IL COLLEGIO DI NAPOLI

composto dai signori:

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

- Dott. Comm. Leopoldo Varriale..... Membro designato dalla Banca d'Italia

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

- Prof. Marilena Rispoli Farina ……..…….Membro designato dal Conciliatore Bancario Finanziario (estensore)

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

nella seduta del 2.11.2010 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 ricorrente, titolare di una carta di credito, in data 12.3.2010 alle ore 9.52 riceveva un SMS che lo informava dell'effettuazione di un'operazione di ricarica, per € 2.451,00, di una carta prepagata; nel messaggio veniva altresì indicata una disponibilità della carta di credito pari a € 49,83 all'ora indicata.
Il cliente, non avendo compiuto l'operazione in questione, provvedeva a bloccare la carta tramite il call center alle ore 10:38; da una verifica sul sito web della banca riscontrava inoltre che la disponibilità della sua carta di credito, inizialmente pari a € 49,83, era passata dopo qualche ora a € 2.500,83 per poi ridursi nuovamente a seguito dell'addebito della contestata operazione di ricarica.
Il giorno successivo sporgeva denuncia presso la locale stazione dei Carabinieri e il 17.3.2010 formalizzava in banca, attraverso l'apposita modulistica, la comunicazione di disconoscimento dell'operazione. La somma in contestazione in un primo tempo veniva accreditata salvo buon fine sul conto del cliente per poi essere addebitata *"per chiusura pratica disconoscimento".*
Con reclamo del 9.4.2010, il ricorrente contestava di non aver ricevuto *"alcun chiarimento in ordine all'addebito e ai motivi della chiusura della pratica di disconoscimento"* e di non aver potuto conoscere *"gli estremi della carta* [prepagata] *destinataria dell'operazione fraudolenta"*. In tale sede, chiedeva il riaccredito della somma contestata adducendo l'esclusiva responsabilità della banca per avergli fornito *"una carta di credito aggredibile e vulnerabile, nonostante la presenza del microchip".*

In assenza di riscontro da parte della banca, il ricorrente, con nota del 10.5.2010, reiterava la richiesta volta a conoscere: il nominativo del titolare della carta destinataria dell'operazione fraudolenta, se tale carta fosse stata emessa dalla banca resistente, se la stessa risultasse clonata o rubata e, in quest'ultimo caso, se fosse stata presentata denuncia all'autorità competente. A quest'ultima nota la banca forniva riscontro il 19.5.2010 e confermava l'impossibilità di aderire alla richiesta di rimborso per i motivi esposti nella precedente comunicazione del 26.3.2010 precisando di non poter comunicare i dati richiesti per ragioni di *privacy*; segnalava comunque di aver prontamente fornito all'Autorità giudiziaria ogni elemento utile alle indagini in corso.

Risulta agli atti una lettera del 26.3.2010 con la quale la banca ha respinto la richiesta di rimborso avanzata dal cliente in quanto *"il movimento contestato è stato regolarmente eseguito attraverso la creazione di una carta virtuale ottenuta mediante l'identificazione con codice utente e password, a suo tempo affidati alla sua personale custodia, escludendosi ogni forma di clonazione".* Inoltre, prospettando la violazione degli obblighi di diligente custodia dei codici in capo al cliente, ha soggiunto che *"non spetta alla banca provare in che modo, eventualmente, ignoti malfattori ne siano venuti in possesso".*

Nel successivo ricorso il cliente, tramite il proprio legale, dopo aver esposto la vicenda nei termini su indicati, ha chiesto all'Arbitro di condannare la banca *"alla restituzione della somma di € 2.451,00 con interessi legali, oltre al pagamento delle spese e competenze legali".*

A sostegno della propria richiesta il ricorrente allega:

1. il reclamo del 9 aprile e quello del 10 maggio 2010;
2. le lettere della banca del 26 marzo e del 10 maggio 2010.

In sede di controdeduzioni l'intermediario, dopo aver rievocato i termini della vicenda, ha prospettato la possibilità che il cliente possa essere rimasto vittima di una truffa telematica attuata tramite il *phishing*. Quest'ultimo, ad avviso della resistente, esula dalla responsabilità della banca e può anzi essere reso possibile solo da comportamenti del cliente stesso. In merito alla erroneità e alla pericolosità di tali comportamenti - che comunque integrano previsioni contrattuali che riconducono al cliente la responsabilità di eventuali conseguenze dannose – nonché alle precauzioni da adottare è presente da tempo sul sito internet della banca una esaustiva pubblicità informativa.

L'intermediario, in termini invero generici, ha fatto presente di aver adottato da tempo *"tutte le misure e le cautele necessarie a prevenire i tentativi di frode, provvedendo ad un costante e rigoroso controllo del sistema informatico, che ha confermato la sua inviolabilità"* anche nel caso di specie. Sono stati altresì introdotti *"strumenti informatici e di supporto"* dei quali lo stesso ricorrente ha potuto beneficiare, ricevendo immediata segnalazione dell'operazione ed essendo posto in condizione di evitare il protrarsi della truffa.

Ha infine osservato che le cautele predisposte dalla banca sono state vanificate da comportamenti del cliente, che hanno reso possibile l'acquisizione dei codici poi utilizzati per effettuare l'operazione contestata e tali da integrare la responsabilità per colpa grave ai sensi delle previsioni contrattuali *"anche alla luce degli ormai consolidati interventi di codesto stesso Organismo"*.

Alla luce delle considerazioni esposte ha chiesto al Collegio di respingere il ricorso.

Oltre alla documentazione prodotta dal ricorrente ha allegato:

1. copia del modulo "contestazione carte di pagamento" presentato dal ricorrente in data 17.3.2010;
2. copia della denuncia presentata il 13.3.2010 dal ricorrente presso la locale stazione dei Carabinieri;
3. le istruzioni di sicurezza per i servizi via internet pubblicate sul sito della banca;
4. un contratto del 17.12.2002 relativo ad una carta di credito prepagata, diversa da quella oggetto del presente ricorso;

5. il contratto del 10.1.2006 relativo all'abilitazione ai servizi on line e le relative condizioni di utilizzo.

Con nota del 1° ottobre 2010 il ricorrente ha ritenuto opportuno precisare di non aver mai ceduto a terzi la carta di credito e di non averne mai divulgato i codici.

DIRITTO

Su casi di utilizzo fraudolento della carta di credito questo Collegio si è più volte pronunziato, condividendo l'orientamento maturato anche dai Collegi di Roma e di Milano, nel senso di una valutazione più rigorosa della posizione dell'intermediario rispetto a quella del cliente nella ripartizione delle responsabilità. Ma vi è da sottolineare che il Collegio di Milano (si veda tra le altre la decisione n. 46 del 15 febbraio 2010) ha sì stabilito che "*la banca la quale offre servizi on line alla propria clientela ha il dovere di adempiere il proprio obbligo di custodia dei patrimoni dei clienti con la diligenza professionale richiesta dall'art. 1176 co.2 c.c., predisponendo misure di protezione … idonee ad evitare l'accesso fraudolento di terzi ai depositi dei propri clienti, o a neutralizzarne gli effetti"*, ma ha inoltre stabilito che "*La violazione dell'obbligo di diligenza da parte della banca non esclude, però, la colpa concorrente del titolare del conto on line, ex art. 1227 c.c., per incauta custodia dei codici di accesso al servizio, nella ipotesi in cui l'operazione fraudolenta sia avvenuta mediante l'uso dei codici in suo possesso*."Non di tale avviso si è mostrato questo Collegio, nella decisione n. 196 del 2.4.2010, in base alla considerazione della natura restitutoria e non risarcitoria della domanda del ricorrente.

In analogo caso e nei confronti del medesimo intermediario resistente, il Collegio di Roma n. 899 del 6/9/2010**,** ha accolto il ricorso e dichiarato l'intermediario tenuto al rimborso della somma indebitamente sottratta. In senso conforme anche questo Collegio, nella decisione n. 482 del 3.6.2010,dove si è sostenuto che *"la domanda di rimborso del ricorrente è fondata e meritevole di accoglimento, essendo non condivisibili le osservazioni dell'intermediario con cui si allega la mancanza di diligenza del cliente, che non avrebbe "riconosciuto" il rischio della frode informatica*" e che "*appare a questo Collegio che, ai fini della decisione, vadano, innanzitutto, considerati i comportamenti del cliente ricorrente, il quale ha diligentemente provveduto a denunciare tempestivamente la presunta "frode informatica". Avendo il cliente stesso dichiarato di non aver fornito ad alcuno i dati necessari per l'accesso, è ragionevole, in effetti, ipotizzare che il sistema di sicurezza predisposto dall'intermediario fosse inidoneo a tutelare l'esclusivo accesso del cliente alla utilizzazione del servizio."*

Ricordiamo infine la decisione di questo Collegio, la n. 190 del 2.4.2010, per la quale *"è pur vero che l'impossibilità di utilizzare la carta di debito senza la conoscenza del codice segreto, può indurre a presumere che il possessore della carta abbia mal custodito, o omesso di mantenere separati, codice e carta ,venendo meno ai suoi obblighi contrattuali. Ma è anche vero che molto spesso le chiavi di accesso ai servizi di pagamento vengono carpite con l'inganno, senza che il titolare abbia la possibilità di rendersi conto del fatto nell'immediato. In tale prospettiva si è posta la recente pronunzia del Tribunale di Roma, Terza Sezione, del 20 marzo 2006, che ha stabilito che in caso di uso illegittimo di una tessera Bancomat, l'ente che eccepisca la colpa concorrente del titolare, per custodia difettosa del codice personale, ha l'onere di provare concretamente tale negligenza, la quale non può ritenersi "in re ipsa" per il solo fatto che una tessera Bancomat, dopo il furto, sia stata utilizzata per prelevare contanti utilizzando il pin".*

Nel caso in esame la banca ha ammesso nelle controdeduzioni presentate la possibilità che il cliente possa essere rimasto vittima di una truffa telematica attuata tramite il *phishing,* ma intende addebitare allo stesso, per aver incautamente custodito la carta di credito e i codici di accesso, le conseguenze dannose dei suddetti comportamenti omissivi. Comportamenti

presunti, ma non dimostrati (dovendosi ritenere gravare sull'intermediario che l'adduce la prova della colpa, per di più grave, del cliente). Come pure la banca non dà adeguata giustificazione alla circostanza e al motivo – che depongono nel senso di una frode informatica conseguente a carenze nella sicurezza dei sistemi dell'intermediario - per cui la disponibilità della carta di credito, di piccolo importo, al momento della ricezione dell'SMS da parte del cliente, sia improvvisamente aumentata (fino a raggiungere la somma di € 2.500) consentendo l'addebito scaturente dall'operazione fraudolenta.

Vi è inoltre da segnalare che il sito internet dell'intermediario indica la tipologia di carta prepagata, destinataria della ricarica fraudolentemente effettuata, tra le tipologie di carte che le banche appartenenti al gruppo possono emettere e che il foglio informativo predisposto dall'intermediario prevede che la (relativa) ricarica possa essere effettuata *"sul sito, mediante utilizzo di un a carta di credito".*

Tutti gli elementi testé elencati inducono a condividere la posizione del ricorrente che sostiene l'esclusiva responsabilità della banca per aver fornito una carta di credito, la cui operatività risulta aggredibile e vulnerabile, nonostante la presenza del microchip.

Va infine ricordato che dal marzo 2010 è in vigore la disciplina comunitaria sui servizi di pagamento, attuata nel nostro ordinamento dal D.lgs. 27 gennaio 2010, n.11, la quale all'art 11 prevede che, nel caso in cui un'operazione di pagamento - come evidentemente nel caso qui esaminato - non sia stata autorizzata, il prestatore di servizi di investimento deve rimborsare immediatamente al pagatore l'importo dell'operazione medesima, qualora questi abbia adempiuto all'onere di comunicare senza indugio tale circostanza.

Quanto alla richiesta refusione delle spese legali, essa è da ritenere non competere non essendo contemplata dalla normativa relativa alla procedura dinanzi all'ABF, ove si prevede come del tutto volontaria ed eventuale la rappresentanza del ricorrente.

P.Q.M.

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto al rimborso della somma di € 2.451,00 a far data dal relativo addebito.

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