Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL COLLEGIO DI ROMA

composto dai Signori:

Dott. Giuseppe Marziale	Presidente
Prof. Avv. Andrea Gemma	Membro designato dalla Banca d'Italia
Dott.ssa Claudia Rossi	Membro designato dalla Banca d'Italia [Estensore]
Avv. Michele Maccarone	Membro designato dal Conciliatore Bancario e Finanziario
Prof. Avv. Maddalena Rabitti	Membro designato dal C.N.C.U.

nella seduta del 28/02/2013 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 ricorrente chiede il rimborso di tre transazioni del complessivo importo di € 17.242,00 fraudolentemente eseguite *on-line* il 14.4.2009, nell'arco di una mezz'ora, a danno del proprio conto corrente: una ricarica telefonica dell'importo di 10,00 euro, effettuata alle ore 13:14; un giroconto di € 8.475,00 disposto a favore di un altro correntista (A) del medesimo intermediario alle ore 13:32; un ulteriore giroconto di € 8.756,00, a favore di un terzo correntista (B) dell'intermediario, effettuato alle 13:39. I fondi così affluiti sui conti di A e B sono stati contestualmente e quasi interamente ritirati per contanti pochi minuti dopo, alle ore 13:42: dal conto di "A" sono stati infatti prelevati € 8.200,00 alla Cassa 10 dello sportello X dell'intermediario convenuto; dal conto di "B", sono stati prelevati € 8.400,00 alla Cassa 6 del medesimo sportello X dell'intermediario. La ricorrente, che dichiara di essersi avveduta della frode solo alcuni giorni dopo, il 20.4.2009, riferisce che nei giorni precedenti alla frode le risultava precluso l'accesso *on-line* al proprio conto. Riferisce altresì che dopo aver riscontrato tali difficoltà aveva ricevuto sulla propria casella di posta elettronica ordinaria un avviso con il quale le veniva segnalato il blocco del proprio codice dispositivo e fornito le istruzioni per sbloccare il conto. La ricorrente ammette di aver inconsapevolmente aderito

all'attacco di *phishing,* non avendo avvertito alcuna differenza rispetto alle consuete pagine *web* dell'intermediario.

La frode veniva immediatamente denunciata alle forze dell'ordine e all'intermediario; quest'ultimo rispondeva in via interlocutoria il 18.5.2009 rinviando ogni valutazione del caso all'esito delle indagini di polizia giudiziaria allora in corso.

La ricorrente rinnovava la richiesta di rimborso attraverso il legale di un'associazione di consumatori con reclamo del 1.3.2012 e, in assenza di risposta, adiva l'ABF con ricorso del 20.7.2012. Secondo la ricorrente all'epoca dei fatti il sistema informatico messo a disposizione della clientela era particolarmente vulnerabile e inadeguato, sia nella definizione dei codici di accesso al sistema dispositivo, sia per l'assenza di sistemi di *sms alert*; la ricorrente ravvisa altresì nel comportamento della resistente una responsabilità ai sensi degli art. 15 e 31 del codice della privacy (d. lgs. n. 196 del 2003), per non aver adeguatamente protetto la riservatezza dei propri dati personali. Chiede conseguentemente il risarcimento: a) del danno patrimoniale, in misura pari all'importo delle transazioni fraudolente (€ 17.242,00), con l'aggiunta della rivalutazione monetaria e degli interessi legali; b) del danno non patrimoniale, da determinarsi in via equitativa, in considerazione delle difficoltà patite a seguito della privazione di una così ingente risorsa finanziaria rispetto al proprio reddito.

Nelle controdeduzioni del 15.10.2012 l'intermediario ravvisa grave negligenza nel comportamento della ricorrente la quale, aderendo all'operazione di *phishing*, ha svelato le proprie esatte e complete credenziali per le disposizioni di addebito via internet, contravvenendo all'obbligo di segretezza dei codici stessi.

L'intermediario evidenzia altresì che il messaggio di *phishing* era pervenuto sulla casella di posta elettronica ordinaria della ricorrente, mentre all'epoca dei fatti era già attiva un'apposita sezione protetta della stessa casella, unidirezionale dall'intermediario verso il titolare dell'account, dove l'intermediario aveva già inviato a partire dal 17.12.2008 le proprie comunicazioni alla clientela; la ricorrente, definita assidua utilizzatrice dei servizi *on-line*, avrebbe già in passato ricevuto su tale casella protetta numerose conferme e ricevute delle proprie operazioni *on line* e avrebbe pertanto dovuto avvedersi della frode.

Per altro verso, l'intermediario riafferma la correttezza e la diligenza del proprio comportamento nell'aver dato seguito a transazioni regolarmente disposte con le

credenziali di accesso della cliente e nell'essersi dotato di sistemi di sicurezza certificati secondo i più rigorosi ed affidabili standard internazionali.

DIRITTO

Il ricorso è fondato, nei limiti di seguito indicati.

La vicenda si inquadra nella casistica del furto di identità elettronica più volte trattato dall'ABF anche in riferimento ad altri analoghi ricorsi avanzati nei confronti del medesimo intermediario.

La materia rientra nell'ambito di applicazione della raccomandazione 97/489/CE del 30.7.1997 e della direttiva comunitaria 2007/64/CE del 13 novembre 2007, che, come già più volte argomentato da questo Collegio (cfr., per tutte, la decisione n. 665 del 2.7.2010), in virtù del principio giurisprudenziale dell'interpretazione conforme, sono da ritenersi applicabili alla fattispecie qui considerata ancorché il d.lgs. n.11 del 27 gennaio 2010 che ha recepito la suddetta direttiva comunitaria sia entrato in vigore il 1 marzo 2010, in data cioè posteriore ai fatti oggetto del presente ricorso. Del resto, all'epoca dei fatti l'iter legislativo della legge delega 7.7.2009 (legge comunitaria 2008), finalizzata al recepimento anche della direttiva europea poc'anzi richiamata, risultava già avviato.

Entrano qui in considerazione gli artt. 59 secondo comma e 61 della citata direttiva (rispettivamente recepiti agli artt. 10, comma 2, e 12 del menzionato decreto legislativo) che attengono alla prova e alla limitazione della responsabilità del cliente.

Si ricorda che l'art. 59, secondo comma, della direttiva espressamente sancisce che l'utilizzo di uno strumento di pagamento, registrato dal prestatore del servizio, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dal titolare, né che questi abbia agito in modo fraudolento o non abbia adempiuto, con negligenza grave o intenzionalmente, agli obblighi espressamente indicati all'art. 56 della medesima direttiva: in altri termini, che non abbia adottato "tutte le ragionevoli misure per proteggerne le caratteristiche di sicurezza personalizzate".

A rafforzamento di tale principio, le citate norme stabiliscono che 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 euro, fatta eccezione del caso in cui il titolare abbia agito con dolo o colpa grave (cfr. art. 12 del d.lgs. n.11/2010, art. 61 della direttiva 2007/64/CE, oltre che art. 6 della raccomandazione 97/489/CE del 30.7.1997).

Conseguentemente, questo Collegio non può che riaffermare i principi dettati dal citato decreto legislativo e della direttiva comunitaria sottolineando che, in base ai criteri che regolano la responsabilità contrattuale (art. 1218 c.c.), l'onere di dimostrare la colpa grave o il comportamento fraudolento del cliente spetta all'intermediario, atteso che la spendita non autorizzata di uno strumento non assume il valore di una prova della negligenza del titolare.

Si tratta pertanto di valutare, nel caso di specie, i comportamenti delle due parti: da un lato, se nel comportamento della ricorrente possano ravvisarsi e siano stati provati gli estremi del dolo o della colpa grave, tali da escludere le previsioni del complesso normativo citato che limitano ad un massimo di 150 euro la responsabilità del cliente in caso di frodi; dall'altro, se l'intermediario, nell'esercizio della propria attività professionale, si sia conformato ai necessari criteri di diligenza e correttezza, mettendo a disposizione strutture adeguate all'operatività offerta alla clientela ivi compresa una tecnologia di sicurezza aggiornata: condizione, quest'ultima, necessaria ma, ovviamente, non di per sé sufficiente ad assicurare la complessiva tenuta in sicurezza del sistema.

Quanto al comportamento della ricorrente che ha subìto un attacco di *phishing*, questo Collegio non può che osservare che l'aver digitato i caratteri che componevano la stringa dei codici dispositivi consentendo quindi ai malfattori di entrare in possesso delle proprie credenziali segrete configuri un colpevole atto di negligenza. Volendo qualificare il grado di tale negligenza, va considerato che l'operazione della quale si discute ora risale al 2009, epoca alla quale, come del resto già osservato in passato '*la percezione sociale della diffusione e della pericolosità del phishing non era così intensa da poter qualificare il comportamento del ricorrente "in termini di leggerezza o imprudenza straordinarie e assolutamente inescusabili*" (cfr. le decisioni n. 1426 del 6.12.2010 e n. 2850 del 27.12.2011); sicché è avviso di questo Collegio che alla ricorrente possa essere al più addossata una colpa lieve e comunque non tale da escludere le previsioni di favore stabilite dalla vigente disciplina di regolamentazione dei sistemi di pagamento. Tanto più che dalla descrizione dei fatti emerge sia che la mail

ricevuta dal cliente non fosse agevolmente riconoscibile, sia che di fatto alla cliente risultava precluso l'accesso al sistema web predisposto dall'intermediario. Né appare significativo al fine di delineare un'inescusabile colpa della ricorrente il fatto che fosse stato messo a disposizione uno specifico canale di comunicazione, apparentemente non utilizzato dai malfattori, innovazione, questa, che peraltro risaliva soltanto a pochi mesi prima.

Per altro verso, questo Collegio osserva che il servizio offerto dall'intermediario presentava evidenti fragilità che si desumono da svariati elementi quali: il fatto che l'accesso al sistema fosse stato bloccato prima dell'adesione della ricorrente all'attacco informatico; un sistema di codifica delle credenziali di accesso già all'epoca obsoleto ed inadeguato a garantire la sicurezza del cliente essendo superato da tipologie di credenziali basate su generatori casuali di *password* (cd. OTP generati da *token*) già invalse presso i principali operatori del mercato e solo più tardi adottate dall'intermediario convenuto; che non fosse stato offerto un sistema di *sms alert* che avrebbe potuto se non prevenire sicuramente contenere la dimensione della frode, specie se fosse intervenuto sin dalla prima transazione di 10 euro che con ogni evidenza costituiva un sondaggio della tenuta dell'operazione fraudolenta.

Inoltre, considerate le modalità di svolgimento della frode, con particolare riguardo alla tempistica degli atti, all'entità delle transazioni e ai soggetti coinvolti (le transazioni di giroconto e i prelievi si sono susseguiti nell'arco di pochi minuti ed a favore, per giunta, di conti intestati ad altri clienti dell'intermediario convenuto; i fondi così ottenuti sono stati immediatamente prelevati per contanti e per cifre molto significative), appaiono evidenti le carenze del sistema di controllo interno dell'intermediario incapace di bloccare la frode: tanto più che si è trattato, nella fattispecie, di importi di entità del tutto straordinaria ed inconsueta rispetto all'operatività della cliente; infatti, a fronte delle transazioni fraudolente, due delle quali superano ciascuna gli 8.000 euro, si osservano, sulla base dei tabulati prodotti dall'intermediario in merito ad una cinquantina di disposizioni on-line impartite dalla ricorrente nel periodo 2007-2012, transazioni prevalentemente costituite da poche decine di euro, con la sola eccezione di n. 5 disposizioni nessuna delle quali raggiunge gli 800 euro. Aspetti questi tutti che attestano una fragilità complessiva dei sistemi di sicurezza e di controllo complessivamente predisposti dall'intermediario come peraltro questo Collegio ha già in passato

avuto modo di sottolineare in analoghe e ripetute circostanze (cfr. tra altre, le decisioni n.2365 del 2011, e nn. 1913 e 2899 del 2012.

Tutto ciò premesso, constatato: che l'intermediario non ha portato evidenze atte a dimostrare la colpa grave o il dolo del cliente nella fattispecie rappresentata; che il sistema complessivamente messo a disposizione del cliente per l'accesso al sistema delle transazioni *on-line* e per la esecuzione delle disposizioni al momento della frode descritta non era in grado di assicurare adeguati standard di sicurezza, questo Collegio ritiene che l'intermediario resistente debba rifondere alla ricorrente l'importo indebitamente sottratto salvo l'applicazione di una franchigia di 150 euro e che sulla somma di € 17.092 così determinata l'intermediario resistente dovrà corrispondere gli interessi legali dalla data del disconoscimento delle operazioni contestate fino al soddisfo.

Quanto alla rivendicazione di un risarcimento dei danni non patrimoniali, questo Collegio, evidenziata l'assenza di elementi a supporto della richiesta, ritiene che la pretesa non possa essere accolta.

Il Collegio, infine, non può non stigmatizzare, a margine, della propria decisione, l'ingiustificabile ritardo dell'intermediario nel corrispondere alla legittima richiesta di rimborso presentata dalla propria cliente e l'inosservanza delle disposizioni in materia di reclami.

P.Q.M.

Il Collegio accoglie la richiesta di rimborso, al netto della franchigia di Euro 150,00; respinge ogni ulteriore pretesa.

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