IL COLLEGIO DI MILANO

composto dai signori:

- Prof. Avv. Antonio Gambaro	Presidente
- Prof.ssa Antonella Maria Sciarrone Alibrandi	Membro designato dalla Banca d'Italia
- Prof. Avv. Emanuele Cesare Lucchini Guastalla	Membro designato dalla Banca d'Italia (Estensore)
- Dott. Mario Blandini	Membro designato dal Conciliatore Bancario Finanziario
- Dott.ssa Anna Bartolini	Membro designato dal C.N.C.U.

nella seduta del 29 novembre 2011, dopo aver esaminato:

- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria Tecnica.

FATTO

In data 11.02.2010 il ricorrente si recava ad uno sportello ATM della convenuta, per effettuare un prelievo con la propria carta di credito prepagata e si avvedeva di non avere più disponibilità a causa di un'operazione dallo stesso non eseguita, dell'importo di Euro 482,00. Si trattava, precisamente, di una ricarica *on line* di altra carta di credito prepagata.
Il 15.02.2010 il cliente sporgeva denuncia alla Pubblica Autorità, ivi precisando:

- di non aver provveduto al blocco della carta, *"dove è rimasta la somma di €0,02"*;
- che la carta *"è sempre stata in …* [suo] *possesso, di non averla ceduta a terzi, né averne subito il furto o lo smarrimento"*.

Il 02.10.2010 presentava reclamo all'intermediario, il quale dava riscontro negativo con missiva del 04.11.2010, comunicando in particolare quanto segue:

- *"i fatti … segnalati* [dal cliente] *rientrano nei casi di «phishing»"*;
- *"la transazione contestata è avvenuta con l'utilizzo di codici di accesso che sono di esclusiva conoscenza del cliente e della cui conservazione e utilizzo è responsabile"*;
- i servizi *on line* della convenuta stessa sono stati realizzati *"rispettando elevati standard di sicurezza"*;
- *"già da tempo"* su internet sono fornite alla clientela informazioni sul pericolo di frodi realizzate con il sistema di *phishing* e "[d]*eve essere peraltro cura del cliente adottare le opportune cautele in tali circostanze";*
- di aver provveduto ad estinguere la carta del cliente.

Il ricorrente, con ricorso all'ABF del 01.06.2011, ha riepilogato il fatto all'origine della controversia, riferendo di aver *"bloccato prontamente la carta"* una volta appreso della

transazione contestata e di aver dichiarato, in sede di reclamo, *"di non aver dato la … password per l'operazione effettuata senza il …* [suo] *consenso"*.
Ha, quindi, richiamato l'art. 10 del D.Lgs. 11/2010 e alcune decisioni dell'ABF, concludendo con la richiesta di rimborso della somma di Euro 482,00.
L'Intermediario ha trasmesso le proprie controdeduzioni via PEC il 01.08.2011, circa venti giorni dopo la scadenza del termine previsto dalla normativa.
Dopo una sintesi della vicenda, nella quale viene anche indicato il nominativo della beneficiaria dell'operazione contestata (dando altresì atto che la stessa ha prelevato *"la totalità della somma"* poco più tardi dell'accredito), la convenuta ha osservato, in parte riprendendo le argomentazioni della risposta al reclamo, che:

- dalle verifiche eseguite è risultato che l'operazione in oggetto è stata disposta mediante il corretto inserimento di tutti i codici identificativi del cliente (userid e password del titolare, numero della carta e data di scadenza della stessa, codice di sicurezza CVV2 riportato sul retro della carta);
- la domanda di rimborso del ricorrente è *"destituita di ogni fondamento"*, in quanto tale domanda dovrebbe essere rivolta a "*colei che, in base a quanto affermato dal ricorrente* [medesimo] *ne sarebbe l'indebita percettrice"*;
- il cliente non ha addotto *"la violazione di alcun obbligo contrattuale"* da parte della resistente, né ha documentato un suo eventuale inadempimento; al riguardo, vengono richiamate le previsioni contrattuali sottoscritte dal ricorrente relative all'uso personale della carta, alla responsabilità del titolare *"di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito della carta e del pin, nonché* d[a]l *loro smarrimento o sottrazione"* (art. 2), alla irrevocabilità delle operazioni compiute on line mediante l'utilizzo di uno o più strumenti di identificazione del titolare indicati nel contratto stesso (art. 7) ed al caso di smarrimento o sottrazione della carta (art. 8);
- l'uso dei codici personali identificativi del ricorrente pone in capo alla medesima convenuta *"l'obbligo contrattualmente stabilito di eseguire le transazioni ordinate con la digitazione delle credenziali"*, al quale *"corrisponde l'obbligo del …* [cliente] *di mantenere segreti tali codici e di accettare gli addebiti relativi ad operazioni disposte mediante l'uso degli stessi"*;
- i sistemi di sicurezza della convenuta sono "*certificati secondo i più rigorosi ed affidabili standard internazionali*";
- dunque, *"ha pienamente assolto agli obblighi contrattuali e di legge con la diligenza qualificata"*, non avendo, di converso, il ricorrente *"dichiarato di aver osservato tutti gli obblighi contrattuali assunti, né … in alcun modo provato la corretta custodia dei propri codici identificativi, in ordine alla quale si è obbligato"*;
- "*fin dal marzo 2005*" ha provveduto ad informare i clienti in ordine ai rischi di furto di identità informatica, fornendo concrete indicazioni a mezzo internet.

Nelle controdeduzioni, l'intermediario ha altresì citato alcuni precedenti della giurisprudenza di merito a sostegno delle proprie argomentazioni.
Richiamando, infine, l'art. 1227, secondo comma, cod. civ., con riferimento all'*"imprudenza nella custodia della carta e dei codici personali"* imputabile al cliente, nonché l'art. 2697 cod. civ., in relazione alla *"mancanza di contestazione di un inadempimento contrattuale da parte …* [della resistente stessa] *e della relativa prova",* l'intermediario ha concluso chiedendo che l'ABF *"respinga l'istanza del ricorrente, in quanto infondata per i motivi sopra esposti"*.
La Segreteria tecnica ha trasmesso al ricorrente, come richiesto, copia delle controdeduzioni con messaggio di posta elettronica del 10.08.2011.

DIRITTO

La questione centrale che questo Collegio deve affrontare per la soluzione del caso che ne occupa attiene ai doveri di custodia dei codici di accesso da parte del cliente che utilizzi una carta prepagata su Internet, da un lato e del grado di diligenza che si può richiedere all'intermediario in relazione all'erogazione di detto servizio, dall'altro lato.
Tuttavia, prima di passare all'esame del merito della questione, è bene ricordare in fatto alcuni aspetti essenziali ai fini della decisione.
Posto che il ricorrente ha contestato un'operazione eseguita con la propria carta di credito prepagata alle ore 11.52 del 09.02.2010, per un importo di Euro 482,00, il caso in esame riguarda fatti precedenti all'entrata in vigore delle previsioni del D.Lgs. 27 gennaio 2010, n. 11, che ha recepito nel nostro ordinamento la Direttiva PSD (Direttiva 2007/64/CE).
Nella denuncia alla Pubblica Autorità il cliente ha riferito di non aver bloccato la carta, poiché il prelievo contestato aveva esaurito la disponibilità sulla carta medesima; nel ricorso ha invece dichiarato di aver eseguito *"prontamente"* il blocco. La circostanza non appare, tuttavia, di particolare rilievo ai fini della decisione in quanto, da un lato, l'operazione contestata prescinde dal fatto che il blocco della carta sia o meno effettivamente avvenuto e, dall'altro lato, nella risposta al reclamo la convenuta ha comunicato di aver provveduto all'estinzione della carta *de qua*, come sembra evincersi anche dalle evidenze informatiche prodotte dalla stessa resistente.
La resistente ha, altresì, esibito la lista dei movimenti della carta di credito ricaricata per mezzo della contestata transazione, dalla quale risulta che la beneficiaria non ha prelevato l'intera somma accreditata a suo favore – come dichiarato dalla resistente nelle controdeduzioni – ma solamente l'importo di Euro 230,00.
Le condizioni contrattuali relative alla carta di credito prepagata, richiesta dal ricorrente in data 28.12.2009, prevedevano – in relazione alla questione oggetto del presente procedimento – quanto di seguito riportato:

ART. 2 - TITOLARITÀ DELLA CARTA E RESPONSABILITÀ PER LA CUSTODIA DELLA CARTA E DEL PIN

1. Titolare della Carta è nella versione standard il richiedente e, nella versione Junior, il minore indicato dal richiedente.
2. La Carta deve essere usata solo dal Titolare e non può essere in nessun caso e per nessun motivo ceduta o data in uso a terzi. Il Titolare è tenuto ad apporre la propria firma nell'apposito spazio sul retro della Carta all'atto della ricezione della stessa.
3. Ad ogni Carta è assegnato un codice personale segreto, denominato PIN (Personal Identification Number).Il PIN è un numero generato automaticamente da una procedura elettronica ed è pertanto sconosciuto anche al personale di Poste Italiane. Il PIN e la Carta sono consegnati al Titolare separatamente in buste sigillate, unitamente alle relative istruzioni di utilizzo.
4. Costituendo la Carta e il PIN, ai sensi del successivo art. 7, gli strumenti di identificazione e legittimazione del Titolare è interesse di quest'ultimo custodirli con ogni cura ed assicurarsi, in particolare, che il PIN rimanga segreto, non sia comunicato a soggetti terzi, non sia riportato sulla Carta né conservato unitamente alla stessa ovvero ai propri documenti. Il Titolare, dal momento in cui riceve la Carta e il relativo PIN, è responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito degli stessi, nonché del loro smarrimento o sottrazione, fatto salvo quanto previsto dall'art. 8.

ART. 6 - MODALITÀ D'USO DELLA CARTA

5. Poste Italiane non risponde dell'eventuale acquisizione di dati e informazioni riguardanti il Titolare da parte di terzi che abbiano in qualunque modo accesso agli strumenti operativi (ad esempio il personal computer) utilizzati dal Titolare per effettuare con la Carta, attraverso la rete internet, le operazioni dispositive e informative di cui al precedente art. 5. Il Titolare è responsabile, tenendone in ogni forma esonerata Poste Italiane, per i danni di qualsiasi natura eventualmente derivanti dall'aver il Titolare stesso incautamente fornito a terzi i propri dati personali e/o strumenti di identificazione e legittimazione (ad esempio PIN, password, etc).

ART. 7 - MODALITÀ DI RICHIESTA DEI SERVIZI FRUIBILI CON LA CARTA

1. Al Titolare può essere richiesta, a seconda del circuito internazionale di riferimento o del mezzo con il quale intende usufruire di un servizio fruibile con la Carta (terminale POS, ATM, Internet), l'apposizione della propria firma su moduli e ricevute o la digitazione del PIN di cui al precedente art. 2 ovvero l'indicazione del numero e della scadenza della Carta (entrambi riportati sul fronte della Carta) nonché del codice di tre cifre (CVV2) riportato sul retro della Carta.
2. Nel caso in cui sia richiesta per l'utilizzazione della Carta presso i terminali POS e ATM la digitazione del PIN, quest'ultimo costituisce l'esclusivo strumento di identificazione del Titolare della Carta.
3. Nel caso in cui all'atto dell'utilizzo della Carta sia richiesta l'apposizione della firma, questa dovrà essere conforme a quella presente sulla Carta, costituendo lo strumento tramite il quale l'esercizio convenzionato, Poste Italiane o le Banche possono verificare che il soggetto possessore della Carta sia il Titolare. Al Titolare potrà essere richiesta anche l'esibizione di un valido documento di riconoscimento.
4. Nel caso in cui sia richiesta per l'utilizzazione della Carta la digitazione del numero, della scadenza e del CVV2 presenti sulla Carta, la digitazione di tali dati costituisce l'esclusivo strumento di identificazione del Titolare della Carta.
5. L'uso della Carta con le modalità di identificazione previste nei commi precedenti ovvero con altre eventuali modalità che potranno in futuro essere introdotte da Poste Italiane e comunicate al Titolare, legittima quest'ultimo a compiere, a valere sulla disponibilità della Carta, le operazioni che la stessa consente di richiedere, con piena liberazione di Poste Italiane.
6. Le richieste di servizi con le modalità di cui al precedente comma 5 sono irrevocabili.
7. I pagamenti di volta in volta effettuati da Poste Italiane su richiesta del Titolare ai sensi del precedente comma 5 e le commissioni che non sono diversamente corrisposte, sono addebitate contestualmente da Poste Italiane, riducendo proporzionalmente il valore monetario per il quale è abilitata la Carta, in base alle registrazioni effettuate automaticamente attraverso internet o dallo sportello automatico (ATM) o dal terminale POS al quale è stata richiesta di eseguire l'operazione. Tali registrazioni costituiscono prova dell'operazione effettuata.
8. Il Titolare, in conseguenza di quanto previsto ai precedenti commi 5, 6 e 7, si impegna ad accettare tutti gli addebiti registrati da Poste Italiane derivanti da operazioni compiute con apparecchiature elettroniche che prevedono la digitazione del PIN o altre modalità di identificazione del Titolare, ed autorizza irrevocabilmente Poste Italiane ad addebitare sulla disponibilità della Carta stessa, qualora non siano percepiti attraverso altro mezzo, oneri, spese e commissioni pro tempore vigenti relativi all'operazione richiesta.
9. Il richiedente si riconosce obbligato al pagamento degli eventuali oneri di carattere fiscale, presenti e futuri, relativi alla Carta e al suo utilizzo.

Tra le clausole appena riportate assume particolare rilievo l'ottavo comma dell'articolo 7, che, peraltro, non rientra nel novero di quelle specificamente approvate per iscritto dal ricorrente e sulla quale si tornerà in prosieguo.

Secondo quanto riferito dall'intermediario, le disposizioni fraudolente sono avvenute mediante la digitazione di tutti i codici di accesso collegati alla carta (userid e password del titolare, numero della carta e data di scadenza della stessa, codice di sicurezza CVV2, riportato sul retro della carta).

Ebbene, così ricostruiti gli aspetti salienti della vicenda, non può che ricordarsi – come già si è avuto occasione di rilevare in altre occasioni – che è opinione assolutamente condivisa che sul cliente gravi l'onere di custodire con la massima diligenza le credenziali e/o i vari codici in suo possesso necessari per compiere operazioni bancarie di vario genere, siano esse prelievi per mezzo del servizio Bancomat, disposizioni di operazioni per mezzo di servizi *on-line* o pagamenti via Internet.

Il punto è essenziale per una corretta interpretazione del rapporto contrattuale, posto che, in linea generale, appare corretto affermare che al cliente sono opponibili le operazioni effettuate con la digitazione dei codici in suo possesso (indipendentemente da chi effettivamente le abbia disposte), proprio perché nell'utilizzo del servizio il cliente viene identificato esclusivamente mediante la verifica delle credenziali e/o dei codici di sicurezza che gli sono stati assegnati.

Quanto appena rilevato rende chiara sia la ragione dell'obbligo di diligente custodia di detti codici, sia il fatto che la violazione di tale obbligo di diligente custodia dei codici di identificazione e/o accesso comporti che il cliente sia chiamato a rispondere di ogni conseguenza dannosa derivante da un eventuale illecito utilizzo di tali codici da parte di terzi.

Dalle osservazioni che precedono deve, dunque, trarsi la seguente conclusione in linea generale, e cioè che – posto che nel servizio bancario relativo ad una carta di pagamento

che consente di effettuare anche pagamenti *on line*, l'uso corretto dei codici di accesso consente l'identificazione del titolare e l'autorizzazione dei pagamenti e/o delle operazioni disposte – le operazioni che siano state eseguite previa corretta digitazione di tali codici sono giuridicamente riconducibili al titolare del servizio.
Ciò chiarito con riferimento al primo dei due aspetti sopra evidenziati, deve ora affrontarsi la diversa questione del grado di diligenza dell'intermediario richiesto con riferimento alla prestazione di servizi bancari per via telematica, non senza aver prima rilevato che il genere di clausola quale quella contenuta nel comma 8° dell'art. 7 delle condizioni generali del contratto stipulato *inter partes* – non solo non risulta specificamente approvata per iscritto dal ricorrente, ma – in quanto finalizzata ad addossare totalmente sul titolare della carta di pagamento il rischio delle perdite derivanti dall'utilizzo della medesima da parte di soggetto non legittimato, è, *in parte qua*, quantomeno vessatoria (*ex* art. 33 codice del consumo), come già in altre pronunce si è avuto modo di rilevare.
Ora, secondo la consolidata opinione della dottrina e della giurisprudenza, l'attività bancaria, in quanto attività riservata, deve sottostare al canone di diligenza previsto dall'art. 1176, comma 2, c.c. ("diligenza dell'accorto banchiere") con conseguente adozione di tutte le cautele necessarie.
Come è noto, la diligenza professionalmente qualificata, cui fa riferimento il secondo comma dell'art. 1176 c.c., deve essere parametrata alle specificità tecnico-scientifiche della professione esercitata, trattandosi di nozione superiore e più specifica di quella relativa al buon padre di famiglia, richiamata dal primo comma dello stesso articolo. L'adempimento dell'obbligazione, quindi, deve avvenire con la diligenza "del regolato ed accorto professionista" (banchiere, nel caso che ne occupa), pena il risarcimento dei danni secondo i normali canoni della responsabilità contrattuale.
Per gli aspetti che qui interessano, tale parametro rileva in relazione alla specificità del servizio bancario oggetto di contestazione, che implica anche l'utilizzazione del canale telematico e l'uso di codici dispositivi.
In particolare, la valutazione coinvolge l'adeguatezza - considerati gli standard esistenti - dei presidi tecnici adottati dall'intermediario per rendere sicure le operazioni *on-line* da attacchi di pirateria informatica e/o dall'uso fraudolento degli strumenti di pagamento.
Sui presidi di sicurezza più idonei a fronteggiare il fenomeno della pirateria informatica non c'è attualmente una specifica normativa vincolante, anche se esistono diversi documenti, sia a livello nazionale che internazionale, che trattano della sicurezza dell'*e-banking* e, in particolare, della diversa efficacia dei vari meccanismi di autenticazione.
L'utente viene, infatti, autenticato attraverso la presentazione di credenziali. Generalmente si intende per "credenziale" uno o più dei seguenti elementi: qualcosa che l'utente "sa" (es. la password); qualcosa che l'utente "ha" (es. il token, che può contenere un certificato digitale); qualcosa che l'utente "è" (in questo caso si parla di caratteristiche biometriche, es. le impronte digitali).
Quando l'autenticazione dell'utente utilizza congiuntamente due di questi sistemi, si parla di autenticazione "a due fattori". Alcune modalità tecniche consentono, infatti, in associazione all'utilizzo di user-id e password, di effettuare un'autenticazione a due fattori: "Segreti condivisi", "Token" e "Tecnologie biometriche".
E' chiaro a questo Collegio che, al tempo del fatto all'origine della presente vertenza, esistevano già mezzi più efficienti per fronteggiare il fenomeno della pirateria informatica e questo costituisce ragione sufficiente per indurre a concludere che un sistema di protezione ad un solo fattore – sebbene composto da userid e password del titolare, numero della carta e data di scadenza della stessa, codice di sicurezza CVV2, non variabili di volta in volta – per permettere l'effettuazione di pagamenti e/o altre operazioni non può essere considerato misura idonea a proteggere adeguatamente il cliente.

In sintesi, dunque, nel caso all'origine del presente ricorso, da un lato, si può verosimilmente ravvisare una responsabilità del ricorrente in relazione alla mancata diligente custodia dei codici relativi alla carta di pagamento in suo possesso, dall'altro lato, non si può negare una concorrente responsabilità dell'intermediario che non abbia predisposto adeguati sistemi per proteggere più efficacemente i propri clienti con riferimento al rischio di truffe perpetrate per via telematica.
Questo Collegio, valutata la gravità delle rispettive colpe in relazione ai fatti illustrati e documentati, ritiene, dunque, di doverle ripartire nella misura del 50% in capo al cliente e nella misura del 50% in capo al resistente.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario restituisca al ricorrente la somma di € 241,00.
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
ANTONIO GAMBARO