

COLLEGIO DI NAPOLI

composto dai signori:

(NA) MARINARI	Presidente
(NA) PARROTTA	Membro designato dalla Banca d'Italia
(NA) GIUSTI	Membro designato dalla Banca d'Italia
(NA) SAMPAGNARO	Membro designato da Associazione rappresentativa degli intermediari
(NA) BARTOLOMUCCI	Membro designato da Associazione rappresentativa dei clienti

Relatore SAMPAGNARO GABRIELE

Nella seduta del 30/11/2015 dopo aver esaminato:

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

FATTO

La controversia sottoposta alla cognizione del Collegio riguarda la richiesta di rimborso di somme fraudolentemente sottratte alla parte ricorrente mediante operazioni di prelievo dalla stessa disconosciute. Questi, in sintesi, i fatti oggetto del procedimento. In data 31.3.2015 la ricorrente subiva il furto del portafogli contenente la carta bancomat. A seguito del furto, venivano effettuati n. 5 prelievi da ATM, tutti in rapida successione, per l'importo complessivo di euro 1.500,00. Contattata da un operatore dell'intermediario, la ricorrente disconosceva le operazioni effettuate; provvedeva quindi a richiedere il blocco della carta e a denunciare l'accaduto alla P.G. La ricorrente, assistita da legale, contesta il mancato funzionamento del servizio di *sms alert*, sottoscritto in sede di apertura del conto corrente, ovvero la sua sospensione unilaterale e priva di preavviso che, di fatti, ha impedito di provvedere al tempestivo blocco della carta ed evitare quantomeno il compimento delle operazioni successive alla prima. Come affermato dalla ricorrente, all'interno del portafoglio erano custoditi il codice PIN della carta; inoltre, il furto è avvenuto in luogo di lavoro aperto alla pubblica utenza. Tuttavia, la circostanza della custodia del PIN congiuntamente allo strumento di pagamento non sarebbe sufficiente a far ricondurre esclusivamente a suo carico le responsabilità della vicenda. Per queste ragioni, la

ricorrente chiede la restituzione dell'importo integrale delle somme addebitate in conseguenza della sottrazione fraudolenta della carta di pagamento.

In sede di controdeduzioni l'intermediario rileva che le operazioni fraudolente sono state effettuate con tecnologia a microchip, utilizzo della plastica originale e digitazione del PIN, come risulta anche dalla perfetta progressione del contatore esadecimale del microchip. In ordine al mancato invio degli *sms alert*, afferma che il servizio è contrattualmente previsto non per tutte le operazioni ma solo per quelle *“ritenute potenzialmente più rischiose”*. Conclude sottolineando che i prelievi fraudolenti sono avvenuti in conseguenza dell'incauta custodia del PIN da parte della titolare della carta, circostanza che ha determinato un grave inadempimento contrattuale delle condizioni di utilizzo della carta stessa e chiede, pertanto, il rigetto della domanda di parte ricorrente.

DIRITTO

La ricorrente è titolare di una carta di debito emessa dall'intermediario resistente e adisce il Collegio chiedendo la restituzione integrale della somma sottratta fraudolentemente a seguito di cinque operazioni eseguite successivamente al furto della carta di pagamento. La controversia si aggiunge al novero di una molteplicità di casi di cui questo ed altri collegi (incluso il Collegio di Coordinamento), si sono stabilmente occupati. Come avvenuto per vicende analoghe, anche al caso di specie va applicata la disciplina del D. Lgs. 27 gennaio 2010 n. 11 in attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, dal momento che i fatti da cui è scaturita la presente controversia si sono svolti successivamente al 01.03.2010, data di entrata in vigore del decreto legislativo. Il quadro normativo dettato dal D. Lgs 11/2011 chiarisce gli obblighi sia del prestatore sia dell'utilizzatore di servizi di pagamento, ed è a questi obblighi che il Collegio deve principalmente prestare attenzione al fine di assolvere al suo ruolo di organo decidente circa i diritti e gli oneri delle parti intervenute nell'odierna controversia. Ciò premesso, e con riferimento agli obblighi dell'utilizzatore, secondo tale disciplina "[...] 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" (art. 12, comma 3); nel contempo, 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'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 precedente" (art. 12, comma 4). A mente dell'art. 7, l'utilizzatore è tenuto ad utilizzare la carta di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso (*lett. a*). La norma tuttavia prosegue, al comma 2, con una disposizione che recita "Ai fini di cui al comma 1, lettera a), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo". Come argomentato dal Collegio di Coordinamento nella sua decisione n. 5305/2013, argomentazione alla quale questo Collegio aderisce pienamente, le due citate disposizioni devono necessariamente essere lette in modo congiunto. Da un lato, l'adozione delle misure idonee a garantire la sicurezza dei codici di accesso deve costituire un elemento necessario ed imprescindibile per l'utilizzo dello strumento di pagamento, tanto è vero che esso è oramai puntualmente regolato dalle pattuizioni

negoziali in uso nei rapporti tra intermediari e clienti. Dall'altro, è possibile configurare un obbligo *ex lege* in capo all'utilizzatore in ordine all'adozione di misure idonee atte a garantire la sicurezza ed il regolare utilizzo dello strumento; la "idoneità" delle misure deve essere interpretata in accezione ampia, potendosi far ricadere in essa una vasta gamma di comportamenti che si distinguono sia sotto il profilo temporale, sia sotto il profilo contenutistico. Quanto al primo aspetto, infatti, deve ritenersi che detti obblighi incombono sull'utilizzatore dal ricevimento dello strumento e sin tanto che l'utilizzatore resti in possesso dello strumento di pagamento. Quanto al secondo aspetto invece, è da ritenersi che l'utilizzatore sia chiamato a rispettare gli obblighi di conservazione e di custodia, inclusa la memorizzazione dei codici di accesso, purché rientranti nella sfera di controllo del cliente, al fine di garantirne il diligente utilizzo. Ed è proprio in relazione ai ridetti obblighi, che il Collegio osserva un incauto comportamento di parte ricorrente. Il complesso delle circostanze riferite attesta, infatti, una responsabilità per colpa, anche grave, in ordine alla mancata custodia e messa in sicurezza sia dello strumento sia del codice identificativo dello stesso. Con riferimento alla conservazione dello strumento, le modalità del furto dichiarate (furto avvenuto in locali aperti al pubblico) denotano quantomeno una scarsa diligenza che pone il comportamento della ricorrente in contrasto con il dato normativo del sopra menzionato art. l'art. 7 del D. Lgs. 11/2010. Con riguardo alla memorizzazione del codice identificativo, va osservato che le stesse operazioni fraudolente sono state commesse a brevissima distanza – temporale e fisica – tra il furto del bancomat ed i primi utilizzi contestati, il che impone di ritenere che le credenziali per l'utilizzo della carta di pagamento fossero facilmente state rinvenute unitamente alla carta medesima. Ed infatti, è la stessa ricorrente che conferma –sia nel ricorso sia nelle denunce presso la P.G.– che all'interno del portafoglio sottratto da ignoti era custodito, oltre alla carta di pagamento, anche un foglietto su cui era stato trascritto il codice identificativo (Pin) della stessa carta di pagamento. Va osservato che questo ultimo elemento deve essere reputato come dato essenziale per il rilievo, da parte del Collegio, della colpa grave in capo alla ricorrente. Con riguardo, inoltre, alle considerazioni di parte ricorrente circa il mancato funzionamento o la supposta sospensione del servizio di *sms-alert*, il Collegio ritiene di non poter imputare all'intermediario alcuna violazione dei criteri di diligenza e buona fede nell'esecuzione del contratto per il solo fatto che questi ha omesso di segnalare l'effettuazione del primo prelievo con un messaggio di alert. Atteso che, come chiarito dall'intermediario, il cliente non aveva aderito al servizio sms premium – pure pubblicizzato come servizio aggiuntivo ed a pagamento rispetto a quello operante in via automatica – che gli avrebbe consentito di ricevere un messaggio di conferma per ogni operazione e non soltanto per quelle di rilevante importo, appare difficile ritenere che, dato il brevissimo intervallo sussistente fra le cinque operazioni (consistente di soli 5 minuti) l'eventuale segnalazione mediante il sistema di alert telefonico potesse interrompere la sequenza di utilizzi fraudolenti della carta (cfr. tra le tante, la decisione n. 55/2014). Non di meno va osservato che, benché il servizio *sms-alert* non fosse operativo perché non sottoscritto, l'intermediario sia comunque intervenuto con tempestività mediante un contatto telefonico grazie al quale, comunicando l'anomala successione di prelievi (contatto peraltro avvenuto con un lasso temporale minimo rispetto ai prelievi fraudolenti), si è consentito alla ricorrente di avvedersi della frode consentendo il successivo blocco della carta.



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

P.Q.M.

Decisione N. 2876 del 31 marzo 2016

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI