COLLEGIO DI MILANO

composto dai signori:

(MI) GAMBARO	Presidente
(MI) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(MI) ORLANDI	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro designato da Associazione rappresentativa degli intermediari
(MI) ROSSI	Membro designato da Associazione rappresentativa dei clienti

Relatore (MI) ROSSI

Nella seduta del 03/07/2014 dopo aver esaminato:

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

FATTO

Nel ricorso protocollato il 27/11/2013, la ricorrente, titolare di un conto corrente presso l'intermediario convenuto, riferisce che su detto conto sono state fraudolentemente realizzate transazioni non autorizzate.
In particolare, precisa che, in data 01/06/2013, verso le 18:00, il legale rappresentante dell'associazione ricorrente operava sul conto corrente di detta associazione per effettuare due bonifici a favore di propri collaboratori.
Dichiara di aver ricevuto, immediatamente dopo tale operazione, un messaggio *e-mail* da cui apprendeva che le operazioni effettuate erano state quattro, due delle quali relative ai bonifici di cui sopra e le altre due di ricarica di carte di credito intestate a soggetti del tutto sconosciuti.
Gli importi di tali operazioni non autorizzate erano pari ad € 2.997,00 la prima e ad € 2.998,00 la seconda, più € 1,00 di commissione per entrambe.
La ricorrente riferisce, in particolare:
- di aver immediatamente contattato la banca chiamando il numero verde, che risultava tuttavia sempre occupato, e di essersi messa in contatto, tramite un secondo numero verde, con un operatore il quale le consigliava di bloccare subito il conto *on-line*, digitando volutamente codici di

accesso errati per tre volte consecutive, e comunque dichiarava che avrebbe provveduto anche autonomamente a bloccare il conto;
- di aver chiesto espressamente all'operatore di bloccare tutti i bonifici in uscita e di avere ricevuto rassicurazioni in tal senso.
- di aver sempre operato dal medesimo computer e di non aver mai ricevuto né risposto a messaggi *e-mail* non identificati o provenienti da sconosciuti, né a maggior ragione a mail di *phishing*.

La ricorrente lamenta che, nonostante l'intervento dell'operatore, i bonifici fraudolenti sono stati tuttavia effettuati e contesta la carenza di sicurezza del sistema informatico dell'intermediario nonché la sua incapacità di gestire simili situazioni, domandando il rimborso della somma di € 5.995,00, pari all'importo complessivo dei due bonifici fraudolentemente effettuati da terzi sul suo conto corrente.

Nelle proprie controdeduzioni l'intermediario dichiara che in data 03/06/2013 il legale rappresentante dell'associazione ricorrente disconosceva formalmente due operazioni di ricarica di carte prepagate di terzi soggetti, effettuate tramite *home banking*, per un importo rispettivamente di € 2.997,00 e di € 2.998,00, presentando altresì denuncia presso il Compartimento di Polizia Postale e delle Comunicazioni, e dichiarando di non aver risposto ad e-mail fraudolente riconducibili al c.d. *phishing.*

Rileva l'intermediario che tali operazioni risultano confermate con regolare utilizzo dell'apparecchiatura c.d. "*o-key*" per la generazione delle cc.dd. "*one time passwords*" e che il sistema di *home banking* in dotazione alla banca è dotato di protezione c.d. "a due fattori" e pertanto, per accedervi è necessario compiere le seguenti attività: 1) una prima identificazione dell'utente attraverso verifica dell'*User-Id*, della *password* generale e della *one time password* prodotta dallo strumento *o-key* di cui sopra; 2) la successiva produzione di nuova *one time password* dispositiva per dare corso alla ricarica.

Per operazioni come quelle in esame, a detta dell'intermediario, è previsto un presidio di sicurezza aggiuntivo, costituito da un codice inviato al cliente tramite sms (cd. OTS)

L'intermediario allega le schermature di tracciatura delle operazioni effettuate dalla ricorrente, dalle quali si evincono gli inserimenti di *password* ad utilizzo singolo, ed afferma che essi possono essere noti solo al titolare del conto corrente o da lui solo generati. Ne desume che questi codici sono stati comunicati dalla ricorrente all'autore della frode, che li ha utilizzati per effettuare le ricariche contestate, e che in ciò si sostanzierebbe quella colpa grave del cliente atta ad escludere ogni pretesa responsabilità dell'intermediario, ai sensi degli artt. 7, c. 2, e 12, c. 3, d.lgs. n. 11/2010.

L'intermediario illustra inoltre in dettaglio i presidi di sicurezza adottati per impedire il verificarsi di comportamenti fraudolenti a danno dei clienti dell'istituto o dell'istituto stesso e pone in evidenza come il contenuto dei messaggi ricevuti dalla ricorrente durante il compimento delle predette operazioni poteva ben evidenziare il tentativo di truffa che si stava compiendo ai suoi danni. In particolare segnala che il sistema subordinava in modo esplicito la ricarica di carte di credito, che la ricorrente assume effettuata da terzi sul proprio conto corrente in modo fraudolento, all'inserimento del codice OTS pervenuto via sms al numero di cellulare indicato dal titolare e di cui si presume che solo quest'ultimo potesse avere conoscenza.

L'intermediario rileva, inoltre, come la ricorrente non abbia specificato di quali sistemi di sicurezza *antivirus/antispamming* fosse dotato il proprio computer precisando che tali sistemi di sicurezza sono normalmente idonei ad impedire frodi simili a quelle denunciate. Afferma che il proprio sistema informatico non può aver subito nessuna violazione e che comunque tale ipotesi non è stata allegata dalla ricorrente, la quale invoca la responsabilità della banca unicamente per non essere intervenuta successivamente al compimento della truffa.

Quanto al proprio comportamento successivo al compimento della frode, segnala che, stante l'immediata esecuzione delle operazioni al momento dell'inserimento dei codici, non poteva trovare effetto il successivo disconoscimento operato dalla ricorrente.

Precisa, tuttavia, che, non appena ricevuta notizia dell'accaduto, ha provveduto a richiedere il blocco delle carte destinatarie delle ricariche contestate e al recupero del residuo ancora presente con riaccredito a favore della ricorrente per le somme di € 194,00 (in merito alla ricarica di € 2.998,00) e di € 79,00 (in merito alla ricarica di € 2.997,00).

Chiede pertanto che l'ABF non accolga il ricorso e la relativa richiesta restitutoria ivi formulata.

DIRITTO

La fattispecie oggetto del presente ricorso è una frode informatica che la ricorrente asserisce essere stata perpetrata a sua danno attraverso lo strumento dell'*home banking.* In materia, la disciplina di riferimento è il d. lgs. 11/2010 relativo alla prestazione di servizi di pagamento che pone in capo all'intermediario specifici obblighi volti a garantire la sicurezza dei sistemi di pagamento (obblighi particolarmente rilevanti ove tali sistemi operino in ambiente informatico) e l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati (v. art. 8 d. lgs. 10/2011). Impone altresì all'utilizzatore di tali servizi un uso corretto e diligente dello strumento di pagamento, ma pone a suo carico le perdite derivanti dal furto, smarrimento o indebito utilizzo dello strumento di pagamento solo laddove egli abbia agito con dolo o colpa grave ove abbia debitamente adempiuto agli obblighi di comunicazione all'intermediario (artt. 7, 9 e 12 d. lgs. 11/2010).
Sulla materia l'ABF si è pronunciato più volte e la questione della ripartizione delle responsabilità per frodi perpetrate attraverso l'*home banking* è stata portata anche all'attenzione del Collegio di Coordinamento che, nella Decisione 3498/12 ha operato un accurato censimento delle fattispecie di frode più diffuse ed ha puntualizzato i termini di valutazione delle questioni connesse.
In particolare, ha sottolineato il regime di particolare favore che il d. lgs. 11/2010 predispone per l'utilizzatore del servizio, cui consegue una ripartizione dei rischi collegati all'utilizzo di strumenti di pagamento in ambiente informatico sfavorevole all'intermediario, sul presupposto che questi sia la parte più attrezzata a gestire detti rischi e, in ultima analisi, il percettore dei vantaggi e delle efficienze legate all'utilizzo dei sistemi informatici di pagamento. Tale opzione giustificherebbe la speciale distribuzione dell'onere della prova di cui al citato decreto, che pone a carico dell'intermediario l'onere di dimostrare che l'operazione disconosciuta dall'utilizzatore sia stata correttamente autenticata, registrata e contabilizzata e che non vi siano state disfunzioni del sistema e delle procedure che abbiano potuto dare causa all'illecita intrusione di terzi. Giustificherebbe altresì la limitazione della responsabilità dell'utilizzatore ai casi di dolo o colpa grave laddove le comunicazioni dovute in tali casi all'intermediario siano state tempestivamente e correttamente effettuate.
Sul piano applicativo, particolare rilevanza assume l'individuazione degli adempimenti di protezione dovuti dall'intermediario al fine di garantire la sicurezza del sistema di pagamento e delle relative procedure, questione che risente, evidentemente, delle pratiche con cui vengono di fatto realizzati gli illeciti in questione.
Sul punto l'orientamento dell'ABF ha subito una progressiva evoluzione, proprio in considerazione dell'emersione di nuove pratiche di illecita violazione dei sistemi informatici di *internet banking*, capaci di superare le tecniche di protezione tradizionalmente predisposte dagli intermediari e generalmente ritenute di provata efficacia.
In particolare, il Collegio di Coordinamento ha rilevato che, se il sistema di autenticazione c.d. "a due fattori", rappresentato dal c.d. sistema OTP, con il collegato rilascio di *password* monouso, è stato considerato per lungo tempo efficace e sicuro, per la riservatezza dei codici assicurata all'unico detentore del dispositivo c.d. *token* (con la conseguente presunzione che ogni utilizzo improprio di tali codici da parte di terzi dovesse trovare causa nella mancata custodia o nella volontaria comunicazione degli stessi a terzi da parte del titolare), la casistica ha evidenziato nuove forme di intrusione nei sistemi informatici di *internet banking* più subdole e capaci di sfuggire anche all'occhio dell'utilizzatore diligente. In particolare, si è rilevata la diffusione di particolari *malware* (c.d. "*man in the browser*") capaci di captare i codici digitati dall'utilizzatore in tempo reale, attraverso una finestra del tutto confondibile con quella ufficiale, e distinguibile solo dal codice di protocollo di trasferimento ipertestuale che, nel caso di specie, appare privo della "s" finale. Si tratterebbe, pertanto, di un particolare sistema di *phishing*, cui l'utilizzatore involontariamente coopera. Il suo comportamento non può tuttavia valutarsi come colposo, data la quasi assoluta impercettibilità dell'intrusione e l'attuale scarsa conoscenza, nell'ambiente dei "non addetti ai lavori", di simili tecniche di captazione dei dati.

Venendo al caso di specie, l'intermediario ha dimostrato di aver predisposto tutti i sistemi di sicurezza c.d. "a due fattori", incrementati dal codice aggiuntivo trasmesso via sms. Ciò non di meno, come osservato, tali presidi non sarebbero stati sufficienti ove fosse entrato in azione un *software* malevolo come quello appena descritto. Ed in effetti le circostanze di fatto fanno presumere che si sia trattato di un'intrusione del tipo descritto, data la tempistica in cui l'illecito è stato perpetrato. Dall'esame delle tracciature delle operazioni, risulta infatti che le operazioni di ricarica di carte di credito sono state effettuate nei momenti immediatamente successivi a quello in cui la ricorrente ha dato disposizioni per i due bonifici, secondo tempi e modalità che risultano tipici del modo di operare dei predetti *malware* (cfr. Collegio di Milano, dec. 25/13).
Né rileva, sul punto, l'allegazione dell'intermediario secondo cui la ricorrente avrebbe potuto e dovuto accorgersi della truffa di fronte ad un messaggio del sistema che richiedeva esplicitamente, ai fini della ricarica delle carte di credito, l'inserimento dei propri codici di autenticazione, poiché è del tutto verosimile, considerate le modalità in cui operano detti *malware*, che, al comparire del citato messaggio, i codici fossero già in mano al terzo intruso in quanto già captati nel momento in cui la ricorrente aveva effettuato la prima operazione.
Del pari non può avere rilevanza l'eccezione dell'intermediario relativa alla mancata prova, da parte della ricorrente, di aver attivato tutti i presidi normalmente idonei ad evitare tali intrusioni (*antivirus e antispamming*) perché la specifica utilità dell'*home banking* risiede proprio nella sua fruibilità anche fuori dalle sedi di residenza o di lavoro dell'utente (locali pubblici, alberghi ecc.) e che pertanto non può essere considerata una negligenza dell'utente il fatto di non provvedere a sistematiche bonifiche prima di ogni utilizzazione del predetto strumento (v. la citata decisione del Collegio di Coordinamento 3498/12)
Il Collegio esclude pertanto che il comportamento tenuto dalla ricorrente nella vicenda in esame possa dirsi connotato da colpa grave. Rileva inoltre la tempestività della comunicazione dell'illecito formulata dalla ricorrente all'intermediario ai sensi dell'art. 7, 1° comma, lett. b), d. lgs. 11/2010, risultante dalle comunicazioni prodotte in atti. Sul punto, in particolare, reputa irrilevante l'eccezione dell'intermediario relativa all'immediata esecuzione delle operazioni di ricarica di carte di credito, dal momento che tale circostanza non è suscettibile di compromettere la tempestività dell'adempimento degli obblighi informativi posti a carico dell'utilizzatore ove effettuati "senza indugio", come nel caso di specie risulta essere avvenuto.
Il Collegio dà atto altresì che l'intermediario ha provveduto a recuperare a favore della ricorrente le somme di € 194,00 e € 79,00 sulle due carte di credito oggetto della ricarica fraudolenta, come risulta dai documenti prodotti in atti.
Ciò premesso il Collegio ritiene che nel caso di specie le perdite derivanti dalla frode denunciata dalla ricorrente debbano essere sopportate dall'intermediario, al netto della franchigia di € 150,00, ai sensi dell'art. 12, comma 3, d. lgs. 11/2010 e di quanto già corrisposto alla ricorrente.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario provveda a corrispondere alla parte ricorrente la somma di € 5.572,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO