IL COLLEGIO DI COORDINAMENTO

composto dai Signori:

Dott. Giuseppe Marziale Presidente del Collegio ABF di Roma	Presidente
Prof. Avv. Enrico Quadri Presidente del Collegio ABF di Napoli	Membro effettivo
Prof. Avv. Antonio Gambaro Presidente del Collegio ABF di Milano	Membro effettivo
Prof. Marilena RISPOLI FARINA Componente del Collegio ABF di Napoli designato dal Conciliatore Bancario Finanziario (per le controversie in cui sia parte un cliente Consumatore)	Membro effettivo
Avv. Chiara PETRILLO Membro supplente Componente del Collegio ABF di Roma designato dal CNCU	Membro supplente [Relatore]

nella seduta del 19/03/2014, dopo aver esaminato

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

Fatto

Con ricorso depositato in data 16.4.2013 il ricorrente chiedeva la condanna dell'intermediario alla restituzione di €. 2.168,00.

Egli narrava che intorno alle 5:00 del mattino del 21.11.2012, trovandosi sull'autobus diretto a Malpensa ove doveva prendere un aereo, consultava sul cellulare l'estratto conto inviato via email dalla convenuta e verificava la presenza di tre prelievi e nove pagamenti tramite carta Bancomat per un totale di € 2.168,00 effettuati fraudolentemente da terzi tra il 17.11 e il 20.11 del 2012.

Alle ore 5:23 del 21.11.2012 bloccava la carta bancomat e, una volta giunto a destinazione, alle ore 13:00 presentava apposita denuncia alle autorità competenti, riferendo che il bancomat non era stato smarrito né oggetto di furto.

Il 23.11.2012 il ricorrente, asserendo l'avvenuta clonazione della carta bancomat, presentava reclamo alla banca disconoscendo n. 12 operazioni: 3 prelievi di € 250 cadauno (totale € 750,00) effettuati il 18.11 alle ore 2.08, il 19.11 alle ore 10:59 e il 20.11 alle ore 11:17; 9 pagamenti POS di cui uno per un importo di € 52,00 effettuato il 17.11 alle ore 22:56 e otto il 18.11 per un totale di € 1.366,00.

Lamentando, inoltre, che il riscontro della convenuta al reclamo gli era stato inviato oltre i 30 giorni previsti dal Regolamento, il ricorrente evidenziava che l'intermediario aveva errato nell'indicare le date dei prelievi disconosciuti, collocando due dei detti prelievi in un momento successivo alla data di blocco della carta (21.11.2013); egli obiettava, infine, che il riscontro della convenuta non faceva menzione dei nove pagamenti POS disconosciuti.

Il ricorrente deduceva e dimostrava, infine, che nei giorni 19 e 20 novembre 2012, al momento di due delle operazioni contestate, egli si trovava sul luogo di lavoro e non avrebbe, dunque, potuto effettuare dette operazioni.

In data 24.6.2013 l'intermediario depositava le proprie controdeduzioni, a mezzo delle quali, precisato che "a causa di un mero errore materiale … venivano indicate come date dei prelievi quelle del 14 novembre 2012, del 26 novembre 2012 e del 5 dicembre 2012, invece di quelle del 18, del 19 e del 20 novembre 2012", rilevava che i tre prelievi erano stati realizzati, prima dunque del blocco della carta bancomat, presso 2 sportelli ATM di BCC – situati a Romano di Lombardia (BG) e a Pagazzano (BG) - attraverso il corretto utilizzo delle credenziali di identificazione della carta stessa, deducendone che deve essere esclusa la clonazione della carta, e quindi che le operazioni devono essere avvenute mediante l'uso della carta originale, tenuto anche conto che "allo stato, non sono mai stati accertati episodi di avvenuta contraffazione di carte dotate della tecnologia microchip".

Rilevava, altresì, l'intermediario che i nove acquisti POS sono stati effettuati tra le ore 22:56 del 17.11.2012 e le 18:57 del 18.11.2012, tutti presso sportelli ATM della banca xxxxx, tra Romano di Lombardia (BG), Bergamo e Milano, ossia tutti in un'area non lontana dalla residenza del ricorrente.

La banca, asserendo quindi la piena regolarità delle operazioni disconosciute, contestava "la mancata applicazione, da parte del ricorrente, delle regole di cautela e diligenza nella custodia del suddetto strumento di pagamento tali da consentire a terze persone di entrare in possesso della carta e del relativo PIN ponendo in essere delle operazioni di cui il titolare della carta rimane comunque responsabile".

Infine l'intermediario richiamava ed allegava la consulenza scientifica commissionata da altro intermediario, nella quale si conclude che il microchip contiene in chiaro il PIN, il quale tuttavia non è ricavabile dall'esterno essendo memorizzato in un'area protetta e inaccessibile.

In considerazione di tutto quanto sopra esposto, l'intermediario instava per il rigetto del ricorso.

Con ordinanza n. 162 del 13 gennaio 2014 il Collegio di Milano, rilevato che relativamente alla soluzione delle controversie attinenti l'utilizzo fraudolento di carte con microchip sussiste una parziale diversità di orientamenti in seno ai Colleghi di questo ABF, rimetteva la questione al Collegio di Coordinamento.

Diritto

Nelle more tra l'ordinanza di rimessione relativa alla presente controversia e la trattazione della stessa in seno al Collegio di Coordinamento sono state tuttavia pubblicate due decisioni del medesimo Collegio di Coordinamento che hanno composto il contrasto dianzi prospettato. Il riferimento è alle decisioni nn. 897 del 14 febbraio 2014, in materia di clonazione della carta libretto postale, e 991 del 21 febbraio 2014, in materia esattamente di clonazione di carte di debito. Le affinità tra i due strumenti di pagamento sono note ed evidenti e dunque non vale qui la pena di indugiarvi ulteriormente, sicché entrambe le decisioni assumono rilievo ai fini della soluzione della presente controversia.

Mediante le citate decisioni si è innanzitutto definitivamente chiarito che alla fattispecie oggetto di esame è applicabile la disciplina dettata dal D. Lgs. n. 11 del 2010, concernente la attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno. Appare, infatti, necessario equiparare ai casi testualmente previsti di furto, smarrimento o utilizzo non autorizzato di una carta di pagamento l'ipotesi della clonazione ad opera di terzi malfattori.

D'altra parte, l'applicabilità di detta disciplina al caso di specie deve essere affermata anche ratione temporis, dal momento che i fatti da cui è scaturita la presente controversia sono successivi al 1° marzo 2010, data di entrata in vigore del sopra menzionato decreto legislativo.

Ciò detto, ai fini della decisione del caso di specie è necessario fare applicazione del disposto normativo degli artt. 7, 10 e 12 del citato decreto.

L'articolo 7 prevede che "1. 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. 2. 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".

Ai sensi della citata disposizione, dunque, sull'utilizzatore incombe - tra l'altro – un obbligo di custodia dello strumento di pagamento.

Il successivo articolo 12 del medesimo decreto prevede, tuttavia, che "3. 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. 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".

L'onere di provare che l'utilizzatore abbia agito con dolo o colpa grave incombe, peraltro, sull'intermediario ai sensi dell'art. 10 del su richiamato decreto, il quale recita: "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".

Come è già stato chiarito dal Collegio di coordinamento (cfr, la decisione n. 3498/2012) e ribadito dalle pronunce dianzi richiamate, la normativa "istituisce quindi un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori" (Coll. Coord. ABF n. 897 del 14.2.2014), i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema.

Si è, per di più, correttamente puntualizzato che neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato.

Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro).

La ratio di tale scelta legislativa è fin troppo notoriamente quella (cfr. Coll. Coord. decisione n. 3498/2012, sulla scorta della decisione del Collegio di Roma n. 1111/2010 e da ultimo Coll. Coord. ABF decisione n. 991 del 21.2.2014) di allocare 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.

Di fronte al su descritto quadro normativo, mentre i Collegi di Milano e Napoli hanno affermato la colpa grave del cliente per il solo fatto che lo strumento di pagamento abusivamente utilizzato fosse dotato del microchip di ultima generazione, ciò che rende "tecnicamente e statisticamente remota e trascurabile la possibilità di una clonazione", la cui prova deve essere fornita dal ricorrente ex art. 2697 cod. civ. (Collegio ABF di Milano, decisioni n. 561/2013; n. 2571/2012 e Collegio ABF di Napoli, decisioni n. 1802/2013, n. 2757/2012), il Collegio di Roma ha invece ritenuto che è l'intermediario – in base ai principi scolpiti con l'art. 1218 c.c. – a dover provare di aver adempiuto agli obblighi di custodia e salvaguardia del denaro del cliente con la diligenza professionale qualificata, identificata dalla ormai costante giurisprudenza come "diligenza del buono ed accorto banchiere", onere non assolto qualora quest'ultimo si limiti ad escludere la clonabilità delle carte che utilizzano il sistema a microchip e per ciò solo a presumere la negligente custodia, da parte del cliente, della carta e dei relativi codici dispositivi (Collegio ABF di Roma, decisioni n. 960/2012 e 292/2013).

A soluzione di tale contrasto il Collegio di Coordinamento, con la decisione n. 897 del 14.2.2014 ha pertanto sancito che "pur senza negare la rilevanza della già evidenziata scelta legislativa di tendenziale allocazione del rischio a carico del fornitore, deve ritenersi che in presenza dell'adozione dei più avanzati dispositivi di sicurezza messi a disposizione dell'evoluzione tecnologica e di circostanze di fatto tali da escludere con sufficiente persuasività una possibile clonazione dello strumento di pagamento e da attestare una non diligente custodia dello stesso, il cliente non possa essere tenuto indenne dalle perdite patrimoniali derivanti dall'utilizzo non autorizzato del mezzo di pagamento in questione", richiedendo quindi un quid pluris rispetto alla semplice dotazione del microchip.

Nel caso di specie certamente manca la prova diretta della negligenza del cliente nella custodia dello strumento di pagamento. È tuttavia pacifico, pur prescindendo dalle decisioni del Collegio di Coordinamento sopra evocate, che l'onere della prova che incombe sull'intermediario possa essere assolto anche attraverso la c.d. presunzione, ossia attraverso l'operazione logica che consente di risalire da un fatto noto ad uno ignoto.

Veniamo, dunque, ai fatti noti, ovvero ai c.d. indizi, che, per assurgere al rango di prova presuntiva, debbono essere gravi, precisi e concordanti, come previsto dall'art. 2729 cod. civ.

L'intermediario sottolinea, innanzitutto, che (quantomeno) i tre prelievi - effettuati nei giorni 18, 19 e 20 – risultano "disposti con l'uso congiunto del PIN e del microchip elettronico presente nella carta, la quale non è materialmente clonabile", allegando a supporto delle proprie allegazioni copia del dettaglio delle operazioni bancomat da cui risulta che i suddetti prelievi sono stati effettuati mediante accesso al sistema con l'utilizzo della tecnologia "microchip", nonché una perizia, predisposta per conto di altro istituto bancario, nella quale si conclude che "non è possibile impartire comandi al chip per comunicare il PIN del richiedente" e comunque che l'estrazione del PIN, astrattamente possibile, richiederebbe comunque la disponibilità materiale della carta ed un periodo di tempo certamente non breve.

In secondo luogo l'intermediario deduce e dimostra che tutte le operazioni sono state compiute tra la provincia di Bergamo e Milano e quindi non lontano dal luogo di residenza del cliente (Milano).

Ad abundantiam, emerge poi dalla narrazione dei fatti tanto di parte ricorrente quanto di parte convenuta che dette operazioni sarebbero state abusivamente effettuate per la maggior parte nell'arco temporale di circa ventiquattro ore e più in generale nell'arco di oltre tre giorni (tra le 22,26 del 17.11.2012 e le 11,17 del 20.11.2012), mentre secondo l'id quod plerumque accidit nei casi di utilizzo fraudolento degli strumenti di pagamento i prelievi vengono effettuati in un brevissimo arco temporale (spesso inferiore all'ora) fino al raggiungimento del plafond nell'intento di trarre il massimo vantaggio dalle operazioni prima che il soggetto defraudato si accorga dell'abuso e provveda al blocco della carta. Ulteriore stranezza è poi che non risulta agli atti che nel giro dei tre giorni di abusi i terzi utilizzatori della carta abbiano raggiunto il plafond.

L'intermediario ha dunque dedotto e documentato una serie di circostanze idonee a costituire indizi chiari, precisi e concordanti nel senso che le operazioni disconosciute sono state poste in essere mediante l'impiego della carta e del codice dispositivo, sicché – pacifico il fatto che la carta stessa è sempre rimasta nella sfera di disponibilità del ricorrente – deve trarsi la ragionevole conclusione che il cliente non l'abbia custodita con la dovuta diligenza, tanto da non accorgersi

che qualcuno l'ha temporaneamente sottratta e utilizzata anche mediante digitazione del relativo PIN.

Né la allegazione del cliente, che ha provato che al momento degli ultimi due prelievi si trovava sul luogo di lavoro e quindi non può esserne l'autore, è sufficiente a togliere vigore al quadro probatorio sopra menzionato, posto che ciò che gli si contesta non è di aver effettuato personalmente i prelievi (e quindi un comportamento fraudolento), bensì di aver colposamente omesso di custodire la carta ed il PIN, sì da averne consentito a terzi l'utilizzazione.

Tuttavia, nel caso di specie l'intermediario non può andar totalmente esente da colpa. La banca, infatti, non solo non risulta aver attivato idonei strumenti di sicurezza, quali l'invio di SMS alert a seguito dei prelievi, come invece prescritto dall'art. 8 D. Lgs. n. 11 del 2010 (a norma del quale il prestatore dei servizi di pagamento è tenuto ad "assicurare che siano sempre disponibili strumenti adeguati affinché l'utilizzatore dei servizi di pagamento possa eseguire la comunicazione di cui all'articolo 7, comma 1, lettera b)"), ma inoltre ha consentito che ben dieci delle dodici operazioni contestate fossero effettuate in poco meno di ventiquattro ore.

Si rileva, infatti, che ai sensi dell'art. 8 del D.M. 30 aprile 2007, n. 112 del Ministero dell'Economia e delle Finanze (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, quando viene raggiunto uno dei seguenti parametri: … (omissis) … 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento".

Di fronte ad un rischio di frode normativamente tipizzato l'intermediario era dunque senz'altro tenuto ad attivarsi per elidere detto rischio, mentre risulta esser rimasto totalmente inerte.

Detta inerzia ha consentito, quindi, l'effettuazione di altre 5 operazioni abusive. Questo comportamento non può che far carico - secondo la disciplina della ripartizione del rischio che sopra si è ricordata, nonché secondo la disciplina generale dettata dall'art. 1227 cod civ. in materia di concorso colposo del creditore nella causazione dell'evento - all'intermediario resistente, cosicché lo stesso deve essere condannato a restituire al ricorrente la somma di denaro sottrattagli a seguito delle operazioni successive alla settima per un totale di euro 906,00.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda al ricorrente la somma di euro 906,00.
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
GIUSEPPE MARZIALE