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 Finanziario (estensore)

- Avv. Roberto Manzione..... Membro designato dal C.N.C.U.

nella seduta dell'11/01/2011 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 controversia all'esame di questo Collegio riguarda una frode informatica avente ad oggetto un bonifico bancario non autorizzato.
I ricorrenti, cointestatari di un conto corrente presso la banca resistente, constatano in data 9 agosto 2010, a seguito di verifiche telematiche, un ammanco sul conto di € 24.800. Contattato telefonicamente un operatore della banca, i correntisti apprendono che il 4 agosto 2010 è stato effettuato – sulla base di un ordine impartito a mezzo del servizio di *internet banking* – un bonifico per l'intero importo dell'ammanco, a favore di un beneficiario residente all'estero (in Slovacchia), sconosciuto agli stessi correntisti.
Immediatamente i ricorrenti provvedevano a presentare denuncia contro ignoti presso la competente autorità di polizia. Con nota del successivo 17 agosto 2010, formulano poi, per il tramite del proprio avvocato, formale reclamo alla banca, disconoscendo l'operazione di bonifico e richiedendo la restituzione della somma. A supporto della pretesa, il legale precisa che i propri assistiti non hanno mai risposto a messaggi di *phishing* e hanno diligentemente protetto il proprio computer da aggressioni *malware* con appositi presidi informatici; inoltre, osserva che l'evidente anomalia dell'operazione, "*alla luce del profilo economico dei clienti e della inusuale destinazione del trasferimento*", avrebbe dovuto indurre la resistente ad adottare ogni cautela prima di dare corso al trasferimento.
La banca fornisce riscontro al reclamo con lettera del 2 settembre 2010, nella quale riferisce di aver effettuato – già a seguito della segnalazione telefonica – tutte le opportune

verifiche in merito alla disposizione contestata, senza tuttavia riscontrare "*alcuna violazione del sistema informatico nel periodo in cui il bonifico è stato eseguito*". La resistente, quindi, conferma che l'ordine su banca dell'Est europeo a favore di beneficiario ivi residente, per l'importo di € 24.840, risulta correttamente impartito in data 4 agosto 2010, attraverso il servizio di *internet banking* con l'inserimento dei codici segreti personali di uno dei ricorrenti. Tanto premesso, l'istituto convenuto precisa anche di avere, a seguito della ripetuta segnalazione telefonica, tempestivamente contattato la banca corrispondente nel tentativo, rimasto infruttuoso, di recuperare l'importo.

Insoddisfatti della risposta ricevuta, i clienti presentano ricorso all'Arbitro Bancario Finanziario in data 4 ottobre 2010. In un'articolata nota, i ricorrenti ripropongono la richiesta di rimborso della somma indebitamente sottratta, oltre interessi.

Innanzitutto, essi rilevano come le caratteristiche dell'operazione, in relazione al profilo economico, alle loro "*abitudini operative*", all'importo del bonifico "*quasi pari all'intero ammortare del deposito*" e alla "*inusuale destinazione del trasferimento*", avrebbero dovuto indurre la banca alla massima cautela, eventualmente anche avvertendo direttamente gli interessati ("*come, peraltro, accaduto in passato con operazioni di importo inferiore destinate a beneficiario italiano*"). Tale cautela, inoltre, sarebbe stata consigliata da un ulteriore elemento di anomalia rispetto alla normale operatività dei clienti, vale a dire l'utilizzo di un IP identificativo di computer diverso da quelli usualmente riscontrati per l'accesso al servizio di *internet banking* (ossia gli IP corrispondenti ai computer di casa e ufficio dei clienti).

I ricorrenti sostengono, inoltre (sempre in sede di ricorso), che la resistente, a differenza di altri operatori che forniscono il servizio di *internet banking*, non ha adottato i sistemi di sicurezza più evoluti basati, ad esempio, su una *one time password*, di volta in volta generata da un apposito supporto tecnologico (quali *token*, *smart card ecc.*) e valida per un singolo accesso.

Non avendo i correntisti mai divulgato le proprie credenziali di accesso né risposto a messaggi di *phishing*, l'intromissione da parte di terzi nel sistema informatico della banca proverebbe l'inadeguatezza dei presidi di sicurezza adottati e la conseguente responsabilità della resistente per violazione degli obblighi di diligente custodia dei patrimoni dei clienti, alla luce del parametro dell'accorto banchiere (ai sensi dell'art. 1176 c.c., come evidenziato anche da recente giurisprudenza: si richiama in proposito, *ex multis*, Cass. sez. I, 12 giugno 2007, n. 13777). Eguali responsabilità in capo alla banca deriverebbero anche alla stregua delle disposizioni del codice civile (artt. 2381, 2403, c.c.) che pongono, a carico dell'organo gestorio, l'obbligo di dotare l'impresa di adeguati assetti organizzativi e, a carico dell'organo di controllo, l'obbligo di valutare l'effettiva congruità di tali assetti.

In allegato al ricorso, è prodotta, oltre al reclamo e alla relativa risposta della banca, la copia della denuncia depositata presso la competente autorità di polizia.

In sede di controdeduzioni, la resistente riferisce i fatti antecedenti alla presentazione del ricorso riportando, in particolare, i contenuti della segnalazione telefonica (registrata, ma non allegata agli atti) effettuata da uno dei cointestatari del conto, in data 9 agosto 2010, dopo aver accertato l'ammanco: secondo quanto emergerebbe dalle dichiarazioni rese in tale occasione, l'interessato avrebbe effettuato, nei giorni precedenti l'operazione contestata, l'accesso a un sito clone della banca resistente, per il tramite di un ordinario motore di ricerca, e avrebbero digitato "*oltre al proprio codice identificativo cliente, e la propria password, anche le ventiquattro serie di terne numeriche utilizzate per confermare le disposizioni*". Tale incauto comportamento avrebbe consentito all'"aggressore" di catturare le chiavi di autenticazione, successivamente utilizzate per impartire l'ordine a mezzo dell'*internet banking*.

Come già riferito in fase di reclamo, la banca - ricevuta la segnalazione del cliente - tenta di recuperare la somma presso l'intermediario slovacco che, tuttavia, comunica di non poter procedere allo storno.

Tanto premesso, la banca conferma la piena correttezza del proprio operato, assicurando che, nel periodo in cui è stata posta in essere l'operazione contestata, il proprio sistema informatico non ha subito alcuna violazione o aggressione esterna. La responsabilità dell'accesso non autorizzato è, quindi, ascrivibile unicamente ai ricorrenti, incorsi nella "*oggettiva violazione dell'obbligo di diligente custodia dei codici identificativi attribuiti ai fini dell'esecuzione* on line *delle operazioni previste dal contratto di* Internet Banking". Tale conclusione sarebbe confermata dalla normativa contrattuale in materia di operazioni e servizi bancari, ai sensi della quale è rimessa in capo al cliente "*ogni conseguenza dannosa che possa derivare dall'utilizzo illegittimo* [dei codici], *nonché dal loro smarrimento o sottrazione*"; "*Nel caso di smarrimento, di furto o indesiderata presa di conoscenza dei suddetti codici da parte dei terzi, il cliente è tenuto ad avvisare immediatamente la banca al numero verde* (...), *facendo seguire entro il giorno lavorativo successivo conferma a mezzo fax*".

Respingendo tutti gli addebiti mossi dai ricorrenti, la resistente afferma poi di avere predisposto un costante presidio dei sistemi informatici e di avere adottato dispositivi di sicurezza per l'operatività *on line* sui conti correnti del tutto adeguati rispetto all'evoluzione tecnologica. In particolare, sono forniti, oltre al "codice identificativo cliente", due chiavi di autenticazione: una *password* di primo accesso da modificare a cura del cliente e una *password* dinamica che, sulla base delle indicazioni fornite dal server al momento dell'accesso, viene tratta dalle ventiquattro matrici numeriche riportate su una "*security card*".

La sicurezza dei presidi informatici è periodicamente sottoposta a verifiche da parte di un soggetto terzo, leader del settore. Recentemente, a conclusione delle analisi effettuate, la banca ha anche provveduto a denunciare presso la polizia postale alcuni siti clone, non autorizzati, appositamente realizzati per catturare le chiavi di autenticazione dei propri clienti.

In relazione a quanto precede, la resistente chiede che il ricorso sia integralmente respinto.

DIRITTO

La controversia rimette in capo al Collegio una duplice valutazione concernente, da un lato, la congruità e l'adeguatezza dei sistemi di sicurezza predisposti dalla banca e, dall'altro, la condotta tenuta dai clienti alla luce degli obblighi di custodia dei codici di accesso.

Quanto alla condotta tenuta dal ricorrente, la resistente sostiene che, nel corso della prima segnalazione telefonica, uno dei cointestatari del conto corrente avrebbe riferito di un accesso ad un presunto sito clone attraverso un comune motore di ricerca. Tuttavia, la necessaria documentazione comprovante tale circostanza non è stata allegata agli atti, come sarebbe stato onere della resistente stessa a fronte di quanto affermato in proposito dal ricorrente. Se è vero che ciò avrebbe meritato considerazione ai fini della valutazione della condotta dei clienti e di una eventuale applicazione dell'art. 1227 c.c., il cliente assicura, peraltro, di avere adottato sempre la massima diligenza nella custodia dei codici di accesso e di non avere mai risposto a messaggi di *phishing*.

Appare, invece, fondata la contestazione del ricorrente alla banca di non avere adottato cautele particolari – ad esempio, contattandolo per ottenere conferma dell'autenticità dell'ordine (accorgimento, del resto, impiegato in precedenti occasioni per bonifici di

minore importo a favore di beneficiario italiano) – in relazione all'anomalia della disposizione, alla luce del profilo economico dei clienti, delle loro abitudini operative, della inusuale destinazione, dell'inconsueto indirizzo IP utilizzato, e, soprattutto, dell'importo in relazione alle disponibilità complessive del conto. Al riguardo, la banca non fornisce alcun elemento di replica.

Circa la lamentata inadeguatezza dei sistemi di sicurezza predisposti dalla resistente, in quanto avrebbero consentito la intrusione da parte di terzi non autorizzati, è da rilevare che il sistema di sicurezza della banca (sopra descritto) tende ad adeguarsi ad una metodologia a due fattori, scelti fra i seguenti tre: "*qualcosa che l'utente conosce (es.: password/PIN)*"; "*qualcosa che l'utente possiede (es.: smart card, token, OTP, Sim cellulare)*"; "*qualcosa che l'utente è (es.: caratteristiche biometriche)*".

Peraltro, le modalità "non hardware" di generazione delle *One Time Password* – come quella adottata dalla resistente – offrono indiscutibilmente minori garanzie di sicurezza, rispetto ai sistemi informatici di autenticazione, ormai di gran lunga prevalentemente diffusi.

Comunque, è da ritenere che a prescindere dagli accorgimenti tecnici di sicurezza, assuma rilievo – e sia destinato ad assumerne in futuro sempre maggiore – il dovere dell'intermediario di provvedere ad un monitoraggio continuo delle transazioni, per riscontrare eventuali anomalie che possano essere indice di attività illecite. Adempimento rispetto al quale l'attività della resistente è stata chiaramente inadeguata.

Circa la distribuzione del rischio e dell'onere della prova nelle ipotesi di utilizzo fraudolento del conto corrente mediante funzionalità *on line,* in sede di controdeduzioni la resistente richiama una disposizione contrattuale, simile ad altre già riscontrate in contratti per la prestazione del servizio di *internet banking*, ai sensi della quale sono rimesse a carico del cliente le conseguenze dannose rivenienti "*dall'utilizzo illegittimo* [dei codici]*, nonché dal loro smarrimento o sottrazione*".

E' da tenere presente però che sulla materia è intervenuto il d.lgs. n. 11/2010 (in particolare v. gli artt. 6, 7, 8, 11, 12) il quale, pur recependo in larga parte gli indirizzi già affermatisi nella prassi contrattuale, assicura una più incisiva ed inderogabile tutela dell'utente di servizi di pagamento, in specie se consumatore. Il complessivo quadro normativo avvalora pertanto l'idea, già elaborata in dottrina, di una c.d. responsabilità da *status* in capo all'intermediario che – in considerazione della propria elevata professionalità – sarebbe tenuto ad adottare le misure e gli standard di sicurezza più evoluti e, come tali, idonei a garantire la clientela.

Ciò soprattutto circoscrivendo alla colpa grave la rilevanza esimente per l'intermediario dei comportamenti del cliente: colpa grave, la cui rilevanza, secondo i prioncipi generali, deve ovviamente essere provata da chi ne invochi la ricorrenza.

Va considerato, infine, l'essersi ormai consolidando un orientamento dell'ABF tendente ad attribuire all'intermediario la responsabilità delle operazioni compiute fraudolentemente per l'inadeguatezza dei presidi di sicurezza adottati, rispetto agli standard tecnologici disponibili al tempo della transazione contestata (*ex multis*, Collegio di Napoli, decisione n. 688/10).

P.Q.M.

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo di € 24.800, oltre interessi al tasso convenzionale a far data dal 04/08/2010.

Il Collegio dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 quale contributo alle spese della procedura e alla ricorrente la somma di euro 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ENRICO QUADRI