

IL COLLEGIO DI ROMA

composto dai signori:

Dott. Giuseppe Marziale.....	Presidente
Avv. Bruno De Carolis.....	Membro designato dalla Banca d'Italia
Prof. Avv. Giuliana Scognamiglio.....	Membro designato dalla Banca d'Italia [Estensore]
Prof. Avv. Dario Casa.....	Membro designato dal Conciliatore Bancario e Finanziario per le controversie in cui sia parte un consumatore
Dott.ssa Daniela Primicerio.....	Membro designato dal C.N.C.U.

nella seduta del 14.01.2011 dopo aver esaminato

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

Fatto

Il cliente è cointestatario con la moglie di un conto corrente bancario con operatività *on line*, avendo aderito nel 2000 alla proposta contrattuale di pari oggetto dell'intermediario, che gli ha garantito la sicurezza del servizio.

Egli ritiene di essere stato vittima di malfattori capaci di forzare il sistema di sicurezza informatica della banca, avendo rilevato il 30 ottobre 2009 dal proprio estratto conto *on line* l'emissione di due ordini di bonifico, entrambi a favore di un medesimo soggetto, a lui sconosciuto, risultato poi residente in un Paese dell'Europa orientale; si tratta di bonifici da lui non autorizzati, datati 26 e 28 ottobre 2009, per un importo totale di € 6.361,32. Il cliente lamenta la scarsa sicurezza del servizio *on line* e dichiara che solo alcuni giorni dopo l'illecita sottrazione di somme per cui è causa ha ricevuto dalla banca, presso il proprio

domicilio, un dispositivo token, avente la funzione di rafforzare la sicurezza delle transazioni on line. Esperita infruttuosamente la fase del reclamo, proponeva ricorso a questo Collegio, chiedendo la restituzione delle somme fraudolentemente sottratte.

Nelle proprie controdeduzioni l'intermediario ribadiva quanto già affermato, imputando la responsabilità dell'accaduto all'incauta custodia, da parte del cliente, dei codici di accesso al conto corrente *on line*; entrambe le operazioni, infatti, erano state disposte attraverso il corretto inserimento dei tre codici di accesso, nei limiti delle disponibilità del conto e senza alcun indice di anomalia, per cui ai sensi dell'art. 66 del contratto dovevano imputarsi al cliente e comunque considerarsi da lui autorizzate. Secondo la banca, i servizi on line che essa offre alla clientela sono caratterizzati da standards di sicurezza elevati; dal 19 ottobre 2009 essa aveva messo gratuitamente a disposizione dei clienti un dispositivo (cd. O-Key) che genera codici operativi monouso, aumentando così il tasso di protezione per ciascun cliente; precisava infine che il servizio di SMS Alert del cliente era stato disattivato qualche giorno prima della esecuzione delle due operazioni contestate.

Chiedeva quindi all'ABF di respingere l'istanza del cliente perché infondata.

Riguardo alla circostanza dell'avvenuta disattivazione del servizio di SMS Alert alcuni giorni prima dei prelievi fraudolenti, si deve registrare che il medesimo evento si è verificato per decine di altre operazioni di prelievo non autorizzato da conti intrattenuti presso il medesimo intermediario. Dalle operazioni, contestate dai malcapitati clienti, sono scaturiti, nell'arco di alcuni mesi, 31 ricorsi a questo Arbitro.

Ritenuto il ricorso maturo per la decisione, questo Collegio lo ha esaminato in data 14 gennaio 2011.

Diritto

1. Si deve preliminarmente ritenere che la domanda del ricorrente rientri nella competenza del Collegio e che i presupposti per la presentazione del ricorso, previsti nel Provvedimento della Banca d'Italia del 18 giugno 2009 e successive modificazioni, si siano verificati nel caso di specie.



2. Passando ad esaminare il merito della controversia, giova premettere che la vicenda descritta nella parte narrativa della presente decisione, lascia supporre che il ricorrente sia rimasto vittima di una di quelle pratiche fraudolente che, mediante tecniche diverse, tendono all'acquisizione abusiva *on line* di dati personali altrui. Una prima tecnica, largamente diffusa, è nota con il nome di *phishing*, e consiste nell'invio di e-mail *fraudolente*, apparentemente provenienti da enti o istituzioni reali, e contenenti messaggi, immagini o informazioni diretti a suggestionare la vittima e ad indurla a connettersi ad una pagina web fittizia, ma del tutto simile a quella "vera"; in tale trappola il fruitore del servizio *on line* viene indotto a digitare i propri dati riservati, che vengono "pescati" dal malfattore, al fine di assumere l'identità del primo e accedere al suo posto ai servizi *on line*, ad esempio di internet banking. Un'altra tecnica consiste invece nella diffusione di codici malevoli, in grado di carpire le credenziali di accesso ai servizi bancari *on line* (c.d. trojan banking), senza alcuna cooperazione colposa da parte del cliente. Tali virus, in continua evoluzione e non sempre rilevati da software antivirus, sono in grado di autoinstallarsi, autoriprodursi, diffondersi ed esportare dati, sfruttando vulnerabilità presenti nei software di sistema e/o applicativi.

In un contesto siffatto, la clausola contrattuale invocata dall'intermediario (Art. 66 - *"Il Cliente è inoltre consapevole del fatto che l'utilizzo dei Codici di accesso comporta l'automatica attribuzione al Cliente delle istruzioni ricevute, con immediato effetto sugli strumenti finanziari e sui valori di pertinenza del Cliente. Pertanto il Cliente si obbliga a custodire i Codici di accesso con la massima cura e riservatezza, impegnandosi fin d'ora a non trascriverli o a rivelarli a terzi, né a conservarli insieme o ad annotarli in un unico documento e resta responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito dei Codici di accesso"*), in quanto esonera la banca da ogni responsabilità per i prelievi fraudolenti subiti dal cliente attraverso una delle tecniche suddette di furto di identità elettronica, appare riconducibile, nei rapporti fra intermediario e consumatore, alla previsione dell'art. 33, comma 2, lettera b) del codice del consumo (d. lgs. n. 206/2005), alla stregua del quale *"si presumono vessatorie fino a prova contraria le clausole che hanno per oggetto, o per effetto, di (...); b) escludere o limitare le azioni o di diritti dei consumatori nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale o di adempimento inesatto da parte del professionista"*. Pertanto, una clausola siffatta,

in quanto vessatoria, deve ritenersi inopponibile al consumatore: la legge citata (art. 36, comma 3) ne sancisce infatti la nullità, la quale *“opera soltanto a vantaggio del consumatore e può essere rilevata d’ufficio dal giudice”*.

3. Ciò posto, e cioè chiarito che la controversia non può essere risolta sulla base della citata clausola delle condizioni generali del contratto intercorrente tra la banca e il cliente, occorre affrontare il problema alla luce dei principi generali in tema di adempimento delle obbligazioni, nonché alla luce dei dati normativi di fonte comunitaria, in assenza – all’epoca dei fatti per cui è controversia – di una disciplina interna relativamente alla distribuzione del rischio inerente alle prestazioni di servizi di pagamento.

I fatti che hanno originato la presente controversia si sono infatti svolti anteriormente, sia pure di poco, al 1° novembre 2009, e cioè alla scadenza del termine fissato per il recepimento, negli ordinamenti nazionali, della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (cfr. art. 94 della direttiva medesima). All’epoca, dunque, la direttiva non era stata ancora attuata nel nostro ordinamento, né era scaduto il termine per il suo recepimento; tuttavia questo Collegio già in altre occasioni (cfr. ad esempio la decisione n. 665/2010) ha ampiamente illustrato le ragioni per le quali ritiene di dover prestare adesione all’orientamento secondo cui, vigente una determinata disciplina di fonte comunitaria, nella specie posta da una direttiva, e sebbene questa non sia stata ancora attuata nell’ordinamento nazionale, deve essere affermato il dovere del giudice nazionale di interpretare ed applicare il diritto interno in modo conforme alla disciplina dettata dalla direttiva, e comunque in modo tale da non addivenire ad un risultato contrario a quello a cui la direttiva mira (cfr. Corte di Giustizia comunità Europee, 5 ottobre 2004, cause riunite da C-397/01 a C-403/01, Pfeiffer): infatti, *“spetta ai giudici nazionali assicurare ai singoli la tutela giurisdizionale derivante dalle norme del diritto comunitario e garantirne la piena efficacia”*.

Alla stregua di queste premesse, si può affermare che ricorrono i presupposti per l’applicabilità, già all’epoca in cui si svolsero i fatti di causa (ottobre 2009), dell’art. 61 della citata direttiva, per il quale *“1. (...) il pagatore sopporta, a concorrenza massima di 150 EUR, la perdita relativa ad operazioni di pagamento non autorizzate derivante dall’uso di uno strumento di pagamento smarrito o*



rubato o, se il pagatore non ha conservato in condizioni di sicurezza le caratteristiche di sicurezza personalizzate, dall'appropriazione indebita di uno strumento di pagamento. /2. Il pagatore sostiene tutte le perdite relative ad operazioni di pagamento non autorizzate subite agendo in modo fraudolento o non adempiendo uno o più degli obblighi a lui incombenti (...) intenzionalmente o con negligenza grave. In tali casi il massimale di cui al paragrafo 1 del presente articolo non si applica”.

4. Nel caso di specie, la disposizione dei due bonifici contestati è avvenuta a totale insaputa del cliente e a favore di persona a lui sconosciuta e residente in un Paese lontano; il cliente, nel controllare diligentemente l'estratto conto, se ne è accorto a breve distanza di tempo ed ha immediatamente disconosciuto le due operazioni, sporgendo altresì denuncia-querela alla competente autorità pubblica.

Le richiamate circostanze confermano il collegamento eziologico tra i fatti per cui è controversia ed il *vulnus* inferto da terzi malfattori alla struttura informatica dell'intermediario; e, quand'anche non valgano ad escludere un comportamento colposo del cliente, certamente non valgono a dimostrare la sua colpa grave.

Pertanto, se – in applicazione della ricordata regola di fonte comunitaria – può essere giustificata l'imposizione di una franchigia di € 150 a carico del cliente, altrettanto giustificato è che, per il rimanente, la perdita sia posta a carico della banca. Ciò in applicazione del principio del “rischio d'impresa” ma anche in considerazione dell'obbligo della banca, alla stregua di un criterio di diligenza professionale qualificata (la “diligenza del buon banchiere”, connotata dal maggior grado di prudenza e di attenzione che la particolare qualificazione professionale dell'agente consente e richiede: cfr., *ex multis*, Cass., sez. I civile, 24 settembre 2009, n. 20543), nell'esecuzione di qualsiasi incarico conferitole dal cliente (cfr. art. 1856 c.c.), di adottare, nell'interesse dei clienti, tutti i presidi di sicurezza che l'attuale stadio di sviluppo della tecnica e della tecnologia consente (cfr. Cass., sez. I civile, 12 giugno 2007, n. 13777).

Si veda in particolare, l'obbligo di adottare – come suggerito nel c.d. Decalogo Abi Lab per le banche - le c.d. misure di sicurezza di secondo livello, idonee (attraverso per esempio l'uso di password o credenziali di accesso generate di volta in volta da un “token” e destinate a valere solo per pochi secondi) a rendere impossibile o comunque molto più difficile, allo stato attuale delle conoscenze



tecniche, il prelievo di denaro da parte di terzi che si siano illegittimamente impossessati, tramite una delle tecniche sopra ricordate, dei dati di un malcapitato correntista.

Tale dispositivo di sicurezza è stato in effetti adottato dall'intermediario resistente, ma solo pochi giorni prima dei fatti per cui è controversia. All'odierno ricorrente, esso venne consegnato soltanto alcuni giorni dopo quei medesimi fatti.

4. Ritiene pertanto il Collegio, pur nella consapevolezza di precedenti anche difformi di questo medesimo Arbitro Bancario Finanziario, che il ricorso vada parzialmente accolto e che al cliente debba essere restituito l'importo che gli è stato illegittimamente sottratto, pari a € 6.361,32, oltre gli interessi legali dalla data del reclamo (2 novembre 2009) e al netto della franchigia di € 150,00.

In ragione della soccombenza, sia pure parziale, l'intermediario è inoltre tenuto a versare alla Banca d'Italia il contributo alle spese della procedura nella misura di € 200,00 e a versare al ricorrente l'importo di € 20,00 quale rimborso della somma dallo stesso corrisposta alla presentazione del ricorso.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso nei sensi di cui in motivazione. Dispone inoltre che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e al ricorrente di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE MARZIALE