COLLEGIO DI COORDINAMENTO

composto dai signori:

(CO) MASSERA	Presidente
(CO) MAUGERI	Membro designato dalla Banca d'Italia
(CO) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(CO) FERRETTI	Membro di designazione rappresentativa degli intermediari
(CO) MARINARO	Membro di designazione rappresentativa dei clienti

Relatore MARINARO

Seduta del 17/07/2018

FATTO

1. - La parte ricorrente espone di essere rimasta vittima di una "frode sulla […] carta di pagamento" (transazione effettuata il 10 novembre 2017 e registrata il giorno successivo) e di non aver ricevuto adeguata assistenza da parte dell'intermediario.
L'unica operazione di pagamento disconosciuta – e di cui è chiesto quindi il "risarcimento" – ammonta a € 1.314,09, come da denuncia presentata il giorno 17 novembre 2017, cui hanno fatto immediatamente seguito il formale disconoscimento dell'operazione ed il blocco dello strumento di pagamento.
2. – L'intermediario resiste al ricorso e precisa che l'operazione contestata è stata eseguita accedendo ad un sito di commercio elettronico sicuro, tramite l'utilizzo delle credenziali della carta e conferma con OTP (password numerica temporanea). Dichiara che, a partire dal 18 giugno 2016, tutte le carte di pagamento abilitate a operazioni online sono state abilitate al "servizio pagamenti sicuri internet", che prevede la digitazione di una password temporanea generata da un dispositivo elettronico in possesso del titolare (c.d. token).
Pertanto, secondo la difesa dell'intermediario, l'operazione non autorizzata non potrebbe che imputarsi ad un comportamento gravemente colposo del ricorrente, il quale non avrebbe custodito in maniera adeguata le credenziali ed il token associati alla carta. Rileva

infine che il ricorrente non avendo attivato il servizio di "sms alert", si è avveduto soltanto tardivamente – a distanza di giorni - dell'operazione fraudolenta.
L'intermediario chiede, in via principale, il rigetto della domanda; in via subordinata, il contenimento della condanna risarcitoria entro i limiti della propria quota di responsabilità, tenuto conto del concorso di colpa della parte ricorrente.
3. – Il Collegio di Torino dopo aver esaminato il ricorso nella seduta del 26 giugno 2018 e, pur avendo rilevato *«molteplici anomalie imputabili sia sul piano sostanziale sia su quello processuale all'intermediario»*, rileva che il tema controverso nel caso di specie «non è l'an della sua responsabilità, ma il quantum: se, cioè, l'intermediario sia tenuto a restituire l'intero importo relativo all'operazione disconosciuta o soltanto la parte eccedente il massimale di spesa convenuto». Pertanto, considerato che *«la soluzione di tale delicata questione può assumere rilevo anche oltre il singolo caso controverso e per importi ben più consistenti»*, il Collegio territoriale ha rimesso la decisione al Collegio di coordinamento.

DIRITTO

1. - La controversia origina dalla richiesta di ripetizione di somme sottratte mediante l'utilizzo fraudolento della carta di pagamento di cui è titolare il ricorrente e della quale dichiara di non aver mai perso la il possesso.
Il ricorso più precisamente ha per oggetto il disconoscimento di un'operazione di pagamento, segnatamente una transazione effettuata online su un sito web di commercio elettronico in data 10 novembre 2017 per un importo pari a 1.314,09 euro; l'intermediario produce la tracciatura informatica dell'operazione disconosciuta.
La parte ricorrente contesta l'operazione suindicata affermando di essere stata vittima di una truffa da parte di ignoti lamentando di fatto l'inadeguatezza del sistema di protezione adottato dall'intermediario, rivelatosi inidoneo a prevenire truffe della specie.
L'intermediario si difende eccependo che, nel caso esaminato, è ravvisabile la colpa grave del ricorrente nella custodia dei suoi dati e dei codici autorizzativi.
2. - La normativa di riferimento per la soluzione del caso sottoposto all'esame di questo Collegio è contenuta nel D.lgs. 11/2010 (attuativo della Direttiva 2007/64/CE, c.d. PSD) ed in particolare negli artt. 5, 10 e 11.
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».
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, comma 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».

3. - Nel caso di specie, dalla tracciatura fornita dalla società che gestisce il circuito di pagamento si evince che la transazione è stata effettuata tramite un sito di commercio elettronico alle ore 9:58 del 10 novembre 2017. Dall'estratto conto versato in atti dall'intermediario risulta che nel medesimo mese, prima e dopo l'operazione disconosciuta, ne sono state effettuate altre mediante il medesimo strumento di pagamento. Risulta anche che tali altre operazioni – non disconosciute dalla parte ricorrente – sono state eseguite "in presenza", cioè non attraverso il canale internet. L'intermediario riferisce che, sulla base delle evidenze documentali prodotte, l'operazione sarebbe avvenuta tramite inserimento delle credenziali della carta e successiva "digitazione della password dinamica prodotta dalla chiavetta O-key (OTP)". Dunque, mediante l'impiego di un presidio di sicurezza "a due fattori" e senza anomalie.

4. – Come puntualmente rilevato dal Collegio rimettente, occorre però evidenziare che il regolamento contrattuale prodotto in atti (sottoscritto nel 2013) non fa alcun riferimento all'esistenza di un "token" (altrimenti detto chiavetta "O-key") né ovviamente alle modalità di suo utilizzo. Ancor più a monte, a giudicare dal tenore letterale dell'art. 27 del contratto, è da rilevare che l'attivazione dei "pagamenti sicuri internet" sarebbe stata addirittura opzionale. Sul punto specifico, l'intermediario resistente si difende dichiarando – senza tuttavia fornire elementi probatori a supporto – di aver abilitato al "servizio pagamenti sicuri internet" tutte le carte di pagamento dei clienti per le operazioni online, a partire dal giugno 2016. Poiché si tratta di asserzione non circostanziata né comprovata, non può darsi per acquisito che la chiavetta sia mai stata consegnata al ricorrente né che egli sia stato reso edotto del relativo funzionamento. A ciò si aggiunga che il servizio di "sms alert", anch'esso presentato in contratto come opzionale (sez. B), non risultava attivo al momento dell'esecuzione dell'operazione disconosciuta.

5. – Sempre come emerge dall'ordinanza di rimessione, l'operazione di pagamento controversa, ammontante – lo si rammenta – ad € 1.314,09, ha superato il massimale mensile associato alla carta di credito (contrattualmente fissato a € 1.000,00). Al riguardo, l'intermediario ha fatto presente (producendo un'evidenza interna riportante la dicitura "V5 Plafond temporaneo") che il massimale sarebbe stato elevato volontariamente dal cliente fino a € 3.000,00 nell'aprile 2017, con la conseguenza che nessuno sforamento si sarebbe realizzato nel novembre 2017.

Invero, come emerge dal contratto unilateralmente predisposto dalla banca e portato alla firma del cliente, in base all'art. 28 che regola le richieste di variazione temporanea del plafond è previsto espressamente che «Il Cliente può in ogni momento chiedere […] di aumentare temporaneamente il massimale della Carta […] comunque non oltre il 50% del massimale concordato con la banca al momento della emissione». E preso atto che il massimale originariamente convenuto era di € 1.000,00, la variazione avrebbe potuto al massimo raggiungere € 1.500,00 (e non € 3.000,00, come invece riferito dalla banca resistente).

Ancor più rilevante è constatare che, a norma del secondo comma dello stesso art. 28, «l'aumento temporaneo è utilizzabile nel mese di ricevimento della richiesta da parte della banca e nel mese successivo». Ne consegue che, pur ammettendo (ma non v'è evidenza documentale che autorizzi a pervenire a tale conclusione) che il cliente abbia formulato la richiesta di variazione per un importo imprecisato nell'aprile 2017, il termine ultimo di efficacia della detta variazione sarebbe stato in ogni caso il 30 giugno 2017.

Deve quindi ritenersi provato – in linea con quanto affermato anche dal Collegio rimettente - che nel mese di novembre 2017 il massimale di spesa mensile fosse fermo a € 1.000,00. Lo sforamento del plafond all'esito di una singola operazione è, dunque, confermato, con ciò concretando anche uno degli indici di frode previsti dal D.M. 112/2007 (art. 8, lett. b, n. 2: «Si configura il rischio di frode … quando viene raggiunto uno dei seguenti parametri: b) riguardo alle carte di pagamento sottoposte a monitoraggio… 2) una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento»).

6. – L'orientamento dei Collegi territoriali ABF è conforme nel ritenere che in situazioni simili occorra *«fare applicazione del principio di diligenza professionale che gli istituti di credito devono osservare nella prestazione dei loro servizi; ambito in cui vengono in rilievo anche i c.dd. "obblighi di protezione" derivanti da un'interpretazione costituzionalmente orientata del combinato disposto degli artt. 1175 e 1375 c.c. data dalla giurisprudenza di legittimità. In questa prospettiva, si deve osservare come alla causazione dell'evento abbia contribuito in maniera determinate il mancato blocco della carta da parte dell'intermediario»* (che nel caso ivi esaminato *«avrebbe ben dovuto accorgersi dell'anomalia delle operazioni in seguito disconosciute, anzitutto in considerazione del fatto che le operazioni di prelievo presso ATM avevano ampiamente superato – come sopra ricordato – i massimali giornalieri contrattualmente previsti»* (Coll. Milano, dec. nn. 1801/2011); pertanto, la resistente, deve ritenersi responsabile *«avendo consentito un prelevamento in eccedenza rispetto ai massimali e trattandosi di responsabilità prescindente dalle superiori valutazioni sulla condotta gravemente colpevole della ricorrente circa la custodia della carta e del codice segreto»* (Coll. Milano, dec. n. 8865/2015; v. anche dec. n. 10551/2017).

Ancora più puntualmente è stato anche ritenuto che in esito all'addebito di un'operazione che ha determinato il superamento di un massimale (plafond) *«non è dunque revocabile in dubbio che il resistente si sia reso inadempiente a un suo preciso obbligo contrattuale, e cioè di non consentire un uso della carta oltre i limiti di importo pattuiti; un obbligo che appunto era previsto nell'interesse dello stesso cliente. Orbene, da questo punto di vista – e indipendentemente da qualsiasi considerazione sul se le diverse operazioni di uso della carta fossero davvero riferibili al titolare, tema, questo, che in relazione al profilo di inadempimento qui dedotto non rileva - il criterio di comportamento corretto a cui si sarebbe dovuto attenere l'intermediario era quello di bloccare in via di principio tutte le operazioni che comportavano il superamento della soglia di spesa»*; appare quindi *«inevitabile concludere che il resistente, avendo proceduto all'addebito di operazioni che hanno comportato il superamento della soglia di spesa, è tenuto a risarcire al cliente il danno derivante da tale inadempimento. Un danno che deve essere necessariamente quantificato in misura pari all'intero importo della singola operazione - … - che ha comportato il superamento della soglia di spesa, e che, per le ragioni descritte, avrebbe dovuto essere bloccata»* (Coll. Napoli, dec. n. 2762/2012).

Nello stesso senso, si è precisato che il superamento dei limiti dispositivi di operatività del bancomat comporta l'integrale restituzione al cliente dell'operazione o delle operazioni che eccedono lo stesso *«essendo responsabilità esclusiva della banca la non osservanza dell'obbligo contrattualmente assunto di limitare i prelievi giornalieri e mensili»* (Coll. Roma, dec. n. 4960/2013; v. anche dec. n. 764/2015 e dec. n. 7857/2015; Coll. Bologna, dec. n. 11146/2017), giungendo a precisare che in tali casi non è possibile applicare la franchigia (ex art. 12, comma 3, D.lgs. 11/2010) *«dal momento che in nessun caso l'intermediario deve consentire che venga superato il massimale giornaliero e che nessun rischio al riguardo possa essere sopportato dagli utilizzatori degli strumenti di pagamento»* (Coll. Roma, dec. n. 7408/2015); d'altronde la franchigia *«essendo prevista per i casi di*

utilizzo indebito dello strumento di pagamento conseguente a furto o smarrimento, non trova applicazione nel caso in esame in quanto trattasi di operazioni non autorizzate (ex art. 5, D.lgs. 11/2010)» (Coll. Bologna, dec. n. 11848/2017; riconoscono il rimborso integrale, ex multis, anche Coll. Napoli, dec. n. 2762/2012, Coll. Roma, dec. nn. 764/2015, 7857/2015; Coll. Milano, dec. n. 7949/2017; Coll. Bari, dec. n. 12185/2018).

7. - Occorre poi rilevare che l'intermediario deduce che il ricorrente non ha attivato il servizio di "sms alert", assumendosi di conseguenza il rischio di subire movimentazioni sospette senza avere la possibilità di riceverne la comunicazione in tempo reale.

Invero, è stato già da tempo ritenuto che *«la mancanza di sistemi di allerta comunemente utilizzati dagli intermediari per diminuire i rischi connessi al furto di strumenti elettronici di pagamento, come l' "sms alert", rappresenta un ulteriore elemento che contribuisce alla causazione dell'evento dannoso ed è imputabile all'intermediario»* (Coll. Milano, dec. nn. 1801/2011).

Al riguardo, i Collegi territoriali ABF hanno costantemente affermato che il servizio "sms alert" costituisce ormai uno standard di sicurezza normalmente esigibile in relazione all'utilizzo delle carte di pagamento e, dunque, un presidio di sicurezza divenuto ormai necessario per la tutela degli utilizzatori di tali strumenti (ex multis, Coll. Roma, dec. n. 2319/2014 e n. 3536/2014; v. anche dec. n. 541/2016; si discorre di obbligo incombente sul prestatore di servizi di pagamento, Coll. Bari, dec. n. 16707/2017, ovvero di un obbligo di applicazione automatica, Coll. Palermo, dec. n. 13205/2017).

La mancanza di questo servizio è, quindi, di per sé idonea a spostare verso l'intermediario il rischio connesso ad operazioni fraudolente avvenute con l'impiego di tali strumenti (Coll. Roma, dec. n. 620/2014, n. 1937/2014 e n. 7227/14; v. anche dec. n. 4131/2015), configurando un'ipotesi di responsabilità da inadeguata organizzazione imputabile esclusivamente all'intermediario resistente (ex multis, Coll. Roma, dec. n. 128/2012, n. 2770/2013, n. 2338/2014 e dec. n. 9262/2015; Coll. Bologna, dec. n. 14975/17; Coll. Bari, dec. n. 12185/2018) e appare opportuno che di tale rilievo sia tenuta adeguata considerazione nelle relazioni con la clientela (Coll. Bologna, dec. n. 10519/18).

Tuttavia, nel caso di specie, la carenza di tale servizio non assume alcuna efficienza causale risultando quindi ininfluente per la decisione, posto che si tratta di una sola operazione di pagamento ed il disconoscimento – sia pur effettuato dopo pochi giorni – non ha aggravato la posizione del cliente e tantomeno la responsabilità della banca.

8. – Ad avviso di questo Collegio il profilo del superamento del c.d. plafond (e cioè di uno dei massimali, nel caso di specie, quello mensile, di utilizzo della carta fissato contrattualmente) è del tutto assorbente di ogni altri rilievo attinente alla responsabilità nella custodia della carta e delle sue credenziali relative alla sua operatività online e ciò in quanto tale fatto (mancato blocco da parte dell'intermediario di una o più operazioni eccedenti rispetto al massimale pattuito) è dotato di efficienza causale dirimente. Infatti, è di palese evidenza, che il blocco per il superamento del plafond avrebbe evitato l'operazione contestata nella sua interezza e l'avviso del mancato buon fine della stessa avrebbe consentito anche al cliente di avvedersi tempestivamente del tentativo di frode in atto (che avrebbe potuto attivarsi per evitare ulteriori tentativi mediante il rapido blocco della carta). D'altronde lo stesso intermediario una volta registrato tale tentativo avrebbe dovuto attivare ogni opportuno controllo a tutela del cliente posto che con tale tentativo si eccedeva l'intero plafond mensile dello strumento di pagamento (art. 8, lett. b, n. 2, D.M. 112/2007).

L'importo dell'operazione disposta fraudolentemente con la quale viene superato uno dei limiti massimi contrattualmente fissati (c.d. plafond) per l'utilizzo dello strumento elettronico di pagamento deve essere quindi interamente restituita al cliente e ciò in quanto difetta del suo consenso risultando difforme alle limitazioni contrattuali di operatività dello stesso. In

tali casi la condotta dell'intermediario concreta la violazione delle norme pattizie poste quali obblighi di protezione gravanti sui prestatori di servizi di pagamento in ragione di un'interpretazione costituzionalmente orientata del combinato disposto degli artt. 1175 e 1375 c.c.

Il limite concordato tra le parti comporta infatti che il sistema predisposto dall'intermediario debba essere impostato in modo tale da non consentire operazioni che superino il plafond, nel senso che ogni operazione eccedente debba essere bloccata automaticamente (tale requisito è necessario perché il sistema si possa ritenere conforme ai presidi di sicurezza imposti dalla legge). Se ciò non avviene l'intera operazione è per ciò stesso illecita, in quanto vìola il limite di operatività della carta sul quale il cliente fa affidamento e deve ritenersi ipso facto non autorizzata se disconosciuta (ex art. 10, comma 1, D.lgs. 11/2010).

Pertanto, nei casi in cui l'intermediario consente l'esecuzione di un'operazione di pagamento che eccede rispetto ai massimali concordati con il cliente è responsabile per la medesima (dal momento che in nessun caso deve consentire tale sforamento) a prescindere dalla condotta di quest'ultimo, non potendo questi essere perciò stesso gravato di alcun rischio e non dovendo dunque sopportare alcun onere. A fronte di un'operazione (o di più operazioni) poste in essere che superano uno dei limiti di utilizzo (plafond), la carenza del consenso del titolare dello strumento di pagamento diviene assorbente in quanto la stessa deve ritenersi non autorizzata (art. 5, comma 1, D.lgs. 11/2010).

9. - Peraltro, nel caso in cui sia stata eseguita un'operazione di pagamento non autorizzata, occorre sottolineare che – secondo quanto previsto dalle legge - il prestatore di servizi di pagamento è tenuto a rimborsare al cliente l'importo dell'operazione medesima immediatamente e, in ogni caso, al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Ed ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore deve riportare il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data della valuta dell'accredito non sia successiva a quella dell'addebito dell'importo (in applicazione di quanto disposto dall'art. 11, comma 1, D.lgs. 11/2010).

Appare evidente che – ed a prescindere in questo caso anche dalla mancata eccezione dell'intermediario sul punto - la franchigia eventualmente prevista contrattualmente sulla base dell'art. 12, comma 3, D.lgs. 11/2010, essendo consentita esclusivamente per i casi di utilizzo indebito dello strumento di pagamento conseguente a furto o smarrimento, non può trovare applicazione in tutte quelle situazioni ove si accerti la sussistenza di operazioni non autorizzate dovendo in simili situazioni essere sempre interamente riaccreditata la somma sottratta con la valuta del giorno dell'addebito.

10. – In conclusione può affermarsi il seguente principio di diritto: «L'operazione di pagamento con la quale viene superato uno dei limiti massimi contrattualmente fissati (c.d. plafond) per l'utilizzo dello strumento elettronico di pagamento, deve essere interamente restituita al cliente in quanto, se disconosciuta, difetta del suo consenso. A tale operazione non risulta applicabile nemmeno la franchigia eventualmente prevista dal contratto per i casi di furto o smarrimento in quanto trattasi di operazione di pagamento non autorizzata».

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 1.314,09, con valuta riferita al giorno dell'addebito.
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