IL COLLEGIO DI MILANO

composto dai signori:

- Prof. Avv. Antonio Gambaro	Presidente (Estensore)
- Avv. Maria Elisabetta Contino	Membro designato dalla Banca d'Italia (Estensore)
- Avv. Valerio Sangiovanni	Membro designato dalla Banca d'Italia
- Dott. Mario Blandini	Membro designato dal Conciliatore Bancario Finanziario
- Avv. Guido Sagliaschi	Membro designato dal C.N.C.U.

nella seduta del 30 marzo 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

Con lettera trasmessa via fax il 18 luglio 2011, l'odierno istante presentava formale reclamo all'intermediaria, con la quale intratteneva un rapporto di conto corrente, per chiedere il rimborso della somma € 4.387,00, oggetto di un bonifico fraudolentemente disposto con addebito sul suo conto in data 13 giugno 2011.
Precisava, essendo stata evidentemente l'operazione effettuata *on line*, di non aver mai comunicato a terzi i dati personali relativi al suo *account* e metteva al contempo in evidenza che tutte le precedenti operazioni erano state disposte dal suo computer personale, dotato di antivirus, utilizzando il lettore fornitogli dall'intermediaria.
Accludeva copia della denuncia sporta il 3 luglio 2011 alla locale Stazione dei Carabinieri e della comunicazione di disconoscimento presentata il successivo 4 luglio 2011 all'intermediaria.
Non ricevendo alcuna risposta, con ricorso pervenuto alla Segreteria Tecnica il 7 settembre 2011, il cliente adiva l'Arbitro Bancario Finanziario per sentire condannare l'istituto alla restituzione dell'importo di € 4.387,00, corrispondente a quanto oggetto del bonifico non autorizzato disposto *on line* sul suo conto corrente in favore di soggetto estero a lui sconosciuto.
Precisava di essere in possesso di una carta di pagamento dotata di microchip, da utilizzare necessariamente anche per effettuare operazioni *on line*, dovendo a tal scopo essere introdotta in un lettore fornito dall'intermediaria, in grado di rilevare il certificato di

sicurezza contenuto nel microchip. Senza carta e senza lettore non era possibile dar corso ad alcuna operazione via internet.
Versava agli atti, unitamente al ricorso, la copia del reclamo del 18 luglio 2011, della denuncia dell'operazione abusiva sporta ai Carabinieri, della dichiarazione di disconoscimento formalizzata utilizzando i moduli dell'intermediaria, dell'estratto del suo conto corrente al 3 luglio 2011 e della contabile relativa all'operazione incriminata.
Nella denuncia ricevuta dall'Ufficiale di pubblica sicurezza il ricorrente chiariva di essersi avveduto dell'operazione in questione solo casualmente, controllando *on line* il proprio conto in data 2 luglio 2011, precisando poi, nell'attestazione di disconoscimento, di avere utilizzato la carta l'ultima volta il 10 giugno 2011 per disporre un bonifico.
Con le controdeduzioni pervenute il 24 novembre 2011, l'intermediaria segnalava innanzitutto che la carta con il microchip, utilizzata per dar corso all'operazione *on line* in questione, era stata consegnata al cliente (che l'aveva poi bloccata il 2 luglio 2011) il 14 gennaio 2010 unitamente al lettore. Metteva in evidenza che tale apparecchiatura, "*in unione con la carta [….] e un certificato digitale memorizzato all'interno del chip, permette al momento della disposizione di una transazione online uno scambio di codici univoci tra il sito e il cliente, al fine di verificarne l'identità*".
Venendo poi all'operazione contestata, rilevava come fosse stata disposta "*da soggetto autenticatosi come legittimo titolare, mediante il corretto inserimento di tutte le successive serie di riconoscimenti informatici indispensabili per l'esecuzione di tale operazione (bonifico estero)*". Chiariva che erano stati utilizzati, infatti, la userid del titolare, la password conosciuta solo da questo e dallo stesso modificabile in ogni momento, il primo codice univoco (cosiddetto "*ID Operazione*") generato dal sistema, da digitare sulla tastiera del lettore, il lettore stesso, inteso come strumento materiale, peraltro utilizzabile solo con l'introduzione della carta dotata di microchip, che risultava quindi regolarmente inserita, il PIN di quest'ultima (da digitare sulla tastiera del lettore), il secondo codice univoco (cosiddetto "*codice risposta*") generato dal lettore, da digitare in apposito campo della schermata che compariva sul video del computer nell'effettuazione di operazioni *on line*.
Sottolineava come il lettore non fosse in alcun modo raggiungibile via web e come il sistema adottato fosse il più sicuro tra quelli ad oggi sviluppati dalla tecnica. Faceva inoltre presente come dopo tre digitazioni errate anche di un solo codice tra password d'accesso, pin della carta o codice risposta, la facoltà di compiere operazioni *on line* si sarebbe bloccata automaticamente.
Sostenendo quindi di avere pienamente adempiuto ai propri obblighi contrattuali, la resistente eccepiva come il cliente non avesse fornito la prova di avere adeguatamente protetto il proprio apparato e la propria connessione web dalle intrusioni informatiche, né di avere adottato un sistema di protezione globale della navigazione internet efficiente e costantemente aggiornato.
Concludendo che l'operazione in questione non potesse quindi che essere stata frutto dell'incauta consegna da parte del cliente a terzi "*dei propri codici dispositivi*" con conseguente grave negligenza agli obblighi di custodia, l'intermediaria chiedeva il rigetto del ricorso.

DIRITTO

I fatti esposti in narrativa sono posteriori all'entrata in vigore del D.Lgs. 11/2010 che ha recepito nell'ordinamento italiano la Direttiva 2007/64/CE. Al caso in esame sono quindi applicabili le disposizioni di detto Decreto, e segnatamente, per quanto qui rileva, quelle

concernenti gli obblighi rispettivamente gravanti sul prestatore di un servizio di pagamento e sul relativo utilizzatore.
Dispone al riguardo il primo comma dell'art. 8 del Decreto che "*Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7*".
In forza della norma ivi richiamata, *"L'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso*" e, a tal fine, è tenuto, "*non appena riceve uno strumento di pagamento*", ad adottare "*le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo*".
Nel caso in esame deve ritenersi che la resistente abbia adempiuto con la dovuta diligenza ai propri obblighi. Questa ha, infatti, messo a disposizione del cliente un sistema per il compimento di operazioni *on line*, che è basato sull'utilizzo contemporaneo di più fattori, ossia quel tipo di sistema che anche questo Collegio non ha mancato di considerare il più sicuro e tale da assicurare la migliore tutela degli utilizzatori in base all'attuale stato della tecnica (cfr., tra le tante, la decisione n. 1694 del 2011, anche se non vi sono strumenti sufficienti a verificare la sussistenza dei requisiti dei sistemi cosiddetti "*a maggior sicurezza*", di cui al Provvedimento della Banca d'Italia del 30 luglio 2011, entrato in vigore il 1° ottobre successivo).
Dalle informazioni rese dal ricorrente e dalle precisazioni fornite dalla resistente, che non sono state contestate, è emerso, infatti, che per il compimento di un'operazione via internet il cliente è tenuto ad utilizzare uno strumento materiale in suo possesso, ossia il lettore, all'interno del quale va introdotta la carta di pagamento a microchip, pure in suo possesso. Egli deve inoltre digitare diversi codici, ora sul lettore, ora nell'apposito spazio sulla schermata che compare sul computer accedendo al servizio per il compimento di operazioni *on line*. Due di detti codici sono generati (si ha ragione di ritenere, casualmente e con modalità "usa e getta") uno dal sistema e uno dal lettore.
Dal tipo di sistema di protezione adottato discende la presunzione, certamente grave e rilevante, che il cliente non avesse viceversa compiutamente custodito i dispositivi personali necessari per l'utilizzo del sistema di pagamento, con negligenza che si presenta rilevante.
Come noto, il "*phishing*" può consistere non solo nell'inviare e-mail fraudolente alle quali incautamente il destinatario risponde, ma anche nella diffusione di codici malevoli, i cosiddetti "*trojan banking",* in grado di carpire in vario modo le credenziali di accesso ai servizi *on line*, alcuni dei quali anche attraverso registrazioni video.
Il ricorrente non ha peraltro neppure fornito la prova di essersi dotato di un efficace e funzionante sistema antivirus e antispam, per cui il Collegio, sulla base dei soli dati in suo possesso, non può ritenere che il comportamento dell'utilizzatore sia scevro da colpa e in particolare da colpa grave, anche se la natura fraudolenta dell'operazione non sembra in contestazione.
In tale situazione, il ricorrente non potrebbe beneficiare della possibile riduzione di responsabilità prevista dal Provvedimento della Banca d'Italia del 30 luglio 2011, che peraltro all'epoca dei fatti non era ancora in vigore (e ferma la necessità di verifiche sulla sicurezza del sistema).
Pacifica tra le parti risulta la circostanza che l'operazione in questione sia stata eseguita attraverso l'utilizzo delle credenziali del ricorrente, nonostante l'intermediaria non ne fornisca la prova. Nella denuncia ai Carabinieri, il cliente contesta, infatti, che vi sia stata

"*acquisizione codici carte di credito (skimming)*" e "*duplicazione codici carte di credito (imprinting)*".
Dovendosi quindi ritenere che l'intermediaria abbia adottato i dispositivi più sicuri in base allo stato della tecnica, che l'operazione sia sta effettuata mediante l'utilizzo di tutte le necessarie credenziali informatiche e che, a converso, il cliente non abbia applicato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, non risultando neppure che si fosse dotato di sistemi antivirus o antispam, omettendo così gli accorgimenti minimi richiesti per garantire la sicurezza di tali dispositivi, il Collegio ritiene, aderendo all'orientamento espresso in fattispecie analoga dal Collegio di Roma (decisione adottata nel ricorso 440770 del 2011), che la domanda del ricorrente non possa trovare accoglimento ex art. 12, 4° comma, del D.Lgs. n. 11/2010.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO