## COLLEGIO DI BOLOGNA

composto dai signori:

| | |
|---|---|
| (BO) MARINARI | Presidente |
| (BO) DI STASO | Membro designato dalla Banca d'Italia |
| (BO) MARTINO | Membro designato dalla Banca d'Italia |
| (BO) LUCARELLI | Membro designato da Associazione rappresentativa degli intermediari |
| (BO) MARINARO | Membro designato da Associazione rappresentativa dei clienti |

Relatore MARCO MARINARO

Nella seduta del 06/06/2017 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 espone, anche a mezzo della documentazione allegata al ricorso, che:

- era titolare di una carta di credito rilasciata dall'intermediario resistente;

- in data 24.11.2016, alle ore 13,17 riceveva un SMS da parte della resistente che lo informava del cambio del numero di cellulare associato alla carta, ove veniva inviato il codice necessario per l'autorizzazione delle operazioni di pagamento on line;

- alle ore 13,30 circa dello stesso giorno contattava il servizio clienti dell'intermediario e, non conoscendo il nuovo numero di telefono abbinato alla carta, provvedeva a bloccare la stessa;

- apprendeva in seguito a email della convenuta (cfr. denuncia acclusa al ricorso) che, mediante la carta di cui era titolare, erano state effettuate due operazioni di pagamento on line dell'importo complessivo di euro 1.115,89: si tratta, in particolare, di un pagamento dell'importo di 599,99 euro e di 515,90 euro per acquisti online;

- in data 24.11.2016 sporgeva denuncia-querela per l'accaduto;

- sempre in data 24.11.2016, presentava formale disconoscimento delle operazioni all'intermediario che, tuttavia, rigettava la richiesta di rimborso sostenendo che il numero di cellulare abbinato alla carta era stato regolarmente variato mediante il portale titolari e che le operazioni di pagamento contestate sono state regolarmente autorizzate mediante il codice OTP necessario per concludere i pagamenti on line;

- rivolgeva plurime richieste all'intermediario volte a conoscere il numero di cellulare a cui erano stati inviati gli OTP necessari per concludere le operazioni on line oltre che l'indirizzo di consegna della merce acquistata on line e di essere riuscito ad ottenere risposta da parte dell'intermediario solo dopo avere pubblicato il racconto dell'accaduto sulla propria pagina facebook;

- in seguito procedeva ad effettuare un'integrazione della denuncia già sporta con le informazioni fornite dall'intermediario;

- precisa, altresì, che la carta mediante la quale sono state compiute le operazioni di pagamento è sempre rimasta in suo possesso e che non ha mai risposto ad email di phishing.

Il ricorrente afferma il proprio diritto al rimborso dell'importo relativo alle operazioni disconosciute, pari a 1.115,89 euro, non avendole autorizzate né effettuate, ma essendo stato vittima di truffa da parte di ignoti.

L'intermediario, nel confermare i fatti, resiste al ricorso ed espone quanto segue:

- la variazione del numero di cellulare abbinato alla carta può essere effettuata solo accedendo, con la digitazione delle credenziali personali, all'area riservata del portale titolari;

- il ricorrente, dopo aver saputo dal servizio clienti che mediante la carta di credito erano state effettuate due operazioni di pagamento on line per un importo di 1.115, 89 euro, alle ore 14,07 del 24.11.2016 ha bloccato la carta;

- le transazioni contestate si sono concluse secondo le regole del "3D Secure", il protocollo di sicurezza voluto dai circuiti internazionali per dare tutela ai clienti( ), come dimostrano: i) i log dei tre passaggi di certificazione delle operazioni; ii) le evidenze dei messaggi di consegna OTP;

- nel caso di specie, chi ha utilizzato le credenziali di accesso al "portale titolari" e ha cambiato il numero di cellulare abbinato alla carta, ha potuto concludere l'acquisto on line grazie alla conoscenza del codice OTP ricevuto via SMS, oltreché dei dati del titolare e dei CVV riportato sul retro della carta;

- l'accesso al portale da parte di soggetti diversi può avere solo due spiegazioni: a) il cliente non ha custodito diligentemente le chiavi di accesso al portale titolari e qualcuno se ne è impossessato; b) il cliente ha fornito utenza e password ad una terza persona, che poi ne ha approfittato.

L'intermediario ritiene che sia ravvisabile "un atteggiamento superficiale e non responsabile" del ricorrente che ha senza dubbio favorito il compiersi dell'episodio fraudolento per il quale, adesso, chiede il rimborso all'intermediario. Pertantom chiede che il ricorso sia respinto.

## DIRITTO

1. - La controversia origina dalla richiesta di ripetizione di somme sottratte mediante

l'utilizzo fraudolento della carta di credito della parte ricorrente.

Il ricorrente in particolare disconosce due operazioni di pagamento effettuate il 24 novembre 2016 mediante la sua carta di credito, su due siti web relativi a noti negozi di elettronica.

Il ricorrente non ha prodotto l'estratto conto e non fornisce prova che le operazioni di pagamento siano state addebitate sulla propria carta. Gli addebiti non sono stati tuttavia contestati dall'intermediario, che ha anzi prodotto i log dell'operazione e l'autenticazione del 3D Secure, da cui emerge conferma: i) della data (24.11.2016, ore 13,31 e ore 13,56); ii) degli importi (515,90 euro e 599,99 euro); iii) dei beneficiari dei pagamenti.

L' intermediario fa presente che il numero dell'utenza telefonica associata alla carta è stato variato mediante il "portale titolari" e, a sostegno, produce la relativa documentazione dalla quale emerge che il numero di telefono associato alla carta è stato modificato alle ore 13,17 del 24.11.2016, pochi minuti prima che fossero compiute le operazioni di pagamento contestate.

Il ricorrente ha prodotto l'SMS, inviato dall'intermediario alle ore 13,17 del 24.11.2016, con cui veniva informato della variazione del numero di cellulare abbinato alla carta:

Il ricorrente, pertanto, riconosce di aver ricevuto il predetto SMS (cfr. anche denuncia allegata al ricorso) e, nella denuncia allegata, afferma di aver tempestivamente contattato il servizio clienti e di aver provveduto al blocco della carta, non conoscendo tale nuova utenza. L'intermediario ha prodotto il log di blocco della carta dal quale emerge che esso è avvenuto in data 24.11.16 alle ore 14,07.

L'intermediario ha prodotto i log delle operazioni di pagamento disconosciute e i log dei passaggi di certificazione dell'operazione che ne attestano la sua conformità alle regole del 3D Secure. L'intermediario ha anche fornito evidenza degli SMS di invio del codice OTP al ricorrente (al numero di utenza cellulare come modificato).

L'intermediario afferma che le transazioni disconosciute dal ricorrente si è correttamente conclusa mediante l'inserimento nel sistema dei rispettivi codici OTP, inviati al numero di telefono cellulare associato alla carta e che tale numero era stato modificato mediante l'accesso al portale titolari.

2. – Rileva il Collegio in via preliminare che alcuna documentazione contrattuale è stata prodotta circa i sistemi di protezione, di accesso e di autenticazione al "portale titolari" che consentono di modificare dati (in particolare il numero di cellulare) che a loro volta consentono poi di carpire il c.d. O.T.S. (codice inviato via sms).

Peraltro, si osserva che l'invio tramite SMS della notifica di variazione dell'utenza cellulare collegata al sistema di autenticazione delle operazioni dispositive appare sicuramente utile ma scarsamente efficiente e sicuramente poco idoneo a tutelare efficacemente la clientela.

Si tratta infatti di un sistema di mera notifica di avvenuta modifica (che potrebbe non giungere tempestivamente a destinazione o potrebbe non giungere affatto per problemi connessi al gestore dell'utenza telefonica mobile, o semplicemente potrebbe essere letto senza la necessaria immediatezza a causa di una serie di variabili fattuali che – ovviamente - non possono essere ascritte ipso facto ad una condotta colposa del cliente), non essendo previsti sistemi di autorizzazione mediante l'utilizzo di diversi canali di comunicazione utili a meglio proteggere il cliente da una tipologia di truffe divenute rapidamente sempre più frequenti in quanto sfruttano un evidente vulnus del sistema di accesso medianti chiavi statiche al "portale titolari".

3. - 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. 5, 7, 10 e 12.

In base all'art. 5, co. 1 e 2, D.lgs. 11/2010 «Il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento. In assenza del consenso, un'operazione di pagamento non può considerarsi autorizzata» ed «Il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento è prestato nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento».

Ai sensi dell'art. 7, comma 1, lett. a) e b), D.lgs. 11/2010 (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: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso; 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 D.lgs. 11/2010 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».

Infine, secondo quanto statuito dall'art. 11, co. 1, D.lgs. 11/2010 (e fatto salvo l'art. 9), «nel caso in cui un'operazione di pagamento non sia stata autorizzata, il prestatore di servizi di pagamento rimborsa immediatamente al pagatore l'importo dell'operazione medesima».

4. - Nel caso di specie appare evidente che l'intermediario pur avendo esibito il "log" delle operazioni non ha fornito prova che il ricorrente abbia effettivamente autorizzato le operazioni in contestazione.

Mediante il c.d. "log" l'intermediario ha provato l'utilizzo di uno strumento di pagamento registrato, ma la sola produzione del medesimo "log" non è sufficiente a consentire di ritenere «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».

Ed infatti, si rileva dall'istruttoria come la parte ricorrente abbia provveduto a richiedere il blocco della carta di credito con immediatezza e che poi abbia presentato denuncia dell'accaduto. Né vi sono ulteriori elementi che possano far ritenere che ragionevolmente il cliente sia venuto meno agli obblighi di custodia della carta di credito e delle credenziali di accesso al "portare titolari".

5 - L'intermediario resistente precisa che le operazioni contestate sono state disposte su siti internet i cui esercenti sono stati censiti come sicuri e certificati ad effettuare solo operazioni che necessitano dell'autenticazione del partecipante. In particolare, le

operazioni disconosciute sarebbero state disposte 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 del codice OTS.

Le transazioni, inoltre, sarebbe avvenute su siti 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.

I Collegi ABF hanno avuto modo di affrontare analoghe controversie rilevando come anche con l'adesione al servizio "Verified by Visa" non possa considerarsi fornita ipso facto 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 (ABF Coll. Roma, dec. n. 1904/2014; dec. n. 562/2015).

6. – Invero, un sistema multifattore con chiave dinamica al portale ed un sistema di autorizzazione protetto di modifica dei dati che concorrono all'attività dispositiva della carta di credito avrebbero concorso sicuramente ad apprestare una più elevata protezione al titolare della carta utile a prevenire simili tipologia di frodi. Come anche il monitoraggio costante non soltanto delle operazioni dispositive, ma degli accessi al portale titolari avrebbe consentito di rilevare questi rischi di frode (si pensi, ad es., al cambio rapido e ripetuto del numero di cellulare, ma anche dell'indirizzo di posta elettronica, quali evidenti elementi sintomatici di un rischio di frode che possono condurre ad un blocco cautelativo ex art. 6, comma 2, lett. b, D.lgs 11/2010).

L'evoluzione costante dei metodi utilizzati per carpire le credenziali informatiche nell'utilizzo delle carte di pagamento (che sfruttano i punti deboli sei sistemi di protezione, come nel caso di specie, dell'accesso al "portale titolari" per la modifica del numero di cellulare ove ricevere la chiave dispositiva OTS azzerandone l'efficacia di strumento di sicurezza), impone una costante attenzione, una puntale analisi ed una incessante evoluzione dei connessi sistemi di protezione del cliente. Qualora i clienti nell'utilizzo di questi sistemi dovessero ritenersi non sufficientemente protetto, inizierebbero a limitarne sino a dismetterne totalmente il loro utilizzo con buona pace della diversa esigenza di rafforzare e diffondere gli strumenti elettronici di pagamento.

Di qui la scelta legislativa dell'inversione dell'onere della prova e del rigore imposto nella valutazione della colpa grave a carico dell'utilizzatore (cfr. Coll. Coord., dec. n. 3498/2012, sulla scorta della decisione del Coll. Roma, dec. n. 1111/2010 e poi Coll. Coord., dec. n. 991/2014) allocando quindi sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento (Coll. Coord., dec. n. 3947/2014).

7. – Pertanto, nella fattispecie in esame, dai fatti rappresentati in narrativa e dalle evidenze disponibili acquisite nel contraddittorio tra le parti, emerge che il ricorrente non ha autorizzato le operazioni contestate e che probabilmente è stato vittima di una macchinazione fraudolenta da parte di terzi malfattori, avente una modalità particolarmente sudbdola ed invasiva. Se ciò è accaduto, è stata la conseguenza di un sistema di protezione scarsamente sicuro apprestato dall'intermediario il quale seppur ha previsto un meccanismo di autenticazione dell'operazione multifattore con chiave dinamica (c.d. 3D Secure con OTS), non ha adeguatamente protetto l'accesso al "portale titolari" dotato di un sistema ad unico fattore con chiave statica e che consente la modifica di dati

da utilizzare per effettuare operazioni (azzerando di fatto la protezione della chiave dinamica mediante OTP da utilizzare per la fase dispositiva). Per cui, anche a voler ammettere che possa ravvisarsi nel comportamento del ricorrente una colpa, quest'ultima non è pertanto suscettibile di essere qualificata come "grave".

Secondo l'insegnamento della Suprema Corte, la colpa grave è costituita infatti 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, comma 1, 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.14456).

In difetto di tale prova questo Collegio considera pertanto le operazioni di pagamento di cui si discute come non autorizzate dal ricorrente e, pertanto, a lui non opponibili, con conseguente sussistenza di un dovere di integrale rimborso in capo all'intermediario ai sensi e nelle forme dell'art. 11, comma 1, del D.lgs. n. 11/2010.

## PER QUESTI MOTIVI

**Il Collegio dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 1.115,89 (millecentoquindici/89).**

**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
MARCELLO MARINARI