COLLEGIO DI MILANO

composto dai signori:

(MI) GAMBARO	Presidente
(MI) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(MI) CONTINO	Membro designato dalla Banca d'Italia
(MI) SANTORO	Membro designato da Associazione rappresentativa degli intermediari
(MI) PERICU	Membro designato da Associazione rappresentativa dei clienti

Relatore CONTINO MARIA ELISABETTA

Nella seduta del 05/06/2014 dopo aver esaminato:

- il ricorso e la documentazione allegata
- le controdeduzioni dell'intermediario e la relativa documentazione
- la relazione della Segreteria tecnica

FATTO

Mediante il proprio legale, con lettera del 26 giugno 2013, il ricorrente chiedeva alla banca, presso la quale intratteneva un rapporto di conto corrente con operatività on-line, di rimborsargli la somma di Euro 2.988,00 illegittimamente sottrattagli il 23 dello stesso mese. Precisava di essersi avveduto dell'ammanco dopo che lo stesso giorno, ricevuta una comunicazione e-mail apparentemente proveniente dall'intermediario che dava notizia di accessi non autorizzati sul conto, aveva eseguito il *login* e "*aperta la home page del proprio home banking*".
La banca respingeva la richiesta, rilevando che l'operazione in questione era stata eseguita tramite il canale internet attraverso l'utilizzo dei codici di accesso corretti, evidentemente sottratti al titolare. Riferiva di essersi, inoltre, immediatamente attivata per bloccare l'operazione, ma senza successo, non riuscendo, pertanto, a recuperare quanto sottratto.
Insoddisfatto della risposta ricevuta, il correntista adiva l'Arbitro Bancario Finanziario con ricorso del 23 luglio 2013, per chiedere disporsi che la banca fosse tenuta a rimborsargli la somma di Euro 2.987,00, ribadendo le motivazioni già addotte con il reclamo e fondando la propria richiesta sulle previsioni del D.Lgs. n. 11 del 2010, eccependo al riguardo la mancata adozione da parte dell'intermediario di sistemi sicuri.

Accludeva copia della contabile di presa in carico dell'operazione in questione da parte dell'intermediario e della denuncia sporta alla locale stazione del Carabinieri, oltre al carteggio scambiato in fase di reclamo.
Con le proprie controdeduzioni, l'intermediario chiedeva rigettarsi la domanda in quanto immotivata e infondata. Riferiva, infatti, che l'operazione contestata, consistente nella ricarica di una carta prepagata, era stata effettuata tramite il servizio home banking con regolare utilizzo dell'apparecchiatura in dotazione del cliente, generatrice delle cosiddette *one time password* necessarie per disporre versamenti *on-line*. Rilevava come il sistema *home banking,* in dotazione del ricorrente, fosse dotato, infatti, di un sistema di protezione a due fattori, se non addirittura a tre, considerando altresì il successivo SMS di conferma.
Metteva in evidenza come lo stesso ricorrente avesse dichiarato di avere ricevuto un'e-mail dal carattere evidentemente fraudolento e dato esecuzione alle istruzioni ivi contenute. Ne conseguiva che l'operazione disconosciuta era stata resa possibile dalla colpa grave con cui l'utilizzatore aveva agito, violando così gli obblighi di custodia dello strumento di pagamento e dei dispositivi che ne consentivano l'utilizzo.
Segnalava, da ultimo, come l'importo dell'illecito trasferimento rientrasse ampiamente nel massimale contrattuale.
Offriva in comunicazione, oltre a copia del contratto di conto corrente con il ricorrente, l'e-mail, ritenuta un *phising,* che lo stesso cliente le aveva inoltrato, e le estrazioni informatiche relative all'operatività contestata.

DIRITTO

La questione sottoposta all'Arbitro Bancario Finanziario attiene alla richiesta di rimborso della somma indebitamente sottratta da un terzo, formulata dal titolare di un conto corrente con operatività *home banking* acceso presso la resistente.
Risulta applicabile, alla fattispecie in esame, il D.lgs. n. 11 del 2010 recante la disciplina dei servizi di pagamento, in quanto i fatti di cui si controverte risalgono a giugno 2013.
Il provvedimento normativo in questione è stato oggetto di numerose decisioni dell'Arbitro Bancario Finanziario, incentrate sui diversi obblighi rispettivamente gravanti sul prestatore e sull'utilizzatore di servizi di pagamento e sulla ripartizione delle relative responsabilità.
Mentre l'art. 8 del Decreto enuclea gli obblighi gravanti sull'emittente di uno strumento di pagamento, tra cui *in primis* quello di assicurare che i dispositivi personalizzati che consentono l'utilizzo di un sistema di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato al suo impiego, l'art. 7 precisa quelli al cui rispetto è viceversa tenuto l'utilizzatore, stabilendo che questi debba avvalersi dello strumento ricevuto nel rigoroso rispetto delle condizioni contrattuali che ne disciplinano l'emissione e l'uso, e che, tal scopo, non appena ricevuto uno strumento, debba adottare tutte le misure idonee a garantire la sicurezza dei dispositivi personali che ne permettono l'impiego. L'utilizzatore è tenuto pertanto alla custodia non solo dello strumento in sé, ma in generale anche dei dispositivi che ne consentono l'uso.
Ciò chiarito, si devono verificare i criteri adottati dal D.lgs. n. 11 del 2010 per la ripartizione delle responsabilità tra le parti in caso di compimento di operazioni non autorizzate, e segnatamente, nel caso che ci occupa, di prelievi effettuati attraverso l'operatività via internet.
Atteso che la *ratio* sottostante al provvedimento è quella di incentivare l'uso degli strumenti di pagamento rispetto al contante, la richiamata normativa viene ad istituire "*un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori*" (così decisone del Collegio di Coordinamento n. 991 del 2014) soprattutto attraverso le disposizioni degli artt. 10 e 12 del Decreto, creando un'evidente disparità di trattamento tra

fornitore e utente del servizio. E', infatti, onere del prestatore di servizi provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti, senza al contempo che l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento sia di per sé 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 a uno o più degli obblighi di cui all'art. 7. Al contempo, infatti, l'utilizzatore può sopportare, per un importo comunque non superiore a Euro 150,00, la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento, salvo "*quando abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7 con dolo o colpa grave*". Mentre nel primo caso, la sua responsabilità sarà limitata a detto importo, nel secondo non potrà viceversa giovarsi di limitazione alcuna.
In linea con gli arresti della Corte di Cassazione, l'Arbitro Bancario Finanziario ha individuato e qualificato la colpa grave come "*quel comportamento consapevole dell'agente che, senza la volontà di arrecare danno agli altri, operi con straordinaria o inescusabile negligenza*" (cfr., anche per i richiami ivi contenuti alla giurisprudenza dell'ABF, la decisione del Collegio di Coordinamento n. 6168 del 2013).
Per stabilire su quale delle parti, ed eventualmente in che misura, gravino le conseguenze di operazioni fraudolente, si tratterà quindi "*di valorizzare le singole e specifiche circostanze relative alle fattispecie di volta in volta sottoposte all'esame dell'ABF, in ordine della quali è necessario verificare se – alla luce degli elementi costitutivi della fattispecie, stretti in intima connessione tra di loro – sia possibile desumere in capo all'utilizzatore un comportamento gravemente colposo*" (così decisione del Collegio di Coordinamento n. 6168 del 2013, cit.), della cui prova è onerato il prestatore di servizi di pagamento, che potrà fornirla anche attraversi indizi gravi, precisi e concordanti, salva l'irrilevanza, sopra accennata, del semplice utilizzo, in sé considerato, di uno strumento di pagamento registrato dal prestatore di servizi di pagamento.
Nel caso in esame, non è stato contestato quanto affermato dalla resistente circa il fatto che l'utilizzo del servizio di *home banking* fosse possibile solo attraverso l'impiego di due fattori di autenticazione. Al contempo, è lo stesso ricorrente a dichiarare di avere "*erroneamente*" dato corso a quanto richiesto da una comunicazione e-mail sospetta.
Sotto il primo profilo, in assenza di anomalie, deve ritenersi quindi che la parte resistente abbia adempiuto con la dovuta diligenza, quella dell'accordo banchiere, ai propri obblighi contrattuali, mettendo a disposizione del cliente un sistema per il compimento di operazioni *on line* basato sull'utilizzo contemporaneo di più fattori, ossia quel tipo di sistema che anche questo Collegio non ha mancato di considerare il più sicuro (ancorché si tratti necessariamente di sicurezza relativa) e tale da garantire la migliore tutela degli utilizzatori in base all'attuale stato della tecnica. Va al riguardo ricordato che le credenziali per il compimento di operazioni via internet possono consistere in qualcosa che "sa" (ad esempio la *password*), in qualcosa che "ha" (ad esempio l'apparecchio che genera *password* del tipo usa e getta) e in qualcosa che "è" (dovendosi avere riguardo a sue caratteristiche biometriche, come le impronte digitali). Un sistema è a più fattori quanto impone l'utilizzo di almeno due di tali credenziali.
Secondo quanto precisato dalla resistente, il cliente poteva, infatti, accedere al servizio solo immettendo la *password* già conosciuta e la *one time password* generata dall'apposito apparecchio di cui era dotato; una nuova *one time password* era necessaria poi per eseguire l'operazione. Da ultimo, all'utente veniva inviato un SMS contendente un ulteriore codice da inserire per autorizzare l'operazione. Nella denuncia ai Carabinieri è lo stesso cliente a dichiarare di avere "*inserito le credenziali e le password di accesso*",

utilizzando il plurale. Da uno dei documenti prodotti dalla resistente contenente i dettagli informatici dell'operazione risulta, inoltre, che il codice di conferma era stato inviato con un SMS al numero di cellulare del correntista riportato nel contratto per l'attivazione del servizio *home banking*.

Quanto, viceversa, al comportamento del ricorrente, è lo stesso ad avere attestato nella denuncia sporta ai Carabinieri di avere ricevuto, da un indirizzo di posta elettronica apparentemente riconducibile alla banca, il seguente messaggio: "*Gentile cliente, il tuo account è stato temporaneamente sospeso per attività insolite, abbiamo trovato che l'accesso al tuo conto non era autorizzato, effettua il login per verificare il tuo conto cliccando qui*", ammettendo quindi: "*Erroneamente ho cliccato sul link il quale ha aperto la home page dell'home banking della mia banca …, ho quindi inserito le credenziali e le password di accesso all'area privata, e ho constatato che sul conto era stata detratta la cifra di 2988,00 comprensivi di commissioni*".

Nonostante, come attestato dal Collegio di Coordinamento (con la decisione n. 3498 del 2012), debba escludersi che l'adozione di un sistema a due fattori da parte dell'intermediario comporti di per sé la sussistenza di una colpa grave del cliente, nel caso in esame, non può ritenersi che il comportamento dell'utilizzatore sia scevro da colpa e in particolare da colpa grave, anche se la natura fraudolenta dell'operazione non sembra in contestazione. Utilizzando un minimo di diligenza non avrebbe, infatti, potuto non accorgersi di avere ricevuto un messaggio di *phishing*, considerando innanzitutto che le banche non dialogano per posta elettronica con i clienti, se non per l'invio di estratti conto, e tenuto conto della genericità delle affermazioni, degli errori di punteggiatura e del tono confidenziale utilizzato al di fuori dei casi di "tu generico". L'esistenza di simili comunicazioni, che spesso riescono a sfuggire anche ai sistemi antispam, costituisce peraltro ormai fatto notorio.

Dovendosi, quindi, concludere che l'intermediario abbia adottato i dispositivi più sicuri in base allo stato della tecnica, adempiendo così agli obblighi sulla stessa gravanti che qui rilevano, e che il cliente si sia viceversa reso gravemente inadempiente all'obbligo di applicare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono lo strumento di pagamento, il Collegio ritiene, aderendo all'orientamento anche recentemente confermato (cfr. le decisioni n. 1873 del 2014 e n. 1302 del 2014), che la domanda del ricorrente non possa trovare accoglimento ex art. 12, 4° comma, del D.Lgs. n. 11/2010.

Qualora, infatti, l'utilizzatore di un sistema di pagamento non abbia adempiuto uno o più degli obblighi di cui all'art. 7 con colpa grave, sopporta tutte le perdite derivanti dalle operazioni di pagamento non autorizzate, senza che possa trovare applicazione il limite di Euro 150.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO