Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL COLLEGIO DI ROMA

composto dai Signori:

Avv. Bruno De Carolis	Presidente
Avv. Alessandro Leproux	Membro designato dalla Banca d'Italia
Avv. Massimiliano Silvetti	Membro designato dalla Banca d'Italia
Avv. Michele Maccarone	Membro designato dal Conciliatore Bancario e Finanziario
Prof. Avv. Maddalena Rabitti	Membro designato dal C.N.C.U. [Estensore]

nella seduta del 24/10/2012 dopo aver esaminato
- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria tecnica,

FATTO

Il ricorrente dichiara di essere stato vittima in data 18 agosto 2011 di una frode informatica perpetrata mediante *phishing* che gli ha provocato un danno per un ammontare complessivo di £ 4.460,00. Espone nel ricorso che la truffa è stata realizzata attraverso cinque pagamenti sul sito www.matchpoint.it, avvenuti a pochi secondi di distanza l'uno dall'altro. Precisa di essersi reso conto delle operazioni, avendo attivato il sistema di *sms alert*, e di avere perciò immediatamente bloccato la carta di credito; effettuato la denuncia e disconosciuto le operazioni. Afferma inoltre che il sito su cui è transitato riproduceva esattamente la grafica dell'intermediario.

Ritiene peraltro che la responsabilità dell'accaduto sia da ascriversi a problemi di sicurezza del sistema, imputabili alla banca. Ad avviso del ricorrente se la banca avesse attivato, non solo in teoria ma anche in pratica, il dispositivo di

sicurezza di secondo livello, i terzi non sarebbero riusciti a carpirgli i dati riservati non avendo egli rivelato a nessuno *secure code,* che da tempo aveva provveduto ad attivare, e che non è stato, a suo avviso, operativo non essendogli stato richiesto nella procedura *on line*.

Precisa infine di non avere avuto adeguata informazione dall'intermediario sul rischio di truffe *on line*, nonostante esse fossero frequenti in quel periodo e di avere avuto una lettera in cui si avvertivano i clienti di questo rischio solo successivamente all'epoca dei fatti oggetto del ricorso. Avendo inutilmente esperito il reclamo, si rivolge all'ABF chiedendo di condannare l'intermediario al rimborso della somma di £ 4.446,00.

L'intermediario chiede il rigetto del ricorso, affermando che sussiste colpa grave del ricorrente per avere egli custodito negligentemente le credenziali di accesso. In particolare, ritiene che le operazioni contestate sono state effettuate digitando le credenziali riservate nonché i codici di sicurezza compreso il *secure code* e che, pertanto, l'illecito non sarebbe stato possibile senza la corresponsabilità del detentore dei dati.

DIRITTO

La questione si colloca nel tema, più volte trattato dall'ABF, dell'attribuzione di responsabilità all'intermediario bancario in caso di frodi perpetrati da terzi ai danni della clientela, nell'ambito della prestazione di servizi di pagamento regolati dal d. lgs. 11/2010.

Il ricorrente ha premesso nel ricorso di essere incorso in *phishing* e di avere dunque rivelato egli stesso alcuni dei dati identificativi necessari per realizzare la truffa *on* line: viene perciò in rilievo, in primo luogo, il profilo della diligente custodia delle credenziali di accesso da parte del ricorrente, imposto dall'art.7 del d. lg. 11/10.

L'interpretazione degli articoli 10 e 12 del d. lgs. 11/10 – secondo i quali spetta all'intermediario dare la prova della colpa grave del cliente, non potendosi ritenere sufficiente a integrare la colpa grave il corretto utilizzo dei codici – in linea con le intenzioni del legislatore, induce a distinguere le ipotesi in cui la circonvenzione del cliente avviene attraverso metodi ormai generalmente conosciuti, quali *e mail* civetta, da metodi più nuovi (o più subdoli) che riescono ancora a "sorprendere" i

clienti. Questo Collegio, più volte chiamato a confrontarsi con il tema, ha affermato che cadere vittima di *phishing* non è di per sé una colpa, ma può esserlo alla luce del circostanze del caso concreto e, più di recente, ha spesso affermato che integra la colpa grave del titolare della carta non impiegare quel grado minimo di diligenza che gli consentirebbe di schivare le fattispecie più diffuse e conosciute di *phishing*. La pronuncia del Collegio di Coordinamento n. 3498/12, in particolare, nell'avvalorare quest'interpretazione attribuisce rilievo anche all'accresciuta campagna di informazione che i media e gli stessi intermediari hanno da tempo attuato sui pericoli della frode informatica.

Nel caso concreto, tuttavia, il Collegio ritiene che l'intermediario non dimostra la colpa grave del ricorrente, considerate le circostanze in cui si è verificata la truffa.

Lo stesso intermediario, infatti, con lettera di riscontro del 28/12/2011, riconosce che le frodi telematiche diffuse in quel periodo si caratterizzavano per un invito, inoltrato via *e mail*, ad accedere a un *link*, cliccando sul quale si sarebbe aperta "*una finestra contenente un falso sito, identico nella grafica a quello ufficiale*". E' dunque lo stesso resistente a fare riferimento ad un sito clone, non facilmente distinguibile dall'originale.

L'Abf ha, in un precedente, escluso la colpa grave del cliente in un'ipotesi in cui il ricorrente: «ha dichiarato di aver ricevuto una *e mail* che lo invitava alla digitazione dei suoi codici identificativi e che perciò è stato presumibilmente vittima di una frode informatica, ma il contesto in cui la stessa si è svolta depone nel senso dell'affidabilità del messaggio e comunque non consente di connotare il comportamento della ricorrente, ancorché non immune da colpa, di quella "*straordinaria e inescusabile imprudenza e negligenza*" consistente nell'omissione di "*anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti*", che secondo l'orientamento della giurisprudenza (cfr. Cass. civ, Sez. III, 13 ottobre 2009, n. 21679), fatto proprio da questo Collegio, qualifica la colpa grave» (Coll. Roma, dec. 8 maggio 2012 n. 1428).

A ciò si aggiunge che l'intermediario, pur consapevole del rischio di truffe del tipo di quella di cui è vittima il ricorrente, si è limitato a darne notizia nel sito con modalità tali da non essere facilmente visibile ai clienti e ad inviare poi, con ritardo

rispetto agli episodi contestati, una comunicazione ai clienti avvertendoli dell'esistenza di questo tipo di truffe.

In conclusione, va esclusa la colpa grave del ricorrente non essendo l'intermediario riuscito a dimostrare quella macroscopica negligenza di cui neppure sarebbe capace un uomo "ordinariamente trascurato" (Collegio Roma, dec. 3264 del 15 ottobre 2012). Quest'ultimo concetto infatti implica una valutazione della condotta «in termini di totale trascuratezza verso i minimi accorgimenti che vengono utilizzati dai consociati al fine di evitare un accadimento dannoso» (Coll. Milano, decisione n. 256, 25 gennaio 2012), che non si presta a descrivere la condotta del ricorrente che è invece persona attenta ai profili di sicurezza, come dimostra il fatto che ha attivato tutti gli strumenti predisposti in tal senso dall'intermediario.

Il Collegio accoglie il ricorso disponendo a carico del resistente il rimborso della somma di £ 4.446,00 al netto della franchigia di £ 150,00.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso nei sensi di cui in motivazione. Dispone inoltre che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e al ricorrente di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS