IL COLLEGIO DI MILANO

composto dai signori:

– Prof. Avv. Antonio Gambaro	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
– 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

Con nota dell'8.10.2009 un'associazione di consumatori chiedeva all'intermediario che il ricorrente fosse "tenuto indenne" dai danni derivati dall'aver "abboccato" ad una e-mail di phishing.
Più, precisamente riferiva che in data 5.9.2009 il ricorrente, "durante l'operazione di stampa del proprio estratto conto", riceveva dei messaggi di posta elettronica che lo invitavano a fornire il proprio codice dispositivo. L'interessato "procedeva a completare le suddette richieste" e solo nel pomeriggio della stessa giornata si accorgeva che non riusciva più ad accedere al sito dell'intermediario. Contattato dal servizio clienti dell'intermediario stesso, apprendeva che ignoti avevano cambiato la sua password e prelevato on-line la somma di € 3.130,00.
Con lettera del 2.11.2009 il ricorrente, non avendo ricevuto riscontro, contestava nuovamente l'addebito sul proprio conto del movimento non autorizzato, osservando che "data la tempestività" con cui aveva denunciato il fatto fraudolento si sarebbe aspettato che l'intermediario non avesse dato seguito alla transazione.
Il 29.3.2010 l'intermediario rispondeva di non poter accogliere la richiesta, in quanto non si riteneva responsabile dei danni subiti dal cliente. A sostegno della propria posizione argomentava che quanto accaduto al ricorrente rientrava tra i casi di frodi informatiche, per difendersi dalle quali è necessario "non cliccare sui link presenti nelle e-mail". Faceva poi presente di offrire un servizio "con elevati standard di sicurezza" e di aver provveduto a mettere "in guardia" la propria clientela con diversi mezzi (comunicazioni scritte, stampa, associazioni dei consumatori, sito internet).

Non ritenendosi soddisfatto, il 26.4.2010 l'interessato presentava ricorso all'ABF, chiedendo la restituzione dei citati € 3.130,00.
Allegava in copia all'istanza, oltre alla corrispondenza già citata, il verbale di denuncia del fatto alla Pubblica Autorità.
Il 26.8.2010, con circa due mesi di ritardo rispetto al termine previsto, sono pervenute le controdeduzioni, con le quali l'intermediario ha chiesto al Collegio di non accogliere il ricorso, in quanto "la domanda … è infondata" sulla base dei seguenti presupposti:

- il ricorrente non ha fornito prova della corretta custodia dei propri codici identificativi; anzi ha dichiarato di avere risposto ad una e-mail di phishing e di aver provveduto a digitare le proprie credenziali, compreso il codice dispositivo: ciò integra gli estremi della colpa grave;
- "in virtù del principio della rappresentanza apparente", l'operazione disconosciuta dal ricorrente è stata disposta da un soggetto autenticatosi quale legittimo titolare, che ha digitato "tutte le successive serie di riconoscimenti informatici indispensabili: … userid, … password e caratteri richiesti dal sistema casualmente tra i dieci caratteri alfanumerici componenti il codice dispositivo";
- l'evento lamentato dall'attore deve essere valutato ai sensi dell'art. 1227 c.c., "al fine della costruzione del nesso eziologico nella catena degli eventi che hanno causato il danno";
- il ricorrente non ha provato l'asserita responsabilità della parte resistente nella vicenda. Non è d'altra parte ipotizzabile l'intromissione di terzi nel suo sistema informatico al fine di una singola frode: un'eventualità di questo tipo avrebbe comportato ripercussioni generalizzate per tutti i correntisti;
- l'intermediario "sin dal 2005" provvede ad informare i clienti dei rischi di furto di identità informatica, fornendo concrete indicazioni a mezzo internet.

Oltre alla corrispondenza già citata, sono allegati in copia alle controdeduzioni il modulo di apertura del conto corrente sottoscritto a suo tempo dal ricorrente, uno stralcio delle condizioni applicate al rapporto, il dettaglio contabile dell'operazione contestata.

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 assolutamente pacifico che il ricorrente abbia risposto ad una e-mail di *phishing* in data 5.9.2010: la circostanza è stata dichiarata dall'interessato anche nella denuncia alla Pubblica Autorità effettuata in data 7.9.2010. Al riguardo il ricorrente ha precisato di avere fornito il proprio codice per ottenere un accredito collegato ad un'operazione a premi, "nell'assoluta certezza" che a richiederlo fosse l'intermediario.
Dall'esame del testo contrattuale si può chiaramente evincere che le principali condizioni sul servizio di home banking fornito dall'intermediario prevedono quanto segue:
"SEZIONE VI
SERVIZIO … ONLINE
ART. 2: STRUMENTI OPERATIVI E MOTIVI DI PROTEZIONE
Il correntista, per l'utilizzo del servizio … è tenuto a identificarsi e a legittimarsi secondo quanto previsto dal presente articolo e dalle istruzioni operative che gli vengono fornite … [dall'intermediario].

3. La sicurezza del servizio … è garantita mediante idonei sistemi di crittografia dei dati di riconoscimento dell'utente. Ai fini del riconoscimento dell'utente sono previsti:
a) l'identificativo utente: fornito … [dall'intermediario] al termine della fase di registrazione del correntista. In caso di omonimia il sistema richiederà una personalizzazione dell'identificativo utente al fine di garantirne l'univocità. Definito l'identificativo utente, questo non potrà più essere modificato;
b) la parola chiave (o password): definita dal correntista in fase di registrazione. La parola chiave costituisce, insieme con l'identificativo utente, la chiave d'accesso al servizio … La parola chiave può essere successivamente modificata dall'utente;
c) il codice dispositivo segreto: generato dal sistema informatico … [dell'intermediario] con procedura protetta. Il codice dispositivo segreto è composto di dieci caratteri alfanumerici ed è inviato al correntista via posta prioritaria in busta sigillata. L'utilizzo del codice dispositivo segreto, richiesto in fase di esecuzione delle operazioni dispositive, avverrà mediante digitazione dei caratteri di volta in volta evidenziati dal sistema con modalità random. Per motivi di sicurezza il codice dispositivo segreto non è attivo al momento del recapito. L'attivazione del codice dispositivo segreto avverrà con le modalità di cui al successivo punto d);
d) la cifra di controllo: generata dal sistema informatico … [dell'intermediario] in occasione dell'attivazione del servizio. La cifra di controllo è composta di cinque caratteri numerici, e viene inviata all'utente all'indirizzo di cassetta postale elettronica attribuitagli … [dall'intermediario] al termine della fase di registrazione, contemporaneamente alla comunicazione di avvenuta attivazione del servizio. Tale cifra va presentata … per richiedere l'attivazione del codice dispositivo segreto di cui al precedente punto c).
4. L'individuazione del correntista e la riferibilità allo stesso delle richieste impartite nell'ambito del presente servizio … avvengono esclusivamente mediante gli strumenti operativi sopraelencati che costituiscono la chiave d'accesso al servizio stesso. … [L'intermediario] adotta una procedura intesa a rendere inaccessibili a terzi i suddetti strumenti operativi, che devono essere mantenuti riservati dal correntista.
ART. 3: ESECUZIONE DELLE OPERAZIONI
1. Le disposizioni impartite dal correntista … [all'intermediario] attraverso il servizio … sono irrevocabili.
… [L'intermediario] ha la facoltà di bloccare l'effettuazione delle operazioni dispositive qualora il cliente non abbia rispettato le specifiche modalità di utilizzo del codice dispositivo segreto di cui al precedente art. 2, comma 3 lettera c).
3. Le disposizioni e le informazioni rispettivamente impartite e richieste … saranno eseguite, a seconda della tipologia di operazione effettuata, entro il termine massimo di 4 (quattro) giorni lavorativi bancari".

Ebbene, così ricostruiti gli aspetti salienti della vicenda, non può che ricordarsi – come già si è avuto occasione di rilevare in altre occasioni (Decisione n. 909/10 del 10.9.2010 e Decisione n. 719/10 del 9.7.2010) – 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".

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 codici di accesso, non variabili di volta in volta (oltre ad un codice dispositivo segreto composto di dieci caratteri alfanumerici "costanti" nel tempo) – 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 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.
Questo Collegio, valutata la gravità delle rispettive colpe in relazione ai fatti illustrati e documentati, ritiene, dunque, di doverle ripartire nella misura del 60% in capo al cliente e nella misura del 40% in capo al resistente.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario che l'intermediario risarcisca al ricorrente la somma di € 1.252,00.
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
ANTONIO GAMBARO