IL COLLEGIO DI ROMA

composto dai signori:

- Dott. Giuseppe Marziale	Presidente
- Avv. Bruno De Carolis	Membro designato dalla Banca d'Italia
- Prof.ssa Avv. Giuliana Scognamiglio	Membro designato dalla Banca d'Italia (relatrice)
- Prof. Avv. Saverio Ruperto	Membro designato dal Conciliatore Bancario Finanziario
- Dott.ssa Daniela Primicerio	Membro designato dal C.N.C.U.

nella seduta del 12 gennaio 2010 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 atto del 26 ottobre 2009, identificato dal numero di protocollo 0316965, ricevuto dall'intermediario in data 29 ottobre 2009, l'interessata ha proposto ricorso dinanzi a questo Arbitro Bancario Finanziario.
Il ricorso si articola in due motivi.
Con il primo motivo, la ricorrente, premesso di essere da anni intestataria di un conto corrente presso la suddetta Banca e di aver aderito ad uno specifico servizio per accedere all'operatività su detto conto tramite internet, espone di aver subito nel mese di febbraio del 2009 (precisamente nel periodo compreso fra il 6 ed il 9 febbraio) prelievi di somme da detto conto ad opera di terzi attraverso frodi informatiche, tipologicamente riconducibili al c.d. phishing.
La ricorrente aveva, infatti, nei giorni precedenti l'attacco di pirateria informatica, ricevuto una mail all'apparenza proveniente dalla Banca e contenente un messaggio, con il quale veniva invitata a digitare i codici di accesso e dispositivi relativi al proprio conto corrente on line allo scopo di attingere ad "informazioni" che la Banca intendeva elargirle. Fidandosi di tale messaggio, la ricorrente aveva effettuato la richiesta digitazione. Ne era conseguita la sottrazione dal suo conto, attraverso diverse operazioni (ricariche verso numeri di cellulare, versamenti a favore di carte prepagate, ecc.), dell'importo complessivo di € 2.100. Di tale importo l'interessata ha richiesto, mediante reclamo in data 21 febbraio 2009, il rimborso all'intermediario, che – pur declinando ogni responsabilità al riguardo ed anzi addebitando tale responsabilità alla reclamante, in quanto questa avrebbe violato l'obbligo di "diligente custodia e gestione dei codici personali", previsto dal contratto a

carico del cliente – tuttavia le riconosceva, in considerazione dei consolidati rapporti ed a titolo di "indennizzo transattivo", la somma di € 1.050, pari alla metà di quella fraudolentemente sottratta dal conto.
Della questione la ricorrente ha successivamente investito anche l'Ombudsman – Giurì Bancario, che con decisione del 14 luglio 2009 ha concluso "per l'inaccoglibilità del ricorso", invocando le clausole di cui agli artt. 6 e 7 delle "Norme che regolano il servizio", riportate nel contratto sottoscritto dalla cliente, alla stregua delle quali il cliente " è tenuto a custodire con ogni cura" il codice utente e la password che gli vengono attribuiti ai fini della sua identificazione ai fini dell'accesso ai servizi di Internet banking ed è "responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito di detti codici".
A sostegno della propria domanda di rimborso integrale delle somme fraudolentemente sottratte, la ricorrente invoca "la particolare vulnerabilità dei servizi di sicurezza informatica" del Gruppo del quale fa parte la Banca convenuta e l'inadeguatezza dei dispositivi previsti contro il rischio di intromissione di terzi nel rapporto di "home banking", rispetto a quelli più sicuri ed affidabili adottati da altre banche italiane ed europee, "come le serie numeriche causali e random generate da dispositivi automatici quali chiavette, digipass, …". Lamenta altresì il fatto che la Banca, prima degli episodi che l'hanno coinvolta, non avesse provveduto ad informare adeguatamente la clientela sul fenomeno della pirateria informatica e sui rischi a questa connessi. Tali comportamenti integrerebbero, secondo la ricorrente, la violazione dell'obbligo di diligenza professionale di cui all'art. 1176, comma 2, c.c., nonché dell'obbligo di buona fede e correttezza ex art. 1175 c.c.
Nelle proprie controdeduzioni del 2 dicembre 2009, la Banca ha respinto ogni addebito, affermando in particolare che i dispositivi di sicurezza da essa istituiti in relazione all'operatività via Internet sui conti correnti erano – all'epoca dei fatti sopra descritti – del tutto adeguati e che, comunque, sarebbe stato dalla ricorrente violato l'obbligo di diligente custodia dei codici identificativi alla stessa attribuiti ai fini dell'esecuzione on line delle operazioni previste dal contratto di Internet banking. Inoltre, sostiene la Banca, il contenuto del messaggio che ha indotto la ricorrente a digitare i propri codici identificativi, in tal modo fornendoli all'autore dell'atto di pirateria informatica era tale da dover mettere sull'avviso la ricorrente (essendo "strana" la circostanza che una Banca chieda tramite Internet ai propri clienti la conferma dei rispettivi codici identificativi) e da doverla comunque indurre alla massima prudenza; tanto più che, ad avviso dell'intermediario, contestando anche su questo punto le affermazioni della ricorrente, erano – già all'epoca dei fatti – presenti nel proprio sito internet apposite comunicazioni rivolte alla clientela e dirette a sensibilizzarla al problema della pirateria informatica.
Con il secondo motivo, la ricorrente lamenta di essere venuta a conoscenza dell'incorporazione del fondo comune di investimento da lei sottoscritto in un nuovo fondo solo a seguito di apposita richiesta alla banca e denuncia pertanto la violazione, da parte dell'intermediario, del dovere di adeguata e tempestiva informazione alla clientela.

DIRITTO

La vicenda sottoposta all'esame di questo Collegio ha riguardo, come già accennato nella narrative dei fatti, a quel peculiare atteggiarsi della frode informatica noto sotto il nome di phishing. Si suole, con detta espressione di origine inglese, ormai entrata anche da noi nell'uso corrente, fare riferimento a comportamenti perpetrati attraverso il c.d. furto di identità telematica, e cioè attraverso l'appropriazione fraudolenta di codici e password identificativi di un dato soggetto in ambito internet allo scopo di conseguirne determinate

utilità (nel caso di specie, l'accesso al conto corrente bancario della ricorrente). In particolare, l'obiettivo dei phishing attacks consiste nell'indurre l'utente a fornire dati o informazioni personali, riguardanti principalmente le credenziali di autenticazione per accedere ad aree informatiche esclusive o a servizi bancari o finanziari on line, i numeri di carte di credito o di pagamento, gli identificativi per l'abilitazione all'accesso a siti di vario genere, gli user id e le password di accesso alla gestione on line dei conti correnti, finanche il numero di conto corrente, il numero o gli estremi della carta d'idendità o della patente di guida. Lo scopo di tali comportamenti è quello di utilizzare i dati in tal modo ottenuti per conseguire l'abilitazione all'accesso a determinati servizi on line, assumendo virtualmente l'identità del legittimo titolare o utente, vittima dell'attacco. Tale attività fraudolenta viene per lo più perpetrata tramite l'invio di e-mail, apparentemente provenienti da enti o istituzioni reali, contenenti messaggi diretti ad indurre l'utente a connettersi ad una pagina web non autentica, ma molto simile a quella delle suddette istituzioni, e ad inserire nei form predisposti dal phisher i dati funzionali all'accesso ad aree informatiche riservate o a servizi on line.

Svolta questa necessaria premessa, il punto nevralgico della questione consiste nel valutare se l'intermediario, con specifico riferimento ai servizi offerti via Internet, avesse adottato tutte le cautele e gli accorgimenti idonei, in base al criterio della diligenza professionale, ad evitare e a prevenire i descritti comportamenti di frode informatica.

Ritiene in proposito questo Collegio che debba prestarsi adesione all'autorevole indirizzo secondo il quale "ai fini della valutazione della responsabilità contrattuale della banca (…) non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio (nella specie si tratta del servizio relativo alla carta bancomat, n.d.r.) da eventuali manomissioni (…): infatti, la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere" (Cass., sezione I civile 12 giugno 2007, n. 13777; cfr. altresì Cass., sez. I civile, 7 marzo 2003, n. 3389; Cass., sez. III civ., 31 luglio 2002, n. 11382).

Tale indirizzo è corroborato – su un piano più generale – dalla ormai (a seguito della riforma societaria del 2003) espressa previsione normativa dell'obbligo, posto a carico dell'organo gestorio, di munire in ogni caso l'impresa di assetti organizzativi adeguati e dell'obbligo, posto a carico dell'organo di controllo, di vigilare sull'adeguatezza di tali assetti (cfr. artt. 2381, 2403, c.c.).

Alla stregua di detti principi va affermata nel caso di specie la responsabilità della Banca, perché, se non è controvertibile che questa avesse adottato determinati accorgimenti tecnici allo scopo di proteggere la sicurezza nell'uso della rete per l'esecuzione da parte dei clienti di operazioni sui propri conti correnti (c.d. internet banking o home banking), è altrettanto incontrovertibile che, all'epoca dei fatti per cui è controversia, la tecnologia aveva già messo a disposizione dispositivi più raffinati, sicuri ed affidabili di quelli in concreto adottati e perciò maggiormente adeguati rispetto all'obiettivo suddetto in quanto capaci di offrire al cliente un terzo livello di protezione, come le serie numeriche casuali e random, generate da dispositivi automatici quali chiavette o token, digipass, et similia.

Orbene, se il corretto adempimento dell'obbligo di diligenza (in particolare, per quanto qui specificamente rileva: dell'accorto banchiere) presuppone l'adozione di tutte le precauzioni e l'istituzione di tutti i presidi di sicurezza adeguati allo scopo e resi accessibili dall'evoluzione scientifica e tecnologica, deve affermarsi la responsabilità per violazione di detto obbligo come conseguenza del mancato adeguamento delle cautele e dei presidi agli ultimi ritrovati ed alle più recenti acquisizioni della scienza e della tecnologia.

Deve tuttavia affermarsi altresì il concorso del fatto colposo della cliente a norma dell'art. 1227 c.c. Infatti, posto che l'uso degli strumenti telematici e della rete Internet per

l'esecuzione di operazioni bancarie giova anche al cliente consentendogli l'operatività a distanza e perciò un notevole risparmio del proprio tempo, il cliente deve tuttavia essere consapevole della delicatezza del mezzo telematico e della possibilità che attraverso quel mezzo siano perpetrate frodi, tanto più insidiose quanto meno facilmente riconoscibili. Nel caso di specie l'atto di pirateria è stato perpetrato per il tramite di un messaggio e-mail che – simulando una comunicazione proveniente dalla stessa banca - richiedeva al cliente la digitazione dei propri codici identificativi e che, perciò solo, avrebbe dovuto metterlo sull'avviso, posta la singolarità del suo contenuto e posto comunque l'obbligo di diligente custodia di detti codici, contrattualmente assunto dalla cliente. Il concorso di colpa può quantificarsi nella misura del 25%, restando dunque a carico della Banca per il 75% la responsabilità ed il conseguente obbligo risarcitorio, che si commisura alla perdita economica subita dalla cliente e si quantifica dunque in € 1.575 (pari al 75% di € 2.100), oltre interessi dalla data del reclamo all'intermediario (21 febbraio 2009) e rivalutazione dalla data di svolgimento dei fatti di causa (9 febbraio 2009).
La domanda puntualizzata nel secondo motivo deve essere dichiarata inammissibile, in quanto investe la materia dei servizi di investimento, che esula dalla competenza di questo Collegio.

P. Q. M.

Il Collegio, in accoglimento parziale del ricorso, dispone che l'intermediario corrisponda a titolo risarcitorio alla ricorrente una somma pari al 75% dell'importo fraudolentemente sottratto da terzi dal suo conto, nella misura complessivamente precisata in motivazione, avuto riguardo anche a interessi e rivalutazione, al netto di quanto eventualmente già versato. Dichiara inammissibile la domanda ulteriore.

Il Collegio dispone, inoltre, ai sensi della vigente normativa che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e al ricorrente di Euro 20,00 (venti/00) quale rimborso della somma versata per la presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE MARZIALE