COLLEGIO DI MILANO

composto dai signori:

(MI) GAMBARO	Presidente
(MI) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(MI) ORLANDI	Membro designato dalla Banca d'Italia
(MI) RONDINONE	Membro designato da Associazione rappresentativa degli intermediari
(MI) PERICU	Membro designato da Associazione rappresentativa dei clienti

Relatore ORLANDI MAURO

Nella seduta del 09/09/2014 dopo aver esaminato:

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

FATTO

Il ricorrente disconosce 5 operazioni, disposte da ignoti tramite internet banking, addebitate sul proprio conto corrente. Egli ha dichiarato che, intorno alle ore 18.00 del 2 giugno 2013 aveva aperto una e-mail, pervenuta dalla banca, contenente all'interno un link, che rimandava ad una schermata, che richiedeva il codice utente, PIN ed ulteriore numero di sicurezza generato dal dispositivo O-K. Dopo aver compiuto tale digitazione tale sito si era bloccato e, pertanto, aveva chiuso il collegamento. Dopo circa un'ora era stato contattato dal servizio di sicurezza della convenuta che aveva chiesto conferma di alcune operazioni "anomale" associata alla carta; avendo disconosciuto tali operazioni, il centro assistenza aveva provveduto a bloccare lo strumento di pagamento.
Replica l'intermediario base della stessa ricostruzione dei fatti della parte attrice dinnanzi alla PG, "nonché per pacifico riconoscimento del ricorrente", la responsabilità dell'accaduto ricadrebbe sul ricorrente, che incautamente avrebbe risposto "ad una evidente e-mail fraudolenta" e, ciò, nonostante l'ampio risalto dato dalla stampa al fenomeno di *fishing* e le raccomandazioni fornite dal gruppo bancario alla sua clientela; dalle verifiche tecnico-informatiche effettuate era emerso che le operazioni contestate

erano state disposte con il corretto inserimento delle credenziali del ricorrente; il sistema di gestione per la sicurezza delle informazioni adottati dal gruppo bancario è certificato ISO/IEC 27001 e, quindi, di elevato standard internazionale per la sicurezza delle informazioni; così pure, il dispositivo token "*O-key*", consegnato al ricorrente, possiede le caratteristiche e le certificazioni internazionali.
Il ricorrente chiede la restituzione della somma sottratta; il resistente insiste per il rigetto.

DIRITTO

Il Collegio, nota in primo luogo che le operazioni contestate risalgono ad un periodo successivo all'entrata in vigore del D. Lgs. 27 gennaio 2010 n. 11 (1° marzo 2010) di recepimento della Direttiva c.d. PSD sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007). È pacifico che il ricorrente abbia inserito le credenziali associate alla carta al fine dell'attivazione di una procedura di sicurezza, in risposta ad una anomala mail, che ne sollecitava la digitazione. Si tratta di un fenomeno c.d. di *phishing*, ossia di fraudolenta acquisizione di dati rilevanti per il mezzo di comunicazioni apparentemente istituzionali, che sollecitano l'inserimento delle credenziali da utilizzare poi per l'indebito uso della carta cui sono associate.
Nel caso di specie, risulta chiaro che le operazioni abusive contestate siano state rese possibili dallo stesso comportamento del ricorrente, che ha dato credito, come dallo stesso affermato, ad una comunicazione anomala e inusuale; con ciò integrando una violazione gravemente colpevole degli obblighi di custodia dei dati identificativi e dispositivi del proprio conto a lui imputabile. Reputando provata la colpa grave del ricorrente, il Collegio non può che dar seguito al proprio consolidato orientamento (v. da ultimo dec. 4317/13), dichiarando imputabile al cliente la comunicazione dei codici segreti di accesso.

P. Q. M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO