COLLEGIO DI ROMA

composto dai signori:

(RM) DE CAROLIS	Presidente
(RM) SIRENA	Membro designato dalla Banca d'Italia
(RM) ROSSI	Membro designato dalla Banca d'Italia
(RM) NERVI	Membro designato da Associazione rappresentativa degli intermediari
(RM) ROSSI CARLEO	Membro designato da Associazione rappresentativa dei clienti

Relatore NERVI ANDREA

Nella seduta del 24/10/2014 dopo aver esaminato:

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

Fatto

La ricorrente espone – in sintesi – quanto segue:

- in data 23.03.2013 dalla lettura di un estratto conto on-line si accorgeva di ventuno operazioni fraudolente sul proprio conto, effettuate nel periodo compreso tra il 12.02.2013 e il 19.03.2013, tramite la propria carta di credito, per un importo complessivo di € 2.911,80. Si tratta di pagamenti all'estero attraverso siti web internazionali a cui la ricorrente non si è mai iscritta;
- nella stessa giornata del 23.03.2013, provvedeva a bloccare la carta telefonicamente, e successivamente il 29.03.2013, sporgeva denuncia presso l'autorità di pubblica sicurezza, ipotizzando una precedente clonazione della carta;
- con lettera ricevuta in data 23.08.2013, l'intermediario rigettava la richiesta di rimborso. La lettera di diniego, secondo la ricorrente, presentava diversi profili di inesattezza: prendeva in considerazione una sola operazione (e non le 21 denunciate); non era firmata; faceva riferimento al Securcode che, tuttavia, diveniva

obbligatorio solo dal 1.04.2013, mentre le operazioni denunciate risalgono ad un periodo precedente;

- la ricorrente sporgeva reclamo in data 4.09.2013, reiterando le stesse lamentele e insistendo sulla negligenza dell'intermediario nella tutela apprestata per i pagamenti on-line. La banca rispondeva in maniera insoddisfacente, riferendosi al Token per la sicurezza che, a detta della ricorrente, non le era mai stato consegnato, né tantomeno proposto, e dichiarando che il numero di cellulare della ricorrente non era registrato correttamente in anagrafica, asserzione infondata come confermato da successiva verifica effettuata su tempestiva richiesta della ricorrente;
- in data 13.10.2013 la ricorrente si rivolgeva tramite e-mail al Customer Care e riceveva una proposta di "conciliazione bonaria della disputa nella misura del 50%", che non accettava. La ricorrente reclama, infatti, l'integrale rimborso degli importi addebitati e contesta la negligenza dell'intermediario anche per l'ingiustificato rifiuto di fornire copia del contratto della carta di credito, non consegnata al momento della sottoscrizione alla cliente e dalla stessa richiesto con plurimi solleciti.

La ricorrente chiede quindi al Collegio di condannare l'intermediario al rimborso dei bonifici fraudolenti per un importo complessivo pari ad euro 2.911,80, oltre agli interessi al tasso convenzionale a far data dal 23.03.2013 (data della scoperta delle operazioni fraudolente).
L'intermediario resiste alla pretesa della ricorrente ritenendo di non essere responsabile per il fatto avvenuto, avendo adottato un sistema sicuro con codici strettamente personali e avendo proposto alla ricorrente l'attivazione di un sistema di sicurezza a due fattori. Nel dettaglio, la resistente argomenta come segue:

- la carta di credito è stata rilasciata nel gennaio 2008 con modalità di rimborso a saldo ed utilizzabile tramite il circuito di pagamento MasterCard;
- le operazioni disconosciute sono state rendicontate con gli estratti conto mensili del 1.03.2013 e del 1.04.2013;
- dagli opportuni approfondimenti presso il circuito MasterCard è emerso che le operazioni in contestazione erano state correttamente concluse;
- tali operazioni sono state effettuate con l'ausilio del servizio "Securcode", a cui la cliente si è registrata, ottenendo il relativo account, una password per effettuare le operazioni on-line sui siti certificati "Securcode" e un "messaggio personale", che appare su ogni schermata di richiesta di inserimento della predetta password al fine di confermarne la legittima provenienza;
- tali elementi di sicurezza, essendo strettamente personali, "non possono essere carpiti se non con la corresponsabilità del detentore dei dati che è responsabile di ogni conseguenza dannosa che possa derivare dall'eventuale uso improprio degli stessi". La ricorrente non ha, pertanto, rispettato gli obblighi di custodia e buon uso della carta previsti dalle Condizioni Generali di contratto della carta;
- la ricorrente conosceva perfettamente le modalità di funzionamento di tale servizio, avendolo già utilizzato per effettuare altre operazioni, mai contestate;
- la ricorrente non fornisce "alcun elemento concreto atto ad identificare la natura fraudolenta delle operazioni", né fornisce alcuna prova dell'adozione delle opportune precauzioni a tutela della propria "postazione d'accesso on-line" (ad es. l'installazione di un programma antivirus sul proprio PC);
- la ricorrente non fornisce neanche alcun elemento probatorio della presunta clonazione della carta, né alcun riferimento circostanziato in ordine al modo e al momento in cui questa si sarebbe verificata;
- la ricorrente ha provveduto tardivamente a bloccare la carta e a sporgere denuncia (rispettivamente in data 23.03.2013 e 29.03.2013), in quanto dagli estratti conto risulta che le operazioni in contestazione sono avvenute per la maggior parte tra la

fine di febbraio 2013 e l'inizio di marzo 2013. Le condizioni contrattuali prevedono, infatti, che in caso di smarrimento, sottrazione, falsificazione o contraffazione, il titolare è tenuto, tra l'altro, ad inviare all'emittente entro le 48 ore successive, copia autentica della denuncia presentata alle autorità competenti;

- la nuova procedura di sicurezza delle password "usa e getta" generate dal "Token" costituisce "una integrazione dei mezzi messi a disposizione del titolare della carta per la sicurezza dei suoi acquisti effettuati on-line, che non lo sottrae dall'osservanza dei menzionati obblighi di custodia e buon uso dello strumento di pagamento" e, all'uopo, essa è stata comunicata nella "Proposta di modifica unilaterale del contratto relativo alla carta di credito" inviata alla ricorrente unitamente all'estratto conto del 31.12.2012.

L'intermediario chiede al Collegio di rigettare il ricorso in quanto infondato.

Diritto

Il ricorso è fondato.
Ad avviso del Collegio, nel caso di specie risultano decisive le seguenti circostanze. In primo luogo, la carta della ricorrente era assistita da un sistema di sicurezza ad un solo fattore. Solo in un secondo momento, e comunque dopo i fatti di causa, l'intermediario resistente ha offerto alla ricorrente la nuova procedura di sicurezza delle password "usa e getta" generate dal "Token" ("Proposta di modifica unilaterale del contratto relativo alla carta di credito" inviata alla ricorrente unitamente all'estratto conto del 31.12.2012, ma con decorrenza dal 1 aprile 2013). Secondo l'orientamento consolidato dei Collegi il sistema di sicurezza ad un solo fattore deve ritenersi inadeguato rispetto all'evoluzione tecnologica ed alle esigenze di sicurezza connessa all'impiego di strumenti di pagamento elettronico (*ex multis*, decisioni n. 203/2013; 598/2014).
In secondo luogo, l'esame delle ventuno operazioni contestate attesta che alcune di esse risultano concentrate lo stesso giorno presso lo stesso operatore; si vedano in particolare quelle recanti la data del 20 marzo 2013 (ben dieci). Trattasi di circostanza indubbiamente anomala, che l'intermediario avrebbe potuto agevolmente rilevare mediante i normali sistemi di monitoraggio in uso presso gli operatori professionali (per un precedente in termini cfr. decisione n. 5058/2014). Del resto, ai sensi dell'art. 8 del D.M. 30 aprile 2007, n. 112 (Regolamento di attuazione della L. 17 agosto 2005, n. 166, recante «Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento») si configura il rischio di frode di cui all'articolo 3, comma 1, della legge citata, quando viene raggiunto – tra gli altri – il parametro di "tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita", oppure il parametro di "sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento". Entrambi i parametri risultano verificati nel caso di specie. In proposito si veda la decisione di questo Collegio n. 3534/2014.
A ciò si aggiunge la mancata attivazione del servizio SMS-alert; rientra infatti nella diligenza dell'intermediario – in quanto operatore professionale – assumere l'iniziativa di mettere a disposizione della propria clientela gli strumenti di protezione idonei a prevenire l'utilizzo fraudolento delle carte di pagamento, e tra questi rientra certamente anche il servizio in discorso. Si vedano sul punto le decisioni di questo Collegio n. 3536/2014 e 2319/2014. La presenza di questo servizio avrebbe potuto consentire al ricorrente di bloccare la carta subito dopo il primo utilizzo fraudolento.
Quanto all'argomento difensivo della resistente, incentrato sul preteso ritardo con cui la ricorrente si sarebbe attivata per bloccare la carta, il Collegio ritiene trattarsi di un'eccezione irrilevante, e comunque inidonea a dimostrare la sussistenza della colpa

grave a carico dell'utilizzatore dello strumento di pagamento. Infatti, fermo restando quanto già osservato circa l'insufficienza dei presidi di sicurezza predisposti dalla resistente, non vi è evidenza del momento in cui la ricorrente avrebbe ricevuto gli estratti conto della carta di credito, momento che – a seguire l'argomentazione dell'intermediario – risulterebbe decisivo ai fini della valutazione del comportamento del cliente.
In conclusione la condotta della ricorrente non è stata connotata dal requisito essenziale della colpa grave e che, pertanto, deve esserle riconosciuto il diritto di essere tenuta indenne dal pregiudizio subito, salva l'imputazione a suo carico dell'importo di cui all'art. 12, 3° comma, D.Lgs. n. 11/2010, che il Collegio quantifica nella misura di € 150 (centocinquanta).
Pertanto, in accoglimento del ricorso, deve statuirsi che l'intermediario sia tenuto a risarcire al ricorrente la complessiva somma di € 2.761,80 (duemilasettecentosessantuno/80), pari alle somme richieste dal ricorrente, detratto l'importo a carico di quest'ultimo di € 150 *ex* art. 12, 3° comma, D.Lgs. n. 11/2010.

P.Q.M.

Il Collegio dispone che l'intermediario corrisponda alla ricorrente la somma di 2.761,80 oltre interessi legali dalla data del reclamo al saldo.
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e al ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS