Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore NICOLA RIZZO

Seduta del 30/05/2024

FATTO

Il cliente, nel ricorso, afferma quanto segue:

- è titolare di un conto corrente presso l'Intermediario convenuto;
- in data 19/07/2023, riceveva un messaggio che sembrava provenire dall'intermediario;
- con l'sms gli veniva comunicato il collegamento dell'app da un nuovo dispositivo;
- non comprendendo la lingua italiana, il cliente non dava corso al messaggio ricevuto e, pertanto, non cliccava sul link in esso contenuto;
- ciononostante, dalla visura del conto, il cliente si accorgeva di un bonifico non autorizzato, eseguito in data 19/07/2023 per un importo di € 2.100,00;
- procedeva a bloccare il conto e a presentare denuncia presso le Autorità;
- presentava disconoscimento e reclamo all'intermediario, il quale rispondeva, in entrambi i casi, negativamente;
- l'Intermediario non ha fornito prova della regolarità formale dell'operazione oggetto di disconoscimento;
- in occasione del bonifico contestato, il PSP non ha richiesto al ricorrente la password dinamica necessaria ai fini della sua corretta esecuzione e autenticazione;

- la mancata ricezione della password dinamica sarebbe indicativa di un malfunzionamento delle procedure del PSP dal quale conseguirebbe la responsabilità dello stesso per la perdita economica subita dal cliente;
- il pagamento contestato è stato sicuramente disposto da un indirizzo IP diverso da quello normalmente utilizzato dal ricorrente e, in ogni caso, l'importo del pagamento stesso risulta eccessivamente superiore all'importo delle transazioni normalmente autorizzate dal ricorrente; trattasi di anomalie in presenza delle quali l'Intermediario avrebbe dovuto disporre il blocco cautelativo della transazione;
- il cliente ha sempre custodito con la massima diligenza e accortezza i propri strumenti di pagamento e le credenziali, non ha mai fornito i propri dati bancari rispondendo ad email o sms, né ha cliccato sul link contenuto nel sms civetta.

Il ricorrente domanda, quindi, il rimborso della somma di € 2.100.

Nelle controdeduzioni, l'intermediario, riportato il fatto, afferma quanto segue:

- il cliente è titolare di un conto corrente abilitato ai servizi telematici;
- i contatti del cliente associati all'utenza non sono mai stati modificati nelle giornate prossime a quelle in cui si è perpetrata la truffa;
- l'sms ricevuto non può essere ricondotto all'Intermediario;
- l'analisi tecnica della banca ha permesso di ricostruire una operatività idonea a delineare, da un lato, la colpa grave del cliente e, dall'altro, la correttezza dell'operato della banca, nonché la carenza di qualsivoglia responsabilità alla stessa imputabile;
- l'operazione è stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali;
- a seguito del disconoscimento del cliente, la banca ha tempestivamente inoltrato richiesta di recall alla banca beneficiaria e ha provveduto ad estinguere il rapporto di home banking del cliente;
- stante il sistema di autenticazione forte in uso presso l'utenza del cliente, rileva che il truffatore ha potuto beneficiare dell'operazione contestata solo grazie alla piena collaborazione del ricorrente;
- sussistono i presupposti affinché sia possibile ritenere che l'operazione in oggetto sia stata autorizzata direttamente dal cliente e tramite il dispositivo in possesso di quest'ultimo;
- l'astrattezza e genericità del ricorso è da ritenersi di per sé idonea a determinare il rigetto del ricorso;
- ad ogni modo, dall'analisi dell'sms ricevuto non si evince alcun riferimento all'Intermediario: il soggetto mittente risulterebbe essere lo stesso cliente;
- fermo restando che non è dato comprendere quali siano state le modalità con cui il terzo frodatore è riuscito a prendere contatti con il Cliente e a carpirne le credenziali personali, rileva che non vi è stata alcuna attivazione e installazione di una nuova licenza smart OTP o APP su un nuovo dispositivo mobile;
- la banca ha sensibilizzato la propria clientela sulle truffe con diverse comunicazioni.

L'intermediario convenuto domanda, quindi, il rigetto del ricorso; chiedendo in via subordinata il riconoscimento del concorso di colpa del danneggiato ex art. 1227 c.c.

DIRITTO

Oggetto della controversia è una operazione contestata, per un importo complessivo di € 2.100,00, posta in essere il 19/07/2023, h. 13:30. Alla data dell'operazione trovava

applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.
È in atti la denuncia del cliente presentata in data 24/07/2023.
In via del tutto preliminare, si rileva che l'intermediario convenuto eccepisce che l'operazione sia stata autorizzata dal cliente.
In mancanza di una descrizione dettagliata delle modalità in cui è stata perpetrata la truffa, la contestazione dell'intermediario si basa sul fatto che l'operazione risulta autorizzata dallo stesso dispositivo in precedenza utilizzato dal ricorrente nonché sulla corretta esecuzione e registrazione del bonifico contestato, in assenza di malfunzionamenti dei propri sistemi informatici. Si rileva che, in nessuna occasione (né nel reclamo, né in denuncia, né nel ricorso), il cliente dichiara di aver posto in essere, nemmeno parzialmente, l'operazione contestata.
Si rammenta l'orientamento dei Collegi ABF secondo il quale, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), 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 PSP. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.Lgs. 11/2010.
Con riferimento alla fase di accesso all'area riservata, l'intermediario afferma che per accedere ai servizi online della banca è necessario inserire il PIN (elemento di conoscenza) e confermare successivamente tale accesso sull'APP del proprio dispositivo su cui giunge la notifica push (elemento di possesso).
Rileva, al riguardo, questo Collegio che, dall'esame dei log prodotti dall'intermediario convenuto, si riscontra evidenza dell'inserimento della password (elemento di conoscenza) in corrispondenza del log in delle ore 13:20 ("AUTH VERIFICA CREDENZIALE - PASSWORD nel riquadro rosso doc 13); si riscontra, altresì, evidenza dell'elemento di possesso, ossia la richiesta di autorizzazione inviata tramite PopUp al dispositivo su cui risulta scaricata l'app (riquadro viola nel "doc a" e il corrispondente valore 1 nella colonna "AUTHSTATUS" di cui all'evidenza "Log eventi di autorizzazione notifica app"); si riscontra che l'esito degli eventi di login è uguale a 000; secondo quanto indicato nella legenda, detto codice indica l'inserimento corretto di tutti i parametri di sicurezza (doc. 4).
Con riferimento all'autenticazione forte dell'operazione contestata, l'intermediario afferma che l'operazione è stata autenticata tramite inserimento del PIN dispositivo e autorizzazione dall'App installata.
Sulla base delle evidenze prodotte dallo stesso intermediario, si rileva che: l'operazione di inserimento del bonifico risulterebbe correttamente confermata, come desumibile dal valore 000 nella colonna "ESITO" che implica che l'evento è confermato con inserimento di tutti i parametri di sicurezza previsti, compreso il PIN; non risulta, tuttavia, evidenza del pin dispositivo che pure l'intermediario afferma essere sempre richiesto per autorizzare l'operazione riepilogata mediante notifica sul dispositivo; si riscontra evidenza dell'elemento di possesso, ossia la richiesta di autorizzazione inviata tramite PopUp al dispositivo su cui risulta scaricata l'app (riquadro rosso nel "doc a" – colonna "AUTH STATUS" e il corrispondente valore 1 nella colonna "AUTHSTATUS" di cui all'evidenza "Log eventi di autorizzazione notifica app").
Pertanto, questo Collegio non può ritenere pienamente raggiunta la prova della corretta autenticazione forte dell'operazione disconosciuta dal ricorrente (cfr. Collegio di Milano, decisione n. 2951/24 del 07/03/2024).

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.100,00.
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

Firmato digitalmente da
FLAVIO LAPERTOSA