Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Collegio di Milano

composto dai signori:

- Prof. Avv. Emanuele Cesare Lucchini Guastalla	Presidente
- Prof. Avv. Mauro Orlandi	Membro designato dalla Banca d'Italia
- Prof.ssa Avv. Diana V. Cerini	Membro designato dalla Banca d'Italia
- Avv. Giuseppe Spennacchio	Membro designato dal Conciliatore Bancario Finanziario (Estensore)
- Avv. Guido Sagliaschi	Membro designato dal C.N.C.U.

nella seduta del 21 febbraio 2013, dopo aver esaminato:
- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario;
- la relazione istruttoria della Segreteria Tecnica.

FATTO

Nel proprio ricorso all'ABF il ricorrente, titolare, unitamente al padre, cointestatario del ricorso, di conto corrente acceso presso l'intermediario convenuto, con annesso servizio di home banking, ha esposto che in data 29 agosto 2011 aveva effettuato un controllo telematico sul proprio conto corrente, e si era accorto che era stata fraudolentemente disposta un'operazione di bonifico online per un ammontare di €. 2.488,00= a favore di un soggetto allo stesso sconosciuto; pertanto aveva contattato il personale della filiale della banca, apprendendo che l'operazione era stata eseguita in data 5 agosto 2011, "*senza che tuttavia né lui né l'altro cointestatario del conto corrente (…) abbiano mai disposto né autorizzato*" la stessa operazione bancaria. Il successivo 30 agosto 2011 aveva sporto denuncia alla Pubblica Autorità, precisando che la chiavetta OTP, necessaria per le operazioni *on line*, era sempre stata in suo possesso.
Con lettera in data 20 settembre 2011 il ricorrente aveva sporto reclamo alla banca per il rimborso del denaro sottratto. Con nota in data 18 ottobre 2011, l'intermediario resistente aveva riscontrato tale primo reclamo del cliente proponendo una ricostruzione dei fatti secondo la quale:
- dalle verifiche effettuate era emerso che il bonifico disconosciuto era stato eseguito "*utilizzando i corretti codici di accesso*";

- tuttavia, stante quanto denunciato dal ricorrente era "*verosimile che l'operazione fraudolenta si* (… fosse) *verificata a causa dell'attacco di un c.d.* Man in The Browser*, un* malware (…) *che si installa sul PC all'apertura di e-mail di* phishing *inviate al cliente o tramite altri sistemi di infezione. Il* software *dannoso si attiva durante una transazione iniziata dall'utente, senza che lo stesso o la banca possano accorgersi dell'intrusione ed è in grado di modificare i dati inseriti dal titolare del conto corrente*";
- grava comunque sul cliente l'obbligo di custodire con la "*massima cura e riservatezza*" le credenziali di accesso al servizio di *home banking*, nonché di utilizzare un sistema informatico protetto con programmi antivirus periodicamente aggiornati;
- pertanto, "*il solo utilizzo dei codici segreti da parte del possessore illegittimo, per un verso induce la Banca a ritenere che l'ordine provenga dal titolare del servizio, per altro verso, integra la prova della omissione della necessaria diligenza nella custodia delle credenziali segrete da parte del titolare*";
- "*anche se la conservazione delle* password*, nel caso di specie, possa per ipotesi ritenersi esente dal configurare una condotta negligente in capo al ricorrente, è indubbio che, in ogni caso, tale condotta sia stata l'unica cosa che, in termini di nesso causale, abbia consentito il determinarsi dell'esecuzione del prelievo fraudolento*".

Con successivo reclamo in data 9 febbraio 2012, presentato con l'assistenza di un legale, il ricorrente aveva insistito nella richiesta di rimborso integrale della somma sottratta dal suo conto corrente ed aveva chiesto altresì il ristoro delle spese legali, pari ad €. 120,00=, ribadendo di non avere alcuna responsabilità in merito alla vicenda poiché aveva adoperato "*la massima diligenza nella custodia delle proprie credenziali segrete e nell'utilizzo dei propri sistemi software per l'accesso al servizio di multicanalità*". Poiché al reclamo non era stato dato riscontro positivo, il ricorrente ha reiterato in sede di ricorso la richiesta di rimborso della somma a lui indebitamente sottratta, maggiorata delle spese legali sostenute per la difesa, facendo rinvio alla querela presentata ed alla restante documentazione allegata.

La convenuta si è costituita riproponendo le motivazioni per le quali aveva già respinto il reclamo del cliente ed ha, dunque, chiesto all'ABF di respingere le istanze del ricorrente, "*non avendo lo stesso custodito le credenziali di accesso del servizio di multicanalità con la diligenza del caso e atteso il corretto comportamento di questa Banca nella vicenda*".

DIRITTO

La fattispecie in esame, concernente un caso di disconoscimento di operazione dispositiva, effettuata tramite bonifico *on line*, con conseguente addebito sul conto corrente del ricorrente, della quale si afferma il carattere fraudolento, è stata più volte sottoposta all'attenzione dell'Arbitro Bancario Finanziario, il quale ha fondato le decisioni assunte in proposito, da un lato, sulla valutazione dell'adeguatezza del sistema di protezione adottato dall'intermediario, quale espressione della diligenza professionale dallo stesso esigibile ai sensi dell'art. 1176, comma 2, c.c. e, dall'altro, sull'adempimento degli obblighi di custodia dello strumento di pagamento, imposti dalla legge e dal contratto intercorso con il prestatore del servizio. Tale obiettivo è stato conseguito con il D.Lgs. 11/10, che ha recepito la Direttiva 2007/64/CE, da un lato, imponendo agli intermediari, nella loro qualità di prestatori di servizi di pagamento, specifici obblighi di precauzione, primo fra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati (ossia diversi dal loro legittimo titolare: art. 8, comma 1, lett. a) e, dall'altro lato, istituendo un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori ex art. 10; infatti in caso di disconoscimento di un'operazione di

pagamento, è onere dell'intermediario dimostrare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema.
L'apparentemente corretta autenticazione non è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca; la responsabilità dell'utilizzatore resta dunque circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento agli obblighi che l'art. 7 del decreto pone a suo carico e che poi si limitano all'utilizzazione dello strumento di pagamento in conformità ai patti contenuti nell'accordo quadro che regola il servizio e alla tempestiva denuncia di furto, smarrimento, distruzione o altro uso non autorizzato dello strumento. Ove una responsabilità non possa affermarsi in capo all'utilizzatore (e chiaramente il correlato onere probatorio incombe sull'intermediario prestatore del servizio), lo stesso non sopporterà le conseguenze dell'uso fraudolento, o comunque non autorizzato, del mezzo di pagamento se non nei limiti di una "franchigia" non superiore ad €. 150,00=.
Nel caso in esame va, dunque, in primo luogo verificato se l'intermediario abbia adottato tutte le misure di sicurezza e di protezione per evitare accessi non autorizzati, richieste dalla disciplina vigente e adeguate agli standard tecnologici più avanzati. Giova puntualizzare in fatto che l'operazione disconosciuta è stata eseguita utilizzando le credenziali del cliente compresa la password dispositiva "OTP" prodotta dal *token* rilasciato al ricorrente in forza del contratto sottoscritto in data 26 gennaio 2010.
L'intermediario aveva già adottato, dunque, all'epoca dell'attivazione del servizio di *internet banking* da parte del ricorrente, il sistema a due fattori (nelle controdeduzioni è specificato che la chiavetta OTP è stata resa obbligatoria per tutti i nuovi clienti a partire dal 3 marzo 2008). Con riguardo alla possibilità di considerare provata la colpa grave del ricorrente per il fatto che nonostante la OTP e gli altri presidi di sicurezza predisposti dall'intermediario si è verificato l'illecito, questo Collegio si allinea a quanto statuito con recente pronuncia dal Collegio di Coordinamento (la n. 3498 del 26 ottobre 2012) che si è soffermato proprio sull'ipotesi in cui l'intermediario abbia messo a disposizione del cliente i più avanzati strumenti tecnici di prevenzione e se ne sia avvalso e, nondimeno, sia avvenuta o comunque sia stata denunciata una fraudolenta intrusione ad opera dei terzi.
Il Collegio di Coordinamento ha delineato una puntuale ricostruzione delle truffe informatiche attuate mediante *software* malevoli, sottolineando la rilevanza delle circostanze del caso concreto e dei comportamenti tenuti dalle parti al fine di assumere una decisione sulle istanze di rimborso conseguenti ad utilizzi fraudolenti in presenza di sistemi di *home banking* a due fattori. Assumono, dunque, una valenza determinante le argomentazioni proposte dalla stessa convenuta nelle risposte ai reclami presentati dal cliente, laddove l'intermediario fa specifico riferimento alla circostanza di come sia "*verosimile che l'operazione fraudolenta si sia verificata a causa dell'attacco di un c.d.* Man in The Browser", cioè di un *malware* particolarmente insidioso e sofisticato, tale da rendere inefficace la protezione degli strumenti informatici usati dall'utente.
La banca rappresenta, al riguardo, che "*nella stessa giornata ed in orari vicini, sono state eseguite anche due ricariche telefoniche, operazioni non disconosciute dal cliente*" ed aggiunge, nella risposta al secondo reclamo, che "*nel merito, si può presumere che, nel tentativo di effettuare le operazioni di ricarica, sia stata richiesta la digitazione dell'OTP una volta in più rispetto alle operazioni che la S.V. aveva intenzione di effettuare*". E', dunque, lo stesso intermediario convenuto a dedurre che l'operazione fraudolenta è stata possibile con l'ausilio di un *malware* annidato nel PC del ricorrente.
Si tratta, in definitiva, di una vicenda di truffa informatica, perpetrata mediante un *software* malevolo, nella quale non sono emersi particolari indici di anomalia nella ricostruzione dei

fatti, potendosi, viceversa, alla luce delle stesse allegazioni della resistente, ritenere pacifica la presenza di un *malware* nel computer utilizzato dal cliente. In tali circostanze, essendo possibile ritenere che l'operazione sia stata disposta senza la disponibilità del *token*, si deve necessariamente concludere che il ricorrente non ha violato gli obblighi di diligente custodia posti a suo carico e che, perciò, non ricorrono le circostanze previste dall'art. 12 del D.Lgs. 11/10 dovendo rimanere a suo carico soltanto la franchigia di legge.
Con riferimento, invece, alla richiesta di rimborso delle spese per l'assistenza del legale, non risulta agli atti alcuna documentazione a supporto della domanda che deve, pertanto, essere rigettata.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda al ricorrente la somma di € 2.338,00.
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
EMANUELE CESARE LUCCHINI GUASTALLA