Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BLANDINI	Membro designato dalla Banca d'Italia
(NA) GATT	Membro designato dalla Banca d'Italia
(NA) ROSAPEPE	Membro di designazione rappresentativa degli intermediari
(NA) PALMIERI	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ANTONIO BLANDINI

Seduta del 12/02/2019

FATTO

Il ricorrente afferma che, a seguito di un controllo dei movimenti della propria carta, veniva a conoscenza della presenza di un'operazione di pagamento on line mai autorizzata, compiuta tramite il servizio di home banking da ignoti in data 19.8.2018, per un importo di € 390,00.
Riferisce in denuncia che riceveva sulla sua utenza mobile un sms contenente un link che lo invitava, al fine di rimuovere un blocco dello strumento di pagamento, ad inserire i dati della propria carta che provvedeva ad ed una volta effettuato quanto richiesto, riceveva un sms contenente un OTP, che inseriva nella schermata: insospettito effettuava un controllo della carta e si avvedeva che era stata disposta la citata operazione.
Con nota di contestazione importi il ricorrente disconosceva formalmente l'operazione fraudolenta, richiedendone l'integrale rimborso; detta richiesta era rigettata dall'intermediario che, nel riscontrare il reclamo, affermava di non poter procedere al rimborso in quanto la transazione risultava legittima.
Il ricorrente richiede la restituzione dell'intero importo relativo all'operazione contestata, pari ad € 390,00 oltre spese legali e competenze della procedura.
Costituitosi ritualmente l'intermediario eccepisce innanzitutto la regolarità dell'operazione contestata, osservando che la tracciatura informatica consente di affermare che la stesse risulta processata tramite il sistema dinamico OTP, inviato sul numero di cellulare indicato dal ricorrente, riscontrabile anche nella denuncia presentata da quest'ultimo.
Alla luce delle precedenti considerazioni, esclude ogni responsabilità nella produzione

dell'evento dannoso affermando di aver messo a disposizione del cliente uno strumento di pagamento rispondente agli attuali standard tecnologici.
Conclude ribadendo che l'operazione contestata è in realtà scaturita da un fenomeno di phishing, in quanto sulla base della descrizione fornita dal ricorrente in denuncia è indubitabile che l'operazione contestata in sia stata resa possibile proprio dalla condotta tenuta dall'utilizzatore.
L'intermediario chiede il rigetto del ricorso tenuto conto della legittima esecuzione dell'operazione e, in subordine, in caso di accoglimento, l'applicazione della franchigia di legge.

DIRITTO

Parte ricorrente ha prodotto una lista movimenti con evidenza dell'operazione contestata, consistente in un'operazione di pagamento on line, effettuata in data 19.8.2018, dell'importo di € 390,00 di cui chiede il rimborso.
In ordine alle modalità di esecuzione dell'operazione il ricorrente pare esser stato vittima di phishing: lo stesso riferisce in denuncia di aver ricevuto sulla sua utenza mobile un sms contenente un link che lo invitava, al fine di rimuovere un blocco dello strumento di pagamento, ad inserire i dati della propria carta, che provvedeva ad effettuare. Una volta effettuato quanto richiesto, riceveva un sms contenente un OTP, che inseriva nella schermata; insospettito effettuava un controllo dei movimenti della carta e si avvedeva che era stata disposta la citata operazione mai autorizzata.
Nel caso di specie l'intermediario produce la tracciatura informatica della modalità di esecuzione della transazione, eseguita senza alcuna anomalia, risultando la disposizione di pagamento regolare, come confermato dalla spunta verde accanto alla stessa. Evidenzia inoltre come l'operazione di pagamento sia stata processata mediante il sistema dinamico OTP mediante l'adesione della ricorrente al protocollo informatico che genera gli OTP tramite sms da inviare su telefono cellulare.
L'intermediario produce prova sia dell'autenticazione che dell'invio dell'sms contenente l'OTP che ha determinato la transazione fraudolenta.
La giurisprudenza di questo Arbitro univocamente stabilisce come in casi siffatti la domanda non possa essere accolta. Per tutte, in un caso del tutto analogo, cfr. Collegio di Napoli - pronuncia n. 7634 del 28.6.2017, nel senso che "in conformità al consolidato orientamento di questo Arbitro sul tema, il comportamento del cliente risulta connotato da colpa grave, anche in relazione a quanto prescritto dal punto 2.1 sez. IV delle disposizioni della Banca d'Italia del 5 luglio 2011 "Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento", secondo cui l'utilizzo di dispositivi personalizzati di sicurezza (es. PIN e password) obbliga l'utilizzatore a mettere in atto gli accorgimenti idonei al fine di preservarne la riservatezza, onde evitare gli utilizzi non autorizzati degli strumenti di pagamento in questione. Il cliente ha infatti fornito le proprie credenziali aderendo ad una sollecitazione che solo apparentemente proveniva dall'intermediario, senza rendersi conto che gli intermediari non inviano tali sollecitazioni… sicché si deve concludere che ricorra quella straordinaria ed inescusabile imprudenza e negligenza in presenza della quale le conseguenze del phishing non possono che ricadere sul cliente utilizzatore, dovendone al contrario rimanere estraneo l'intermediario (cfr. in senso conforme Collegio Napoli, decisione n. 997/2017 e n. 2188/2017)". Ed ancora, cfr. Collegio di Napoli - pronuncia n. 9343 del 20.10.2016, nel senso che "non può disconoscersi come il ricorrente abbia ammesso di avere "abboccato" ad un phishing, fornendo i propri dati in seguito alla richiesta delle credenziali, contenuto in un messaggio

solo in apparenza proveniente dall'intermediario. Pertanto, si può qui ragionevolmente ravvisare una responsabilità del cliente – come tale rilevante ai sensi dell'art. 1227 c.c. – in relazione alla mancata diligente custodia dei codici d'accesso al servizio di home banking, dal momento che è opinione unanimemente condivisa, sulla base della disciplina vigente, che sul cliente gravi l'onere di custodire con la massima diligenza i vari codici in suo possesso, necessari per compiere operazioni bancarie di vario genere, siano esse prelievi per mezzo del servizio Bancomat come disposizioni di operazioni per mezzo di servizi on line".

Ne vi sono in atti evidenze differenti, rappresentate soltanto dal ricorrente, circa la possibile provenienza dell'atto fraudolento da soggetti in qualche modo riferibili all'intermediario.

Il ricorso, alla luce di quanto esposto, e della giurisprudenza di questo Arbitro, che si condivide, non può essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE LEONARDO CARRIERO