Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Collegio di Milano

composto dai signori:

- Prof.ssa Antonella Sciarrone Alibrandi	Presidente
- Prof. Avv. Emanuele Lucchini Guastalla	Membro designato dalla Banca d'Italia (Estensore)
- Prof.ssa Cristiana Maria Schena	Membro designato dalla Banca d'Italia
- Dott. Mario Blandini	Membro designato dal Conciliatore Bancario Finanziario
- Avv. Paolo Bertazzoli Grabinski Borglio	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 27 luglio 2010 dopo aver esaminato:
- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario;
- la relazione istruttoria della Segreteria Tecnica.

FATTO

Con tre operazioni di bonifico on-line sono state fraudolentemente trasferite dal conto corrente del ricorrente somme per complessivi € 13.271,00. In merito, l'interessato ha presentato denuncia alla Polizia di Stato e ha chiesto alla banca il rimborso dei fondi fraudolentemente sottrattigli. La banca ha provveduto a stornare il terzo dei bonifici contestati (€ 3.103,00).
L'interessato, accedendo al proprio conto corrente on-line (29 settembre 2009), ha accertato l'esistenza di tre bonifici da lui mai autorizzati (€ 5.312,00 del 21 settembre 2009; € 4.856,00 del 23 settembre 2009 e € 3.103,00 del 28 settembre 2009).
Il 1° ottobre 2009 – dopo aver presentato denuncia alla Polizia – il ricorrente ha chiesto alla banca lo storno delle somme fraudolentemente trasferite a terzi, evidenziando di non aver "*mai smarrito né comunicato ad alcuno i codici di sicurezza internet banking*" e di aver protetto il computer con "*regolare antivirus che si aggiorna automaticamente ad ogni connessione nonché con firewall*".
In particolare, l'interessato ha rilevato che le operazioni contestate presentavano alcuni elementi di anomalia che avrebbero dovuto indurre la banca ad attivare dei sistemi di protezione ("*servizio di allerta o di messaggio automatico, chiamata da un operatore*") per verificarne la liceità. L'interessato ha rilevato, infatti, che i tre bonifici sono stati effettuati "*nell'arco di 7 giorni*" tutti a favore della stessa persona e che già con la seconda operazione si era venuto a determinare un saldo a debito pari a -11.838,62 ("*più del doppio del massimo scoperto che il mio conto ha raggiunto nell'ultimo anno*"), mentre con il terzo bonifico era stato raggiunto un saldo negativo abnorme ("*che mi sembra di*

ricordare essere il massimo scoperto mai raggiunto dal mio conto nella quasi quinquennale durata del rapporto").
Nell'evidenziare, quindi, la carente capacità della banca nel "*monitorare, identificare e segnalare ai clienti i movimenti anomali sul conto*" e la mancata offerta di sistemi di protezione e sicurezza più evoluti per l'operatività on-line ("*token, SMS di avviso ordine bonifico, SMS PIN, codici crittografati su USB, …, strumenti che invece alcuni altri istituti di credito più attenti al tema della sicurezza informatica hanno introdotto già da tempo e spesso offerto a titolo gratuito ai propri clienti*"), il ricorrente ha chiesto il rimborso della somma fraudolentemente bonificata (€ 13.271,00).
In data 26 ottobre 2009 l'interessato ha presentato - tramite legale - nuovamente il reclamo alla banca.
La banca il 27 ottobre 2009 ha risposto al reclamo mettendo in evidenza che "*dalle verifiche espletate non si evince alcuna responsabilità* [a proprio carico] *nello svolgimento dello specifico servizio*" e che, in base alle disposizioni contrattuali il cliente "*resta pienamente responsabile della protezione, della conservazione e del corretto uso delle credenziali di accesso, nonché dell'eventuale utilizzo improprio o fraudolento delle stesse, anche da parte di terzi*".
In particolare, la banca ha rilevato che i fruitori del servizio di Internet Banking ricevono, quando si trovano ad operare on-line, specifici messaggi volti a prevenire i casi di frode informatica ed, inoltre, possono richiedere – al fine di assicurarsi una maggiore protezione – un ulteriore strumento: il token.
Nel rigettare la richiesta di rimborso, la banca ha sottolineato che, comunque, "*grazie al tempestivo intervento degli addetti della dipendenza di Jesi e dei competenti servizi centrali*" è stato possibile stornare il terzo bonifico, con riaccredito della relativa somma (€ 3.103,00) sul conto corrente.
Il ricorrente - tramite il proprio legale – ha riprodotto le argomentazioni rilevate in fase di reclamo, ribadendo la mancata attivazione da parte della banca a tutela della clientela di adeguati sistemi di rilevazione degli indici di anomalia sull'operatività on-line in conto corrente. In particolare, è stata nuovamente evidenziata la singolare incidenza sul saldo debitore delle operazioni di bonifico ("*le movimentazioni di cui ai bonifici sopra indicati, effettuate in tempi molto vicini e per importi elevati, rispetto al normale trend di movimentazione del conto corrente, avrebbe dovuto destare qualche sospetto o attivare un sistema di alert autin, in particolar modo in occasione del secondo bonifico effettuato, per un importo pari a -4.856,00, il conto in questione a raggiunto un saldo di conto pari a -11.838,62, ossia più del doppio del massimo scoperto che il medesimo conto abbia mai raggiunto nell'ultimo anno …*").
Ciò considerato, il ricorrente chiede all'ABF la restituzione di € 10.168,00 (considerato che la banca ha già provveduto allo storno del 3° bonifico), oltre agli interessi nel frattempo maturati.

L'intermediario ha presentato le controdeduzioni con PEC tramite il Conciliatore Bancario l'11/05/2010.
La banca, nel respingere ogni addebito, ha richiamato le disposizioni del contratto sottoscritto dal ricorrente per la fruizione del servizio di Internet Banking che prevedono a carico del cliente un obbligo di diligenza nella custodia delle credenziali di accesso.
In particolare, la banca ha evidenziato che per l'operatività on-line il cliente dispone di 3 diversi codici di accesso (User Id; password e password dispositiva), il cui utilizzo rende a lui opponibili le corrispondenti operazioni. La banca ha rilevato, inoltre, che dalle verifiche effettuate è stato riscontrato l'uso delle credenziali di accesso del ricorrente per tutti i bonifici contestati.

La banca ha, altresì, evidenziato che le operazioni non presentavano - contrariamente a quanto sostenuto dal ricorrente - particolari indici di anomalia in quanto esse "*potevano considerarsi normali alla luce dei rapporti intrattenuti in autonomia dal cliente* (…); *a seguito dei bonifici in questione del resto, peraltro, effettuati in giorni diversi con un intervallo di due giorni lavorativi l'uno dall'altro, non si è mai generato alcuno sconfinamento rispetto alla disponibilità esistente sul conto per effetto degli affidamenti accordati*". A dimostrazione della propria diligenza, la banca ha sottolineato l'impegno profuso – "*non appena venuta a conoscenza dell'accaduto*" – nello storno del 3° bonifico ("*per gli altri importi … le somme erano già state prelevate*").

Come richiesto, le controdeduzioni della Banca sono state trasmesse al ricorrente con e-mail.

DIRITTO

La questione che questo Collegio deve affrontare per la soluzione del caso attiene ai doveri di custodia dei codici di accesso da parte del cliente che utilizzi il servizio di *home banking*, da un lato, e del grado di diligenza che si può richiedere all'intermediario in relazione all'erogazione di detto servizio, dall'altro lato.
Ora, nel corso del presente procedimento è emerso che il servizio di home banking utilizzato dal ricorrente necessitava di ben tre codici distinti (User Id; password e password dispositiva) e che in base alle verifiche effettuate è stato riscontrato l'uso delle credenziali di accesso del ricorrente per tutti i bonifici oggetto di contestazione nel presente procedimento.
Nel contempo, appare indubbio che nel giro di pochi giorni siano state compiute operazioni per un importo non indifferente e con un unico identico beneficiario, operazioni che – seppure non abbiano mai generato alcuno sconfinamento rispetto alla disponibilità esistente sul conto – hanno tuttavia fatto sì che il saldo negativo del medesimo rapporto raggiungesse livelli anomali rispetto alla normale operatività del ricorrente.
Ebbene, così ricostruiti brevemente i fatti salienti della vicenda, non può che ricordarsi – come già si è avuto occasione di rilevare in altre occasioni – che è opinione assolutamente condivisa che sul cliente gravi l'onere di custodire con la massima diligenza i vari codici in suo possesso necessari per compiere operazioni bancarie di vario genere, siano esse prelievi per mezzo del servizio Bancomat, come disposizioni di operazioni per mezzo di servizi on-line.
Il punto è essenziale per una corretta interpretazione del rapporto contrattuale, posto che, in linea generale, appare corretto affermare che al cliente sono opponibili le operazioni effettuate con la digitazione dei codici in suo possesso (indipendentemente da chi effettivamente le abbia disposte), proprio perché nell'utilizzo del servizio di home banking il cliente viene identificato esclusivamente mediante la verifica dei codici di sicurezza che gli sono stati assegnati.
Quanto appena rilevato rende chiara sia la ragione dell'obbligo di diligente custodia di detti codici sia il fatto che la violazione di tale obbligo di diligente custodia dei codici di accesso comporti che il cliente sia chiamato a rispondere di ogni conseguenza dannosa derivante da un eventuale illecito utilizzo di tali codici da parte di terzi
Dalle osservazioni che precedono deve, dunque, trarsi la seguente conclusione in linea generale, e cioè che – posto che nel servizio di home banking, l'uso corretto dei codici di accesso consente l'identificazione del titolare e l'autorizzazione dei pagamenti disposti – i bonifici fraudolenti che siano stati eseguiti previa corretta digitazione di tali codici sono giuridicamente riconducibili al titolare del servizio.

Ciò chiarito, con riferimento al primo dei due aspetti sopra evidenziati, deve ora affrontarsi la diversa questione del grado di diligenza dell'intermediario richiesto con riferimento alla prestazione di servizi bancari per via telematica.
Secondo la consolidata opinione della dottrina e della giurisprudenza, l'attività bancaria, in quanto attività riservata, deve sottostare al canone di diligenza previsto dall'art. 1176, comma 2, c.c. ("*diligenza dell'accorto banchiere*") con conseguente adozione di tutte le cautele necessarie.
Come è noto, la diligenza professionalmente qualificata cui fa riferimento il secondo comma dell'art. 1176 c.c. deve essere parametrata alle specificità tecnico-scientifiche della professione esercitata, trattandosi di nozione superiore e più specifica di quella relativa al buon padre di famiglia, richiamata dal primo comma dello stesso articolo. L'adempimento dell'obbligazione, quindi, deve avvenire con la diligenza "*del regolato ed accorto professionista*" (banchiere, nel caso che ne occupa), pena il risarcimento dei danni secondo i normali canoni della responsabilità contrattuale.
Per gli aspetti che qui interessano, tale parametro rileva in relazione alla specificità del servizio bancario oggetto di contestazione (home banking) che implica l'utilizzazione del canale telematico e l'uso di codici dispositivi.
In particolare, la valutazione coinvolge l'adeguatezza - considerati gli standard esistenti - dei presidi tecnici adottati dall'intermediario per rendere sicure le transazioni on-line da attacchi di pirateria informatica.
Sui presidi di sicurezza più idonei a fronteggiare il fenomeno della pirateria informatica non c'è attualmente una specifica normativa vincolante, anche se esistono diversi documenti, sia a livello nazionale che internazionale, trattano della sicurezza dell'e-banking e, in particolare, della diversa efficacia dei vari meccanismi di autenticazione.
L'utente viene, infatti, autenticato attraverso la presentazione di credenziali. Generalmente si intende per "*credenziale*" uno o più dei seguenti elementi: qualcosa che l'utente "sa" (es. la password); qualcosa che l'utente "ha" (es. il token, che può contenere un certificato digitale); qualcosa che l'utente "è" (in questo caso si parla di caratteristiche biometriche, es. le impronte digitali).
Quando l'autenticazione dell'utente utilizza congiuntamente due di questi sistemi, si parla di autenticazione "a due fattori". Alcune modalità tecniche che consentono, in associazione all'utilizzo di user-id e password, di effettuare una autenticazione a due fattori: "Segreti condivisi", "Token" e "Tecnologie biometriche".
E' chiaro a questo Collegio che, al tempo dei fatti all'origine della presente vertenza, esistevano già mezzi più efficienti per fronteggiare il fenomeno della pirateria informatica e questo costituisce ragione sufficiente per indurre a concludere che un sistema di protezione ad un solo fattore – composto da tre codici di accesso, non variabili di volta in volta – per permettere l'esecuzione di disposizioni bancarie non può essere considerato misura sufficiente a proteggere adeguatamente il cliente.
A ciò deve aggiungersi che, come questo Collegio ha già avuto occasione di sottolineare (decisione n. 46 del 2010), "*la banca la quale offre servizi on line alla propria clientela ha il dovere di adempiere il proprio obbligo di custodia dei patrimoni dei clienti con la diligenza professionale richiesta dall'art. 1176 co. 2 c.c., predisponendo misure di protezione – tra le quali l'invio di sms di conferma dell'eventuale disattivazione del servizio di sms-alert e l'invio di sms di avviso dell'esecuzione dell'ordine di bonifico - idonei ad evitare l'accesso fraudolento di terzi ai depositi dei propri clienti, o a neutralizzarne gli effetti*". Ebbene, pare che la semplice adozione di tali elementari strumenti di avviso avrebbe sicuramente evitato il pregiudizio lamentato in questo procedimento, conclusione quest'ultima che trova ulteriore conferma nella circostanza che per l'ultimo dei tre bonifici in questione è stato possibile procedere allo storno.

Oltre a quanto appena rilevato, non può sottacersi neppure un ulteriore aspetto di criticità della fattispecie al vaglio di questo Collegio, e cioè che nel giro di pochi giorni sono state compiute tre operazioni di rilevante importo, con un unico identico beneficiario e che hanno determinato un saldo negativo del conto corrente assolutamente non in linea con l'operatività "*storica*" del ricorrente; ciò induce a considerare "*anomale*" tale operazioni per l'importo, il beneficiario e la frequenza.
Di ciò, avrebbe dovuto avvedersi l'intermediario, non certo monitorando direttamente ogni singola operazione, ma predisponendo sistemi automatici di blocco delle operazioni da postazione remota in presenza di comportamenti decisamente non in linea con l'operatività corrente del proprio cliente.
Del resto, non può certo passare inosservato che il c.d. "Decalogo ABI", tra l'altro, consiglia agli intermediari di predisporre strumenti di monitoraggio delle transazioni dei propri conti on-line, in modo da evidenziare eventuali comportamenti anomali.
Ciò, nel caso di specie, non è avvenuto e, di conseguenza, l'intermediario che non abbia predisposto idonei strumenti per evidenziare e/o bloccare automaticamente comportamenti che siano evidentemente anomali, non può andare esente da responsabilità.
In sintesi, dunque, nel caso all'origine del presente ricorso da un lato si può verosimilmente ravvisare una responsabilità del cliente in relazione alla mancata diligente custodia dei codici d'accesso al servizio di home banking, dall'altro lato non si può negare una concorrente responsabilità dell'intermediario che non abbia predisposto adeguati sistemi per proteggere più efficacemente i propri clienti con riferimento al rischio di truffe perpetrate per via telematica, nonché per evidenziare e/o monitorare comportamenti anomali e/o sospetti in relazione al medesimo servizio.
Questo Collegio, valutata la gravità delle rispettive colpe in relazione ai fatti illustrati e documentati, ritiene, dunque, di doverle ripartire nella misura del 50% in capo al cliente e nella misura del 50% in capo al resistente.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario restituisca al ricorrente la somma di € 5084,00.

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
ANTONELLA MARIA SCIARRONE ALIBR