

COLLEGIO DI ROMA

composto dai signori:

(RM) SCIUTO	Presidente
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) PROTO	Membro designato dalla Banca d'Italia
(RM) GRANATA	Membro di designazione rappresentativa degli intermediari
(RM) PETRILLO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - GRANATA ENRICO

Seduta del 11/01/2019

FATTO

Con ricorso presentato in data 30.3.2018 il ricorrente, titolare di una carta di credito collegata a un conto corrente intrattenuto presso l'intermediario convenuto, riferisce di aver ricevuto da detto intermediario, alle ore 17:25 e 17:27 del 5.9.2017, tre *sms* da cui emergeva che erano in atto delle transazioni sul proprio conto corrente.

Precisa che, appurato di essere ancora in possesso della propria carta di credito e certo di non aver autorizzato nessuno al compimento delle operazioni in questione, accedeva alla propria area personale sul portale dell'intermediario per verificare l'accaduto, riscontrando due pagamenti effettuati con la propria carta di credito alle ore 15:27 e 17:26, rispettivamente per l'importo di € 409,00 e € 979,00.

Riferisce di aver immediatamente telefonato all'apposito numero verde al fine di procedere al blocco della carta. Lamenta di non aver ricevuto alcun *sms* che segnalasse il compimento della prima transazione. Ritiene che i due *sms* inviati dall'intermediario (alle ore 17:25 e 17:27) si riferissero soltanto alla seconda transazione, ossia quella effettuata alle ore 17:26, sottolineando che la propria tempestiva attivazione al fine di impedire il compimento dell'operazione sia stata vanificata dagli *"oltre 30 minuti di attesa necessari per contattare l'operatore del numero verde"*. Una più sollecita risposta da parte dell'operatore avrebbe permesso di impedire l'effettuazione della transazione.

Precisa che la propria carta di credito non era abilitata ad effettuare transazioni a favore di siti denominati “scommesse e *gaming online*”, mentre la prima transazione risulta essere stata effettuata proprio in siti specializzati in tale tipo di attività.

Ritiene che l'intermediario non abbia attuato tutte le misure necessarie per impedire la frode.

Riferisce di aver presentato denuncia all'A.G. l'8.8.2017 e, il giorno successivo, ulteriore denuncia ad integrazione della precedente nonché reclamo all'intermediario tramite modulo di disconoscimento delle due operazioni in questione, ove dichiara di non aver ceduto la carta o rivelato il PIN a terzi.

Chiede il rimborso della somma di € 1.388, corrispondente all'importo complessivo delle operazioni disconosciute.

Con le controdeduzioni, l'intermediario precisa che la carta in questione è una carta di pagamento.

Afferma che non è possibile accogliere l'istanza di rimborso degli importi delle operazioni contestate, in quanto le verifiche effettuate hanno accertato la legittima esecuzione e sostanziale regolarità delle operazioni stesse.

Evidenzia che i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità nell'effettuazione delle transazioni, in quanto le stesse sono state disposte a seguito di diretta ed immediata autenticazione da parte del legittimo titolare ed eseguite con sistema dinamico di autenticazione (codice OTP).

Chiede che il ricorso sia rigettato e, ove accolto, che sia applicata la franchigia di legge.

DIRITTO

Le operazioni contestate sono state effettuate in vigenza del D.Lgs. 27 gennaio 2010, n. 11, il quale ha attuato nell'ordinamento giuridico italiano la direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno europeo, prima dell'entrata in vigore delle modifiche apportate dal D.Lgs. 218/2017. La responsabilità di un prestatore di servizi di pagamento è disciplinata dall'art. 12 del D.Lgs. 11/2010 nel testo vigente all'epoca delle transazioni.

Nel caso di specie, le operazioni di pagamento non autorizzate dal ricorrente sono state compiute prima che esso effettuasse all'intermediario resistente la comunicazione prevista dall'art. 7, 1° comma, lett. b), del D.Lgs. n.11 del 2010.

L'art. 12, 3° comma, del medesimo decreto statuisce che *«salvo il caso in cui 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'art. 7, 1° comma, lett. b), l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a € 150,00 la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento»*.

Alla luce di tale disposizione, trattandosi di un fatto impeditivo dell'esercizio del diritto risarcitorio da parte della parte ricorrente, l'onere di provare la colpa grave (o addirittura il dolo) di quest'ultima grava sull'intermediario resistente, ai sensi dell'art. 2697, 2° comma, c.c. Tale soluzione è stata espressamente affermata dal Collegio di Coordinamento di questo Arbitro nella decisione n. 5.304 del 17 ottobre 2013. Secondo la giurisprudenza di legittimità, la colpa grave è costituita da una *«straordinaria e inescusabile»* imprudenza, negligenza o imperizia, la quale presuppone che sia stata violata non solo la diligenza ordinaria del buon padre di famiglia di cui all'art. 1176, 1° comma, c.c., ma anche *«quel grado minimo ed elementare di diligenza generalmente osservato da tutti»* (Cass., 3 maggio 2011, n. 913; Cass., 19 novembre 2001, n. 14.456). Questo Arbitro si è

costantemente richiamato a tale orientamento giurisprudenziale, com'è stato ribadito dalla già richiamata decisione del Collegio di Coordinamento n. 5.304 nonché dalla decisione n. 6.168 del 2013.

Va inoltre considerato quanto disposto dall'art. 10, 2° comma, del D.lgs. n. 11 del 2010, il quale statuisce che *«quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzazione 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 ... non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7»*.

Venendo al caso di specie il ricorrente disconosce due operazioni per l'importo rispettivamente di € 409,00 e di € 976,00, effettuate *online* il 5.9.2017. Afferma di non aver ceduto la carta di pagamento o rivelato il PIN a terzi.

Dalle evidenze informatiche prodotte dall'intermediario resistente risulta che tali operazioni sono state effettuate rispettivamente alle 15:26 GMT del 5.9.2017, per l'importo di € 976,00,00 a favore di un esercente italiano, e alle 15:27 GMT del 5.9.2017, per l'importo di € 409,00 a favore di un esercente britannico, senza alcuna anomalia o irregolarità, tramite sistema dinamico di autenticazione attraverso l'utilizzo di codice OTP.

L'intermediario riferisce che tale codice viene inviato al cliente tramite *sms* e fornisce prova dell'avvenuto invio dello stesso, per ciascuna delle due operazioni contestate, a numero di cellulare coincidente con quello indicato dal ricorrente nel modulo di disconoscimento delle operazioni presentato all'intermediario, oltretutto nella denuncia all'A.G. L'intermediario fornisce inoltre evidenza dell'avvenuta digitazione manuale del PAN della carta ai fini dell'effettuazione delle operazioni in questione.

Il ricorrente produce fotocopia due messaggi *sms* inviati a nome dell'intermediario resistente alle ore 17:25 e alle ore 17:27 (del 5.9.2017) contenenti ciascuno una *password* dispositiva. Sostiene che gli stessi si riferiscono soltanto alla seconda transazione contestata e lamenta il mancato invio di *sms* che segnalasse l'effettuazione della prima operazione. Si rileva peraltro che gli orari di detti messaggi, espressi in ore italiane (pari a GMT + 2), sono coerenti con quelli delle operazioni contestate espressi in GMT; non vi è pertanto motivo di ritenere che si riferissero entrambi, come affermato dal ricorrente, alla seconda operazione contestata, dovendosi invece concludere che con ciascuno di essi sia stata comunicata la *password* necessaria per l'effettuazione di ciascuna delle operazioni contestate.

Dalle evidenze sopra indicate, emerge pertanto l'adozione da parte dell'intermediario di un sistema di protezione, basato su congegni in grado di generare mutevoli *password* monouso (codice OTP) che, aggiungendosi alla *password* fissa nota solo all'utente e/o alle sue credenziali (numero della carta, PAN, CVC2 e data di scadenza) concorrono a formare un sistema di autenticazione forte a "due fattori". Per costante indirizzo di questo Arbitro, tale sistema viene considerato elevare al massimo livello attualmente possibile il grado di protezione del cliente (Collegio di Roma, decisione n. 6.606 del 20 luglio 2016) e idoneo a precludere qualunque altro modo per il terzo di poter accedere sul conto del cliente.

Dalla documentazione in atti non emergono elementi utili alla ricostruzione delle modalità con cui soggetti terzi possano essere venuti in possesso delle credenziali del ricorrente e dei codici autorizzativi necessari per il compimento delle operazioni. Peraltro, considerata sia la qualità del sistema di protezione basato su requisiti di autenticazione forte sia la circostanza che le *password* necessarie per l'effettuazione delle operazioni contestate risultano essere state effettivamente inviate all'utenza intestata a parte ricorrente, può ragionevolmente presumersi, in mancanza d'ogni altra allegazione da parte attorea che

consenta di supporre diverse ipotesi, che tali operazioni siano imputabili a negligente custodia dei codici di accesso e dei dispositivi personalizzati da parte del ricorrente medesimo (Coll. Roma, decisione n. 6606/16; Collegio Torino n. 673/2018).

Si aggiunge che, trattandosi nel caso di specie, di due operazioni effettuate in immediata successione non rileva l'adozione o meno, da parte dell'intermediario, di un sistema di *sms alert*.

Il ricorso non è pertanto meritevole di accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MAURIZIO SCIUTO