

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) SEMERARO	Membro designato dalla Banca d'Italia
(BA) ROSSI	Membro designato dalla Banca d'Italia
(BA) COSTANTINO	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARIA MADDALENA SEMERARO

Seduta del 19/01/2023

FATTO

Il ricorrente, titolare di un rapporto cointestato con un altro soggetto, il quale aderisce al presente ricorso, fa presente di avere subito tra il 14 e il 15 aprile 2022 alcuni prelievi fraudolenti per l'importo complessivo di € 35.971,00.

Riferisce di avere ricevuto alcuni sms dal numero istituzionale dell'intermediario con cui veniva invitato ad effettuare alcune verifiche per il ripristino della sicurezza. Lamenta il malfunzionamento dei sistemi di sicurezza approntati dall'intermediario, che non avrebbero protetto le sue credenziali di accesso al conto corrente e i suoi dati personali con misure idonee a garantire la sicurezza del servizio di pagamento telematico, né avrebbero rilevato gli accessi anomali. In particolare evidenzia che gli ignoti operatori sarebbero stati in possesso dei suoi dati personali. Fa presente, inoltre, di avere inviato alcune missive all'intermediario e di avere sporto denuncia all'autorità.

Chiede, pertanto, l'integrale rimborso dell'importo illecitamente sottratto e il risarcimento del danno subito, stimato equitativamente in € 10.000,00, per non avere disposto nei giorni successivi dei fondi necessari per il sostentamento e la regolare gestione della famiglia.

L'intermediario, costituitosi, rappresenta che, per effettuare il login e le operazioni di inquiry, è previsto l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) e del codice OTP e che, per disporre le operazioni, dopo avere effettuato il login, è prevista la conferma con codice PIN e OTP.

Specifica che il codice OTP viene generato in modo silente dal mobile token, integrato nell'App dell'intermediario e attivato sullo strumento/device utilizzato dal cliente. Aggiunge che l'attivazione del mobile token è resa possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'home banking.

Ciò posto evidenzia che, nel caso di specie, in data 14.04.2022, alle 15:09:05, risulta inviato all'utenza telefonica del ricorrente un SMS contenente il codice OTP necessario per l'attivazione del mobile token. Afferma che il ricorrente non avrebbe dovuto comunicare il codice OTP a terzi, come raccomandato nel testo dell'SMS.

Rileva che, dalla denuncia presentata il 23.04.2022, emerge che il cliente avrebbe incautamente assecondato le istruzioni ricevute dagli ignoti malfattori via SMS e per telefono. La frode sarebbe dunque riconducibile a un caso di phishing. Al riguardo, evidenzia che i link contenuti negli SMS ricevuti dal cliente non appaiono riconducibili all'intermediario. Rileva inoltre che con una semplice ricerca in internet il cliente avrebbe potuto avvedersi che si trattava di un link ingannevole.

Quanto alla asserita riconducibilità degli SMS ricevuti a un'utenza riconducibile all'intermediario, evidenzia che il "caller ID" che appare sul telefono non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display. Sono infatti disponibili numerosi servizi e App che consentono di eseguire chiamate esponendo un numero di telefono diverso dal proprio.

Rappresenta, inoltre, che lo stesso cliente avrebbe dichiarato di avere sostituito l'App ufficiale della banca con un'altra estranea, peraltro non disponibile nell'App store ufficiale, consentendo in tal modo ai truffatori di eseguire i bonifici sconosciuti. Evidenzia, inoltre, che il cliente non si è avveduto della frode nonostante i numerosi SMS ricevuti contenenti link ad App sconosciute.

Osserva che da tempo ha posto in essere una campagna informativa contro i rischi di frode. Afferma che, dalle verifiche effettuate, non è emerso alcun malfunzionamento del sistema. Descrive quindi i log prodotti.

Evidenzia, infine, di avere inviato al cellulare del cliente una notifica push e un sms alert per ciascuna operazione sconosciuta.

Quanto alla richiesta risarcitoria, eccepisce che il ricorrente non ha dimostrato i presunti danni subiti e il nesso causale tra gli stessi e il lamentato comportamento della banca.

Chiede, pertanto, di respingere il ricorso in quanto infondato.

In sede di repliche, il ricorrente contesta il contenuto delle controdeduzioni, ribadendo che l'intermediario non ha custodito i suoi dati personali e in particolare il suo numero di cellulare.

Rileva inoltre che i presidi di sicurezza approntati dall'intermediario non prevedevano l'inserimento della domanda segreta al momento dell'attivazione del token, la quale è stata inserita solo successivamente alla realizzazione della frode.

Rileva che non risulta attivato il servizio di SMS alert collegato al suo numero di telefono ed afferma di non avere ricevuto alcun SMS e notifica per l'attivazione del token sul suo numero di telefono certificato, né gli SMS che annunciavano le operazioni sconosciute. Fa presente che il contitolare del conto non avrebbe ricevuto alcun avviso o comunicazione relativamente all'operatività sconosciuta.

Evidenzia, inoltre, che dai tabulati prodotti dall'intermediario risulta che il token è stato attivato su un altro device, con un indirizzo IP diverso da quello del cliente e mai utilizzato in precedenti occasioni. Inoltre fa presente che l'SMS contenente il codice OTP per l'attivazione del token risulta inviato a un numero non certificato. Richiama alcune pronunce della Corte di Cassazione sulla responsabilità dei prestatori di servizi di pagamento.

Insiste, pertanto per l'accoglimento del ricorso.

In sede di controrepliche, l'intermediario ribadisce quanto rappresentato in sede di controdeduzioni, sottolineando l'incauto affidamento del ricorrente nonostante gli SMS con cui veniva comunicato l'inserimento dei bonifici. Evidenzia che il codice OTP necessario per autorizzare le operazioni dispositive non viene inviato via SMS, ma generato in modo silente dal mobile token attivato in precedenza.

Quanto all'attivazione del mobile token, rappresenta che il codice OTP è stato inviato via SMS sul telefono cellulare del cliente e che è possibile attivare il mobile token su due dispositivi senza informare la banca. Rileva inoltre che non risulta alcuna modifica del codice PIN e blocco delle notifiche push, correttamente consegnate sul numero di telefono del ricorrente. Insiste, pertanto, per il rigetto del ricorso.

DIRITTO

Il ricorrente chiede la restituzione della somma di € 35.971,00, a lui addebitata a seguito dell'esecuzione di alcune operazioni di pagamento non autorizzate.

In particolare, il ricorrente afferma di avere ricevuto il 14.04.2022 un SMS da un numero apparentemente riconducibile all'intermediario resistente, contenente un link che reindirizzava a una finestra in cui veniva chiesto di inserire il codice cliente e la password. Precisa di non avere completato l'inserimento delle credenziali e di avere cliccato su tasto per ricevere l'assistenza di un operatore.

Riferisce di essere stato contattato attraverso il medesimo numero da un sedicente operatore, il quale gli inviava un SMS contenente un link a seguito del quale si installava automaticamente una nuova App sul suo telefono. Afferma di avere ricevuto un ulteriore SMS di conferma dell'installazione effettuata, con cui veniva invitato ad attendere alcuni giorni lavorativi per utilizzare i servizi di pagamento.

Rileva poi di essere stato ricontattato il 15.04.2022 dal sedicente operatore telefonico per effettuare una nuova installazione dell'App e di essere stato invitato ad attendere tre giorni lavorativi. Aggiunge, infine, di essere stato contattato un'ulteriore volta dal sedicente operatore, il quale rappresentava la necessità di attendere fino al giorno 20.04.2022 per il completamento dell'operazione.

La disciplina applicabile al caso di specie è contenuta nel d.lgs. n. 11 del 2010, come modificato dal d.lgs. 15 dicembre 2017, n. 218, attuativo della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2). Essa si caratterizza per il particolare favore riservato al cliente, il quale è chiamato a sopportare le conseguenze dannose derivanti dall'utilizzo non autorizzato di uno strumento di pagamento soltanto nei limiti in cui detto utilizzo sia imputabile alla sua condotta dolosa o gravemente colposa. Sul piano probatorio, il riflesso di tale favore è costituito dall'onere posto a carico dell'intermediario, il quale, per andare esente da responsabilità, deve provare sia la regolare esecuzione dell'operazione di pagamento, sia la stessa colpa grave del cliente. L'art. 10 del d.lgs. n. 11 del 2010 dispone infatti che "qualora l'utente 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"; a ciò aggiungendo che "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".

Con particolare riferimento alla prova della regolare autenticazione delle operazioni di pagamento, secondo il consolidato orientamento di questo Arbitro, l'onere gravante sull'intermediario può reputarsi assolto soltanto qualora egli dia prova di avere adottato misure di sicurezza rispondenti a standard elevati, tali da rendere residuali ed eccezionali le ipotesi di intromissioni da parte di terzi non autorizzati nei sistemi di pagamento riferibili ai clienti (Coll. Roma, decisione n. 8829, del 2017; Coll. Torino, decisione n. 7678 del 2018). Quanto, poi, alla prova della colpa grave o del dolo del cliente, è costante l'orientamento che considera assolto l'onere gravante sull'intermediario anche per via presuntiva, purché ricorrano indizi gravi precisi e concordanti (Coll. Coord., decisione n. 1033 del 2012; Cass., 18 gennaio 2010, n. 654).

Nel caso di specie, a essere contestati sono 12 bonifici, di cui 10 (dieci) eseguiti il giorno 14.04.2022 e 2 (due) eseguiti il giorno 15.04.2022. L'importo di ciascuna operazione è di € 3.000,00, ad eccezione della decima che è pari ad € 2.971,00.

Sulla regolarità formale delle operazioni di pagamento, l'intermediario afferma, in via generale, che l'attivazione del mobile token è resa possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente tramite SMS al numero di cellulare certificato. Evidenzia, in particolare, che il 14.04.2022, alle ore 15:09:05, prima dell'esecuzione dei bonifici contestati, è avvenuta l'attivazione del mobile token tramite inserimento del PIN e dell'OTP trasmessa via sms, con "verifica a due fattori". Produce il log relativo alla suddetta operatività, con la relativa legenda esplicativa, da cui si evince l'inserimento delle OTP. Dalla schermata del Log, tuttavia, non risulta l'inserimento del PIN.

A tal riguardo, il Collegio osserva che l'attivazione del mobile token è operazione preliminare alla esecuzione delle operazioni di pagamento, atteso che da quanto riportato dall'intermediario, è tramite il mobile token che si produce l'OTP di volta in volta necessaria per autorizzare le operazioni. Ad avviso di questo Collegio, la documentazione allegata da parte resistente risulta carente proprio sotto il profilo della prova della regolare attivazione del mobile token, considerato che dalla schermata del Log allegata non risulta l'inserimento del PIN, passaggio descritto come fondamentale dallo stesso intermediario.

Il Collegio reputa, pertanto, che non sia stata fornita la prova della regolare autenticazione delle 11 operazioni di pagamento contestate.

La domanda di rimborso merita di essere accolta.

Non merita di essere accolta invece la domanda risarcitoria, in quanto sfornita di supporto probatorio.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 35.971,00.

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 al ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI