

## COLLEGIO DI ROMA

composto dai signori:

(RM) MASSERA	Presidente
(RM) SIRENA	Membro designato dalla Banca d'Italia
(RM) POZZOLO	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro designato da Associazione rappresentativa degli intermediari
(RM) MARINARO	Membro designato da Associazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Nella seduta del 21/07/2016 dopo aver esaminato:

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

### Fatto

In data 31 agosto 2015, alle ore 01:12, veniva effettuato un acquisto di € 963,98 via web (e-commerce), in località Surrey (GB), con le credenziali della carta di credito della ricorrente. La ricorrente veniva a conoscenza della suddetta operazione attraverso il servizio di Sms Alert.

Custodiva sempre diligentemente la carta ed i relativi codici, senza portarli mai a conoscenza dei terzi. Pertanto, contestava immediatamente l'operazione non autorizzata.

Alle 6:30 dello stesso giorno, l'attrice inviava un fax alla resistente per bloccare la carta e per contestare l'operazione.

In data 9 settembre, compilava un ulteriore modulo di contestazione tuttavia, alcuni giorni dopo le veniva ugualmente addebitato sul c/c, collegato alla carta di credito, l'importo oggetto dell'operazione contestata.

In data 23 novembre, veniva a conoscenza dal call center dell'intermediario, del mancato accoglimento dell'oggetto del reclamo, inoltrava un'ulteriore nota di contestazione sia all'intermediario convenuto che alla Visa, gestore del circuito di pagamento.

L'11 dicembre 2015, la convenuta confermava il rigetto del reclamo in quanto il pagamento online era, a suo dire, avvenuto attraverso il sistema 3D Secure (verified by Visa) e,

dunque, non si poteva trattare di una frode. La ricorrente sottolinea come tale affermazione non veniva mai provata dalla resistente.

Inviava una diffida al riaccredito della somma illegittimamente prelevata dal conto. L'intermediario rispondeva rigettando la richiesta con le medesime motivazioni del primo diniego.

L'istituto non verificava, presso il rivenditore, a chi fosse stata consegnata la merce pagata e né forniva alcuna prova che, nella transazione fosse stato utilizzato il codice di sicurezza.

Anche nel caso in cui fosse stato utilizzato, questi fa presente che è orientamento costante dell'ABF ritenere che il codice di sicurezza 3D sia una "chiave statica" e quindi, non in linea con i più recenti standard di sicurezza. Inoltre, "il sistema 3 D Secure" presenta degli elementi di sicurezza, in quanto richiede anche una password personale per effettuare acquisti on line. Tuttavia, per la presenza di una chiave "statica" e non dinamica, come più volte ha rilevato questo Collegio, il sistema non rientra tra i sistemi considerati maggiormente validi, ai fini di assolvere l'obbligo di predisporre presidi di sicurezza rafforzati, così come si evince dalle disposizioni della Banca d'Italia in materia" (Collegio di Roma n. 4807/2013).

La ricorrente chiede quindi il rimborso della somma di € 963,98 per l'operazione non autorizzata.

L'intermediario resiste al ricorso e precisa quanto segue.

Dall'analisi effettuata, emerge che l'operazione contestata è stata disposta su un sito internet, il cui esercente è stato censito come "sicuro" (Full 3 D Moto 5) e abilitato ad effettuare solo operazioni che necessitano dell'autenticazione del partecipante.

Nello specifico, la transazione contestata è stata eseguita mediante il sistema di protezione antifrode 3 D Secure (Verified by Visa), il quale prevede, durante l'acquisto, l'inserimento del numero carta, del codice di sicurezza riportato sul retro della carta (CVV), nonché della password personale e segreta stabilita dalla cliente.

Ribadisce che il suddetto sistema di autenticazione inibisce l'utilizzo della carta per gli acquisti on line in assenza dell'autorizzazione del titolare. Nel caso di specie infatti, l'esecuzione della transazione è stata disposta solo previo inserimento di credenziali note unicamente al titolare della carta. La titolare della carta di pagamento si è registrata al sistema di protezione antifrode in data 5 febbraio 2014.

Alla luce di quanto esposto, è ascrivibile alla ricorrente una violazione gravemente colposa degli obblighi di conservazione della carta di credito e dei codici personali e dunque, è applicabile la disciplina prevista ai sensi dell'art. 12 comma 4, D.lgs. 11/2010, che prevede l'esclusione della franchigia nella sopportazione delle perdite, qualora l'utilizzatore abbia agito in modo fraudolento, o non abbia adempiuto ad uno o più obblighi di cui all'art. 7 con dolo o colpa grave.

L'intermediario chiede dunque che venga rigettato integralmente il ricorso non sussistendo alcuna responsabilità in capo alla parte convenuta e, in subordine, chiede l'applicazione della franchigia ai sensi art. 12 comma 3 D.lgs. 11/2010. Inoltre, egli chiede il rigetto della richiesta risarcitoria in quanto infondata.

## **Diritto**

La controversia origina dalla richiesta di ripetizione di somme sottratte mediante l'utilizzo fraudolento della carta di credito della parte ricorrente.

La disciplina di riferimento per la soluzione del caso sottoposto all'esame di questo Collegio è contenuta nel D.lgs. 11/2010 ed in particolare negli artt. 7, 10 e 12. Infatti, ai sensi dell'art. 7, comma 1, lett. b) (che individua gli obblighi a carico dell'utilizzatore dei

servizi di pagamento in relazione agli strumenti di pagamento): «L'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di ... b) comunicare senza indugio, secondo le modalità previste nel contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza».

L'art. 10 codifica poi l'inversione dell'onere della prova: «1. Qualora 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. - 2. Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è 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».

Alle norme citate si collega poi quella prevista dall'art. 12 (che regola la responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento), che al comma 1, dispone che «Salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b)»; al comma 3, invece prevede che «Salvo il caso 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, prima della comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b), l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a 150 euro la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento»; e in base al comma 4 «Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7 con dolo o colpa grave, l'utilizzatore sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 150 euro di cui al comma 3».

La controversia in esame è relativa al disconoscimento di una operazione non autorizzata per la somma di euro 963,98 effettuata in data 31 agosto 2015 (la carta è stata utilizzata alle ore 1.12, per compiere un'unica operazione per un acquisto su un sito web estero).

Si rileva dall'istruttoria come la parte ricorrente abbia provveduto a richiedere il blocco della carta di credito inviando un fax il giorno stesso dell'avviso ricevuto tramite sms dell'operazione fraudolenta e che poi abbia presentato denuncia dell'accaduto.

L'intermediario rileva che l'operazione contestata è stata disposta su un sito internet il cui esercente è stato censito come "sicuro" e certificato ad effettuare solo operazioni che necessitano dell'autenticazione del partecipante. In particolare, l'operazione disconosciuta sarebbe stata disposta attraverso il sistema 3D-Secure (verified by Visa), che inibisce l'utilizzo della carta di credito in assenza di autorizzazione del titolare, prevedendo il sistema in questione l'inserimento del codice titolare, del codice riportato sul retro della tessera e della password personale.

La transazione, inoltre, sarebbe avvenuta su un sito internet qualificato da appositi protocolli di sicurezza previsti da circuiti internazionali, che permettono l'esecuzione di transazioni mediante l'utilizzo di credenziali note unicamente al titolare della carta.



Peraltro, nel caso di specie, non è presente prova del fatto che, per quella specifica operazione disposta il 31/08/2015, sia stato inserito l'ulteriore codice richiesto dal sistema di sicurezza citato.

Questo Collegio ha avuto modo di affrontare analoghe controversie rilevando come anche con la adesione al servizio "Verified by Visa" non possa considerarsi fornita prova certa dell'elemento del dolo o colpa grave del ricorrente, la cui presenza soltanto potrebbe integrare la sua responsabilità per l'accaduto. Non è invero escluso che una intrusione illecita nel sistema sia comunque potuta avvenire (in termini, Coll. Roma, dec. n. 1904/2014; dec. n. 562/2015).

Deve dunque ritenersi applicabile nella specie la norma dell'art. 10, comma 2, D.lgs. 11/2010 e la domanda proposta con il ricorso deve essere integralmente accolta.

Applicata la franchigia di euro 150,00 di cui all'art. 12, comma 4, D.lgs. 11/2010, l'importo che l'intermediario dovrà corrispondere alla parte ricorrente è pari ad euro 813,98

### **PER QUESTI MOTIVI**

**Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 813,98 con 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 alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE

Firmato digitalmente da  
MAURIZIO MASSERA