COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) MINNECI	Membro designato dalla Banca d'Italia
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) MANENTE	Membro designato da Associazione rappresentativa degli intermediari
(MI) TINA	Membro designato da Associazione rappresentativa dei clienti

Relatore (MI) TENELLA SILLANI

Nella seduta del 18/04/2017 dopo aver esaminato:

- il ricorso e la documentazione allegata
- le controdeduzioni dell'intermediario e la relativa documentazione
- la relazione della Segreteria tecnica

FATTO

Il ricorrente ha chiesto il riaccredito del controvalore di 4 operazioni di pagamento *on line* - rispettivamente 2 ricariche di carte prepagate e 2 bonifici - disposti mediante canale *home banking* a valere sul conto corrente che intrattiene presso l'intermediario convenuto. Ha fra l'altro precisato di essere "*estraneo a cessioni di codici, di dati e di strumenti posseduti*", contestando il rilievo dell'intermediario secondo cui il suo sistema informatico non sarebbe stato violato da alcuno, non avendo lo stesso approfondito alcuni profili relativi alla sicurezza informatica segnalati nei vari reclami. Chiede pertanto al Collegio il riaccredito del controvalore delle operazioni disconosciute, pari a € 11.000,00.
L'intermediario, con le controdeduzioni, riepilogati i fatti oggetto di controversia, assume che il ricorrente sia rimasto vittima di *phishing*, accedendo a un "sito truffaldino" e inserendo tutti i codici richiesti per confermare l'esecuzione delle quattro operazioni successivamente disconosciute. Precisa che dalla tracciatura delle operazioni si evince che in data 24/11/2015: "- *alle 15.37 è stato effettuato un login con le credenziali del ricorrente «mediante app su telefono» con sistema operativo Android; - alle 15.38 è stata disposta la prima ricarica di € 3.000,00 [oltre a 1,00 di commissioni] a favore di una carta prepagata [emessa dallo stesso intermediario] intestata a persona diversa dal ricorrente; - pochi secondi dopo è stata disposta la seconda ricarica di € 2.000,00 a favore della*

medesima carta prepagata; - alle 15.39 è stato disposto il primo bonifico di € 2.000,00; - dalle 15.40 alle 15.42 è stato disposto il secondo bonifico di € 4.000,00, a favore del medesimo beneficiario del precedente; - ciascuna operazione è stata «confermata dal ricorrente, inserendo sul sito la relativa OTP […] utilizzando la sua chiavetta O-Key […], e in assenza di anomalie; - immediatamente dopo è stato registrato un terzo tentativo di bonifico di € 4.900,00, «identico ai precedenti», ma l'operazione è stata interrotta per l'inserimento di una OTP errata; - le operazioni truffaldine sono state effettuate da un indirizzo IP mai utilizzato in precedenza dal cliente, il che confermerebbe essersi trattato di un episodio di phishing; - alle 18.16 è stato effettuato un nuovo login, con i dati del cliente, da un indirizzo IP «che si può presumere del cliente», con una richiesta di rendiconto [verosimilmente a seguito della telefonata con cui l'intermediario ha avvertito il ricorrente di avere bloccato l'accesso all'home banking per attività anomala]". Sottolinea altresì di essersi attivato immediatamente per tentare il recupero delle operazioni disconosciute, senza peraltro riuscirvi; in ogni caso, ribadisce l'assenza di violazioni con riguardo ai propri sistemi informatici, di cui descrive i presidi di sicurezza. Ciò premesso, chiede al Collegio, in via principale, di dichiarare inaccoglibile, in quanto infondata e immotivata, la richiesta restitutoria del ricorrente; in subordine, di definire la ripartizione del danno fra le parti anche ai sensi dell'art. 1227 c.c. in misura proporzionale alle effettive responsabilità.

DIRITTO

La questione riguarda quattro operazioni di pagamento - rispettivamente due ricariche di carta prepagata e due bonifici per un controvalore totale di € 11.000,00 - disposte mediante canale *home banking*, fra le 15:38 e le 15:40 del 24/11/2015, disconosciute dal ricorrente. Dalla "*relazione servizi informativi*" e dal tabulato "*tracciatura operazioni* internet", allegati agli atti dalla parte resistente, emerge quanto segue: 1) nella giornata del 24/11/2015 l'intermediario ha rilevato diverse sessioni aperte con regolare *login* da indirizzi IP operati da un *internet service provider* italiano, la cui rete è utilizzata regolarmente dal cliente; la convenuta presume che dette sessioni, nelle quali è stata effettuata esclusivamente attività rendicontativa, siano state aperte dal cliente stesso; 2) l'ultima delle suddette sessioni è iniziata alle 15:30, risultando ancora attiva alle 15:37, momento nel quale è stato registrato un *login* effettuato con le credenziali del cliente e OTP "mediante *app* su telefono Android", proveniente da un indirizzo IP operato da una società con sede in Irlanda, mai utilizzato dal cliente in altre sessioni; il sistema di tracciatura ha pertanto rilevato una "sessione multipla", ovvero l'avvio di una nuova sessione mentre era ancora attiva una aperta precedentemente; 3) la sovrapposizione della seconda sessione - ritenuta dall'intermediario truffaldina - a quella ricondotta al cliente avrebbe invalidato la prima; il messaggio di allarme previsto per tale ipotesi non sarebbe stato tuttavia visualizzato dal ricorrente in quanto egli non avrebbe tentato ulteriore attività nel corso di quella sessione; 4) nei tre minuti successivi sono state disposte le quattro operazioni contestate e per ciascuna è stato registrato l'inserimento della OTP corretta; 5) è seguito un ulteriore tentativo di inserimento di bonifico, non andato però a buon fine a causa dell'inserimento di una OTP errata.
L'intermediario assume che il correntista sarebbe rimasto vittima di *phishing*: nella "*relazione servizi informativi*" di cui sopra, si considera infatti verosimile un "*real time phishing*" stante l'indirizzo IP di provenienza delle operazioni fraudolente; più precisamente, alla luce di tale documento, parte resistente ipotizza che il cliente avesse attiva - contemporaneamente a quella di sola consultazione sul sito autentico dell'intermediario, rilevata dal relativo sistema di tracciatura - una ulteriore sessione su un

sito clone, nel corso della quale egli avrebbe fornito al truffatore le OTP necessarie per l'accesso e per l'autorizzazione delle quattro disposizioni di pagamento.
Il Collegio, rilevato che le operazioni contestate risalgono ad un periodo successivo all'entrata in vigore del D.lgs. 27.01.2010, n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13.11.2007) e del relativo Provvedimento attuativo della Banca d'Italia del 05.07.2011. del D.lgs. n. 11/2010 di recepimento della PSD (Direttiva 2007/64/CE), richiamato l'art. 12, commi 3 e 4 del suddetto decreto, secondo cui le perdite derivanti dall'uso fraudolento di uno strumento elettronico di pagamento, prima della comunicazione di allerta, sono sopportate dal cliente entro la franchigia di € 150,00, e quelle in esubero dall'intermediario, a meno che quest'ultimo provi il dolo o la colpa grave del cliente nell'osservanza delle cautele ad esso imposte dalla legge o dal contratto, ritiene che tale prova sia carente nel caso concreto, considerato che dalla ricostruzione dei fatti, come offerta da entrambe le parti e a prescindere dalle supposizioni di parte resistente, non pare ravvisarsi alcuna grave negligenza nel comportamento del cliente. Se infatti, in presenza di sistemi di autenticazione delle operazioni c.d. a due fattori, questo Arbitro ha generalmente valorizzato le evidenze informatiche fornite dagli intermediari resistenti in ordine al corretto inserimento dei codici richiesti per il perfezionamento delle operazioni dispositive (rigettando pertanto le richieste di rimborso avanzate dai clienti), tale soluzione non appare applicabile nella specie, trattandosi di un particolare caso di apertura contemporanea di una sessione di *home banking* pacificamente attribuita al titolare e di un'altra ritenuta fraudolenta. La possibilità tecnica di generare un nuovo codice di autenticazione sulla base della conoscenza di un altro codice della stessa specie generato in precedenza, è, del resto, un'ipotesi presa in considerazione dal "*Draft regulatory technical standards on strong customer authentication and common and secure communication under Directive 2015/2366 (PSD2)*", reso noto dall'Autorità Bancaria Europea (EBA) in data 23.02.2017, bozza contenente le norme tecniche di regolamentazione (*Regulatory Technical Standards o RTS*) in tema di autenticazione forte del cliente e comunicazione sicura ai sensi della PSD2 (cfr. Chapter 2. *Security measures for the application of strong customer authentication*; Article 4. *Authentication code*).
Se non sembra potersi ravvisare alcun comportamento gravemente colposo da parte del ricorrente, occorre invece rilevare che l'intermediario non ha dato corretta esecuzione al contratto stipulato con il cliente nel 2001: in esso si prevede infatti un limite giornaliero di € 5.000,00 per disposizioni di bonifico ordinario, limite che appare superato dalle due contestate operazioni di bonifico di € 6.000,00. Si conclude pertanto che il ricorrente abbia diritto al rimborso, con applicazione della franchigia (€ 11.000,00 - € 150,00 = € 10.850,00).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario restituisca alla parte ricorrente la somma di € 10.850,00.
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