Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Collegio di Milano

composto dai signori:

- Prof. Avv. Antonio Gambaro	Presidente
- Prof.ssa Antonella Sciarrone Alibrandi	Membro designato dalla Banca d'Italia
- Prof. Avv. Emanuele Lucchini Guastalla	Membro designato dalla Banca d'Italia
- Prof. Vittorio Santoro	Membro designato dal Conciliatore Bancario Finanziario (Estensore)
- Avv. Paolo Bertazzoli Grabinski Broglio	Membro designato dalla Banca d'Italia e nominato, in via provvisoria, quale supplente del componente effettivo designato dal C.N.C.U

nella seduta del 30 settembre 2010 dopo aver esaminato:
- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario;
- la relazione istruttoria della Segreteria Tecnica.

FATTO

In data 15 dicembre 2009 – tramite un'associazione dei consumatori – il ricorrente chiede alla convenuta il rimborso della somma fraudolentemente sottratta (€ 4.250,62) dal proprio conto corrente attraverso due operazioni di bonifico on-line. L'interessato evidenzia che il 29 luglio 2009, constatata la presenza di due bonifici non autorizzati, ha subito informato la banca del fatto "*affinché ne prendesse buona nota al fine del riaccredito delle somme*" e ha presentato denuncia ai Carabinieri.
Il ricorrente ipotizza di essere stato vittima di pratiche fraudolente di "*phishing*" ovvero di "*pharming*" ed evidenzia che le operazioni contestate presentavano margini di anomalia in quanto disposte a pochi giorni di distanza l'uno dall'altro, per importi analoghi e nei confronti dello stesso beneficiario. Pertanto, il ricorrente rileva che, con ogni evidenza, la banca non ha adottato adeguate procedure di monitoraggio/blocco delle operazioni anomale che avrebbero consentito di evitare il danno subito.
A dimostrazione della propria buona fede, l'interessato dichiara di aver ricevuto sul proprio cellulare - pochi giorni prima del 29 luglio 2009 - un messaggio con cui la banca comunicava la revoca del servizio di SMS-alert ("*ciò dimostra che ciò era stato artatamente posto in essere da esperti manovratori della rete al solo fine di inibire le potenzialità del cliente tese a controllare lo stato delle operazioni sul proprio conto corrente*").
La banca, in data 27 gennaio 2010, riscontra negativamente il reclamo. In particolare, la banca, nell'evidenziare che ha già provveduto alle comunicazioni di rito agli organi di Polizia competenti, trasmette al ricorrente i dati relativi alle due operazioni di bonifico (beneficiario, causale, importo, ecc…). La banca, inoltre, evidenzia che l'operatività on-line

è garantita dalla tecnologia Verisign - "*leader mondiale della sicurezza su Internet*" - e che, per arginare il fenomeno delle frodi telematiche sono previsti limiti operativi giornalieri e mensili all'effettuazione di operazioni via rete.
Nel successivo ricorso all'ABF, il ricorrente ripete le proprie argomentazioni. In particolare, egli imputa alla banca l'esclusiva responsabilità di quanto accaduto per non essersi dotata di un sistema informatico sicuro per l'operatività on-line. Il ricorrente rileva, infatti, che per entrambi i bonifici fraudolenti non ha funzionato il servizio di SMS-alert, oggetto di manomissione. A riprova dell'inadeguatezza dei presidi informatici adottati dalla banca, il ricorrente richiama il fatto che la stessa, a causa del ripetersi di episodi di truffa telematica, ha dovuto cambiare il proprio sistema di sicurezza.
Nelle controdeduzioni la banca richiama le disposizioni sui servizi on-line contenute nel contratto sottoscritto dal ricorrente (26 settembre 2000), in particolare, fa riferimento all'art. 66 che prevede l'obbligo di custodia dei codici identificativi in capo al cliente e la conseguente responsabilità per eventuali conseguenze dannose derivanti da abuso o uso illecito di detti codici. La stessa disposizione prevede l'accesso ai servizi on-line attraverso l'uso di tre codici diversi il cui uso determina l'automatica attribuzione dell'operazione al loro titolare. La banca precisa che il "*codice titolare*" è assegnato dalla banca e non è modificabile, il "*codice segreto*", inviato scaduto al cliente, viene da esso modificato al primo accesso e il "*codice operativo*" è creato anch'esso dal cliente sempre in occasione del primo accesso ("*nessuno ne è in possesso prima e oltre il cliente; tale circostanza garantisce che esso sia di esclusiva conoscenza del titolare*").
La banca evidenzia che - come risulta dalla denuncia presentata ai Carabinieri - il cliente può aver involontariamente favorito il "*pescaggio*" dei propri codici di accesso da parte di terzi, aprendo una e-mail sospetta; inoltre, pur avendo ricevuto un messaggio di revoca del servizio di SMS-alert l'interessato non si è attivato per segnalare l'anomalia al numero verde ovvero per riattivare il servizio. Al riguardo, la banca sottolinea che la segnalazione del ricorrente avrebbe consentito di adottare le misure idonee a prevenire la frode.
Infine, per quanto concerne l'affermazione del ricorrente circa la mancata adozione di presidi di sicurezza adeguati la banca rileva che l'aver messo a disposizione della clientela da ottobre 2009 un nuovo dispositivo (uno strumento che genera password monouso che variano ogni 5 secondi - cd. "*token*") non attesta affatto l'inefficacia del sistema precedentemente adottato. In base alle disposizioni contrattuali, infatti, la banca ha la "*possibilità di adottare strumenti o modalità o sistemi diversi che permettano la comunicazione a distanza*" (art. 67).

DIRITTO

Ritiene il Collegio che la questione debba essere risolta sulla base dei principi generali dell'ordinamento, in forza dei quali (artt. 1175, 1176 e 1375 c.c.) le parti si devono reciprocamente correttezza di comportamento consistente, tra l'altro, nel reciproco obbligo di avviso.
Orbene nel caso in esame il cliente ha trascurato di avvertire la banca in ordine ad una circostanza che, qualora fosse stata nota per tempo, avrebbe potuto mettere quest'ultima nella condizione di prevenire il danno. Infatti, il ricorrente riconosce espressamente di aver ricevuto un messaggio sul cellulare nel quale si comunicava la revoca del servizio di SMS-alert, da lui non disposta, e, nonostante ciò, non si è preoccupato di avvertire la banca dell'intrusione fraudolenta nel sistema informatico affinché potessero essere predisposti blocchi e cautele in ordine alla prevenzione di ulteriori intrusioni fraudolente che successivamente si sono, invece, puntualmente verificate in relazione a due bonifici non autorizzati, per complessivi € 4.250,62.

In considerazione di tale circostanza, il Collegio ritiene preponderante la responsabilità del ricorrente.
Non va esente, tuttavia, da responsabilità concorrente la banca: in ragione della qualità professionale che le compete essa ha il compito di adottare le protezioni migliori per il proprio sistema informatico e, in ogni caso, ne rimane responsabile per le inefficienze. Orbene, all'epoca dello svolgimento dei fatti, al fine di fronteggiare il fenomeno della pirateria informatica, esistevano mezzi più efficienti rispetto a quelli effettivamente in uso presso la resistente. La stessa banca, del resto, ha messo in opera tali sistemi, ma solo successivamente ai fatti di cui si discute, vale a dire a partire dall'ottobre 2009.
Questo Collegio, pertanto, valutata la gravità delle rispettive colpe in relazione ai fatti quali illustrati e documentati dalle parti, le ripartisce in misura dell'80% in capo al ricorrente e del 20% in capo alla banca resistente.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario restituisca la somma di € 850,12 al ricorrente.

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