COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) PARROTTA	Membro designato dalla Banca d'Italia
(NA) BLANDINI	Membro designato dalla Banca d'Italia
(NA) ROTONDO	Membro designato da Associazione rappresentativa degli intermediari
(NA) BARENGHI	Membro designato da Associazione rappresentativa dei clienti

Relatore BARENGHI ANDREA

Nella seduta del 25/05/2015 dopo aver esaminato:

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

FATTO

Con atto dell'11.11.2014, facendo seguito al conforme reclamo del 12.09.2014 poi riscontrato dall'intermediario resistente in data 20.10.2014, la ricorrente lamenta l'addebito in conto corrente di € 11.100,00 che sarebbero stati prelevati illecitamente da terzi mediante frode informatica in data 8.09.2014. Riferisce di essere stata informata telefonicamente il giorno successivo da un operatore della banca, il quale – ottenuta conferma circa il carattere fraudolento delle operazioni compiute sul conto – le comunicava l'immediato blocco dei codici di accesso e la sostituzione della 'security card'. Rileva di aver provveduto a presentare denuncia alle competenti autorità inviando già in data 13.09.2014 una lettera raccomandata all'intermediario, e di aver ottenuto la restituzione di € 3.932,00. Attribuendo quindi alla negligenza dell'intermediario (in particolare all'assenza di dispositivi più avanzati della 'security card', messi a disposizione solo successivamente e del resto non previsti come unica piattaforma disponibile, e l'indisponibilità della funzione di sms alert) il danno subito, chiede la restituzione dell'importo di € 7.168,00, oltre interessi legali da quando dovuti fino al soddisfo e spese sostenute.

L'intermediario resistente, precisando di essersi attivato immediatamente per il recupero degli importi sottratti (con esito positivo solo per una parte del complessivo importo, pari a € 3.932,00) e lamentando il ritardo con cui la circostanza gli sarebbe stata comunicata dalla cliente, rileva che, all'esito delle verifiche, è risultato che le operazioni contestate sono state effettuate con corretto inserimento dei codici personali del cliente, donde a suo avviso l'«*oggettiva violazione dell'obbligo di diligente custodia dei codici identificativi*», che, a norma degli artt. 6 del doc. C e 8 del do. L del contratto quadro, la violazione dell'obbligo di custodia comporta che il cliente resti responsabile di ogni conseguenza dannosa che possa derivare dall'utilizzo illegittimo degli stessi, nonché dal loro smarrimento o sottrazione. Circa la sicurezza dei sistemi, sottolinea il costante controllo dell'infrastruttura e l'adeguatezza dei presidi allora esistenti, dotati di codice identificativo del cliente, codice segreto, security card, nonché l'esistenza di controlli ulteriori e di adeguate informazioni alla clientela mentre il servizio sms non era attivabile solo perché l'utente non aveva introdotto un numero di telefono sul proprio profilo, oltre all'ulteriore possibilità da aprile 2012 di avvalersi della password usa e getta, previa chiamata al numero verde dedicato. Chiede quindi di respingere il ricorso e in subordine applicare la franchigia contrattuale.

DIRITTO

Osserva il Collegio che nel caso di specie il sistema di sicurezza risulta pacificamente utilizzato nell'esecuzione delle disposizioni contestate. Risulta altresì, d'altra parte, che il sistema base adottato dall'intermediario non appare, come correttamente osservato dalla ricorrente, rispondente ai migliori *standard* esistenti (in particolare l'intermediario non ha adottato la procedura di creazione automatica di una *password ad hoc*), mentre la possibilità di accedere ad un *call center* per la creazione di un *password ad hoc* non solo appare particolarmente macchinosa ma non risulta comunicata in modo personalizzato agli utenti del sistema, né sembra meritevole di considerazione il rilievo dell'intermediario sulla mancata utilizzazione del servizio di sms *alert*, atteso che nel caso di specie l'sms *alert* non avrebbe evitato la frode (né è dimostrato che avrebbe diminuito il danno).
Nel caso di specie non sussistono indicazioni univoche da cui poter dedurre la sussistenza di una colpa grave da parte della cliente, che siano tali da integrare l'onere della prova, molto gravoso, posto dalla legge a carico dell'intermediario.
È ben noto che L'art. 7 del d.lgs. 11/2010 impone al prestatore di servizi «*assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo»,* mentre il successivo art. 10 prescrive che quando «*l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti»* d'altra parte escludendo che *«l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento*» sia «*di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7*», dovendo altrimenti a norma dell'art. 11 il prestatore «*rimborsa[re] immediatamente al pagatore l'importo dell'operazione medesima»,* pur potendo

«*dimostrare anche in un momento successivo che l'operazione di pagamento era stata autorizzata*» (pretendendo quindi la restituzione).

La giurisprudenza dell'Arbitro ha già chiarito ripetutamente che il gravoso onere della prova che la legge pone a carico del prestatore dei servizi di pagamento è riconducibile al «*rischio d'impresa, ossia all'idea secondo la quale è ragionevole far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano una vasta platea di consumatori o di utenti, sull'impresa, in quanto quest'ultima è in grado di distribuire su tale moltitudine il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento, evitando che gravino direttamente ed esclusivamente sul singolo pagatore*» rilevando altresì che «*la concreta applicazione del principio non può prescindere da un'esatta delimitazione delle rispettive sfere di responsabilità del prestatore e dell'utilizzatore del servizio di pagamento …* [verificando] *se il fornitore abbia adottato tutti i migliori accorgimenti della tecnica per scongiurare tali impieghi fraudolenti, dall'altra, se – di là dall'ipotesi in cui la condotta del cliente sia connotata dal dolo, sì da escludere l'operatività di qualsivoglia presidio – l'eventuale negligenza del titolare dello strumento di pagamento sia tale da ricadere o meno nella nozione di colpa grave al cui ricorrere il summenzionato art. 12 esclude ogni responsabilità dell'intermediario … la presenza di un comportamento gravemente colpevole dell'utente deve essere provata dal fornitore del servizio, il quale sarà tenuto ad allegare indizi precisi e concordanti che supportino tale qualificazione, mentre il mero fatto che sia stato utilizzato il dispositivo di sicurezza dell'utente non può configurare una grave negligenza*» (Collegio di Coordinamento, decisione n. 991/2014), e che «*a fronte della dichiarazione del cliente di avere sempre operato in modo diligente e accorto e di avere dotato la propria postazione informatica di adeguati strumenti di protezione contro virus e malware informatici, come anche attestato dal fatto di avere utilizzato il servizio di home banking senza mai rimanere in passato vittima di comportamenti fraudolenti*» non sembrando sufficiente l'introduzione di un ulteriore sistema di protezione «*genericamente offerto a tutta la clientela tramite il sistema di "messaggio inbox"»* e non mediante comunicazione personalizzata (Collegio di Napoli, decisione n. 6888 del 2014).

Alla luce delle disposizioni applicabili e dei rilievi contenuti nella precedente giurisprudenza, ritiene in definitiva il Collegio che non possa dirsi raggiunta nel caso di specie la prova della colpa grave dell'utilizzatore, in presenza di un sistema di sicurezza che non impiega gli *standard* più elevati di protezione, ovvero che li introduce attraverso procedure macchinose e non comunicate in termini personalizzati alla clientela, non potendosi quindi impedire l'attivazione della responsabilità prevista dalla legge in capo al prestatore di servizi di pagamento proprio in funzione del rischio d'impresa da quest'ultimo assunto e controllato.

Quanto alla franchigia contrattuale, il Collegio rileva che nella documentazione prodotta non risulta la specifica approvazione di tale clausola, donde l'infondatezza della richiesta in tal senso formulata dall'intermediario.

Ne consegue l'accoglimento del ricorso, nei termini di cui in dispositivo, oltre gli interessi legali dalla data del reclamo.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo di € 7.168,00, oltre interessi legali dalla data del reclamo.

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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE LEONARDO CARRIERO