COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(MI) CONTINO	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 25/11/2014 dopo aver esaminato:

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

FATTO

La ricorrente verificava due operazioni di ricarica dell'importo di Euro 500,00 ciascuna, effettuate on-line in data 3.06.2013, senza alcuna autorizzazione, sul proprio conto corrente attivato presso l'intermediario resistente.
Le operazioni venivano effettuate in modo fraudolento in seguito a una procedura di autenticazione richiesta dal sito successivamente all'effettuazione del login nell'area personale e "*non facevano riferimento a importi di denaro*". Lo stesso giorno, la ricorrente provvedeva al blocco della propria carta di pagamento e a presentare denuncia-querela presso la locale stazione dei Carabinieri.
Nelle proprie controdeduzioni, l'intermediario resistente ha precisato quanto segue:

- in data 3.06.2013, la ricorrente accedeva al sito predisposto dall'intermediario convenuto e, dopo aver effettuato il login inserendo l'user id e la password, si apriva una finestra di verifica dei dati personali. La ricorrente provvedeva ad inserire tutti i dati richiesti e, dopo la comparizione di un secondo avviso, secondo cui l'operazione andava ripetuta per un errore tecnico, la ricorrente provvedeva ad effettuare un nuovo inserimento di tali dati;

- è la stessa ricorrente a confermare, nelle dichiarazioni rese all'interno della denuncia, di aver inserito le proprie credenziali in una finestra web comparsa in seguito al login sul sito dell'intermediario. L'intermediario "*non chiede mai, attraverso avvisi, di fornire i codici personali relativamente al conto corrente e alle carte ad esso associate. Inoltre, il codice autorizzativo di ciascuna transazione viene richiesto esclusivamente, come ultima istanza, solo dopo aver scelto il tipo di operazione da effettuare*";
- alla luce di tali dati "*è intuibile (…) che la ricorrente abbia inserito i suddetti dati su una pagina web clone dell'originale (…) Questo tipo di intromissione sono frutto della mancanza di programmi antivirus adeguati nei pc degli utenti, in grado di poter arginare l'ingresso di hacker informatici nei computer*";
- dalla ricostruzione dello sviluppo di una transazione tipo, avente ad oggetto una ricarica telefonica, si evidenzia che l'ultima maschera, relativa ai vari passaggi dispositivi della transazione, si apre solo dopo aver svolto una serie di attività preliminari, mentre il sito non mostra mai alcun avviso attraverso il quale vengano richiesti i dati personali e il codice autorizzativo (fornito dal lettore PCR) subito dopo il login;
- la ricorrente era solita utilizzare il sito dell'intermediario, per cui avrebbe dovuto accorgersi immediatamente dell'anomalia;
- a partire dal marzo del 2005, l'intermediario ha attivato una campagna di informazione con riferimento alle frodi informatiche e, comunque, "*nessuna violazione è avvenuta a carico dei sistemi informatici centrali dell'intermediario, la cui sicurezza e qualità sono state certificate secondo i più rigorosi e affidabili standard internazionali*".

DIRITTO

La questione centrale che questo Collegio deve affrontare, per la soluzione del caso che ne occupa, attiene ai doveri di custodia della carta di pagamento e dei codici di sicurezza ad essa relativi, da un lato, e del grado di diligenza che si può richiedere all'intermediario in relazione all'erogazione di detto servizio, dall'altro lato.
Le operazioni contestate dalla ricorrente sono avvenuti in data 3.06.2013, successivamente, quindi, all'entrata in vigore del D. Lgs. 27 gennaio 2010, n. 11 (Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno), attraverso un sistema di autenticazione a due fattori.
In più occasioni, 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 fisico di un Personal Card Reader" (PCR) che, insieme alla carta dotata di microchip e a un certificato digitale (memorizzato all'interno del chip della carta) permette, al momento della disposizione di una transazione online, la generazione e lo scambio di codici univoci tra il sito web e il correntista.
L'impiego di un sistema di autenticazione a due fattori richiede, tuttavia, che l'esame del presente ricorso venga effettuato alla luce dei criteri indicati dal Collegio di Coordinamento dell'ABF, con la decisione n. 3498 del 26.10.2012, che ha 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 a danno del cliente 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.
È, infatti, evidente la profonda differenza strutturale fra i metodi più "tradizionali", quali il c.d. phishing, e, ad esempio, il c.d. fenomeno del man-in-the-browser, che si verifica attraverso l'interposizione fraudolenta di ignoti nella fase di dialogo fra il computer impiegato dal ricorrente e i sistemi di ricevimento della banca: nel primo caso, il cliente è vittima di una colpevole credulità in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario, mentre, nel secondo caso, il subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto- sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che appare genuino.
Ciò chiarito, in ragione della ricostruzione dei fatti operata dalla ricorrente, e non espressamente smentita dall'intermediario resistente, deve ritenersi che la ricorrente sia stata vittima di un caso di pharming. Il pharming è un'altra forma di frode on-line molto simile al phishing. I "*pharmers*" si affidano a siti Web falsi e al furto d'informazioni riservate per perpetrare truffe on-line; essi risultano particolarmente insidiosi perché non fanno affidamento sul fatto che la vittima accetti il messaggio "esca". Anziché utilizzare falsi messaggi, e-mail, nei quali inducono gli utenti a fare clic su dei collegamenti, i pharmers reindirizzano le vittime direttamente sul sito Web fasullo, anche quando queste digitano correttamente l'indirizzo di una banca o altro servizio on-line nel browser Web. Si tratta di una forma assai subdola di truffa on-line, che implica una sorta di duplicazione della pagina web, la quale si presenta perciò identica all'ignaro utente on-line.
Deve, pertanto, escludersi la colpa grave della ricorrente e, per l'effetto del combinato disposto degli artt. 7, 10 e 12 del d.lgs. 11/2010, la ricorrente non è tenuta a sopportare conseguenza alcuna, ulteriore e diversa dalla franchigia di Euro 150,00. Il Collegio accoglie pertanto il ricorso e dispone che l'intermediario corrisponda al ricorrente la somma di Euro 850,00 (=1.000-150).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 850,00.
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
FLAVIO LAPERTOSA