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
Dr.ssa Claudia Rossi…….	Membro designato dalla Banca d'Italia [Estensore]
Avv. Michele Maccarone …… ……. …	Membro designato dal Conciliatore Bancario e Finanziario – per le controversie in cui sia parte un consumatore
Prof.ssa Liliana Rossi Carleo……	Membro designato dal C.N.C.U.

nella seduta del 13/04/2012 dopo aver esaminato
- il ricorso e la documentazione allegata;
- la relazione istruttoria della Segreteria tecnica,
- le controdeduzioni dell'intermediario e la relativa documentazione;

Fatto

Controllando il proprio estratto conto la parte ricorrente rilevava la sera del 13 luglio 2011 una disposizione di bonifico internazionale dell'importo di 5.638,00 euro, eseguita a sua insaputa alle ore 7.01 del mattino a favore di un beneficiario sconosciuto. Il giorno successivo denunciava l'accaduto alle forze dell'ordine, precisando di non aver mai ricevuto mail di phishing e di avvalersi per l'esecuzione delle transazioni on-line del particolare dispositivo generatore di password fornitole dall'intermediario; specificava inoltre che, per un bonifico nazionale di 6.541,00 euro regolarmente disposto alcuni giorni prima, l'intermediario le aveva chiesto telefonicamente un'apposita conferma.

La ricorrente provvedeva altresì a far verificare la propria postazione elettronica da un tecnico informatico il quale registrava problemi nel browser Microsoft Internet Explorer, dovuti ad un software malevolo, e la presenza di uno Spyware avente la funzione di raccogliere ed inviare a soggetti terzi le credenziali di accesso dell'utente. Concludeva, l'esperto, che tutte le credenziali della ricorrente potessero essere state "esposte, non per sua colpa o dolo, a terzi".

Non avendo ottenuto risposta dall'intermediario in merito al reintegro della somma fraudolentemente prelevata, la ricorrente si è rivolta a questo Collegio per il riconoscimento delle proprie ragioni.

Nelle proprie controdeduzioni l'intermediario resistente, in conformità con una posizione dallo stesso espressa in precedenti analoghi ricorsi che lo hanno interessato, ha confermato il proprio diniego argomentando che: 1) la domanda di rimborso deve essere rivolta all'indebito percettore; 2) Il comportamento della ricorrente è risultato gravemente negligente, 3) non può essere addossata alcuna responsabilità all'intermediario che ha eseguito una transazione "correttamente" disposta; 4) i propri sistemi informatici centrali risultano a tutt'oggi inviolati ed "assolutamente sicuri" a differenza dell'apparato informatico del cliente risultato, a suo dire, insicuro e non adeguatamente protetto; 5) tenuto conto dell'art. 1218 C.C., eventuali pretese risarcitorie nei confronti dell'intermediario sono ammissibili solo a fronte di un suo inadempimento, inadempimento che il ricorrente non ha contestato all'intermediario.

Nella fattispecie concreta il convenuto aggiunge che la transazione contestata è avvenuta "mediante il corretto inserimento di tutte le successive serie di riconoscimenti informatici indispensabili per l'esecuzione di tale operazione (bonifico estero)", ivi compresi: "l'utilizzo del primo codice univoco proposto da(l) sistema" … che deve essere digitato sull'apposito strumento generatore di password fornito dall'intermediario; il "corretto utilizzo" di tale strumento mediante inserimento della carta personale del cliente e del PIN collegato alla carta medesima, noto soltanto al cliente; la digitazione sul web dell'intermediario, appositamente dedicato, del codice generato dal dispositivo: strumento, questo, che "non (sarebbe) in alcun modo raggiungibile via web". L'intermediario imputa in particolare alla ricorrente di non aver adottato le misure necessarie al fine di garantire la sicurezza informatica minimale necessaria ad una diligente attività finanziaria on-line, la negligenza del cliente essendo attestata dalla perizia versata in atti dalla ricorrente medesima; inoltre, stigmatizzando il fatto che la ricorrente non ha fornito notizie in ordine allo stato di aggiornamento del suo p.c. prima dell'operazione disconosciuta e prima dell'intervento della ditta informatica, ipotizza che i virus siano stati "inoculati durante una precedente navigazione nel web effettuata in modo non protetto o con protezione scarsa, inefficiente o non aggiornata".

Diritto

Il ricorso è fondato nei limiti di seguito indicati.

La vicenda si inquadra nella casistica del furto di identità elettronica e pertanto, come già più volte osservato da questo Collegio nell'esame di analoghi ricorsi, deve essere valutata alla luce delle vigenti disposizioni normative in materia di servizi di pagamento, con particolare riguardo all'art. 10, comma 2 del d.lgs. n.11 del 27 gennaio 2010 che ha recepito la direttiva 2007/64/CE del 13 novembre 2007 e sancisce espressamente che "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento 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 dolo o colpa grave ad uno degli obblighi di cui all'art. 7": in altri termini, che non abbia adottato "tutte le ragionevoli misure per proteggerne le caratteristiche di sicurezza personalizzate".

A rafforzamento di tale principio, la vigente disciplina stabilisce 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 ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento" (cfr. art. 12, comma 3 del d.lgs. n.11/2010).

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.

Tutto ciò premesso, risulta essenziale per la risoluzione del contenzioso la verifica del comportamento delle due parti, essendo entrambe tenute a specifici obblighi: la custodia e la segretezza delle credenziali informatiche, per quanto riguarda il cliente; l'affidabilità e la sicurezza complessiva del servizio di pagamento offerto al cliente, per quanto riguarda l'intermediario; sicurezza, questa, che attiene sia al sistema informatico –centrale e periferico- sia al sistema organizzativo e di controllo.

Nel caso qui sottoposto alle valutazioni di questo Collegio l'addebito di grave negligenza addossato dall'intermediario al cliente sembra essere fondato sia sui particolari requisiti di affidabilità presentati dal generatore di password messo a disposizione del cliente, sia sulla perizia informatica disposta da quest'ultimo immediatamente dopo la scoperta della frode, perizia che attesta – come precedentemente rilevato - che il computer utilizzato dalla ricorrente è risultato affetto da virus informatici e che tutte le credenziali della ricorrente sono verosimilmente state esposte a terzi, deducendo da ciò che la stessa abbia contravvenuto alle regole contrattuali che impongono diligenza nella custodia delle credenziali informatiche.

Ora, se è indubitabile che il prelievo abusivo di fondi sul conto del cliente sia avvenuto per effetto di un atto di pirateria informatica, questo Collegio non può non osservare che la messa a disposizione dell'innovativo strumento di generazione della password non può essere considerata di per sé prova (presuntiva) della violazione degli obblighi di custodia in senso lato gravanti sul cliente; d'altro canto, resterebbe da provare che la ricorrente, per il solo fatto di aver subìto un attacco informatico, abbia tenuto una condotta gravemente negligente; in altri termini, è da dimostrare che l'attacco informatico ai danni della postazione del cliente sia riconducibile ad una sua condotta gravemente omissiva e negligente. Ostano a tale conclusione tanto l'affermazione del perito che nell'attestare la visibilità a terzi delle credenziali informatiche per effetto del virus esplicitamente esonera la ricorrente da ogni colpa o dolo al riguardo, quanto la stessa ammissione dell'intermediario, su cui grava, come è ben noto, l'onere di dimostrare la colpa grave del cliente, di non conoscere lo stato dell'apparato utilizzato prima della frode, essendosi egli limitato a formulare alcune ipotesi, vale a dire che il p.c. fosse non protetto o non adeguatamente protetto o non aggiornato. Per altro verso, emerge dalla vicenda che la ricorrente si sia prontamente accorta della frode e che altrettanto tempestivamente si sia adoperata per segnalare l'accaduto all'intermediario, tentando di bloccare l'operazione, e che abbia senza indugio fatto verificare da un esperto il proprio apparato informatico. Consta altresì che la ricorrente si è dotata sin dal 3.6.2010 del particolare dispositivo all'epoca da poco offerto dall'intermediario alla propria clientela, così denotando particolare sensibilità ai temi della sicurezza delle transazioni: elementi, tutti, che contrastano con il quadro di "grave negligenza" ipotizzato dall'intermediario.

I fatti complessivamente esposti fanno ritenere a questo Collegio che l'intermediario non abbia evidenziato elementi gravi, precisi e concordanti che lascino presumere una grave violazione in capo alla ricorrente dell'obbligo di custodia delle proprie credenziali, tali da far

venir meno le previsioni favorevoli al cliente disposte dal decreto legislativo sopra citato. Sicché, ad avviso di questo Collegio, e in applicazione del disposto di cui all'art. 12, comma 3, del citato decreto legislativo, l'intermediario dovrà rimborsare alla ricorrente l'importo di € 5.488,00 pari alla somma sottratta detratta la franchigia di 150,00 euro.

Quanto ai presidi di sicurezza disposti dal fornitore del servizio di pagamento, questo Collegio, pur prendendo atto che l'intermediario ha dotato il cliente di un dispositivo generatore di password, decisamente più avanzato rispetto alle credenziali statiche di primo livello, ritiene di dover evidenziare elementi di criticità nel sistema di controlli predisposti a presidio della sicurezza delle transazioni: ne è riprova il fatto che per un bonifico di importo di poco superiore disposto pochi giorni prima dalla ricorrente l'intermediario stesso avesse ritenuto opportuno acquisire una conferma preventiva, laddove nella transazione contestata che, riguardando un bonifico internazionale rivestiva carattere di maggiore delicatezza, siffatto controllo è venuto a mancare.

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