Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

- Prof. Avv. Antonio Gambaro	Presidente (Estensore)
- Prof.ssa Antonella Maria Sciarrone Alibrandi	Membro designato dalla Banca d'Italia
- Prof. Avv. Emanuele Cesare Lucchini Guastalla	Membro designato dalla Banca d'Italia
- Dott. Mario Blandini	Membro designato dal Conciliatore Bancario Finanziario
- Prof. Avv. Andrea Tina	Membro designato dal C.N.C.U.

nella seduta del 12 giugno 2012 dopo aver esaminato

- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria tecnica

FATTO

La ricorrente è titolare di conto corrente con annessi servizi di carta di debito e di internet banking presso l'odierna resistente.

Con nota del 1° agosto 2011, indirizzata ad una filiale della convenuta, la ricorrente informava di essersi avveduta, in data 31.07.2011 "facendo una stampa della lista movimenti", della presenza di un "ordine di bonifico estero" scritturato il 28.07.2011, dell'importo di Euro 2.544,00 a favore di un soggetto sconosciuto, dalla stessa non effettuato; peraltro la predetta operazione era stata eseguita "utilizzan[do] altresì € 1.353,69 e € 50,00 di fido…".

Nella stessa nota, la ricorrente dichiarava, tra l'altro, che:

il giorno 28.07.2011, intorno alle ore 22:00, intenta ad effettuare una ricarica della propria carta prepagata, inseriti tutti i codici per portare a termine l'operazione, si accorgeva di un rallentamento della pagina internet della convenuta che presentava un messaggio (attendere backing), al quale non dava particolare rilievo, posto che intorno alle ore 22:42 ha "concretizzato la ricarica" della prepagata. Con nota del 6/08/2011 disponeva la chiusura del conto online.

La convenuta non ha riscontrato le comunicazioni suddette.

Con il ricorso proposto all'ABF sottoscritto il 2.03.2012, la ricorrente ha rappresentato di:

- ✓ essere stata vittima di una frode telematica "in quanto ignoti sono entrati nel sito dell'[intermediario] e quindi nel mio conto online e hanno effettuato un bonifico … estero per l'importo di € 2.544,00";
- ✓ aver immediatamente bloccato la carta e sporto denuncia ai Carabinieri;
- ✓ aver denunciato l'accaduto sia alla filiale dell'intermediario ove era radicato il conto e sia all'Ufficio frodi telematiche;
- ✓ non avere ottenuto alcun riscontro e "chiaramente alcun risarcimento".

L'Intermediario ha trasmesso le controdeduzioni, via PEC, il 25.05.2012, anziché entro il termine del 23.04.2012.

Ha innanzitutto riepilogato la vicenda all'origine della presente controversia, evidenziando in particolare che la ricorrente:

- ha acceso il rapporto di conto corrente il 26.08.2005, al quale, in data 3.09.2006, è stato associato il servizio di internet banking; il 28.10.2009 le è stato consegnato "*il dispositivo necessario ad autorizzare le transazioni on-line, il cosiddetto LETTORE*" della carta"; questo dispositivo in unione alla carta di debito dotata di microchip, contenente il certificato digitale, permette al momento della disposizione di una transazione on-line la generazione e lo scambio di codici univoci tra il sito web e il correntista al fine di verificarne l'identità;
- il 27.07.2011, alle ore 22:19, ha disposto regolarmente l'operazione online di bonifico estero di € 2.544,00, accreditato alla banca estera il successivo 1°.08.2011;
- il 31.07.2011 ha presentato denuncia all'A.G. e il successivo 1°agosto 2011 ha provveduto a disconoscere presso l'Ufficio di…..la suddetta operazione.

Nel merito, l'intermediario ha rilevato che:

- L'operazione contestata è stata disposta *"da soggetto autenticatosi come legittimo titolare, mediante il corretto inserimento di tutte le successive serie di riconoscimenti informatici indispensabili per l'esecuzione di tale operazione"* in particolare:
  - ✓ userid del titolare;
  - ✓ password conosciuta esclusivamente dal titolare e modificabile in ogni momento dallo
  - ✓ stesso;
  - ✓ utilizzo del primo codice univoco usa e getta proposto da sistema *("ID Operazione")* e che deve essere digitato sul LETTORE ….(PCR);
  - ✓ corretto utilizzo del PCR mediante la Carta …. Microchip EMV n…..;
  - ✓ utilizzo del PIN di quest'ultima, noto solo al titolare;
  - ✓ digitazione del secondo codice univoco usa e getta ("codice *risposta")* fornito dal PCR e da introdurre nell'apposito campo della schermata della piattaforma web dell'Internet Banking, mentre si esegue la stessa transazione on line, e senza il quale la disposizione non può terminare.
- la possibile presenza di malware sulla macchina utilizzata dalla cliente "tendente ad inserire degli input da riga di comando (es. DOS o telnet, oppure in linguaggio macchina evoluto), eseguibili esclusivamente durante l'utilizzazione dell'apparato e durante la connessione, per instaurare attività contemporanee in modalità presumibilmente trasparente all'enduser." ;
- l'operazione è stata evasa perché risultata regolarmente autorizzata in seguito alla corretta esecuzione delle attività previste dal sistema di securizzazione delle operazioni on-line[1];
- "[n]*essuna violazione è avvenuta a carico dei sistemi informatici*" della stessa resistente, che *"tuttora risultano inviolati ed assolutamente sicuri*", precisando che *"diversamente i malfattori non si sarebbero limitati alla sola carta dell'odierno ricorrente, bensì il fatto avrebbe avuto risvolti estremamente più elevati e ciò sarebbe certo divenuto oggetto di notizia"*;

[1] In relazione a ciò, la resistente ha descritto in modo dettagliato il funzionamento e le fasi necessarie per arrivare a disporre un bonifico online, al fine di dimostrare l'impossibilità di operare senza la materialità della carta […] e del relativo lettore.

- emergerebbe con tutta evidenza che nella data dell'operazione contestata "la ricorrente o qualcuno al suo posto" abbia "maneggiato [gl]i … strumenti" di autenticazione necessari per concludere l'operazione;
- la ricorrente non avrebbe riferito "pressoché nulla in merito alla sua esperienza della giornata della transazione contestata, se - ad esempio - durante la connessione internet riferita nella denuncia alla P.G. ed in altri scritti (agli atti del ricorso), si siano verificate situazioni particolari o inconsuete, o se nel corso di tale connessione (o nei giorni precedenti) abbia avuto richiesta (via email, via link a pagine web cloni del genuino sito web o in altra forma) di erogare parte o tutti i 5 differenti codici di riconoscimento informatico";
- "*le condizioni contrattuali del conto corrente sottoscritte …* [dal] *cliente prevedono che …* [lo stesso intermediario] *debba eseguire l'ordine impartito con l'uso dei codici identificativi del cliente"*, illustrando analiticamente le modalità di utilizzo delle funzionalità dispositive del servizio di internet banking, che richiedono l'identificazione del cliente attraverso "*5 codici personali diversi"*, da inserire *"ciascuno in una specifica fase protetta*" per il buon esito della transazione, che si intende così *"non più revocabile"*;
- l'ordine del bonifico contestato è stato impartito attraverso il corretto ed esatto utilizzo dei codici personali e, pertanto, l'intermediario ha l'obbligo, contrattualmente sancito, di darvi esecuzione
- al descritto obbligo a suo carico "*corrisponde l'obbligo del correntista di mantenere segreti tali codici e di accettare gli addebiti relativi ad operazioni disposte mediante l'uso degli stessi*";
- la sicurezza del servizio di home banking "*è garantita … mediante un sistema di crittografia dei dati di riconoscimento dell'utente e di protezione di questi ultimi da intercettazioni e violazioni*" e che tale sistema è stato certificato "*secondo i più rigorosi ed affidabili standard internazionali*";
- stante quanto sopra, *"ha pienamente assolto agli obblighi contrattuali e di legge con la diligenza qualificata"*, non avendo di converso il ricorrente *"fornito la prova, di cui è onerato a norma dell'art. 2697 c.c., di un inadempimento da parte"* della convenuta stessa, né *"affermato e tanto meno dimostrato di aver osservato l'obbligo di mantenere riservati i codici personali relativi all'operatività on line sul suo conto"* e neanche *"di aver dotato il proprio computer di un sistema di protezione globale della navigazione internet efficiente e costantemente aggiornato";*
- "*fin dal marzo 2005*" provvede ad informare i clienti in ordine ai rischi di furto di identità informatica, fornendo concrete indicazioni a mezzo internet e tramite altri canali di comunicazione.

Nelle controdeduzioni, l'intermediario ha altresì citato alcuni precedenti della giurisprudenza di merito a sostegno delle proprie argomentazioni.

Infine, affermando che "*il verosimile comportamento …* [ascrivibile alla ricorrente] *della consegna ad un terzo dei propri codici dispositivi, non può che essere affetto da grave negligenza*" e richiamando sia l'art. 1227, secondo comma, C.C. con riferimento all'*"imprudenza nella custodia della carta e dei codici personali"* imputabile al cliente, sia gli 'artt. 1218 e 2697 C.C. in relazione alla *"mancanza di contestazione di un inadempimento contrattuale da parte …* [della resistente stessa] *e della relativa prova",* l'intermediario ha concluso chiedendo che l'ABF *"respinga l'istanza della ricorrente, in quanto infondata per i motivi sopra esposti"*, rappresentando la circostanza che in

controversie analoghe il Collegio ha respinto i ricorsi con le decisioni nn. 1462/12 e 1521/12.

DIRITTO

Giova puntualizzare in fatto che l'utilizzo per finalità dispositive del servizio di home banking, all'epoca dei fatti, richiedeva: a) userid del titolare; b) password conosciuta esclusivamente dal titolare e modificabile in ogni momento dallo stesso; c) utilizzo del primo codice univoco usa e getta proposto da sistema *("ID Operazione")* e che deve essere digitato sul LETTORE PCR; d) corretto utilizzo del PCR mediante la Carta […] dotata di Microchip EMV; e) utilizzo del PIN di quest'ultima, noto solo al titolare; f) digitazione del secondo codice univoco usa e getta ("codice *risposta")* fornito dal PCR e da introdurre nell'apposito campo della schermata della piattaforma web dell'Internet Banking, mentre si esegue la stessa transazione on line, e senza il quale la disposizione non può terminare. Giova altresì ricordare che risulta in atti che, contestualmente all'inserimento dell'ordine di bonifico, l'intermediario ha segnalato via mal l'operazione alla ricorrente invitandola a verificare la capienza del conto, e che successivamente, l'intermediario ha dato riscontro del buon esito dell'operazione con una mail di elevata chiarezza.
In punto di diritto si deve premettere i fatti esposti in narrativa sono posteriori all'entrata in vigore del D.Lgs. 11/2010, che ha recepito nell'ordinamento italiano la Direttiva 2007/64/CE. Al caso in esame sono quindi applicabili le disposizioni di detto Decreto, e segnatamente, per quanto qui rileva, quelle concernenti gli obblighi rispettivamente gravanti sul prestatore di un servizio di pagamento e sul relativo utilizzatore.
Dispone al riguardo il primo comma dell'art. 8 del Decreto che "*Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7*".
In forza della norma ivi richiamata, *"L'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso*" e, a tal fine, è tenuto, "*non appena riceve uno strumento di pagamento*", ad adottare "*le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo*".
Nel caso in esame deve ritenersi che la resistente abbia adempiuto con la dovuta diligenza ai propri obblighi. Questa ha, infatti, messo a disposizione del cliente un sistema per il compimento di operazioni *on line*, che è basato sull'utilizzo contemporaneo di più fattori, ossia quel tipo di sistema che anche questo Collegio non ha mancato di considerare il più sicuro e tale da assicurare la migliore tutela degli utilizzatori in base all'attuale stato della tecnica (cfr., tra le tante, la decisione n. 1694 del 2011, la decisione 1462 del 2012).
Dalle informazioni rese dalla ricorrente e dalle precisazioni fornite dalla resistente, che non sono state contestate, è emerso, infatti, che per il compimento di un'operazione via internet il cliente è tenuto ad utilizzare uno strumento materiale in suo possesso, ossia il lettore, all'interno del quale va introdotta la carta di pagamento a microchip, pure in suo possesso. Egli deve inoltre digitare diversi codici, ora sul lettore, ora nell'apposito spazio sulla schermata che compare sul computer accedendo al servizio per il compimento di operazioni *on line*. Due di detti codici sono generati (si ha ragione di ritenere, casualmente e con modalità "usa e getta") uno dal sistema e uno dal lettore.

Dal tipo di sistema di protezione adottato discende la presunzione, certamente grave e rilevante, che il cliente non avesse viceversa compiutamente custodito i dispositivi personali necessari per l'utilizzo del sistema di pagamento, con negligenza che si presenta rilevante. Inoltre non riesce ad essere spiegata, salvo che nell'ipotesi di una momentanea perdita di controllo dell'hardware, la mancata presa in considerazione delle due mail di controllo generate dal sistema della resistente. Sicché il Collegio, sulla base dei soli dati in suo possesso, non può ritenere che il comportamento dell'utilizzatore sia scevro da colpa e in particolare da colpa grave.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO