COLLEGIO DI NAPOLI

composto dai signori:

(NA) QUADRI	Presidente
(NA) CARRIERO	Membro designato dalla Banca d'Italia
(NA) CONTE	Membro designato dalla Banca d'Italia
(NA) RISPOLI FARINA	Membro designato da Associazione rappresentativa degli intermediari
(NA) BARTOLOMUCCI	Membro designato da Associazione rappresentativa dei clienti

Relatore RISPOLI FARINA MARILENA

Nella seduta del 09/09/2014 dopo aver esaminato:

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

FATTO

Il ricorrente, titolare presso la banca resistente di un conto corrente con operatività anche tramite canale home banking, in data 24.03.2013 riscontrava un addebito fraudolento a seguito di una transazione telematica – ricarica di una carta prepagata intestata a beneficiario sconosciuto - posta in essere da ignoti.

Con il ricorso in esame, lamenta la mancata adozione da parte della banca dei "migliori sistemi di sicurezza tecnologici per escludere qualunque accesso fraudolento al conto corrente" e chiede la restituzione dell'importo sottratto dal conto a lui intestato, pari ad € 2.000,00.

Nel procedere ad una più dettagliata ricostruzione della vicenda il cliente espone:

- di aver ricevuto lo stesso giorno 24.03.2013, alle ore 14:30 circa, al proprio indirizzo di posta elettronica una e-mail apparentemente proveniente dalla resistente e la cui autenticità pareva indubbia;

- con la predetta comunicazione la banca invitava il cliente, al fine di verificare una operazione contabile sospetta, ad effettuare un accesso al conto attraverso un apposito link;

- dopo aver inserito i dati di accesso al proprio conto, ha rilevato un addebito fraudolento di € 2.000,00 a favore di una carta di credito prepagata a lui sconosciuta e ha ricevuto un SMS con cui veniva avvertito dell'avvenuta modifica dell'utenza mobile destinataria degli avvisi di "operazioni sospette";

- procedeva nell'immediatezza della scoperta a contattare il servizio clienti dell'intermediario per comunicare l'accaduto e richiedere la revoca dell'operazione;

- alle ore 17:30 circa, sporgeva denuncia presso la locale stazione dei Carabinieri

In punto di fatto la resistente ha chiarito che il ricorrente, in data 02.09.2011, sottoscriveva un "contratto di servizi via internet, cellulare e telefono", relativo al conto corrente in questione, con espresso richiamo, "ad integrazione di quanto specificato in contratto", alla "Guida ai Servizi" disponibile nella sua versione più aggiornata sul suo sito web (cfr. allegato 2).

La controparte, sulla base della narrazione della vicenda fatta da parte attiva, ha ricondotto la fattispecie in esame ad una ipotesi di phishing che integra una violazione degli obblighi contrattuali (in particolare degli obblighi di diligente custodia di cui all'art. 5 comma 2) e rende quindi riconducibile a grave negligenza del cliente stesso la responsabilità per eventuali conseguenze dannose.

La resistente si è dilungata su una descrizione del fenomeno, sulla campagna informativa in merito predisposta (con particolare riferimento alla "guida ai servizi" sopra citata) e sugli accorgimenti di sicurezza predisposti a presidio dell'infrastruttura tecnologica che, nel caso di specie, non è risultata violata.

In particolare, a garanzia della sicurezza delle transazioni informatiche, la banca ha predisposto differenti livelli di sicurezza che, nel caso di specie, hanno correttamente funzionato. Sono richieste, in dettaglio, tre password per l'accesso al sistema: due statiche (codice utente e PIN) ed una dinamica temporizzata generata dall'apposita chiavetta personale "utilizzabile una volta sola". L'effettuazione della transazione in concreto è subordinata poi alla digitazione di un'ulteriore password dinamica fornita ancora dalla chiavetta e che compare sul display per alcuni secondi "premendo l'apposito pulsante". Qualora l'operazione di pagamento presenti "indici di anomalia rispetto all'ordinaria operatività del cliente" è richiesto anche l'utilizzo di un codice di sicurezza inviato via SMS al numero di telefonia mobile a tal fine fornito accompagnato dalla descrizione dell'operazione; purtroppo nella fattispecie, l'SMS in questione è stato recapitato al numero cellulare ormai modificato (cfr. allegato 12).

Sono stati, altresì, evidenziati quali fattori di valutazione della colpa grave del cliente nella causazione dell'illecito: 1) l'aver abboccato ad una e-mail di dubbia autenticità 2) il non aver contattato immediatamente il servizio clienti anche a fronte del falso avvertimento che il conto fosse stato "bloccato" per "operazioni sospette". L'intermediario, infatti, nella "Guida ai servizi" precisa che, per motivi di sicurezza, in nessun caso richiede al cliente la comunicazione via internet dei codici d'accesso: " Le politiche di sicurezza del nostro sito non prevedono in alcun caso la richiesta di fornire i codici di accesso via e-mail o

telefonicamente; nel caso ricevesse richieste di questo tipo, la invitiamo a contattare prontamente il nostro servizio clienti". Sono state quindi richiamate a supporto:

- la decisione del Collegio di Coordinamento n. 3498/12, per inferirne che la negligenza del cliente nel consentire a terzi di carpire i propri codici personali è prevalente rispetto alla diligenza professionale che l'intermediario deve prestare per prevenire fenomeni di frode informatica;

- talune decisioni del Collegio di Napoli (tra le più recenti le nn. 2533/13, 504/13, 1798/13, 1718/13 e 3408/13), di quello di Milano (da ultimo la n.3689/13) e del Collegio di Roma (decisioni nn. 1699/13 e 1820/13).

E' stato infine reso noto l'esito negativo a cui hanno condotto tutti i tentativi compiuti per il recupero delle somme.

Il ricorrente in sede di replica insiste nella richiesta di restituzione della somma di € 2.000,00 indebitamente sottratta dal proprio conto corrente.

In particolare, contesta il sistema di tutela predisposto dalla banca per la procedura di modifica del numero di cellulare del cliente, ritenendo che, in presenza di una maggior livello di protezione, l'evento dannoso non si sarebbe verificato, pur in presenza del furto delle credenziali di accesso.

In conclusione, il ricorrente chiede al Collegio di "provvedere al risarcimento del danno subito pari ad € 2.000,00, oltre interessi sino al soddisfo, nonché spese legali pari ad € 250,00". La resistente, a seguito delle argomentazioni esposte, richiede che il Collegio voglia "riconoscere e dichiarare l'inaccoglibilità del ricorso in quanto manifestamente infondato".

DIRITTO

Il Collegio deve decidere in merito alla richiesta del ricorrente, titolare di un conto corrente con servizio di Home banking, a seguito di un riferito episodio di phishing, di ottenere le somme fraudolentemente prelevate.
Come in numerosi casi analoghi, la richiesta di rimborso delle somme fraudolentemente sottratte implica la valutazione dei profili di responsabilità della banca in caso di operazioni poste in essere senza autorizzazione dell'utilizzatore del servizio di pagamento.
In questi casi, l'operatività di strumenti di pagamento si connota per la rilevanza di due tipologie di obblighi: da un lato, quelli del cliente, di custodire con diligenza lo strumento di pagamento (nell'ipotesi in questione i codici di accesso al servizio Home banking) e, dall'altro, quelli dell'intermediario che deve adempiere il proprio compito di salvaguardia dei patrimoni dei clienti con la diligenza professionale e qualificata richiesta dall'art. 1176, comma 2, c.c. predisponendo misure di protezione adeguate rispetto agli standard esistenti, anche sotto il profilo dei presidi tecnici adottati.
La normativa di riferimento per la prestazione di servizi e strumenti di pagamento è contenuta nel d.lgs. n. 11/2010, in particolare agli artt. 7-12. Come evidenziato dalla dottrina, ma anche dalle decisioni dell'Arbitro Bancario Finanziario, le norme del d.lgs. n. 11/2010 se, da un lato, intendono incentivare l'utilizzo degli strumenti di pagamento, dall'altro impongono che ciò avvenga nel rispetto di presidi di sicurezza che siano in grado di preservare l'utilizzatore da impieghi fraudolenti, scoraggiando condotte negligenti che favoriscano pratiche illegali ad opera di terzi.

In relazione agli obblighi incombenti sull'utilizzatore, la stessa disciplina fa discendere un duplice ed alternativo regime di responsabilità: una prima responsabilità, limitata, che opera rispetto alle operazioni poste in essere prima della tempestiva comunicazione al prestatore dei servizi e nei limiti della franchigia di € 150,00; la seconda, illimitata, che opera ogni qualvolta la violazione di tali obblighi sia imputabile ad un comportamento (oltre che fraudolento) doloso o gravemente colposo dell'utilizzatore.
In tali casi, al pari della presente controversia, appare decisiva l'indagine circa la sussistenza di elementi soggettivi integranti ipotesi di colpa grave, il cui onere della prova incombe, secondo la dottrina, sull'intermediario in base ai principi che regolano la responsabilità contrattuale (art. 1218 c.c.). La giurisprudenza di legittimità ha chiarito che la colpa grave consiste in "un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti" (cfr., per una simile prospettiva, in tema di gravità della colpa, Cass. civ., 19 novembre 2001, n. 14456; ma v. anche Collegio di Milano, dec. n. 40/2012; n. 2310/2011; Collegio di Roma, dec. n. 2157/2011; n. 712/2010).
Una valutazione siffatta deve essere compiuta alla luce di tutte le circostanze di fatto che, di volta in volta, caratterizzano il caso di specie, sia con riferimento agli obblighi di custodia dello strumento di pagamento, sia a quelli di memorizzazione del codice identificativo.
Va allora detto che, a garanzia della sicurezza delle transazioni informatiche, la banca, come ha compiutamente allegato nella sua difesa, oltre ad avere provveduto a informare adeguatamente la clientela delle modalità delle possibili frodi informatiche, ha predisposto differenti livelli di sicurezza che, nel caso di specie, hanno correttamente funzionato. Sono richieste, in dettaglio, tre password per l'accesso al sistema: due statiche (codice utente e PIN) ed una dinamica temporizzata generata dall'apposita chiavetta personale "utilizzabile una volta sola". L'effettuazione della transazione in concreto è subordinata poi alla digitazione di un'ulteriore password dinamica fornita ancora dalla chiavetta e che compare sul display per alcuni secondi "premendo l'apposito pulsante". Qualora l'operazione di pagamento presenti "indici di anomalia rispetto all'ordinaria operatività del cliente" è richiesto anche l'utilizzo di un codice di sicurezza inviato via SMS al numero di telefonia mobile a tal fine fornito accompagnato dalla descrizione dell'operazione. Purtroppo, deve rilevarsi che nella fattispecie in esame, l'SMS in questione è stato recapitato al numero cellulare ormai modificato. Ciò è stato possibile in quanto, "abboccando" al messaggio mail ricevuto il cliente ha comunicato le sue credenziali consentendo l'utilizzo delle disponibilità esistenti sul conto on line. Né, come rileva la banca, ha contattato immediatamente il servizio clienti anche a fronte del falso avvertimento che il conto fosse stato "bloccato" per "operazioni sospette".

Ai fini di una migliore valutazione del grado di colpa in cui è incorso il ricorrente, si può ricordare il testo delle disposizioni della Banca d'Italia del 5.7.2011 "Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento" che, alla Sez. IV, Paragrafo 2.1 (Riservatezza dei dispositivi di sicurezza): recita "Quando uno strumento prevede l'utilizzo di dispositivi personalizzati di sicurezza (es. PIN e password) è fatto obbligo all'utilizzatore di mettere in atto gli accorgimenti idonei al fine di preservarne la riservatezza onde evitare gli utilizzi non autorizzati degli strumenti di pagamento in questione. Tale esigenza rileva in modo specifico nel caso in cui il pagamento sia effettuato a distanza, ad esempio per mezzo di un dispositivo telefonico o di un sito internet. E' necessario che l'utilizzatore ottenga l'autorizzazione del proprio prestatore di servizi di pagamento prima di fornire a terzi i codici per l'utilizzo del servizio o dello strumento di pagamento: in tal modo è possibile per il prestatore individuare le richieste

dei codici di sicurezza provenienti da soggetti che simulino la legittimità della richiesta medesima, come nel caso del phishing. In aggiunta, ciò consente di limitare i rischi connessi con l'eventuale utilizzo di piattaforme per i pagamenti su internet (in particolare quelli a valere su un conto, quali i bonifici) che non sono autorizzate dal prestatore di servizi di pagamento di cui l'utilizzatore si avvale (cc.dd. overlay services). Qualora il contratto tra utilizzatore e prestatore di servizi di pagamento faccia divieto al primo di comunicare a terzi i codici di sicurezza, la violazione di tale divieto integra una condotta negligente da parte dell'utilizzatore, non consentendogli di avvalersi dell'esenzione di responsabilità di cui al successivo paragrafo".

Ancora poi , ribadiscono le disposizioni (Paragrafo 2.2, Responsabilità dell'utilizzatore): "Il rispetto degli obblighi di condotta diligente da parte dell'utilizzatore esime quest'ultimo da responsabilità per utilizzi non autorizzati dei servizi e degli strumenti di pagamento. Il mancato adempimento di tali obblighi può invece comportare la sua responsabilità per gli utilizzi non autorizzati. La violazione degli obblighi posti in capo all'utilizzatore dalla legge o dal contratto in essere con il suo prestatore di servizi di pagamento integra una condotta negligente. Al fine di favorire la diffusione dei servizi e degli strumenti di più elevata qualità sotto il profilo della sicurezza, la Banca d'Italia, ai sensi dell'art. 12, comma 5, del Decreto, dispone la riduzione delle responsabilità dell'utilizzatore che scelga detti prodotti di pagamento. Rientrano nella fattispecie in esame gli strumenti di pagamento aventi le caratteristiche di sicurezza individuate nel documento "Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza". Per questi strumenti - fatti salvi i casi in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento - l'utilizzatore non risponde neppure della franchigia di cui all'art. 12, comma 3, del Decreto". Di particolare rilievo, infine, il Paragrafo 3 (Obblighi del prestatore di servizi di pagamento in relazione alla prestazione di servizi e all'emissione di strumenti di pagamento), che detta : "Con specifico riferimento ai servizi di pagamento fruibili in ambiente internet, al fine di prevenire utilizzi fraudolenti, è necessario che i prestatori di servizi di pagamento aderiscano a piattaforme tecniche che consentano ai propri clienti di effettuare pagamenti in rete in condizioni di elevata sicurezza".

E, ancora, al Paragrafo 3 si precisa (Obblighi del prestatore di servizi di pagamento in relazione alla prestazione di servizi e all'emissione di strumenti di pagamento): "Con specifico riferimento ai servizi di pagamento fruibili in ambiente internet, al fine di prevenire utilizzi fraudolenti, è necessario che i prestatori di servizi di pagamento aderiscano a piattaforme tecniche che consentano ai propri clienti di effettuare pagamenti in rete in condizioni di elevata sicurezza".

Pertanto, come ha anche precisato il Collegio di coordinamento, decisione n. 3498/2012, nel caso del Phishing 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 in esame, il ricorrente avrebbe dovuto astenersi dal comunicare i dati che hanno consentito ai male intenzionati di accedere al conto on line, che risulta invece essere stato adeguatamente protetto dal sistema adottato dall'intermediario, cui quindi non può essere addossata la responsabilità – dato il carattere sicuramente determinante del comportamento del ricorrente sotto il profilo causale – per i danni derivanti dall'utilizzo fraudolento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ENRICO QUADRI