COLLEGIO DI MILANO

composto dai signori:

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

Relatore RONDINONE

Nella seduta del 14/01/2014, 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 protocollato in data 16.5.2013 il consumatore, titolare di un conto corrente presso la convenuta, esponeva di avere ricevuto il 20.1.2013 una mail avente ad oggetto "*attività sospette sul tuo conto*", con la quale gli veniva chiesto di collegarsi tramite la stessa mail al sito della banca in modo da consentire operazioni di verifica ed eliminare eventuali restrizioni imposte a seguito della menzionata attività sospetta.
Il ricorrente, interpretando in buona fede tale comunicazione, tramite il *link* indicato nella mail, si collegava al sito della banca e inseriva "*il codice titolare, il pin e il codice chiavetta o-key*", senza riuscire peraltro a "*entrare sul conto*". Indi, alle ore 14.10 circa, riceveva un sms dal seguente tenore: "*per confermare la variazione del numero di cellulare … effettuato sul sito internet della banca, inserire il codice xxx*"; inseriva tale codice nella *homepage* della banca e immediatamente riceveva un altro sms riportante: "*modificato il numero abilitato al servizio di invio codice sms per conferma operazioni sospette. Il nuovo nr. è* yyy".
Insospettito dall'intera procedura, il consumatore chiamava il numero di cellulare da cui erano provenuti gli sms: la persona che gli rispondeva, qualificatasi operatore

dell'intermediario, riferiva che "*il problema si sarebbe risolto il giorno 21/01/13 essendo tale giorno lavorativo*". Sennonché Il giorno successivo, alle ore 12.17, il correntista riceveva una telefonata sul proprio cellulare da un "vero" operatore della banca, che lo informava di essere stato vittima di una truffa, invitandolo a sporgere denuncia all'autorità giudiziaria.
Il ricorrente si avvedeva quindi che nella giornata del 20.1.2013 dal suo conto corrente erano state effettuate *on line* due ricariche su una stessa carta prepagata, che, seppure segnalate come irregolari dal sistema ed eseguite superando il limite giornaliero di ricarica di € 3000,00 indicato sui fogli informativi del prodotto, non erano state bloccate dall'intermediario. Disconosceva quindi tali operazioni e presentava reclamo alla banca il 24.1.2013. Tuttavia, l'intermediario non poneva in essere alcuna attività per il recupero dei fondi e riscontrava negativamente il reclamo in data 14.2.2013.
Il ricorrente, vista la negligenza della convenuta secondo i canoni di cui agli artt. 7 e 10 D. Lgs. n. 11/2010, e rilevato che comunque la frode è stata *"perpetrata con l'utilizzo di specifici software, che permettono di carpire i codici senza che il cliente ne perda il possesso",* ha chiesto all'ABF di ordinare alla banca di rimborsargli € 5.000,00.
L'intermediario presentava le proprie controdeduzioni tramite il Conciliatore Bancario Finanziario il 30.10.2013, rappresentando che il ricorrente era rimasto vittima di un "*phishing*" reso possibile da comportamenti che lo stesso ricorrente aveva decritto come erronei e ingenui, avuto riguardo alla "*grossolanità della mail ricevuta*". Tali comportamenti, integranti la colpa grave, avrebbero vanificato la sicurezza dell'architettura tecnologica posta a presidio dell'integrità delle operazioni, le quali "*risultano confermate con regolare utilizzo dell'apparecchiatura …"O-Key", con la quale … vengono generate le … "one time passwords*" *necessarie all'accesso al servizio, ed al conferimento dei singoli ordini dispositivi*".
La convenuta ha altresì osservato che le pattuizioni contrattuali che regolano il servizio di *home banking* non prevedono alcuna limitazione circa le disposizioni impartite con tale modalità. Nessun valore potrebbe in particolare essere attribuito al foglio informativo prodotto dal ricorrente, in quanto riferito a limiti di utilizzo della carta prepagata nel caso in cui il cliente "*sia effettivamente titolare di tale strumento di pagamento*".
La resistente ha quindi chiesto al Collegio di "*dichiarare inaccoglibile, in quanto immotivata ed infondata, la richiesta di rimborso di € 5.000,00".*
Le controdeduzioni sono state trasmesse via mail al ricorrente.

DIRITTO

Il Collegio, rilevato che le operazioni contestate sono successive al 1.3.2010, data di entrata in vigore del d. lgs. n. 11/2010 di recepimento della PSD (Direttiva 2007/64/CE) e che quindi per la decisione del ricorso in esame occorre fare riferimento a tale normativa – e in specie all'art. 12, commi 3 e 4, per cui le perdite derivanti dall'utilizzo fraudolento di strumenti elettronici di pagamento prima della comunicazione di allerta sono sopportate interamente dal cliente nel caso siano provati il dolo o la colpa grave dello stesso – ritiene che consti agli atti la prova di un comportamento gravemente colpevole del ricorrente che ha consentito a ignoti l'effettuazione delle operazioni fraudolente.
E' pacifico che tutti gli accessi compiuti sono stati posti in essere utilizzando le credenziali necessarie senza alcun errore, ossia che l'autore fosse a conoscenza di tutti i codici consegnati al cliente per la gestione della sua sicurezza. Lo stesso ricorrente ammette di avere fornito tali dati, compreso il codice prodotto dal dispositivo *token*, nel rispondere a una mail manifestamente sospetta – con la quale era stato invitato a collegarsi al presunto

sito della banca tramite *link* – il cui contenuto avrebbe dovuto allertare un utente minimamente diligente. Il consumatore ha inoltre comunicato ai malfattori anche quanto necessario per neutralizzare il tempestivo funzionamento del sistema di *sms-alert*.
Il ricorrente ha insomma risposto a comunicazioni poco credibili concretanti un tipico caso di *phishing*, nonostante la notorietà e la pericolosità di tale fenomeno, che dovrebbe indurre i consociati ad assumere condotte connotate da quel grado minimo di prudenza che consente di scongiurare il rischio di frodi grossolane. In effetti, il "*phishing*" operato tramite semplice mail deve ritenersi fenomeno normalmente inidoneo a trarre in inganno qualunque utente dotato di media avvedutezza e prudenza.
Non essendovi stata una *captatio* posta in essere con modalità particolarmente sofisticate, secondo il consolidato orientamento in materia dell'ABF (v., da ultimo, Coll. Milano, n. 1173/2013 e n. 3124/2013; Coll. Roma, n. 1699/2013 e n. 1820/2013), in definitiva si conferma che al cliente è imputabile una violazione gravemente colpevole degli obblighi di custodia dei dati identificativi e dispositivi del conto *on line*, sicché la perdita subita dal medesimo non può che rimanere interamente a suo carico.
Anche per quanto riguarda la contestazione del ricorrente che l'intermediario avrebbe accreditato sulla stessa carta prepagata l'importo complessivo di € 5.000,00, benché i fogli informativi riferiti a tale strumento pubblicizzassero il limite di € 3.000,00 quale ricarica massima effettuabile *online* con addebito in conto, essa non ha pregio, in quanto tale limite si riferisce al caso in cui fosse lo stesso titolare della carta prepagata a effettuare la ricarica. Mentre, sulla base di quanto versato in atti, non consta vi fossero limiti di operatività del servizio *home banking* a beneficio di soggetti terzi.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO