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) RONDINONE	Membro designato da Associazione rappresentativa degli intermediari
(MI) TINA	Membro designato da Associazione rappresentativa dei clienti

Relatore TINA ANDREA

Nella seduta del 07/10/2014 dopo aver esaminato:

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

FATTO

In data 09/09/2013, il ricorrente, recatosi presso la filiale dell'intermediario resistente con cui intratteneva un rapporto di conto corrente, dall'esame della lista movimenti del conto verificava la sottrazione dell'importo di Euro 48.903,24. La somma risultava, infatti, oggetto di bonifico bancario estero eseguito tramite home banking "*nella tarda serata tra il 5/6 settembre*" con beneficiario una società con sede in Bulgaria e causale "*leasing,doc.1*". Il ricorrente provvedeva, pertanto, a disconoscere l'operazione. I funzionari dell'intermediario ivi presenti "*preso atto dell'evidente frode a mezzo internet […] rassicuravano*" il ricorrente, comunicandogli che avrebbero "*prontamente*" chiesto il blocco delle somme alla banca beneficiaria.
Non ricevendo alcun riscontro dalla propria filiale, il ricorrente inoltrava reclamo in data 18/09/2013, presentando, inoltre, denuncia-querela dell'accaduto, con la quale precisava che il proprio coniuge gli aveva comunicato delle "*circostanze anomale*": aveva, infatti, ricevuto un sms contenente dei "*codici di sicurezza che normalmente la banca inviava per concludere una operazione di bonifico online*", operazione che, però, non era stata effettuata. La moglie del ricorrente ignorava, pertanto, l'sms ricevuto, "*ritenendolo un errore di sistema*". Nel riscontrare il reclamo del ricorrente, l'intermediario respingeva la

richiesta di restituzione delle somme "*illegittimamente prelevate*", sostenendo la mancata attivazione "*del sistema di avviso nel sistema home banking, e (…) la probabile riconducibilità dell'accaduto a malware presenti sul pc e possibili risposte a richieste di credenziali non originali*".

Ricevuto il riscontro negativo dell'intermediario, il ricorrente ha presentato ricorso all'ABF, con il quale ha evidenziato come le giustificazioni addotta dall'intermediario appaiano "*generiche ed insufficienti*" e come il comportamento dell'intermediario resistente sia "*privo totalmente della necessaria diligenza nell'esecuzione del mandato*". Il ricorrente ha, inoltre, precisato quanto segue:

- di utilizzare il sistema di home banking "*prevalentemente*" al fine di monitorare il proprio conto corrente compiendo "*sparute operazioni bancarie e fornendo (…) quale utenza telefonica collegata, quella intestata al proprio coniuge*";
- fino al luglio 2013 non aveva "*mai posseduto giacenze di tale ammontare in conto corrente, tanto meno* [aveva] *mai eseguito simili operazioni*";
- nei primi giorni di settembre accedeva al proprio conto online dalla home page dell'intermediario dalla quale "*si* [riteneva fosse] *avvenuta la sottrazione dei dati sensibili*"; non rispondeva ad alcuna richiesta pervenuta a mezzo posta elettronica; le credenziali venivano inserite "*esclusivamente ed unicamente a richiesta della pagina di accesso al conto*" una volta collegatosi al sito tramite il proprio pc aziendale "*fornito di adeguati sistemi di protezione*"; ogni eventuale sottrazione delle credenziali era "*riconducibile ad intrusioni da parte di terzi nel sistema di home banking*" dell'Intermediario.

Il ricorrente rileva, quindi, "*l'inadeguatezza dei sistemi* [e] *la superficialità*" con la quale l'intermediario aveva consentito un'operazione contenente "*sicuramente le caratteristiche dell'anomalia*", senza chiedere informazioni e/o immediata conferma; la convenuta avrebbe dovuto fornire e garantire un sistema di maggiore standard e sicurezza "*tra cui l'utilizzo del dispositivo token*".

Con le proprie controdeduzioni, l'intermediario resistente ha precisato che:

- la trasmissione sicura dei dati avveniva con l'uso di certificati digitali per cifrare i dati e verificare l'identità del server della banca; erano previsti, oltre ai sistemi di "*autenticazione forte*" a conferma delle operazioni disposte basati su codici usa e getta (OTP), ulteriori strumenti a disposizione del cliente tra cui il sistema di sms alert per le operazioni disposte tramite home banking;
- tale servizio "*non risulta*[va] *mai essere stato attivato dall'utenza intestata*" al coniuge del ricorrente;
- sono state adottate adeguate misure di sicurezza, come già affermato con il riscontro al reclamo; già nella pagina di apertura del sito vi era la possibilità di accedere alla sezione "*sicurezza online*" contenente tra le altre le informazioni sul servizio di sms alert "*a cui il cliente* [aveva] *ritenuto di non aderire*";
- le "*evidenti carenze*" del sistema di sicurezza del ricorrente hanno "*sicuramente consentito l'infezione da malware*";
- è "*significativo*" quanto affermato nella denuncia-querela presentata in riferimento alla ricezione di un sms contenente dei codici di sicurezza che, ritenuto un errore, era stato ignorato con "*superficialità*".

DIRITTO

Il Collegio, ricordato che l'operazione contestata è successiva all'entrata in vigore del D.Lgs. 11/2010 (1° marzo 2010) di recepimento della PSD (Direttiva 2007/64/CE) e

rilevato che l'operazione non autorizzata è stata effettuata utilizzando le corrette credenziali del cliente, tra cui in particolare il codice generato dall'intermediario e inviato mediante sms sull'utenza telefonica indicata dal ricorrente, in linea con il proprio indirizzo interpretativo non accoglie il ricorso.

In più occasioni, infatti, il Collegio ha avuto modo di valutare i livelli di sicurezza adottati dagli intermediari con riferimento all'accesso a servizi di *internet banking* e ha ripetutamente espresso il proprio assenso rispetto all'adozione di sistemi "a due fattori", quale quello utilizzato dall'intermediario nel presente caso, dove le disposizioni contestate sono avvenute non solo mediante la digitazione delle credenziali previste, ma anche attraverso l'utilizzo del codice di autorizzazione appositamente generato dall'intermediario per ogni singola operazione e inviato via sms sull'utenza telefonica indicata dal ricorrente; modalità che permette, al momento della disposizione di una transazione online, la generazione e lo scambio di codici univoci tra il sito web e il correntista. Ad avviso del Collegio, l'adozione di un sistema a "due fattori" induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, da un lato, che la banca abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del D.lgs. n. 11/2010 e, dall'altro lato, che il cliente si sia reso gravemente inadempiente all'obbligo di custodia degli strumenti e dei codici di accesso che consentono l'utilizzo del servizio online e l'invio di ordini di bonifico a valere sul conto a lui intestato. Alla luce delle caratteristiche tecniche di sicurezza adottate dall'intermediario sembra dunque lecito presumere che l'operazione fraudolenta di cui si discute sia stata resa possibile da un comportamento inadempiente del cliente, il quale ha omesso di adottare tutte le cautele necessarie a custodire i codici di accesso e i dispositivi connessi. Né varrebbe obiettare, in contrario, che così facendo si violerebbe il disposto dell'art. 10 del D.Lgs. n. 11/2010, nella parte in cui esclude che l'utilizzo dello strumento di pagamento possa costituire di per sé prova della violazione degli obblighi (nella specie, di custodia) da parte del cliente; la lettera della disposizione non sembra infatti incompatibile con l'interpretazione qui accolta, in quanto l'espressione "*non è di per sé necessariamente sufficiente a dimostrare*" non esclude che, al ricorrere di determinate condizioni (particolare affidabilità tecnica dello strumento, assenza di ulteriori elementi di anomalia dell'ordine), tale idoneità possa invece sussistere ed essere apprezzata dal giudicante come prova (presuntiva) della violazione degli obblighi gravanti sul cliente.

In senso contrario non depone neppure la recente pronuncia del Collegio di Coordinamento n. 3498/2012. Con tale decisione, il Collegio ha certamente escluso un "automatismo" tra l'utilizzo di un sistema a due fattori da parte dell'intermediario e la sussistenza di una colpa grave imputabile al cliente, ben potendosi, infatti, verificare la "cattura dei codici" ad opera di terzi anche in presenza di un comportamento diligente da parte del cliente. Più in particolare, nella decisione sopra richiamata, il Collegio di Coordinamento ha escluso ogni responsabilità a carico del cliente in ragione dell'accertata aggressione informatica operata attraverso un *malware* particolarmente sofisticato, "capace di sorprendere la buona fede anche di un pur normalmente attendo fruitore del servizio" e tale, quindi, da escludere ogni sua colpa.

Nulla di tutto questo è invece ravvisabile nel caso in esame, né il ricorrente lamenta, del resto, alcuna di quelle circostanze in fatto che, in altre occasioni, hanno indotto altri Collegi dell'ABF a individuare una colpa concorrente dell'intermediario (email di *phishing*, ecc.). Pur escludendo una necessaria ed automatica corrispondenza biunivoca tra il sistema di sicurezza a due fattori adottato dall'intermediario ed una colpa grave del ricorrente nella custodia dei propri codici identificativi e, come nel caso in esame, del proprio telefono cellulare utilizzato per la ricezione del codice autorizzativo delle singole operazioni, da una valutazione delle circostanze di fatto come descritte dalle parti e dall'adozione di un

sistema di sicurezza a due fattori approntati dall'intermediario – che, salvo il ricorrere di meccanismi informatici particolarmente sofisticati (nel caso in esame nemmeno allegati dal ricorrente), consente di escludere accessi non autorizzati da parte di terzi – il Collegio ritiene, quindi, di poter presumere che l'operazione fraudolenta sia stata resa possibile da un comportamento inadempiente del ricorrente.

Nel caso in esame, infatti, non è possibile neppure ipotizzare quell'aggressione informatica particolarmente sofisticata che, in altre occasioni, ha indotto il Collegio ad escludere una colpa grave del cliente anche in presenza di un sistema di sicurezza "a due fattori" predisposto dall'intermediario. Lo stesso ricorrente esclude, infatti, di aver avviato alcuna operazione on-line nel corso della quale i propri codici identificativi e il successivo codice autorizzativo inviato via sms avrebbero potuto essere fraudolentemente sottratti da terzi. Il ricorrente conferma anzi la ricezione del codice autorizzativo indispensabile per la successiva esecuzione dell'operazione disconosciuta. Del resto, l'intermediario resistente ha fornito piena prova della generazione del codice autorizzativo, dell'invio dello stesso tramite sms al numero cellulare indicato dal ricorrente e del suo successivo utilizzo per l'esecuzione dell'operazione disconosciuta. Ne consegue che la sottrazione del codice autorizzativo che ha reso possibile l'esecuzione dell'operazione di pagamento contestata non può che essere avvenuta nella sfera di controllo dello stesso ricorrente e trovare, pertanto, ragione in una inadeguata attività di custodia di quest'ultimo.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA