IL COLLEGIO DI NAPOLI

composto dai signori:

- Prof. Avv. Enrico Quadri	Presidente
- Dott. Comm. Leopoldo Varriale	Membro designato dalla Banca d'Italia
- Prof. Avv. Ferruccio Auletta	Membro designato dalla Banca d'Italia
- Prof. Gennaro Rotondo	Membro designato dal Conciliatore Bancario (estensore)
- Avv. Roberto Manzione	Membro designato da C.N.C.U.

nella seduta del 20 luglio 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

Il caso in decisione concerne l'utilizzo fraudolento di un conto corrente, operativo anche *on line,* al quale è collegata una carta di debito.

Con reclami del 13 gennaio e 23 febbraio 2010 il ricorrente, anche tramite il proprio legale, espone di aver subito in data 5 ottobre 2009 un "*furto on line*" concretizzatosi nell'addebito di un bonifico – da lui mai disposto – per un importo di € 3.050,00, di cui chiede la restituzione all'intermediario.

Il cliente sostiene che l'accesso fraudolento è stato reso possibile dalle carenze del sistema di sicurezza predisposto dalla banca, connotato soltanto dall'utilizzo di un codice cliente (user - id) e da una password, della quale il sistema chiede necessariamente il cambiamento al primo accesso; il ricorrente dichiara che vane sono, invece, rimaste le richieste volte ad ottenere la consegna di un ulteriore dispositivo di sicurezza rappresentato da un c.d. token (introdotto dalla banca solo successivamente).

Per i fatti occorsi, il ricorrente ha sporto il 22 ottobre 2009 formale denuncia-querela per truffa. Egli sostiene, altresì, che la beneficiaria del bonifico – che avrebbe sporto controquerela asserendo di essere stata, a sua volta, vittima di truffa – avrebbe trattenuto parte della somma trasferendo la restante su un c/c estero.

Con nota del 15 febbraio 2010 la banca resistente riconosce che "la questione prospettata" integra l'ipotesi di frode informatica "concepita per effettuare furti d'identità" (c.d. phishing).

Nel merito l'intermediario:

- richiama l'ordinanza del Tribunale di Milano del 10 ottobre 2008 secondo la quale, tra l'altro, "*nel fenomeno del phishing, il danneggiato diretto del reato è, e resta, solo il correntista, al quale sono state carpite maliziosamente le chiavi di accesso informatico al proprio c/c*" e "soltanto l'esistenza di un preciso obbligo contrattuale in capo all'istituto depositario di tenere indenne il cliente da ogni tipo, o quanto meno da questo tipo, di aggressioni alla provvista depositata potrebbe attribuire all'ente la qualità di danneggiato diretto dal reato".
- sostiene che "*per la normativa italiana, gli istituti di credito non sono tenuti a garantire i clienti da frodi informatiche*";
- eccepisce l'esonero da ogni responsabilità richiamando le relative disposizioni contrattuali a disciplina dell'utilizzo del servizio on line:

In sede di ricorso il legale rappresentante del ricorrente riprende quanto già esposto con reclamo in relazione al "*furto on line di € 3.050,00*", chiedendo a questo Collegio di condannare la resistente alla restituzione del relativo importo "oltre che al risarcimento dei danni…da determinarsi in via equitativa e non inferiori a € 1.500,00". La responsabilità della banca per "*colpa grave*" viene, in particolare, ravvisata nel non aver predisposto un sistema di sicurezza adeguato a preservare il canale informatico da accessi illeciti, a nulla rilevando le clausole contrattuali di esonero da responsabilità, che possono essere considerate vessatorie. A supporto di quanto sostenuto, la parte ricorrente ha prodotto la nota inviata dall'istituto di credito a tutti i titolari di c/c *on line* (ricevuta dal ricorrente il 14 gennaio 2010) recante l'invito a "*ritirare il token*", introdotto "per motivi di sicurezza" con azzeramento dei "*massimali dispositivi per le stazioni non dotate di token…con decorrenza immediata*".

In sede di controdeduzioni, la banca preliminarmente eccepisce l'improcedibilità del ricorso all'ABF in quanto la questione contestata sarebbe già sottoposta al vaglio dell'A.G. per effetto della riserva, formulata dal ricorrente, di costituirsi parte civile nel giudizio penale eventualmente attivatosi in relazione alla denuncia-querela sporta.

La banca sostiene di aver assunto "*le cautele e le tutele atte ad evitare episodi quali quello in contestazione*" e richiama nuovamente le clausole contrattuali, già riportate in sede di reclamo, per sostenere l'opponibilità "*al cliente di* (…) *tutte le operazioni effettuate con la digitazione dei codici in suo possesso – indipendentemente da chi le abbia effettivamente disposte*". La resistente sostiene che l'operazione disconosciuta è stata presumibilmente resa possibile dalla "palese negligenza ed imprudenza" del ricorrente "*per aver fornito senza alcuna cautela ed accortezza le proprie credenziali a soggetti non legittimati*" e/o per non aver installato sul pc utilizzato per operazioni di internet banking adeguati sistemi di protezione. Ciò posto, l'intermediario chiede all'ABF di rigettare il ricorso.

Con nota del 24 giugno 2010, il legale rappresentante del ricorrente contesta l'eccezione di improcedibilità, non essendo allo stato pendente alcun procedimento giudiziario per i fatti oggetto di denuncia-querela. Replica che il bonifico in contestazione è l'unico ad essere stato disposto tramite il canale telematico dal c/c del ricorrente, il cui pc, tra l'altro, è dotato "*dei più efficienti sistemi di protezione*"; il legale, infine, ribadisce che i più adeguati sistemi di sicurezza, rappresentati dal "token" e il "cps" sono stati "*introdotti solo successivamente alla vicenda*". Difatti, a partire dal 30 marzo 2010, la banca ha previsto per i conti on line rispetto ai quali non sia stato attivato il token, il "*codice personale segreto*" (CPS), una sorta di "*evoluzione della password statica alfanumerica*".

DIRITTO

Il Collegio ritiene opportuno pronunciarsi, preliminarmente, sulla eccezione di improcedibilità del ricorso avanzata dalla resistente in quanto la questione contestata "*sarebbe*" già sottoposta al vaglio dell'A.G.

Sul punto, va richiamata la Sezione I.4, delle Disposizioni sui Sistemi di Risoluzione Stragiudiziale delle Controversie in Materia di Operazioni e Servizi Bancari e Finanziari, del 18 giugno 2009, secondo cui "*non possono essere proposti ricorsi inerenti a controversie già sottoposte all'autorità giudiziale, rimesse a decisione arbitrale[. …]".*

La norma fa riferimento, con tutta evidenza, alla instaurazione (da parte dell'intermediario) di un procedimento giudiziario o arbitrale che abbia il medesimo oggetto (stessi *petitum* e *causa petendi*) di quello in corso dinanzi all'ABF e non si ritiene rientri in questa fattispecie l'eventuale instaurazione di un giudizio penale (che nel caso di specie sarebbe legato alla denuncia-querela per truffa presentata dal ricorrente). In aggiunta, allo stato, non risulta sia in corso alcun procedimento dinanzi all'autorità giudiziaria.

Venendo a valutare i profili di merito circa le richieste del ricorrente, questo Collegio ha ripetutamente evidenziato, come la predisposizione, da parte degli intermediari, di canali di operatività *on line* si connoti per la rilevanza di due tipologie di obblighi: da un lato, gli obblighi di diligenza e custodia del cliente, ivi compresa la dimostrazione di avere adottato tutti gli accorgimenti necessari ad evitare il verificarsi di episodi di utilizzo fraudolento degli strumenti informatici. Anche il cliente, difatti, deve essere ben consapevole della delicatezza del mezzo telematico e della possibilità che per questo tramite siano perpetrate frodi di varia natura.

Dall'altro, vi sono gli obblighi dell'intermediario che, nell'offrire tali servizi, deve adempiere il proprio compito di custodia dei patrimoni dei clienti con la diligenza professionale e qualificata richiesta dall'art. 1176, comma 2, c.c. predisponendo misure di protezione adeguate rispetto agli standard esistenti, anche sotto il profilo dei presidi tecnici adottati.

Ulteriori norme di riferimento per la controversia, in esame, sono gli artt. 1710 c.c. (diligenza del mandatario) e 1856 c.c. (esecuzione di incarichi). Va richiamato, altresì, il decreto legislativo n. 11/2010 (di recepimento della direttiva comunitaria sui servizi di pagamento) il quale, pur non essendo direttamente applicabile al caso in questione in considerazione della difforme sfera temporale di operatività, assume un rilevante valore ermeneutico ai fini dell'applicazione delle norme del codice in materia di corretta esecuzione di incarichi per conto del correntista (cfr. Collegio ABF di Napoli, n. 482/10) e in conformità all'ampliamento delle forme di tutela dei clienti che utilizzano strumenti di pagamento (on line).

Il Collegio rileva che, nella fattispecie, la banca non ha posto in essere tutti gli accorgimenti necessari per garantire la sicurezza del sistema informatico e prevenire eventuali utilizzi fraudolenti dello stesso da parte di terzi, non adempiendo con la dovuta diligenza professionale (ex art. 1176, comma 2) ai suoi doveri di custodia del patrimonio del cliente. Circostanza comprovata dall'introduzione, di poco successiva alle contestazioni del ricorrente, di ulteriori e più avanzate misure di sicurezza per i conti correnti con operatività on line (quali, ad esempio, il c.d. "token", v. supra).

Per altro verso, si deve altresì ribadire che la suddetta violazione degli obblighi di diligenza da parte della resistente non vale ad escludere la colpa concorrente del ricorrente, ex art. 1227 c.c. (cfr. Collegio ABF Milano n. 46/10; n. 87/10; Collegio ABF Roma n. 33/10). Nel caso in decisione, il ricorrente non dimostra di avere custodito con la necessaria diligenza i codici di accesso al conto *on line* (la password, ad esempio, andava cambiata al primo

accesso, ma il ricorrente afferma di non aver effettuato disposizioni, salvo poi dichiarare di avere consultato il conto tramite il canale telematico); soprattutto non vi è prova delle reiterate richieste che il ricorrente avrebbe inoltrato alla banca per ottenere sistemi di sicurezza aggiuntivi (disponibili, seppure non obbligatori), che con buona probabilità avrebbero impedito il verificarsi del lamentato evento fraudolento. Pertanto, per le ragioni fin qui esposte questo Collegio ritiene che il ricorrente abbia concorso a cagionare il danno nella misura del 50%.

Infine, per quanto concerne la richiesta di risarcimento da "*determinarsi in via equitativa e non inferiore a € 1.500,00*", il Collegio ritiene che la stessa sia generica e non comprovata da elementi sostanziali in relazione all'ulteriore pregiudizio verificatosi a danno del ricorrente e, come tale, non accoglibile.

P.Q.M.

In parziale accoglimento del ricorso il Collegio dispone che l'intermediario sia tenuto al rimborso della somma di € 1.525,00.

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
ENRICO QUADRI