Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL COLLEGIO DI ROMA

composto dai signori:

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

nella seduta del 02.07.2010 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 cliente, titolare – unitamente al coniuge – di un conto corrente bancario a cui è annesso un servizio di home banking, riscontrava il 30 novembre 2009 n. 3 prelievi illegittimi dal proprio conto corrente per un importo complessivo di € 15.000,00; un primo effettuato in data 23 novembre 2009 pari ad € 4.184,11, un secondo del 25 novembre di € 5.184,11, un terzo del 28 novembre di € 6.184,11, tutti attraverso bonifici bancari on line non autorizzati, indirizzati al medesimo beneficiario, persona "totalmente sconosciuta" al cliente stesso. Il terzo bonifico veniva tempestivamente bloccato dal cliente ed il relativo importo riaccreditato. Il

1° dicembre 2009 il cliente si recava in filiale ed avanzava richiesta di rimborso, formalmente inoltrata a mezzo raccomandata il 4 dicembre 2009, chiedendo la restituzione delle somme prelevate "abusivamente e illegittimamente" dal proprio conto corrente, quantificabili in € 9.368,22 ed adducendo l'inadempimento della Banca ai propri obblighi di custodia del denaro depositato dai correntisti ex artt. 1834 ss. c.c.

L'intermediario, in data 28 gennaio 2010, dava riscontro negativo alla richiesta risarcitoria, imputando l'accaduto al fenomeno del c.d. phishing, con conseguente responsabilità esclusiva del cliente, il quale da contratto ha un obbligo di custodia e utilizzo corretto dei codici di accesso del conto corrente. Specificava altresì di aver adottato, conformemente al principio di diligenza professionale dell'intermediario, tutte le cautele e gli accorgimenti idonei, per evitare le frodi informatiche, e di aver messo a disposizione dei propri clienti il dispositivo di sicurezza denominato "token".

Il 15 marzo 2010 il cliente presentava ricorso a questo Collegio, chiedendo la restituzione di complessivi 9.368,22 Euro, prelevati "illegittimamente" il 23 e 25 novembre 2009. Ribadendo l'obbligo della Banca di custodire il denaro depositato dal correntista, sottolineava che l'unico beneficiario dei bonifici contestati era persona a lui "totalmente sconosciuta" e che, come constatabile dalle movimentazioni del conto corrente in oggetto, nessuna operazione bancaria on line, dall'apertura del conto ai prelievi non autorizzati, era stata effettuata dal cliente. Aggiungeva che, comunque, le credenziali di accesso al suo conto corrente on line erano sempre rimaste segrete ed in suo possesso.

Il 27 aprile 2010, l'intermediario, nelle proprie controdeduzioni, imputava l'accaduto al phishing e ribadiva l'obbligo contrattualmente assunto dal cliente di custodia e utilizzo corretto dei codici di accesso e l'impegno alla predisposizione di tutte le cautele e misure idonee, sulla base del criterio di diligenza professionale, al fine di prevenire le frodi. Chiedeva pertanto che il ricorso venisse respinto.

Ritenuto il ricorso maturo per la decisione, questo Collegio lo ha esaminato in data 2 luglio 2010.

Diritto

Si deve preliminarmente ritenere che la domanda della ricorrente rientri nella competenza del Collegio e che i presupposti per la presentazione del ricorso, previsti nel Provvedimento della Banca d'Italia del 19 giugno 2009, si siano verificati nel caso di specie.

Venendo al merito della questione, si osserva che il rapporto contrattuale fra il cliente e l'intermediario è regolato, per quanto attiene al profilo che viene in considerazione nella presente controversia, sulla base della seguente clausola: il cliente è responsabile della custodia e dell'utilizzo corretto dei codici di accesso al servizio di internet banking; nel caso di indesiderata presa di conoscenza di tali codici da parte di terzi il cliente è tenuto a farne immediata denuncia alla banca e alla competente autorità pubblica; fino al momento del blocco del servizio il cliente risponde di tutte le operazioni effettuate, anche se mediante indebito o illecito utilizzo da parte di terzi dei codici di accesso.

Ora, clausole siffatte, sulla base delle quali si vorrebbe affermare il principio della irresponsabilità della banca, non possono ritenersi valide: infatti, esse sono riconducibili, in considerazione del loro contenuto, 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, la clausola sopra riportata, 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*".

Ciò posto, e cioè messa fuori gioco la clausola inserita nel contratto che regola il servizio di internet banking, stipulato fra la banca ed 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.

La banca, nei rapporti contrattuali con il cliente, "risponde secondo le regole del mandato" (art. 1856 c.c.) e la diligenza a cui è tenuta va valutata con particolare rigore: come più volte statuito dalla giurisprudenza, anche della Suprema Corte,

"la diligenza del buon banchiere deve essere qualificata dal maggior grado di prudenza e attenzione che la connotazione professionale dell'agente consente e richiede" (cfr. di recente, fra le altre, Cass., sez. I civile, 24 settembre 2009, n. 20543).

In particolare, con specifico riferimento all'utilizzazione di servizi e strumenti, con funzione di pagamento o altra, che si avvalgono di mezzi meccanici o elettronici, "non può essere omessa (…) la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio (…); infatti, la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere" (cfr. Cass., sez. I civile, 12 giugno 2007 n. 13777).

Poiché si verte in tema di responsabilità contrattuale, è la banca convenuta a dover fornire la prova della propria diligenza; prova che nel caso di specie non è stata raggiunta, essendosi la Banca limitata a dedurre sul punto di aver profuso il proprio impegno nella informazione dei clienti in ordine al fenomeno delle frodi informatiche mediante phishing e nella predisposizione di dispositivi di sicurezza tecnologicamente evoluti, come il "token", che già dal settembre 20087 era stato posto a disposizione della clientela. Ora, la semplice "offerta" del dispositivo di sicurezza alla propria clientela non vale ad integrare quel grado di diligenza professionale che, secondo l'autorevole insegnamento sopra richiamato è richiesto alla banca, tanto più che nel caso di specie risulta dalla documentazione prodotta trattarsi di un cliente poco avvezzo all'utilizzo del mezzo informatico, a tal punto che nessun bonifico on-line era stato da lui mai eseguito.

Né la banca ha offerto la prova dell'inadempimento da parte del cliente al proprio obbligo di diligente custodia delle credenziali d'accesso al conto corrente; la negligenza, d'altra parte, com'è ormai ampiamente riconosciuto, non può ritenersi implicita nella circostanza che i bonifici sono stati comunque eseguiti mediante la digitazione di userid e password attribuiti a suo tempo al cliente, perché allo stato delle conoscenze tecnologiche, non si può affatto escludere la possibilità della sottrazione al cliente, da parte del terzo frodatore, dei codici identificativi attribuiti al primo per l'accesso ai servizi bancari *on line* o per l'utilizzo

di strumenti di pagamento, senza che al comportamento del cliente stesso possa riconoscersi alcuna efficienza causale nella produzione del fatto illecito (il "furto" dei detti codici d'accesso o numeri identificativi): cfr. *Rapporto ABI CIPA CNIPA sul furto di identità elettronica tramite internet*, Bancaria editrice, 2006, p. 23 ss.

Sul piano, poi, dell'assetto impresso dalla banca al rapporto contrattuale avente ad oggetto l'accesso del cliente al servizio di internet banking, deve osservarsi che, all'epoca dei fatti oggetto della presente controversia, era già entrata in vigore la Direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, pubblicata nella GUCE del 5 dicembre 2007.

Ora, l'art. 60 della citata Direttiva enuncia, in termini generali, l'obbligo di integrale rimborso, da parte del prestatore di servizi di pagamento e in favore del pagatore, dell'importo relativo ad un'operazione di pagamento non autorizzata; l'art. 61 specifica che, in deroga al precedente art. 60, il pagatore sopporta, fino alla concorrenza massima di € 150,00, la perdita relativa ad operazioni di pagamento non autorizzate derivanti dall'uso di uno strumento di pagamento smarrito o sottratto o di cui altri si è indebitamente appropriato; la franchigia di € 150,00 non si applica, con la conseguenza che le perdite rimangono a carico esclusivamente del pagatore, (soltanto) nel caso in cui questi abbia agito in modo fraudolento o con negligenza grave.

Le citate disposizioni della direttiva riprendevano a loro volta il contenuto della Raccomandazione n. 97/489 CE del 30 luglio 1997, il cui art 6.1 era così formulato: "Fino al momento della notificazione, il titolare sostiene la perdita subita in conseguenza dello smarrimento o del furto dello strumento di pagamento elettronico nei limiti di un massimale non superiore ai 150 ECU. Detto massimale non si applica ove il titolare abbia agito con colpa grave, in violazione dell'articolo 5, lettere a), b) e c), oppure in maniera fraudolenta". In termini non dissimili si era già espressa, in precedenza, la Raccomandazione CE. n. 88/590/CEE del 17 novembre 1988 (*Allegato*, § 8.3)

Si tratta di una disciplina evidentemente ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto

quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi. Si tende, in altri termini, a "spalmare" sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento, sì da evitare che esso gravi esclusivamente e direttamente sul singolo pagatore, in funzione dell'obiettivo di incrementare la fiducia del pubblico riguardo ai suddetti strumenti e di incentivarne l'uso e la diffusione, in quanto strumenti atti a facilitare e perciò a moltiplicare le transazioni commerciali, nell'interesse delle imprese, degli stessi utenti/consumatori, nonché, ovviamente, delle banche.

E' il caso di osservare, peraltro, che – all'epoca dei fatti per cui è causa (novembre 2009) – la menzionata direttiva comunitaria non era stata ancora attuata nel nostro ordinamento interno, pur essendo stata già emanata le relativa legge di delega, ma era spirato il termine assegnato per il suo recepimento (1° novembre 2009); l'attuazione, comunque, sarebbe intervenuta qualche mese dopo, con il d. lgs. 27 gennaio 2010, n. 11.

Al riguardo, è noto, ovviamente anche a questo Collegio, l'indirizzo interpretativo secondo il quale le disposizioni delle direttive comunitarie non ancora attuate o non correttamente attuate negli ordinamenti nazionali,quando siano (come si reputano essere quelle sopra richiamate) incondizionate e sufficientemente precise (c.d. autoesecutive) e sia scaduto il termine per il loro recepimento, sono immediatamente applicabili nei rapporti fra Stato (o pubbliche amministrazioni in genere) e soggetti privati (c.d. efficacia verticale), non invece nei rapporti "orizzontali" fra privati; tale indirizzo ha ricevuto in più occasioni l'avallo sia della Corte di Giustizia europea sia della nostra Corte Suprema (di recente cfr. Cass., sez. IV civile, n. 19771/2009; Cass., sez. I civile, n. 23937/2006).

Questo Collegio ritiene tuttavia che la limitazione così introdotta all'operatività negli ordinamenti nazionali delle disposizioni, di contenuto puntuale ed incondizionato, contenute in direttive comunitarie che sono ancora inattuate (o non correttamente attuate) e delle quali sia scaduto il termine per l'attuazione, non sia del tutto soddisfacente; condivide pertanto l'orientamento interpretativo di

maggiore apertura, assunto da autorevole dottrina, secondo il quale dette disposizioni, quando abbiano un contenuto sufficientemente dettagliato, preciso ed incondizionato, possono essere invocate, all'interno degli Stati membri, anche nelle controversie tra privati. Del resto, la Corte di Giustizia - pur riaffermando la propria adesione all'orientamento contrario alla diretta applicabilità delle direttive nei confronti dei soggetti privati - ha, in più di un'occasione, puntualizzato che "*il giudice nazionale deve interpretare il diritto nazionale per quanto possibile alla luce del testo e dello scopo della direttiva* [rimasta in tutto o in parte inattuata] *onde conseguire il risultato* [da essa] *perseguito*". Viene così a realizzarsi, come non si è mancato di rilevare, un effetto orizzontale "indiretto" delle direttive, mediante un'interpretazione "teleologicamente orientata alla realizzazione dei risultati prescritti" dal legislatore comunitario", che non deve rimanere circoscritta alle norme interne eventualmente introdotte per recepire la direttiva, ma deve essere esteso "*a tutto il diritto nazionale, per valutare in quale misura possa essere applicato in modo tale da non addivenire ad un risultato contrario a quello a cui mira la direttiva*" (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*".

Ora, l'insegnamento autorevole testé ricordato vale a corroborare ulteriormente l'assunto dell'impossibilità di risolvere la presente controversia alla stregua della regola, recepita nel contratto fra la banca ed il cliente, che addossa a quest'ultimo il rischio degli eventuali prelievi fraudolenti ad opera di terzi, facendo capo all'obbligo, che è contrattualmente imposto al cliente medesimo, di diligente custodia delle proprie credenziali di accesso al servizio di internet banking.

La questione deve essere invece risolta sulla base dell'opposto principio enunciato nella direttiva comunitaria, e cioè del principio, ispirato al criterio del rischio d'impresa, per cui il rischio dell'utilizzo fraudolento dello strumento informatico, salvo il caso in cui il cliente sia incorso in colpa grave (o abbia commesso dolo), ricade principalmente sulla banca, che è pertanto tenuta a rimborsare le somme illecitamente prelevate da terzi, al netto di una franchigia,

che costituisce la quantificazione forfetaria della frazione di rischio addossata al cliente e vale ad incentivarne comportamenti responsabili e prudenti, di € 150,00.

Nel caso di specie, la colpa grave del cliente non è stata provata dalla banca, su cui grava il relativo onere. Non può infatti sostenersi che sia indice di colpa grave il fatto che il ricorrente non si sia avvalso della possibilità, semplicemente offerta a tutti i propri clienti dalla banca convenuta, di utilizzare il dispositivo di sicurezza denominato “token”. Tale comportamento appare oltre tutto almeno in parte giustificato – sì da escludere in ogni caso la gravità della colpa – dalla circostanza, non contestata, che il cliente non si era mai avvalso dello strumento informatico per l’esecuzione di bonifici o di altre operazioni bancarie; dato – questo – che avrebbe dovuto, d’altra parte, richiamare l’attenzione della banca (nell’adempimento del dovere di diligenza professionale sopra richiamato), quando, nel mese di novembre del 2009, vennero da questa eseguiti ben tre ordini di bonifico per importi non irrisori nell’arco di pochi giorni e tutti a favore di un medesimo beneficiario.

Il Collegio, pertanto, in parziale accoglimento del ricorso, dichiara dovuto il rimborso nella misura richiesta dal cliente (€ 9368,22), detratto l’importo di € 150,00.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso nei sensi di cui in motivazione.

Dispone, inoltre, ai sensi della vigente normativa, 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 quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE MARZIALE