Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) MASSERA	Presidente
(RM) SCIUTO	Membro designato dalla Banca d'Italia
(RM) SIRGIOVANNI	Membro designato dalla Banca d'Italia
(RM) GULLO	Membro di designazione rappresentativa degli intermediari
(RM) CHERTI	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - CHERTI STEFANO

Seduta del 21/02/2019

FATTO

1) La ricorrente chiede la restituzione della somma di euro 4.600,00 corrispondente all'importo di un'operazione di bonifico disconosciuta eseguita fraudolentemente da terzi non autorizzati. In particolare, in data 18/2/2018 riceveva una mail apparentemente proveniente banca, in cui le veniva richiesto di confermare il proprio numero di telefono accedendo tramite un link entro 24 ore, al fine di evitare il blocco del conto corrente. Nel predetto sito internet le veniva richiesto di digitare i codici di accesso alla banca multicanale, cosa che la ricorrente faceva.
2) In seguito, alle ore 17.39 la ricorrente riceveva un sms dalla banca che la informava del blocco del servizio multicanale; immediatamente, verificava il conto corrente, e così si avvedeva che era stato addebitato l'importo di 4.600 euro tramite bonifico a favore di tale Irina Burcea. Non avendo autorizzato tale operazione, provava invano ad annullarla via banca multicanale; tuttavia, trattandosi di bonifico istantaneo, esso era già stato addebitato, nonostante fosse stato effettuato in giorno festivo (domenica).
3) L'intermediario, costituendosi, evidenzia come la mail ricevuta dalla ricorrente non è sicuramente stata inviata dalla banca, ma è invece una mail di *phishing*, rispondendo alla quale la ricorrente ha di fatto messo a disposizione di ignoti le credenziali di accesso alla Banca Online; la ricorrente avrebbe dovuto saperlo, in quanto "*da anni nella pagina di accesso alla Banca Via Internet si comunichi che non si richiede l'aggiornamento dei dati tramite invio di mail, né viene mai richiesto via mail l'inserimento delle credenziali per l'accesso al sistema*".

4) Inoltre, dopo il messaggio sms con cui la banca avvisava i ricorrenti del blocco della Banca Multicanale a seguito di operazione anomala, la ricorrente eseguiva l'accesso online e si avvedeva del bonifico. Il giorno stesso la banca ha inserito a sistema una richiesta di blocco/richiamo del bonifico; tale richiesta non è però andata a buon fine, in quanto il trasferimento di fondi all'altra banca si era perfezionato immediatamente la stessa domenica mattina, trattandosi di bonifico istantaneo.

DIRITTO

Il Collegio si è in più occasioni occupato di fattispecie in cui il cliente è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario, successivamente alla ricezione di un messaggio ingannevole che indirizza ad una data pagina web. In particolare, il *phishing* operato tramite semplice email o sms (chiamato, in quest'ultimo caso, *smishing*) viene ritenuto fenomeno ormai diffusamente noto, che quanto meno qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso dell'*home banking*, dovrebbero conoscere.
Dalla documentazione versata in atti, il Collegio rileva come nel caso di specie l'intrusione non autorizzata nel sistema - lungi dall'essere causata da un insufficiente grado di protezione informatica del servizio offerto dall'intermediario - appare ascrivibile a colpa grave della cliente, incappata, per l'appunto, nel *phishing* con conseguente utilizzo abusivo delle sue credenziali di accesso.
Ed, infatti, la stessa ricorrente sostanzialmente ammette di aver dato seguito alle istruzioni contenute nel messaggio ricevuto sulla propria posta elettronica, che erroneamente credeva provenire dall'intermediario resistente. Come rilevato dal Collegio di Coordinamento (decisione n. 1820/13), nell'ipotesi del "phishing", "*il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di internet*".
Avendo riguardo alle circostanze del caso concreto, la credulità della ricorrente appare non scusabile, in quanto le modalità con cui la truffa è stata perpetrata rientrano tra quelle più diffuse (c.d. *phishing*), che qualunque cliente dotato di normale avvedutezza e prudenza deve essere in grado di individuare, non facendosi trarre in inganno. Tutto ciò premesso, allo stato delle risultanze agli atti, deve ritenersi che la ricorrente sia incorsa nella violazione degli obblighi prescritti dall'art. 7 del D. Lgs. n. 11/2010, avendo in particolare omesso di comunicare tempestivamente alla banca il fattore di pericolo derivante dall'intervenuto "*phishing*".
Ne consegue che nel comportamento della ricorrente è ravvisabile la colpa grave che non consente di accogliere la richiesta di rimborso della somma indebitamente sottratta (cfr. Collegio Roma, 20.04.2015, n. 3076).

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MAURIZIO MASSERA