Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 5460 del 04 aprile 2022

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) TOMMASI	Membro designato dalla Banca d'Italia
(BA) RUSSO	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) CATERINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - DANIELA CATERINO

Seduta del 24/03/2022

FATTO

Il ricorrente dichiara di aver ricevuto un SMS dal numero di telefono utilizzato usualmente dall'intermediario per effettuare comunicazioni, con il quale veniva richiesto di collegarsi alla piattaforma informatica apparentemente riferibile all'intermediario stesso.
Riferisce inoltre di avere scoperto "poco dopo" che erano state eseguite sul suo conto due transazioni non autorizzate: un bonifico - operazione giroconto - di € 14.989,00 e un bonifico di € 10.100, 00.
Chiede "la restituzione delle somme sottratte indebitamente per euro 25.089,00 oltre interessi in quanto il sistema non ha una autenticazione forte, non ha standard di sicurezza adeguati, non è dotata di sistemi idonei che consentano di individuare e bloccare transazioni che presentano profili di anomalie e rischio frode".
L'intermediario riferisce che la richiesta del ricorrente, titolare di un conto cui è associata una carta di pagamento, ha ad oggetto il rimborso della somma pagata per effetto di due operazioni di giroconto on line disposte il 14 ed il 15 maggio 2021, delle quali è riportata evidenza contabile. In proposito, rileva che le verifiche svolte hanno accertato la legittima esecuzione e sostanziale regolarità delle contestate operazioni, posto che il ricorrente si è correttamente autenticato sull'internet banking con le proprie credenziali nelle date indicate e che le transazioni sono state eseguite con sistema dinamico di autenticazione;

ciò in quanto l'esecuzione delle stesse ha necessitato l'utilizzo del codice *** ID in App dell'intermediario.

Dalle evidenze elettroniche risulta infatti che le operazioni in disamina sono state effettuate dalla suddetta applicazione, per la cui installazione e configurazione degli strumenti di pagamento è necessario conoscere:

- le credenziali di accesso ai servizi internet-banking;
- i dati della carta utilizzata per effettuare i pagamenti on line (PAN, CVV2 e data di scadenza);
- password dinamica "usa e getta" inviata sul numero di cellulare rilasciato dal cliente all'intermediario.

L'intermediario ritiene che nel caso di specie il ricorrente abbia comunicato tutti i codici sopra menzionati, causando di fatto la violazione del sistema di autenticazione informatica c.d. "a due fattori" e che pertanto abbia favorito l'indebito utilizzatore con un comportamento gravemente colposo. Evidenzia, peraltro, che, da un lato, il ricorrente non ha mai richiesto il blocco della propria carta di pagamento - ancora attiva alla data delle controdeduzioni – dall'altro, che è lo stesso ricorrente a dichiarare di aver ricevuto sul proprio cellulare un sms con un link truffaldino, non facente capo all'intermediario resistente, tramite il quale è entrato nel sito "civetta" all'interno del quale ha poi inserito i propri dati. Secondo l'intermediario, la presente frode sarebbe pertanto riconducibile alla tipologia di c.d. "phishing" definita "classica" dal Collegio di coordinamento, della quale ha edotto la propria clientela da tempo, e che avrebbe potuto essere evitata dal ricorrente utilizzando la diligenza media, posto che l'intermediario interloquisce con i suoi clienti soltanto tramite canali ufficiali e non richiede mai di comunicare dati relativi agli strumenti di pagamento forniti.

Chiede di rigettare nel merito la richiesta di rimborso avanzata dal ricorrente; nella denegata ipotesi in cui il Collegio la ritenesse meritevole di accoglimento, richiede la decurtazione della prevista franchigia.

Nelle repliche, il ricorrente rileva che l'intermediario non ha fornito riscontro in merito alle richieste di verifica sulle movimentazioni dei conti intestati ai correntisti a favore dei quali sono stati effettuati i bonifici in discussione, sebbene ne conosca l'identità, né ha precisato se i relativi conti siano stati successivamente bloccati o siano ancora attivi come potenziali strumenti per ulteriori truffe verso altri clienti. Afferma, inoltre, che l'intermediario, da un lato, fonda la responsabilità del ricorrente su una serie di supposizioni non dimostrate, in contrasto con le disposizioni di cui agli artt. 2727 e 2729 c.c., e, dall'altro, non ha assolto l'onere di provare il buon funzionamento della piattaforma di pagamento da remoto. Evidenzia, altresì, che l'intermediario non ha attivato il sistema di SMS Alert per ogni disposizione sul conto del ricorrente; in proposito, rileva che il fatto che fosse disponibile sull'applicazione la possibilità di attivare il servizio non esimeva l'intermediario dall'obbligo di attivarlo automaticamente. Il ricorrente contesta inoltre all'intermediario di non avere fornito l'indirizzo IP dei dispositivi utilizzati per l'effettuazione delle operazioni contestate. Per quanto attiene il mancato blocco della carta, precisa che la stessa non è abilitata ad operazioni on line e che il dipendente intervenuto su istanza del ricorrente non ha proceduto al blocco del conto stesso, nonostante la richiesta effettuata in presenza di testimoni, ma ha anche "consigliato e operato affinché venissero cambiati esclusivamente i codici di accesso alla piattaforma". Specifica, inoltre, che l'intermediario ha ignorato il tentativo di mediazione del 12 luglio 2021 proposto presso l'organismo deputato. Insiste pertanto per l'accoglimento del ricorso, chiedendo oltre al ristoro delle somme sottratte anche interessi, danni morali e spese legali.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 5460 del 04 aprile 2022

DIRITTO

La controversia attiene al disconoscimento di tre operazioni non autorizzate dal ricorrente. Nello specifico, si tratta di un giroconto on line di euro 14.989,00 eseguito il 14/05/2021, e un altro giroconto on line di euro 10.100,00 per anticipo delle spese di ristrutturazione di un albergo; operazioni intervallate dal rimborso su richiesta (asseritamente non effettuata dal cliente) di buoni dematerializzati, a nome del ricorrente per l'importo di euro 10.018,99; dal momento che l'operazione di rimborso non ha in sé intaccato il patrimonio del ricorrente, ma è servita a ripristinare la liquidità necessaria a compiere il secondo giroconto, non formerà oggetto di esame da parte del Collegio.

Il ricorrente dichiara di aver ricevuto sul proprio cellulare, il 14/05/2021 alle ore 16:31, un SMS proveniente da un mittente apparentemente riconducibile all'intermediario, con cui veniva informato che le sue utenze stavano per essere sospese "per mancato aggiornamento" e che al fine di evitare tale sospensione avrebbe dovuto cliccare su un link ivi contenuto. L'SMS non è in atti e pertanto non si può verificare se il mittente possa dirsi riconducibile all'intermediario e se, di conseguenza, possa ritenersi sussistere un legittimo affidamento dell'utente circa la genuinità del messaggio.

Il ricorrente riferisce poi di avere cliccato sul link e di essere stato reindirizzato ad una pagina con il logo dell'intermediario, in cui veniva invitato ad inserire alcuni suoi dati personali. Al riguardo precisa di non avere comunque inserito i propri codici di sicurezza. Il 17/05/2021 si avvedeva di non avere più fondi a disposizione sulla carta e, pertanto, si presentava a uno sportello dell'intermediario, presso il quale veniva informato del compimento delle suddette operazioni. In tale occasione l'intermediario provvedeva solo a rigenerare i codici di sicurezza del conto del ricorrente, mentre non disponeva il blocco della carta, a suo dire non richiesto.

Le operazioni sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018.

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10, d. lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti".

Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è altresì precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

L'intermediario afferma che le operazioni controverse sono state effettuate tramite l'app e sono state autorizzate mediante l'utilizzo del "codice xxxxID" in app. In particolare, dichiara che l'autenticazione delle operazioni controverse si è articolata in due fasi:
preliminarmente, l'installazione dell'applicazione dell'intermediario su smartphone, con onboarding dello strumento di pagamento e configurazione del ****ID all'interno dell'app;
a seguire, la disposizione delle operazioni fraudolente tramite inserimento del codice ****ID in app.
L'intermediario fornisce altresì un'articolata spiegazione generale del meccanismo di funzionamento delle procedure di installazione e configurazione, nonché delle modalità di funzionamento nel perfezionamento della transazione con il dispositivo *****ID, allegando alle controdeduzioni un documento denominato La soluzione *****ID in ottica strong customer authentication e un dettagliato schema di funzionamento del sistema.
Non consta una posizione condivisa dai Collegi in merito alla conformità del sistema di autenticazione adottato dall'intermediario rispetto all'esigenza di garantire la Strong Customer Authentication (SCA) ai sensi della vigente disciplina; tuttavia, è evidente che in ogni caso, ai fini della prova della regolare autenticazione, esecuzione e contabilizzazione delle operazioni contestate, non è sufficiente la descrizione in astratto del processo, ma occorre che l'intermediario fornisca prova specifica di come le operazioni si sono svolte (cfr. ex multis Coll. Bari, dec. n.20583/2021).
Ora, nel caso di specie le allegazioni versate in atti dall'intermediario resistente non paiono a questo Collegio sufficienti a ritenere adempiuto l'onere probatorio.
In particolare, sono in atti:
una schermata attestante l'enrollment della carta di pagamento al sistema autorizzativo di tipo dinamico, funzionante mediante invio con sms della password dinamica sul numero di cellulare del cliente, coincidente con quello riportato nella denuncia;
la tracciatura dei messaggi "ricevuti dal cellulare del cliente, a riprova dell'impiego del c.d. sistema di autenticazione "a due fattori" per il perfezionamento della frode in esame", da cui si evince l'invio di n. 2 sms in data 14/05/2021 alle ore 17:13:08 e 17:15:46, al numero di cellulare del ricorrente. Con tali messaggi, secondo quanto rappresentato dall'intermediario, sarebbero state trasmesse le OTP necessarie ai fini dell'"onboarding" della carta e della configurazione del *****ID all'interno dell'APP.
delle schermate con il dettaglio delle operazioni contestate successivamente eseguite, attestanti secondo la resistente "la legittima esecuzione e sostanziale regolarità" dello stesso.
Peraltro, le schermate in questione consentono di stabilire il canale utilizzato per l'esecuzione delle operazioni (l'APP dell'intermediario), ma non forniscono elementi decisivi in merito alle modalità di autenticazione. Nello specifico, non sono presenti i log delle operazioni contestate, dai quali possa evincersi il funzionamento, nel caso concreto, della modalità autorizzativa pur astrattamente descritta (negli stessi termini Coll. Milano, dec. n. 14699/2021 e Coll. Bari, dec. n. 14232/2021).
Il mancato assolvimento dell'onus probandi da parte dell'intermediario rende superfluo l'accertamento in ordine ai profili di colpa grave ascrivibili alle parti. Il Collegio si limita a rilevare, incidentalmente, la mancata prova dell'attivazione del meccanismo di alert, che a detta dell'intermediario verrebbe fornito di default nell'APP di home banking (e v. Coll. Coordin., dec. n. 24366/2019) e che avrebbe potuto impedire l'esecuzione del secondo giroconto, compiuto il giorno successivo al primo.
In assenza di prova dell'autenticazione, corretta registrazione e contabilizzazione delle operazioni contestate, l'intermediario sopporta – in ogni caso – integralmente il peso economico delle operazioni disconosciute, peraltro senza possibilità di applicazione della richiesta franchigia, dal momento che l'art. 12, comma 3, del D.lgs. 27 gennaio 2010, n.

11, come modificato dal D.lgs. 15 dicembre 2017, n. 218, prevede una franchigia a carico del cliente di € 50,00 soltanto in caso di "operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita", dovendosi dunque ritenere esclusa in fattispecie diverse di utilizzo illecito, come quella oggetto del presente ricorso (si veda, tra le molte, Collegio di Bari, decisione n. 5298/2020).

Alla luce delle considerazioni svolte, il Collegio reputa che la domanda del ricorrente debba trovare accoglimento, e che l'operazione debba restare integralmente a carico dell'intermediario.

Vanno al contrario respinte tanto la richiesta di ristoro delle spese legali, quanto quella di risarcimento dei danni morali, inammissibili in quanto introdotte solo in sede di repliche (v. ex plurimis Coll. Bari, dec. n. 14723/2020) e in ogni caso infondate nel merito, in quanto prive di qualsivoglia supporto probatorio.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 25.089,00, oltre gli interessi legali dalla data del 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 al ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI