IL COLLEGIO DI MILANO

composto dai signori:

– Prof. Avv. Antonio Gambaro	Presidente
– Prof. Avv. Emanuele Lucchini Guastalla	Membro designato dalla Banca d'Italia
– Prof.ssa Cristiana Maria Schena	Membro designato dalla Banca d'Italia
– Dott. Mario Blandini	Membro designato dal Conciliatore Bancario Finanziario (Estensore)
– Dott.ssa Anna Bartolini	Membro designato dal C.N.C.U.

nella seduta del 14 ottobre 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

Tra il ricorrente e la banca sussisteva un contratto di conto corrente, per il quale il cliente aveva attivato la funzionalità di *home banking* in data 1° ottobre 2002. Il 25 febbraio 2008, l'interessato ha richiesto la riemissione completa dei codici di accesso al predetto servizio.
Il 25 agosto 2009, il correntista, dopo aver ricevuto un «*avviso cartaceo di avvenuto bonifico*», è venuto a conoscenza di tre bonifici di importo complessivo pari ad euro 13.741,68, disposti tra il 4 e il 10 agosto 2009, verso un conto tenuto presso una banca svedese. Immediatamente, l'interessato ha provveduto – telefonando al numero verde della banca – a bloccare la propria utenza e, tramite e-mail del giorno successivo, a specificare le operazioni disconosciute. In particolare, i movimenti *de quibus* sono:
- bonifico di euro 4.726,83 effettuato il 4 agosto 2009;
- bonifico di euro 5.000,00 effettuato il 7 agosto 2009;
- bonifico di euro 4.014,58 effettuato il 10 agosto 2009.

Lo stesso 26 agosto 2009, ha sporto denuncia contro ignoti presso il locale commissariato di Polizia.
Con lettera datata 18 settembre 2009, la banca ha comunicato «*che il tentativo di recupero presso il beneficiario non ha avuto successo* [e poiché le operazioni contestate possono] *essere impartit*[e] *esclusivamente tramite il corretto inserimento dei tre diversi codici di accesso, non* [...] *sussist*[o]*no i presupposti per il risarcimento*». Il 27 ottobre 2009, l'interessato ha replicato – tramite raccomandata A.R. – notando come le contabili cartacee siano arrivate «*ben 21 giorni dopo il primo bonifico*», così rendendo vano qualsiasi tentativo di recupero, e ritenendo «*che ci siano tutti i presupposti per un*

risarcimento». L'istituto ha risposto con lettera in data 26 novembre 2009, ribadendo l'irrisarcibilità «*dei bonifici esteri effettuati in maniera fraudolenta*».

A fronte del rifiuto opposto dalla banca, il 22 marzo u.s. il cliente ha presentato ricorso all'Arbitro Bancario Finanziario ("ABF") in qualità di consumatore, col quale ha richiesto «*che la banca* [...] *provveda a rimborsar*[e] *totalmente o in parte la somma di euro 13,741,68*».

A sostegno della propria domanda, il ricorrente sottolinea, in primo luogo, che i «*malintenzionati* [hanno] *disattivato l'avviso di avvenuto bonifico al* [proprio] *cellulare*». Inoltre, lo stesso evidenzia «*che per accedere al sito internet della* [banca] *occorre indicare due codici (utente e* password*). Un terzo, codice (chiamato codice dispositivo) viene richiesto solo in occasione di operazioni* [dispositive] *quali bonifici ecc.*[, di non aver] *mai utilizzato il codice dispositivo* [e] *che alla data del fatto i dati utilizzati per l'accesso al sito internet* [della banca] *erano codici fissi e non codici monouso* [...]*. Inoltre, l'avviso cartaceo di avvenuto bonifico,* [...] *è stato recapitato ben 21 giorni dopo l'effettuazione della operazione vanificando in questo modo ogni tentativo di recupero del denaro*». In proposito, «*la sequenza degli eventi (disattivazione dell'avviso telefonico, contemporanea effettuazione di bonifici all'estero, cliente che non ha mai effettuato operazioni* [dispositive]*) avrebbe dovuto insospettire* [l'istituto]*; sarebbe bastata una semplice telefonata* [...] *per smascherare la truffa.* [Infatti,] *a partire dal mese di novembre 2009* [la] *banca* [...] *ha adottato importanti misure per garantire la sicurezza dei propri clienti quali l'adozione di un codice monouso e un'informativa giornaliera ai propri promotori finanziari*». Pertanto, il ricorrente ritiene fondata la propria domanda alla luce delle «*inadeguate misure di sicurezza adottate dalla banca* [...] *(almeno fino al mese di novembre 2009), i numerosi furti di codici* (phishing*) dal vero sito internet* [dell'intermediario resistente] *tramite operazioni di* redirect *e la inadeguata tempestività nell'informare i propri clienti*».

Con un messaggio di Posta Elettronica Certificata, in data 17 giugno 2010 l'intermediario ha presentato, tramite il Conciliatore Bancario Finanziario, le proprie controdeduzioni.

In tale sede, l'istituto osserva preliminarmente che «*la banca,* [non appena ricevuta la segnalazione del ricorrente]*, ha subito predisposto le azioni di recupero presso la banca terza che, tuttavia, hanno avuto esito negativo*». Poi, «*in seguito alla dovuta analisi dei fatti in questione non sono emersi* [...] *gli elementi per cui la banca avrebbe dovuto procedere al risarcimento, dal momento che non sono risultate anomalie o irregolarità di alcun tipo che potessero ricondurre le responsabilità dell'accaduto alla banca* [...]. [...] *infatti, la procedura di accesso al sito ed all'area dell'utente risulta effettuata regolarmente e le istruzioni di addebito risultano correttamente impartite* [...] *e* [...] *chi ha impartito gli ordini era in pieno possesso dei codici operativi*».

Ciò premesso, l'intermediario sottolinea che «*nelle norme contrattuali che regolano il rapporto di conto corrente* [...]*, parte settima – operatività a distanza (servizi* online*) – vengono elencate le regole che disciplinano il rapporto. In particolare, l'art. 66 specifica che l'accesso al sito richiede l'inserimento di tre diversi codici. La banca spedisce i primi due, separatamente e in forma anonima. Si tratta del "codice titolare", che identifica il cliente, viene assegnato dalla banca e non è modificabile, e del "codice segreto", che viene spedito al titolare già scaduto, affinché il cliente al primo accesso al sito lo modifichi personalmente e quindi il nuovo codice sia noto soltanto a lui. Per quanto riguarda il terzo codice, detto "codice operativo", necessario per processare ed autorizzare eventuali addebiti,* [...] *esso viene creato* ex novo *dal cliente al primo accesso, e quindi nessuno ne è in possesso prima e oltre il cliente; tale circostanza garantisce che esso sia di esclusiva conoscenza del titolare. L'accesso ai servizi* online *prevedeva necessariamente entrambe le operazioni di variazione del codice segreto e di creazione del codice titolare, pena la*

mancata attivazione dell'utenza. Lo stesso art. 66 specifica inoltre che "l'utilizzo dei codici di accesso comporta l'automatica attribuzione al cliente delle istruzioni ricevute, con immediato effetto sugli strumenti finanziari e sui valori di pertinenza del cliente. Pertanto il cliente si obbliga a custodire i codici di accesso con la massima cura e riservatezza, impegnandosi (...) a non trasferirli o rivelarli a terzi, né a conservarli insieme o annotarli in un unico documento, restando responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito dei codici di accesso". Il cliente, documentatosi in internet, ha verificato che nel 2008 sono stati registrati degli episodi di phishing *a carico di clienti di* [questa] *banca* [...] *ed adduce, come possibile causa dell'uso fraudolento dei suoi codici, una presunta carenza di sicurezza da parte della banca. Posto che l'episodio, verificatosi nel 2008, è stato prontamente circoscritto e immediatamente risolto, esso non è in alcun modo segnale di inadempienza da parte della banca. Il sistema di sicurezza della banca prevede l'impiego della tecnologia Verisign, leader mondiale in materia (connessione protetta con collegamento di tipo ssl a 128 bit). Il ricorrente ritiene un'ulteriore manifestazione della presunta pericolosità del sito la recente adozione di un più moderno strumento di accesso. Da ottobre 2009 la banca fornisce l'O-Key (un* token *che genera codici operativi monouso), come previsto dall'art. 67 del contratto relativamente alla possibilità di adottare strumenti o modalità o sistemi diversi che permettano la comunicazione a distanza; ciò non dimostra affatto che la precedente modalità fosse inadeguata. In tema di sicurezza la banca ricorda frequentemente la necessità di utilizzare e conservare i codici con la massima prudenza e invita i propri clienti a proteggere il proprio* computer *con appositi* software*, poiché l'identificazione del cliente nei sistemi* online *avviene per mezzo delle sue credenziali. Per questo sul sito sono presenti una serie di avvisi e indicazioni di pronta consultazione* [...]*. D'altra parte è auspicabile che i fruitori di internet si attengano ad un comportamento giudizioso e consapevole, soprattutto se e quando si tratta della possibilità di effettuare operazioni in denaro. Dal punto di vista pratico la banca mette a disposizione inoltre un servizio di* alert *mediante SMS, che il cliente può liberamente attivare dalla sua area personale all'interno del sito; l'SMS di avviso viene inviato ad ogni richiesta di bonifico* online *e fornisce cifra e beneficiario dell'operazione. Sebbene il ricorrente avesse in precedenza chiesto di ricevere l'*alert *via SMS fornito dalla banca, detto servizio risulta disattivato il 2 agosto alle ore 21.2041. In tale occasione il sistema ha generato un messaggio automatico con il seguente testo: "*[nome della banca]*: è stato disabilitato il servizio di notifica bonifici internet via SMS – 02/08/09"*[...]*. Il cliente non ha tuttavia segnalato la cosa alla banca, né ha provveduto a riattivarlo, né ha segnalato la sua estraneità alla disposizione. In seguito a questo messaggio, inoltre, si evidenzia che il cliente non ha proceduto ad accedere al sito per verificare la sua situazione né ha effettuato alcuna verifica per lungo tempo, dal momento che dichiara di aver saputo delle operazioni fraudolente solo grazie alla conferma cartacea, circa due settimane dopo. Se è vero che il cliente non è obbligato a consultare il sito con regolare frequenza, alla ricezione di un* alert *che notifica una variazione non riconosciuta sarebbe quantomeno auspicabile un contatto con la banca per prevenire eventuali possibili disagi*».

Sulla scorta di tali osservazioni, la banca, «*ritenendo che il fatto lamentato dal cliente non sia stato in alcun modo generato da improprio comportamento della* [stessa]», chiede «*che questo spettabile Arbitro voglia respingere la domanda del ricorrente perché non fondata*».

DIRITTO

Il Collegio, sulla base dei fatti oggettivamente emersi dalla documentazione acquisita e, in coerenza con una linea di indirizzo assunta in precedenza per casi analoghi, ritiene che la domanda del ricorrente possa essere accolta solo parzialmente.

Va premesso, innanzitutto, il principio al quale questo Collegio intende informare la presente decisione: «*Il principio di correttezza e buona fede nell'esecuzione del contratto, espressione del dovere di solidarietà fondato sull'art. 2 Cost., impone a ciascuna delle parti del rapporto obbligatorio di agire in modo da preservare gli interessi dell'altra e costituisce un dovere giuridico autonomo a carico di entrambe, a prescindere dall'esistenza di specifici obblighi contrattuali o di quanto espressamente stabilito da norme di legge; ne consegue che la sua violazione costituisce,di per sé, inadempimento e può comportare l'obbligo di risarcire il danno che ne sia derivato*» (Cass. civ. Sez. I, 22 gennaio 2009, n. 1618).

Ciò posto, è innegabile che le operazioni illecite subite dal ricorrente siano state rese esperibili dal fatto che lo stesso sia stato vittima di un "*furto di identità elettronica tramite internet*", attuato attraverso una operazione di *phishing* e che, conseguentemente, non possa mettersi in dubbio che tale operazione sia stata resa possibile dalla violazione, da parte del cliente, dell'obbligo contrattuale di custodire i codici di accesso con la massima cura e riservatezza impegnandosi a non trasferirli o rivelarli a terzi né a conservarli insieme o annotarli in un unico documento, restando responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito dei codici di accesso.

Per converso, non può essere taciuta la corresponsabilità della banca (nella percentuale del 40%) la quale – offrendo servizi bancari mediante mezzi informatici – aveva "*l'obbligo di proteggere mediante gli accorgimenti più idonei il suo sistema di trasmissione dati*" (ABF MI, decisione n. 87/2010).

In concreto, la intermediaria aveva un sistema di sicurezza nell'accesso al sito *internet* costituito da tre codici fissi che la stessa banca, dopo appena due mesi dal fatto in esame, aveva rafforzato adottando, oltre ai due codici fissi un terzo codice "monouso", prevedendo, inoltre, una informativa giornaliera ai promotori finanziari, dimostrando, così, la inadeguatezza dei sistemi informativi adottati in precedenza, resa evidente dal numero di episodi di *phishing* registrati a carico di clienti di quella stessa banca.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda al ricorrente la somma di € 5496,67, equitativamente determinata.

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

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO