COLLEGIO DI MILANO

composto dai signori:

(MI) GAMBARO	Presidente
(MI) ORLANDI	Membro designato dalla Banca d'Italia
(MI) CERINI	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 (MI) ORLANDI

Nella seduta del 10/12/2013 dopo aver esaminato:

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

FATTO

Espone la ricorrente che, a seguito della richiesta di un estratto conto *on line*, alle ore 15:00 circa del giorno 12.2.2013 constatava che *"ignoti, durante questa operazione, in modo fraudolento, si impossessavano, dei* suoi *dati per effettuare una ricarica di 2.400,00 euro a favore della carta prepagata nr. (...)"*, senza la sua autorizzazione. Nel reclamo, dichiara che il conto corrente è stato bloccato. Esprime, inoltre, delusione per non essere stata avvisata in modo informale dell'operazione e preoccupazione per la mancanza di sicurezza dei sistemi informatici. Nella successiva integrazione la ricorrente afferma *"di aver sempre rispettato la regola di custodire le (...) credenziali di accesso"* e riconduce il mancato riconoscimento della truffa ai *"ripetuti malfunzionamenti"* riscontrati nel servizio internet banking dopo le recenti variazioni apportate della banca.
Replica l'intermediario come *"dagli accertamenti effettuati è emerso che non vi sono state anomalie o malfunzionamenti imputabili alla* (...) *scrivente"*. In particolare, "dall'analisi del log internet banking della ricorrente, è emerso che *"nell'arco temporale dalle ore 15:40:26 alle ore 15:55:33, la cliente ha digitato le password monouso, generate da lei stessa, attraverso la chiave elettronica n. (...) per ben 5 volte"* (...) *"non sulla pagina web*

dell'intermediario *ma su una maschera fake di login che si è interposta fra il pc della cliente e la pagina stessa di login del PasKey" (...)*, che "*è generata da un software malevolo annidato nel pc del cliente: nello specifico si tratta d una variante del Trojan denominato "Zeus"...*". La ricorrente avrebbe così disatteso quanto indicato nella sezione sicurezza del sito internet inserendo nei vari form proposti dalla maschera fake tutti i parametri di sicurezza. Le modalità di protezione da truffe analoghe a quella in esame sono riportate nella sezione sicurezza della multicanalità, integrata del sito internet. La ricorrente non ha fornito prova di aver adottato tutte le cautele necessarie per evitare l'intrusione dei truffatori nel proprio pc e avrebbe operato "*inconsapevolmente*" sull'*home banking* "*in modo imprudente e con imperizia, rendendosi inoltre negligente rispetto all'adozione de sistemi cautelativi posti a sua disposizione*".
La ricorrente chiede la restituzione delle somme sottratte. La convenuta chiede di respingere il ricorso.

DIRITTO

Risulta pacifico come la ricorrente sia stata vittima di un *software* malevolo (*malware*), derivato dal c.d. malware *Zeus*, che la letteratura informatica riporta siccome scoperto nel 2007, diffusosi nel 2009 e 2010, debellato dalle autorità statunitensi, e rieditato in altre consimili forme, grazie alla messa in rete dei codici sorgente (codici necessari per l'esecuzione, la manipolazione e la riprogrammazione del malware), disposta dalle stesse autorità. Il principio operativo di tale tecnica intrusiva viene definito in gergo *man-in-the-browser* in ragione dell'interposizione che questo genere di malware è in grado di operare fra il sistema centrale dell'intermediario e quello del singolo utente. Il programma malevolo, una volta annidatosi in un certo numero di computer, genera quella che in gergo suole definirsi una *botnet*, ossia per l'appunto una rete di macchine egualmente infettate dallo stesso virus. Il malware – riconducibile alla più ampia categoria dei cc.dd. *trojan* ("cavalli di Troia") e dotato di sofisticate capacità di elusione dei migliori antivirus – si annida in modo silenzioso nel computer della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il malware resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (*targeted banks*). In quel preciso istante il malware "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso (c.d. protocollo di trasferimento ipertestuale, *Hyper Text Transfer Protocol*) "http" e non già "https" (dove la "s" finale sta per *secured*, protetto). Ignaro dell'intervenuta sostituzione della pagina, l'utente è indotto a ritenere di trovarsi nel normale ambiente sicuro in cui normalmente egli opera. A quel punto, il malware attiva una finestra a modulo, che pare sempre provenire dal sito dell'intermediario in cui si trova (crede di trovarsi) l'utente, ove è richiesta una conferma di sicurezza con l'invito a compilare i campi del modulo con i propri dati e il codice generato dal dispositivo OTP; procedura che gli intermediari stessi talora attivano per controlli di sicurezza (specie come quando, nel caso in esame, l'accesso abbia luogo da una macchina diversa da quella abitualmente utilizzata dall'utente e come tale segnalata al server della banca da un differente indirizzo di provenienza: c.d. IP, *Internet Protocol*), il che rafforza nell'utente il convincimento della piena regolarità della situazione e della normalità del controllo

automaticamente disposto dal sistema. L'utente, con ciò doppiamente ingannato, compila quindi i campi del modulo che il malware prontamente trasmette all'intruso. Questi, così callidamente interpostosi nell'operazione, ha modo di captare tutti i fattori di autenticazione e di utilizzarli in tempo reale, nel mentre l'utente viene ulteriormente ingannato da un messaggio di attesa che, qualche minuto dopo, si conclude con la segnalazione dell'impossibilità di procedere all'operazione e con l'invito a ritentare in un secondo momento.

Tale fenomeno appare ricorrere nel caso in esame (sul fatto che di tale frode si sia trattato v'è pacifica convergenza di vedute fra le parti contendenti), che ha visto la ricorrente, una volta acceduta al sito dell'intermediario, cadere in questo infido e impercettibile tranello. La tentata operazione di bonifico che la ricorrente intendeva porre in essere non avrà seguito in quanto la schermata di cattura, formulata col descritto illusionismo informatico, la indurrà a comunicare i propri dati e il codice monouso generato dall'OTP, salvo poi vedersi, dopo qualche minuto, comunicare dalla stessa schermata l'impossibilità di procedere e l'invito a provare in un momento successivo. Non appare ragionevolmente ravvisabile, in tale contesto, alcun elemento tale da poter riqualificare siccome colposa, e tanto meno siccome gravemente colposa (ai fini di cui all'art. 12 comma 2° d. lgs. cit.), la condotta dell'utilizzatore del servizio. Per quanto non possa negarsi che il cliente sia caduto nella tagliola ed abbia materialmente permesso l'esecuzione dell'operazione fraudolenta cooperandovi involontariamente, non c'è chi non veda la profonda differenza strutturale fra i dianzi citati metodi "tradizionali" di *phishing* e il descritto fenomeno del *man-in-the-browser.* Nel primo caso, il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet. Nel caso che ci occupa, invece, 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 a chiunque non potrebbe apparire che genuino, posto che l'unica "differenza" consta, come si è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale "http" e non già come un "https" protetto. Ma va da sé che una simile variazione, che compare solo nella stringa di intestazione della video schermata intrecciata ad almeno cinquanta o sessanta ulteriori caratteri, barre e altri segni di punteggiatura informatica, sfugge normalmente all'attenzione di chiunque si accosti ad una pagina della rete e più che mai sfugge a chi si accosti alla pagina di un sito bancario per compiere un'operazione, in un momento in cui l'attenzione dell'utente è concentrata sul contenuto della schermata e non certo sugli incomprensibili codici che la circondano e che fanno parte del normale apparato di contorno delle consultazioni in rete (v. in termini Coll. coord. 3498/12). Deve dunque disporsi la restituzione della somma sottratta, salva franchigia di legge (2400-150)= 2250.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla ricorrente la somma di € 2.250,00.
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 ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANTONIO GAMBARO