensi dell'esenzione di cui all'art. 10, quando è eseguita un'operazione di pagamento elettronico nell'ambito della stessa sessione, a condizione che siano soddisfatte le condizioni appena descritte.
Nel caso di specie, a prescindere da quanto dedotto dall'intermediario il Collegio rileva – come già ha avuto occasione di chiarire in altri precedenti – che gli accessi *de quibus* non hanno preceduto un'operazione meramente informativa, bensì l'operazione dispositiva vera e propria; essi, quindi, non possono ritenersi rientrante nell'ambito di applicazione del richiamato art. 10, con la conseguenza che non può considerarsi applicabile la prevista esenzione dalla SCA (cfr. Coll. Milano, dec. n. 10636/2024; n. 8155/2024; n. 7574/2024).
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 il rimborso del controvalore delle operazioni contestate.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.461,00.
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