COLLEGIO DI ROMA

composto dai signori:

(RM) DE CAROLIS	Presidente
(RM) MELI	Membro designato dalla Banca d'Italia
(RM) SILVETTI	Membro designato dalla Banca d'Italia
(RM) MACCARONE	Membro designato da Associazione rappresentativa degli intermediari
(RM) MARINARO	Membro designato da Associazione rappresentativa dei clienti

Relatore MELI VINCENZO

Nella seduta del 07/04/2014 dopo aver esaminato:

- il ricorso e la documentazione allegata
- le controdeduzioni dell'intermediario e la relativa documentazione
- la relazione della Segreteria tecnica

FATTO

Con ricorso pervenuto il 21/11/2013, il ricorrente espone di essere titolare di un conto corrente, cointestato, presso l'intermediario resistente, con operatività anche attraverso *home banking*. Afferma di essere stato vittima di un'operazione di *phishing*, consistente nell'invio di una mail, recante i loghi della banca, attraverso la quale, con un pretesto, è stato indotto a comunicare le credenziali d'accesso al proprio conto *on-line*, accedendo ad un *link*, e ad inserire successivamente un codice inviatogli mediante sms. La mattina dopo ha scoperto che nello stesso giorno gli erano stati prelevati dal conto € 2.989,00, che chiede gli vengano rimborsate dall'intermediario.

Con controdeduzioni del 30/01/2014, l'intermediario chiede il rigetto del ricorso. Contesta la configurabilità di una propria responsabilità e sostiene l'attribuibilità di quanto lamentato alla mancanza di cautela del cliente (il quale ammette di essere stato poco accorto).

Questi ha risposto ad una evidente mail fraudolenta, fornendo in risposta i propri codici di sicurezza e ciò nonostante l'ampio risalto dato anche dalla stampa al fenomeno del *phishing* ed in particolare le raccomandazioni sulla sicurezza fornite alla clientela, come per esempio quella di prestare attenzione alle mail sospette e quella di diffidare da *link* che prevedano l'inserimento di password. Le operazioni contestate sono state disposte mediante l'utilizzo dei codici identificativi, resi noti dalla banca esclusivamente all'interessato, nonché di ulteriori codici identificativi, la creazione dei quali postula l'utilizzo dello strumento consegnato al ricorrente (*token*) al fine di consentirgli la produzione di *passwords* ad utilizzo singolo, sia in sede di accesso al servizio che a conferma di specifici ordini dispositivi.

DIRITTO

Il Collegio ritiene il ricorso infondato.

L'art. 12, co. 3, del d. lgs. n. 11 del 2010 (di attuazione della direttiva 2007/64/CE), stabilisce che, "salvo il caso in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, prima della comunicazione eseguita ai sensi dell'art. 7, co. 1, lettera b), l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a € 150,00 la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento". Il legislatore pone, dunque, di regola, a carico del prestatore del servizio di pagamento il rischio dell'utilizzo fraudolento, ad opera di terzi, degli strumenti di pagamento, ma prevede un'eccezione laddove l'utilizzo indebito dello strumento di pagamento sia stato consentito o agevolato da un comportamento gravemente negligente del titolare o da cattiva custodia, da parte sua, dello strumento di pagamento. Nel caso di specie, lo svolgimento dei fatti non è controverso: il ricorrente è stato vittima di una classica operazione di *phishing*. Operazione fraudolenta, il cui successo è però legato alla collaborazione, sia pure inconsapevole, del titolare dello strumento di pagamento. Orbene, secondo quanto rilevato dal Collegio di Coordinamento (dec. n. 3498/2012), la valutazione della sussistenza o meno di una colpa grave in capo all'utilizzatore che aderisce ad una operazione di *phishing* non può essere operata in astratto, dato che il *phishing* si può presentare sotto diverse vesti. In una forma più insidiosa, esso ha luogo tramite un "*subdolo meccanismo di aggressione (che) ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di*

un messaggio che a chiunque non potrebbe apparire che genuino". In forma più tradizionale, quale quella che appare ricorrere nel caso in esame, esso si concretizza nell'invio di una semplice *mail*, non collegata all'utilizzo del sito della banca, anche se recante loghi o scritte che sembrano ricondurre alla medesima, con la quale si invita il cliente ad accedere ad un link e a fornire le proprie credenziali segrete. Nella richiamata decisione, cui questo Collegio ritiene di dover prestare adesione, si afferma che deve riconoscersi una notevole differenza fra le due fattispecie, per cui solo nella prima deve escludersi la ravvisabilità di una colpa grave del cliente; invece, nel secondo caso, quello del *phishing* c.d. tradizionale, la credulità dell'utente appare non scusabile. In effetti, il *phishing* operato tramite semplice mail deve ritenersi fenomeno ormai del tutto noto, tanto che qualunque utente dotato di quella normale avvedutezza e prudenza che si richiede a chi utilizzi servizi di *home banking* dovrebbe essere in grado di sottrarsi all'inganno.

Nel caso di specie, lo stesso ricorrente afferma di aver ricevuto una *mail*, con la quale gli si comunicava che, a seguito della riorganizzazione del sito della banca, il suo conto era stato bloccato, e gli si chiedeva di accedere ad un *link*, inserendo le credenziali di accesso al conto; cosa che il ricorrente puntualmente faceva, ma non fermandosi a questo. Riceveva, infatti, anche un sms sulla propria utenza mobile, con un codice da inserire utilizzando lo stesso *link*, e aderiva anche a questo invito, che apriva definitivamente ai truffatori l'accesso al suo conto bancario. Tutto ciò premesso, deve ritenersi che ricorra l'eccezione di cui al citato art. 12, co. 3 e 4, del d. lgs. n. 11 del 2010, non potendosi dunque accogliere la richiesta del ricorrente di rimborso delle somme pur indebitamente sottrattegli.

P.Q.M.

Il Collegio respinge il riscorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS