Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL COLLEGIO DI ROMA

composto dai Signori:

Avv. Bruno De Carolis	Presidente
Prof. Avv. Andrea Gemma	Membro designato dalla Banca d'Italia [Estensore]
Prof. Avv. Pietro Sirena	Membro designato dalla Banca d'Italia
Prof. Massimo Caratelli	Membro designato dal Conciliatore Bancario e Finanziario
Prof. Avv. Marco Marinaro	Membro designato dal C.N.C.U.

nella seduta del 22/02/2013 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 chiede il rimborso della somma di €. 1.600,00, prelevata fraudolentemente dal proprio conto corrente tramite disposizione di bonifico non autorizzata. Riferisce di essere stato vittima di un fenomeno di c.d. *phishing*, attuato mediante una mail apparentemente proveniente dall'intermediario in cui si chiedeva di collegarsi ad un link e procedere alla verifica dei dati e dell'identità. Espletata tale procedura constatava l'avvenuta sottrazione dal suo conto corrente della somma pari ad €. 1.600,00 utilizzata per accreditare una carta prepagata. Fa presente di aver proceduto all'immediato disconoscimento dell'operazione e alla denuncia alle competenti autorità. Lamenta che l'intermediario abbia rigettato la propria richiesta di rimborso, stante l'indisponibilità delle somme sottratte sulla carta fraudolentemente accreditata, se non per la minor somma di €. 78.80.

Nelle proprie controdeduzioni l'intermediario contesta: **(i)** di aver approntato i più aggiornati sistemi di sicurezza per evitare le frodi informatiche; **(ii)** di aver reso adeguata e tempestiva informativa al cliente del rischio di frodi informatiche e delle

modalità di realizzazione di tali frodi, nonché degli accorgimenti cui è tenuto al cliente al fine di scongiurare detti fenomeni; **(iii)** che l'operazione fraudolenta sarebbe stata eseguita tramite c.d. *phishing* delle credenziali di accesso, la cui operatività è stata possibile a causa della negligenza del cliente nell'uso del sistema e nell'inserimento delle credenziali segrete. Eccepisce, dunque, la colpa grave del cliente, nonché la violazione delle disposizioni contrattuali in tema di custodia delle credenziali di accesso e chiede il rigetto del ricorso.

Diritto

Risulta incontestato tra le parti che l'operazione disconosciuta dal ricorrente sia scaturita da un fenomeno di c.d. *phishing* realizzato da ignoti malfattori ai danni del cliente. In particolare, il ricorrente ha pacificamente ammesso di aver dato seguito ad un messaggio e-mail che lo invitava a collegarsi ad un link per la verifica delle credenziali di accesso e della propria identità. Da tale circostanza la banca ritiene di poter inferire che l'accesso non autorizzato al conto e l'esecuzione della disposizione di bonifico sarebbe imputabile ad un comportamento negligente del ricorrente, il quale non avrebbe osservato le misure minime volte a garantire la sicurezza del servizio.

La fattispecie risulta regolata dall'art. 10, comma 1, d. lgs. n. 11/2010 (entrato in vigore il 1° marzo 2010 e quindi applicabile al caso di specie), che stabilisce: "*qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già 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*" e che "*quando l'utilizzatore neghi di aver autorizzato un'operazione di pagamento eseguita, 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 ad uno o più degli obblighi di cui all'articolo 7*".

Nel caso di specie, l'intrusione non autorizzata nel sistema, lungi dall'essere causata da un insufficiente grado di protezione informatica e del servizio offerto dall'intermediario, come lamentato dal correntista, è ascrivibile a colpa grave del cliente *incappato* in un c.d. *phishing* che attua le frodi informatiche mediante sottrazione delle credenziali di accesso.

La disamina dei documenti e la palese inaffidabilità della e-mail ricevuta che, marchianamente, esibisce contenuti falsi e d'immediata riconoscibilità anche per un utente non esperto e la dinamica degli eventi restituiscono, infatti, un quadro di grave negligenza a carico del cliente, atteso che la frode è stata attuata con modalità ormai ben note ed a dir poco grossolane: l'e-mail di *phishing* di cui il ricorrente è stato vittima, infatti, proviene da un indirizzo assolutamente generico ed è redatta in un italiano approssimativo, con errori lessicali e grammaticali che avrebbero dovuto allertare un cliente minimamente diligente.

Sul punto, non può non rilevarsi che il fenomeno del c.d. *phishing* è ormai noto alla generalità dei consociati, sensibilizzati dagli intermediari ad assumere condotte connotate da quel grado minimo di prudenza che consente di scongiurare il rischio di frodi grossolane. Dal canto suo, l'intermediario ha dato prova di aver adeguatamente pubblicizzato le istruzioni di sicurezza disattese dal ricorrente.

Sicché deve concludersi che, nel caso di specie, il cliente è stato vittima di una sua colpevole credulità che esclude ogni obbligo di rimborso a carico dell'intermediario.

P.Q.M.

Il Collegio respinge il ricorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS