Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) STELLA	Membro designato dalla Banca d'Italia
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) MANENTE	Membro di designazione rappresentativa degli intermediari
(MI) DE VITIS	Membro di designazione rappresentativa dei clienti

Relatore STELLA GIOVANNI

Seduta del 22/01/2019

FATTO

Il ricorrente chiede nei confronti dell'intermediario la restituzione degli importi relativi a due operazioni disconosciute, effettuate da terzi non autorizzati.
In particolare, con il ricorso il ricorrente riferisce:
- di essere stato vittima di una truffa, in data 17.08.2017;
- di aver ricevuto, circa una settimana dopo aver effettuato un bonifico verso l'estero (Romania), un messaggio nel quale si comunicava il blocco del suo conto e la procedura per sbloccarlo: in particolare, il messaggio richiedeva l'accesso a un sito internet;
- di avere inserito i propri dati di accesso nel sito indicato nel messaggio ricevuto, e di avere, successivamente, inviato i codici necessari a completare le operazioni di pagamento nella convinzione che questi fossero dei codici necessari a confermare lo sblocco del conto;
- di avere contattato il servizio clienti, al fine di bloccare la sua carta, dopo essersi reso conto della truffa subita.
Ciò esposto il ricorrente chiede la condanna dell'intermediario alla restituzione delle somme riferibili alle operazioni contestate (che risultano ammontare a € 416,50 ed essere avvenute nei Paesi Bassi).
Con le controdeduzioni l'intermediario eccepisce che:
- le verifiche effettuate hanno accertato che il processo di autenticazione, con riferimento alle operazioni contestate, è avvenuto correttamente;
- le operazioni disconosciute sono state eseguite tramite sistema dinamico di autenticazione, mediante l'utilizzo di codici OTP;

- le operazioni contestate sono state, dunque, rese possibili dal comportamento tenuto dal ricorrente, avendo quest'ultimo dato credito ad una comunicazione costituente un evidente caso di phishing;
- pur non essendo fornita evidenza del messaggio ricevuto, il fatto che il ricorrente abbia indicato le 15.40, del 17/08/2017, come orario di ricezione della comunicazione escluderebbe che una delle due operazioni contestate (di € 297,50, eseguita secondo la documentazione allegata alle ore 06.44 del giorno 17/08/2017) sia riferibile, in ogni caso, alla vicenda.

Con le controdeduzioni l'intermediario chiede di rigettare nel merito il ricorso, applicandosi in caso contrario la decurtazione della prevista franchigia.

DIRITTO

Le operazioni contestate sono state effettuate il 17/08/2017, sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD) e del provvedimento di attuazione della Banca d'Italia del 5 luglio 2011.

Si tratta più specificamente di n. 2 operazioni contestate, di importo complessivo pari a € 416,50. In base alla documentazione prodotta dall'intermediario, risulta che la 1ª operazione, per € 297,50, è stata effettuata in data 17/08/2017, alle h. 6:44. La 2ª operazione, per € 119,00 è stata compiuta in pari data alle 15:46.

Si rileva che la 1ª operazione - avvenuta come detto, da evidenze documentali, alle h. 6.44 - non parrebbe riconducibile a una vicenda di phishing, posto che il ricorrente ha affermato di avere effettuato l'accesso al sito indicato nel messaggio esca alle h. 15.40 locali. Va, peraltro, precisato che in parte della documentazione agli atti le due operazioni risultano compiute, rispettivamente, alle ore 13.44 e 13.46 indicate come "ore GMT". Tenendo presente che il divario fra i due orari (GTM / locale Paesi Bassi) dovrebbe essere di 2 ore - considerando il fuso orario [GMT+1], maggiorato di un'ulteriore ora per l'ora legale [17/08/2017] - le due operazioni sarebbero immediatamente successive (fra le 15.44 e le 15.46, ovvero fra le 13.44 e le 13.46 GMT) alla ricezione del messaggio esca (15.40 / 13.40 GMT) e all'invio dei codici OTP.

In sede di denuncia (sporta il 26/08/2017, alle h. 11:26) il ricorrente ha dichiarato quanto esposto nel ricorso.

L'intermediario ha prodotto documentazione attestante la legittima esecuzione e la sostanziale regolarità delle operazioni eseguite, posto che i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità (la regolarità dell'operazione si evince anche dai termini *"Approved"* e *"Pan digitato manualmente"*); dalla stessa documentazione risulta che dette transazioni sono state eseguite con un sistema dinamico di autenticazione, basato su codici OTP che il ricorrente afferma di avere - pur inconsapevolmente - fornito.

A sostegno di ciò l'intermediario produce apposita evidenza documentale attestante l'invio con sms della password dinamica sul numero di cellulare indicato dal cliente.

Il numero di cellulare riportato nella documentazione coincide con quello dichiarato dal ricorrente sia in sede di denuncia presso i carabinieri, sia in sede di ricorso.

Sulla base di quanto esposto, risulta che nel caso di specie il sistema di autenticazione predisposto dall'intermediario per l'effettuazione delle operazioni di pagamento on-line è a più fattori, tra cui una password dinamica (OTP) inviata al numero di cellulare del cliente.

Non si può, quindi, che applicare il principio consolidato nell'orientamento di questo Collegio secondo cui l'adozione di un sistema "a più fattori", con inserimento di OTP, induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, da un lato, che la banca abbia assolto all'onere di provare l'adempimento degli obblighi su di essa

gravanti ai sensi dell'art. 8 del D.lgs. n. 11/2010 e, dall'altro lato, che il cliente si sia reso inadempiente all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio online e l'invio di ordini di bonifico a valere sul conto a lui intestato (cfr. Coll. Milano nn. 7450/2015; 6396/2015; 1458/2015; 4818/2013).
Quanto sopra trova conferma nel fatto che le operazioni abusive contestate sono state rese possibili dal comportamento del ricorrente, che ha dato credito, come da egli stesso affermato, ad una comunicazione costituente un evidente caso di *phishing*, nonostante la notorietà di tale pratica e la sua pericolosità. Pertanto, tale circostanza rende palese che, da parte del correntista, vi sia stata la colpevole violazione degli obblighi di custodia dei dati identificativi e dispositivi del proprio conto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA