Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL COLLEGIO DI NAPOLI

composto dai signori:

- Prof. Avv. Enrico Quadri..... Presidente

- Prof. Avv. Ferruccio Auletta ……..... membro designato dalla Banca d'Italia

- Prof. Avv. Giuseppe Leonardo Carriero ..... membro designato dalla Banca d'Italia

- Prof.ssa Marilena Rispoli Farina ……. membro designato dal Conciliatore Bancario Finanziario per le controversie in cui sia parte un cliente consumatore (estensore)

- Avv. Roberto Manzione ……. membro designato dal C.N.C.U.

Nella seduta del 17.04.2012, 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 ricorrente, titolare di una carta prepagata rilasciata dall'intermediario resistente il 30.10.2008, chiede in sede di reclamo il rimborso della complessiva somma di € 730, addebitata in conseguenza di n. 13 operazioni di pagamento *on-line* eseguite in data 11.11.2011 e da lui disconosciute. Riferisce di aver provveduto all'immediato blocco della carta nonché a sporgere denuncia presso le autorità competenti.
L'intermediario, in sede di replica, con nota del 9.12.2011, contesta il diritto del ricorrente al rimborso in quanto *"il sito sul quale sono state effettuate le operazioni* (…) *viene identificato come sito sicuro, in quanto l'esercente (o l'*acquirer*) partecipa ai protocolli* 3D Secure *(un servizio di ulteriore verifica della genuinità e paternità delle transazioni su* web*)"*. La circostanza, a suo dire, impedirebbe di prendere qualsiasi iniziativa nei confronti della Banca che gestisce gli incassi del *merchant*. Evidenzia, infine, che le operazioni sarebbero avvenute con "*il corretto impiego delle credenziali di utilizzo della carta che sono di* […] *esclusiva conoscenza* [del cliente] *e della cui conservazione è responsabile".*
Il ricorrente ha successivamente anche precisato, in data 22.12.2012, di non aver mai divulgato a terzi i dati della propria carta; di non aver subito furti della stessa; di aver custodito le credenziali di accesso con la massima diligenza. Evidenzia di non essere "*mai stato iscritto al sito web del portale in cui risultano effettuate le transazioni*" e di non aver mai ricevuto alcuna comunicazione da parte dell'intermediario circa i pagamenti effettuati con il proprio nominativo.

In sede di successivo ricorso del 5.01.2012, nel reiterare la richiesta di rimborso avanzata in sede di reclamo, il cliente precisa di utilizzare la carta prepagata rilasciata dall'intermediario resistente "*saltuariamente per esigenze di natura personale e/o svago*".
Evidenzia l'applicabilità *ratione temporis* del D.lgs. n. 11/2010 adottato in attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento, in virtù del quale "*il cliente risponde delle operazioni disconosciute eseguite fraudolentemente da terzi entro il limite di € 150,00, salvo i casi di dolo o colpa grave, che tuttavia devono essere provati dall'intermediario e non si presumono*".
A sostegno delle proprie ragioni, rappresenta di aver prontamente contestato l'accaduto e che, in ogni caso, la negligente custodia dei codici di accesso sostenuta dall'intermediario non potrebbe presumersi e discendere unicamente dal loro utilizzo da parte di terzi. In merito al comportamento tenuto dall'intermediario, rappresenta che su quest'ultimo incombe l'onere di predisporre sistemi automatici di blocco delle operazioni in presenza di comportamenti "*anomali*", in quanto non in linea con l'operatività del cliente; ciò, come nel caso di specie, tenuto conto del numero delle operazioni (n. 13 disposizioni di pagamento) e del ristretto intervallo temporale (19 minuti) in cui queste sono state poste in essere. Richiama, a sostegno delle proprie ragioni le decisioni del Collegio ABF di Milano nn. 1812/11; 394/10; 1030/10.
Alla luce di quanto esposto chiede il "riaccredito di € 730,00", oltre interessi e rivalutazione monetaria dalla domanda al soddisfo, nonché il risarcimento del danno conseguente all'inadempimento contrattuale […] da liquidare in via equitativa ai sensi dell'art. 1226 c.c.
In sede di controdeduzioni, l'intermediario ritiene del tutto infondata la richiesta avanzata dal ricorrente, in quanto le operazioni contestate sarebbero state effettuate attraverso il corretto inserimento di tutti i codici identificativi del ricorrente (numero e scadenza della carta, nome e cognome del titolare, codice CVV2 riportato sul retro della carta e noto solo al portatore della medesima). Rappresenta che i dati dell'account *"*[…] *sono stati perfettamente utilizzati per mettere a segno l'operazione contestata. Ne consegue che* […] *gli apparati informatici utilizzati dal titolare per connettersi al web non potevano che essere viziati da una particolare fragilità operativa, per cui gli ignoti autori dei fatti in discussione sono stati facilitati dalla scarsa diligenza della titolare, nel mantenere od introdurre un adeguato ed efficiente livello di protezione informatica dei propri strumenti operativi, con particolare riguardo ai dati d'interesse finanziario"*
Espone che i frodatori avrebbero avuto accesso all'account informatico del titolare *"in virtù di quest'ultimo e suo malgrado"* ma comunque non per propria responsabilità.
Osserva poi che la somma relativa alle transazioni oggetto del ricorso, in esecuzione dell'ordine regolarmente impartito, è stata trasferita ai beneficiari, a cui dovrebbe semmai essere rivolta la richiesta di rimborso, citando giurisprudenza di merito.
Esclude che, nel caso di specie, sussistano i presupposti probatori *ex* art. 2697 c.c. per la dichiarazione di una responsabilità contrattuale ai sensi dell'art. 1218 c.c., richiamando altresì le disposizioni del contratto di rilascio della carta che prevedono l'obbligo di eseguire le disposizioni impartite mediante l'utilizzo dei corretti codici dispositivi, che valgono a far riconoscere il *cardholder* quale legittimo titolare, nonché gli obblighi di custodia e di riservatezza del titolare.
Ancora, a riprova della sicurezza del sistema informatico nell'esecuzione delle operazioni *on-line,* richiama le molteplici certificazioni conseguite dal sistema, rilasciate "*secondo i più rigorosi ed affidabili standard internazionali*"nonché le numerose campagne "*di informazione e sensibilizzazione della clientela"* realizzate per stimolare nei propri clienti l'attenzione necessaria a evitare l'impropria diffusione dei propri dati a terzi.

Invoca, infine, l'art. 1227, comma 2, c.c., in virtù del quale il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza. A suo dire l'imprudenza nella custodia della carta e dei codici personali, integrerebbe gli estremi della colpa grave nel comportamento del ricorrente. Chiede, pertanto, il rigetto del ricorso

DIRITTO

Il Collegio è chiamato a decidere un ennesimo caso di utilizzo fraudolento di strumento di pagamento, contestato nei confronti della resistente. Nel caso in esame, il ricorrente disconosce numerosi pagamenti *on line* effettuati con carta prepagata emessa dall'intermediario resistente nell'ottobre 2008.
Come in altre decisioni, assunte nei confronti di quest'ultimo, occorre in primo luogo verificare il rispetto, da parte del ricorrente, delle disposizioni dettate in materia di custodia della carta e dei codici di identificazione e, da parte della banca, dell'adozione di tutti i presidi atti a rendere sicuro lo strumento di pagamento e il sito utilizzato per le operazioni *on line.* Nella fattispecie, il cliente ha provveduto a bloccare la carta e a sporgere denunzia presso le competenti Autorità. Dal canto suo, la resistente non allega circostanze determinanti ai fini del diniego della domanda del cliente né fornisce alcun riscontro probatorio al fine di rimanere sollevato dall'onere del corretto adempimento delle obbligazioni contrattuali. Anche nell'ipotesi in esame, gli estremi fattuali e la condotta difensiva della resistente sono sostanzialmente corrispondenti a quelli dei casi precedenti che, pertanto, questo Collegio ritiene opportuno richiamare con riguardo alla presente lite (v., tra gli altri, Collegio ABF di Napoli, decisioni n. 2515/2011, n. 246/12, n. 247/12, n. 266/12).
Giova ricordare che la normativa di riferimento per la prestazione di servizi e strumenti di pagamento, anche *on line*, è contenuta nel d.lgs. n. 11/2010, di recepimento della direttiva sui servizi di pagamento. Siffatta disciplina prevede anzitutto che "quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione eseguita, l'utilizzo di uno strumento di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave ad uno o più degli obblighi di cui all'articolo 7" (art. 10, comma 2 d.lgs. n. 11/2010). Ne consegue non solo che l'utilizzo fraudolento dello strumento di pagamento non è sufficiente a imputare tale condotta al cliente, ma anche che non spetta a quest'ultimo l'onere di provare che la banca sia inadempiente agli obblighi di legge. Spetta, invece, all'intermediario provare che il cliente sia incorso in dolo o colpa grave rispetto agli obblighi di diligenza che le norme gli impongono, al fine di liberarsi dalla responsabilità sancita dal d.lgs. n. 11/2010 per le operazioni non autorizzate. A fronte del disconoscimento da parte del cliente, infatti, "Il prestatore dei servizi di pagamento rimborsa immediatamente al pagatore l'importo dell'operazione medesima (…)" (così, l'art. 11, comma 2, d.lgs. n. 11/2010). In numerose decisioni dei Collegi che compongono questo Arbitro, la valutazione del "comportamento" dell'intermediario assume particolare rilievo, in quanto è da ritenere che sia la mancata adeguatezza dei sistemi di sicurezza predisposti ad avere consentito l'illegittima intrusione da parte di terzi non autorizzati nell'utilizzo degli strumenti di pagamento. Quindi, con riferimento al caso in esame, non appaiono fondate le eccezioni della banca, basate sulla circostanza che l'operazione contestata sarebbe stata conclusa regolarmente e, conseguentemente, addebitabile al cliente, in quanto disposta tramite il corretto inserimento

di tutti gli elementi identificativi della carta (*userid, password*, numero e scadenza della carta, codice "CVV2"), mancando ogni concreto riscontro probatorio alle sue affermazioni circa la (grave) negligenza della ricorrente nella custodia dello strumento di pagamento e dei relativi codici.

In particolare, si deve osservare che per consentire le operazioni (bonifici, giroconti, *trading online*) gran parte degli istituti di credito utilizza da tempo - oltre ai normali codici di accesso al sito di *home banking* - anche una protezione "di secondo livello" o "rafforzata" (ulteriore *password* dispositiva, firma digitale, chiavette elettroniche personalizzate che creano una password "dinamica" diversa ogni 30 secondi, ad es. *Token, One Time Pass word*). Dal sito internet dell'intermediario si ricava, al contrario, l'informazione che soltanto dal mese di febbraio 2011 è attivo un nuovo sistema per l'effettuazione di operazioni dispositive on-line che prevede l'impiego di due strumenti: la carta prepagata e il telefono cellulare "associato alla carta" sul quale viene inviata via SMS la *password* dispositiva "usa e getta". Per le carte acquistate o attivate prima del 22.12.2010, come nel caso di specie, il passaggio al nuovo sistema di sicurezza rimane peraltro facoltativo; pertanto, il titolare è libero di continuare a effettuare le operazioni dispositive con la modalità precedente. Sta di fatto che al momento dell'operazione contestata non era presente alcuno dei sistemi di sicurezza più avanzati, basati cioè sul sistema di sicurezza c.d. di secondo livello. Né, dall'esame della documentazione disponibile si ricava alcuna informazione circa la fruibilità di servizi di *SMS*- o *mail- alert*, né circa le debite comunicazioni alla clientela sulla possibilità di aderirvi.

L'intermediario, rifiutando il rimborso, ha anche opposto che il sito sul quale sono avvenute le transazioni è un sito sicuro in quanto protetto dal sistema SECURE 3D. Il sistema in questione, va per precisione ricordato, viene considerato più sicuro in quanto richiede, oltre che altri sistemi di sicurezza, anche una password personale. L'esercente che aderisce al sistema, viene esonerato da responsabilità nel caso in cui il titolare disconosca l'operazione e la responsabilità passa dalla banca di appoggio dell'esercente alla società che ha emesso la carta. Tuttavia, la traslazione di responsabilità avviene se tutte e tre le parti coinvolte nel pagamento (esercente, emittente e titolare) hanno attivato il servizio, mentre se il solo esercente ha aderito, ma non anche l'emittente, né il titolare, non vi è un apprezzabile miglioramento delle condizioni di sicurezza nell'utilizzo della carta. Inoltre, la *password* richiesta per gli acquisti *on line* non è "dinamica" ma "statica" e il titolare della carta non sempre è obbligato a richiedere l'attivazione del sistema.

In definitiva, al momento dell'operazione in contestazione il sistema predisposto dall'intermediario non presentava caratteri di adeguata protezione e il carattere sicuramente "anomalo" delle operazioni contestate (effettuare in numero elevato su un sito scommesse con singolare vicinanza temporale e rapidità, assolutamente non consone al profilo del cliente) depone a favore della ricostruzione degli eventi formulata dal ricorrente e quindi per l'accoglimento della sua richiesta di rimborso.

Da ultimo, va contrastato anche un ulteriore argomento difensivo addotto in maniera quasi "standardizzata" dall'intermediario resistente (in questo come nei casi analoghi sopra citati) e consistente nel sollecitare il ricorrente a richiedere la restituzione della somma sottratta al terzo che se ne è appropriato fraudolentemente. Come più volte ribadito da questo Collegio, appare infondata l'affermazione, ripetutamente utilizzata dalla resistente, secondo cui sarebbe il cliente a dover agire nei confronti del percettore (che peraltro l'intermediario sostiene di aver identificato). E' evidente, invece, come dalla disciplina generale e speciale possa dedursi che gravi solo sull'intermediario la responsabilità di assicurare il corretto funzionamento del sistema, anche sotto il profilo dell'adeguato accesso ad esso degli utenti, e conseguentemente il rischio connesso all'eventuale azione di recupero nei confronti di soggetti beneficiari di operazioni fraudolentemente disposte (v., ad es., Collegio ABF di

Napoli, decisione n. 1163/2011). In senso conforme, cfr pure Collegio di Napoli decisione n. 245/2012, n. 266/2012 e 931/2012; da ultimo decisione n. 780 del 16.3.2012).
In merito alla richieste risarcitoria di danni, avanzata dal ricorrente, va ribadito che, per principio giurisprudenziale consolidato, spetta al danneggiato l'onere di fornire la "prova di un concreto pregiudizio economico subito ai fini della determinazione quantitativa e della liquidazione del danno" (cfr. tra le tante: Cass., Sez. I, n. 721 del 25/3/2009). In mancanza della "prova del danno nella sua esistenza", non può procedersi neppure a valutazione del danno stesso in via equitativa (v. Cass., Sez.III, n. 10607). In ordine, poi, ai danni non patrimoniali, va richiamato l'ulteriore principio giurisprudenziale in base al quale non sono meritevoli di tutela risarcitoria, invocata a titolo di danno esistenziale, i pregiudizi consistenti in disagi, fastidi, disappunti, ansie ed ogni altro tipo di insoddisfazione concernente gli aspetti più disparati della vita quotidiana che ciascuno conduce nel contesto sociale. Al di fuori dei casi determinati dalla legge ordinaria, solo la lesione di un diritto inviolabile della persona concretamente individuato è fonte di responsabilità risarcitoria **(s**i veda, in proposito, la decisione n. 572/12 del Collegio ABF di Napoli).
Pertanto, sotto questo profilo, il ricorso non va accolto, potendosi accordare solo la reintegrazione rappresentata dagli interessi legali dalla data del reclamo.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto al rimborso di € 730,00 oltre interessi legali dalla data del reclamo.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ENRICO QUADRI