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 (Estensore)
- Dott. Dario Purcaro	Membro designato dal Conciliatore Bancario Finanziario
- Prof. Avv. Alberto Monti	Membro designato da Confindustria, di concerto con Confcommercio, Confagricoltura e Confartigianato

nella seduta del 17 giugno 2010 dopo aver esaminato:
- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario;
- la relazione istruttoria della Segreteria Tecnica.

FATTO

In data 13 maggio 2009 - attraverso l'accesso fraudolento al conto corrente on-line intestato alla società ricorrente - veniva effettuato un bonifico per complessivi € 3.750,00. Il rappresentante legale della società (di seguito: il ricorrente) sporgeva denuncia per truffa ai Carabinieri e chiedeva alla banca il rimborso della somma indebitamente accreditata a terzi.
Il ricorrente, collegandosi on-line in data 14 maggio 2009 al conto corrente intestato alla società, accertava l'esistenza di un bonifico di € 3.750,00 effettuato il giorno precedente a favore di persona a lui sconosciuta. Il 15 maggio 2009 il ricorrente sporgeva denuncia ai Carabinieri evidenziando che, appena verificata l'esistenza dell'operazione, aveva contattato la banca convenuta per il disconoscimento del bonifico e per bloccarne il pagamento.
In particolare, nella querela il ricorrente specificava che una dipendente della banca gli avrebbe riferito di aver contattato l'intermediario presso cui risultava acceso il conto corrente destinatario dell'accredito per chiedere il blocco del pagamento e che, "*poco dopo aver ricevuto tale comunicazione*", la banca avrebbe comunque pagato la somma alla beneficiaria presentatasi nel frattempo allo sportello. Il ricorrente, inoltre, specificava che i codici di accesso al conto corrente on-line erano sempre stati in suo possesso "*in modo esclusivo*", per cui riteneva che gli fossero stati carpiti con "*artifizi e raggiri*".
La banca, con lettera del 10 luglio 2009, evidenziava che in relazione alle "*operazioni dispositive disconosciute*" non risultavano anomalie nei tracciati per quanto riguardava l'immissione delle credenziali né in fase di accesso, né in fase dispositiva e, pertanto, l'uso illegittimo dei codici per l'operatività on-line era "*da imputarsi ad un'acquisizione degli stessi da parte di terzi*".

Il ricorrente, in data 10 settembre 2009, inviava tramite e-mail le "videate" di accesso al servizio di home-banking – riferite rispettivamente al proprio PC e ad un altro PC dell'ufficio – mettendo in evidenza che, per quanto riguardava quelle relative al proprio PC, prima della segnalazione dell'episodio di truffa compariva una "stringa" per l'inserimento della password di accesso, successivamente scomparsa. In base a tali elementi, il ricorrente escludeva che si trattasse di un caso di "phishing", sostenendo il malfunzionamento del sistema informatico della banca.
Il ricorrente, nel "*ribadire il disconoscimento del bonifico*", ha chiesto all'Arbitro Bancario Finanziario il rimborso della somma indebitamente accreditata a terzi.
L'intermediario ha presentato le controdeduzioni con PEC tramite il Conciliatore Bancario il 23/04/2010.
La banca ha evidenziato che l'operazione fraudolenta di cui è stato vittima il ricorrente è riconducibile al cd. "phishing".
Attraverso tale pratica truffaldina, quindi, sono stati carpiti i codici di accesso e dispositivi per operare sul conto corrente on-line. In merito, la banca ha rilevato che l'analisi dei tracciati degli accessi e delle successive operazioni sul conto - effettuati dalle competenti funzioni aziendali - non presentano anomalie. In particolare, in fase di accesso i tentativi sono andati tutti a buon fine, mentre in fase dispositiva risultava un tentativo fallito.
Per quanto concerne la "videata" che consente l'accesso al servizio di home banking, la banca ha evidenziato che su quella ufficiale non compare la "stringa" relativa alla password di accesso.
La banca, inoltre, ha specificato che sul proprio sito internet è presente un link dedicato alle misure di protezione da episodi di pirateria informatica con tutte le specifiche per utilizzare i servizi on-line in sicurezza. In particolare, la banca ha rilevato che dalle "videate" prodotte dall'interessato si evince che, quella relativa al suo PC, presentava – al momento dei fatti - un format diverso da quello ufficiale.
Ciò considerato, tenuto conto che la presunta frode non è stata causata da una violazione del proprio sistema informatico, la banca ha chiesto il rigetto del ricorso.

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

La banca è stata sollecitata per confermare l'avvenuta ricezione del ricorso. In merito, come evidenziato nelle controdeduzioni - per disguidi postali interni – la banca ha avuto contezza in ritardo dell'arrivo del ricorso.

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.
In relazione al caso in questione giova notare che risulta documentalmente provato che il cliente è stato vittima di un atto di pirateria informatica, posto che su uno dei PC in suo possesso è stato richiesto, per un certo periodo, di digitare una password non richiesta dal sito ufficiale dell'intermediario.
Dalla documentazione in atti è, infine, emerso che il servizio di home banking utilizzato dal ricorrente necessitava – oltre ad un "identificativo utente" e un codice "operatore" – di almeno due ulteriori codici distinti: uno per accedere al servizio e uno per impartire disposizioni.

Ebbene, così ricostruiti 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, che 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".
Sempre a proposito del pericolo delle frodi informatiche deve ricordarsi in proposito il "Decalogo ABI per banche e clienti sui sistemi di protezione dal "phishing"", nel quale si suggerisce agli intermediari, fra l'altro, di:

1) Definire policy aziendali stringenti per il contatto del cliente via e-mail;
2) Pubblicizzare ai dipendenti e ai clienti della banca le policy di utilizzo dell'email;
3) Aggiungere un ulteriore livello di autenticazione (con password differenziata) per l'esecuzione di operazioni dispositive tramite il servizio di home banking;
4) Predisporre strumenti di monitoraggio delle transazioni dei propri conti on-line, in modo da evidenziare eventuali comportamenti anomali.

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 due soli codici di accesso, non variabili di volta in volta (oltre ad un "identificativo utente" e un codice "operatore") – per permettere l'esecuzione di disposizioni bancarie non può essere considerato misura sufficiente a proteggere adeguatamente il cliente.
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 per il servizio di home banking, dall'altro lato, non si può negare una concorrente responsabilità dell'intermediario che non ha predisposto adeguati sistemi per proteggere più efficacemente i propri clienti con riferimento al rischio di truffe perpetrate per via telematica.
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 risarcisca al ricorrente la somma di € 1.875,00, a titolo di concorso di colpa nell'evento.

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