Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SCIUTO	Presidente
(RM) PAGLIETTI	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) NERVI	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - PAGLIETTI MARIA CECILIA

Seduta del 26/06/2020

Esame del ricorso n. 0228340/2020 del 19/02/2020

proposto da [redacted]

nei confronti di 2008 - [redacted]

COLLEGIO DI ROMA

composto dai signori:

(RM) SCIUTO	Presidente
(RM) PAGLIETTI	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) NERVI	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - PAGLIETTI MARIA CECILIA

Seduta del 26/06/2020

FATTO

Il ricorrente, tramite il proprio rappresentante volontario, espone di aver appreso, in occasione della consultazione dell'estratto conto della propria carta di credito rilasciata dall'intermediario convenuto, dell'esistenza di operazioni di pagamento disposte senza autorizzazione. Sporta denuncia (in data 01.11.2019), insoddisfatto del negativo riscontro al reclamo previamente esperito in data 19.12.2019, sostenendo di aver sempre rispettato gli obblighi di sicurezza nella custodia della propria carta bancomat e del pin (cfr. art. 7, comma 1, lett. a) e comma 2, d.lgs. 11/2010), chiede il rimborso della somma sottratta, negando di aver mai prestato il consenso alle operazioni contestate, delle quali non era a conoscenza stante l'assenza di alcun sistema di notifica. Deduce l'anomalia delle operazioni contestate, riferendo che l'utilizzo normale della carta consisteva in singole operazioni e mai in operazioni multiple nell'àmbito della medesima giornata. Specifica infatti che:

- la prima operazione è stata effettuata su sito e-commerce russo, "*avente caratteri in cirillico ed importi esclusivamente in Rubli*"; l'operazione è pertanto "*diametralmente al di fuori dalle normali abitudini di spesa*" del ricorrente, pensionato;
- la seconda operazione è stata autorizzata appena un minuto dopo la prima; si tratterebbe di "*una vera e propria frode seriale perpetrata nei confronti di altri soggetti, come da denuncia querela di altro soggetto", cliente del medesimo difensore*" (in particolare: "*presenza di un importo del tutto simile, esatta*

coincidenza del rivenditore (...) *ed ancora medesima residenza dei frodati – Roma*");

Contesta, dunque, la negligente condotta della resistente, lamentando il mancato blocco della carta nonostante i chiari indici di anomalia delle operazioni rispetto al normale utilizzo. Lamenta, inoltre, il mancato ricevimento di alcun messaggio di allerta. Sottolinea che, nonostante dalla lettura dell'estratto conto allegato, si evinca che la banca abbia previsto un limite di utilizzo mensile di euro 2.000,00, la convenuta ha autorizzato l'operazione di euro 1.394,49 mentre sul conto il saldo utilizzato era di euro 1.652,94; per questo motivo, l'operazione "*non solo non doveva in alcun modo essere autorizzata,*" ma la banca avrebbe dovuto altresì disporre il "*blocco automatico per quanto disposto dall'art. 68 della Direttiva 2015/2366/UE, poiché richiedente un pagamento in misura superiore ai limiti concordati*". Rileva, inoltre, che la banca non ha permesso al ricorrente "*l'adozione di sistemi di sicurezza personalizzati*", "*quali ad esempio la limitazione dell'utilizzo della carta in particolari sistemi o circuiti od ancora categorie merceologiche o Paesi intra ed extra UE*".

Conclusivamente imputa la realizzazione delle operazioni fraudolente all'insufficienza del sistema di sicurezza predisposto dalla banca. Il ricorrente chiede la restituzione della somma di euro 1.578,31.

Costituitosi, l'intermediario chiede il rigetto del ricorso in quanto infondato.

Quanto alla propria condotta, deduce l'assolvimento di tutti gli obblighi previsti a proprio carico dal D.Lgs 11/2010, fornendo evidenza dell'adozione dei presidi di sicurezza a due fattori, e di un protocollo di sicurezza antifrode 3D Secure. Specifica che le operazioni sono state autorizzate a mezzo inserimento, oltre che dei dati della carta (16 cifre, data scadenza, nome del titolare, cvc2/cvv2), del codice di autorizzazione previsto per le operazioni di e-commerce generato dal dispositivo che fornisce, tempo per tempo, al titolare della carta, password usa e getta (OTP), configurando così la c.d. autenticazione forte; produce i relativi log. Imputa alla "*incauta custodia degli strumenti di pagamento*" da parte del ricorrente la realizzazione delle operazioni.

L'intermediario ritiene dunque probabile che gli autori del *phishing*, in possesso delle credenziali della parte ricorrente, abbiano modificato l'utenza mobile abbinata alla carta di credito, così che i codici OTP venissero correttamente generati ed inviati al nuovo numero. Eccepisce l'avvenuto invio, alla parte ricorrente, di due sms alert (riproduce la relativa schermata); si duole, dunque, della colpevole inerzia del ricorrente il quale avrebbe dovuto tempestivamente bloccare la carta, laddove, al contrario, il blocco della carta è avvenuto "*solo molti giorni dopo*". In relazione alla contestazione di avvenuto superamento del plafond, rimanda alla documentazione allegata "*dove è chiaramente evidente che una delle operazioni riportate nell'estratto conto del mese di ottobre* (...) *sia in effetti da riferire al mese di settembre e pertanto ricompresa nel plafond del mese precedente* (...)"; evidenzia la presenza di due operazioni, tra quelle non disconosciute dal cliente, tentate in data 18.10.2019, non autorizzate per esaurimento del plafond, a riprova del corretto funzionamento del blocco per superamento del massimale. In sede di repliche, il ricorrente ribadisce le proprie posizioni.

DIRITTO

Con riguardo al caso che occupa (due operazioni di pagamento online disconosciute, effettuate a valere sulla carta di credito del ricorrente in data 03.10.2019 -ore 13:35 e ore 13:36-, per un importo totale di euro 1.578,31, comprensivo della commissione per cambio divisa estera sulla seconda operazione), il Collegio rileva preliminarmente che la collocazione temporale delle operazioni disconosciute fa rientrare l'accertamento del diritto

fatto valere da parte ricorrente nell'àmbito della nuova disciplina sui sistemi di pagamento, d. lgs. 11/2010, così come modificato dal d. lgs. 218/2017, di recepimento della Direttiva 2015/2366 (cosiddetta PSD2). In particolare, viene in gioco l'art. 12 nella sua nuova formulazione, che concerne la responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento. Nell'applicare la disposizione richiamata, il Collegio si basa sull'interpretazione che ritiene immodificati il regime della responsabilità e quello probatorio precedentemente applicati (Coll. Milano, Dec. n. 9465/2019).
Così individuata la disciplina applicabile *ratione temporis*, va specificato che la fattispecie in esame è stata più volte sottoposta all'attenzione dell'ABF, che ha fondato le proprie decisioni sulla valutazione, da un lato, dell'adeguatezza del sistema di protezione adottato dall'intermediario (art. 8, D.Lgs. 11/2010); e, dall'altro, dell'adempimento del corretto obbligo di custodia dello strumento di pagamento da parte dell'utilizzatore (cfr. art. 7, comma 1, lett. a) e comma 2, D.Lgs. cit.).
Il Collegio ritiene che, ai fini della soluzione della controversia che occupa, dirimente appaia l'omessa allegazione, da parte della resistente, della presenza di un sistema di autenticazione a doppio fattore.
Ricordato che la condotta della banca nella predisposizione di sistemi anti-frode, deve sottostare al canone dell'art. 1176, comma 2, c.c. (noto essendo che l'attività bancaria è attività riservata: Coll. Milano, decisione n. 1241/2010), ed essere idonea soddisfare il livello di diligenza professionale e qualificata dell'accorto banchiere, va rilevato che il parametro assunto da questo Arbitro per valutare la diligenza è l'adeguatezza dei presidi di sicurezza informatica a prevenire l'uso fraudolento degli strumenti di pagamento e ad elevare al massimo livello attualmente possibile il grado di protezione del cliente (*ex multis* Coll. Roma, decisione n. 6606/16; Coll. coord., decisione n. 3498/12 cit.).
È opinione risalente e consolidata di questo Arbitro – anche anteriore all'entrata in vigore del d.lgs. 11/2010 - che la diligenza dell'accorto banchiere implichi, sul piano del diritto generale dei contratti, l'obbligo di adozione di un modello organizzativo adeguato alla tipologia di operazioni poste in essere, essendo l'attività bancaria ascritta alla categoria delle attività pericolose (art. 2050 c.c.), tale per cui lo sforzo tecnico protettivo debba essere idoneo a prevenire possibili eventi pregiudizievoli. Sulla scorta di questa impostazione, e anche a séguito dell'introduzione di una disciplina di diritto speciale di rango primario (art. 10-bis, d.lgs. 11/2010 nella versione vigente, di recepimento della Dir. 2013/2066) e subprimario (Circolare n. 285/2013 della Banca d'Italia, "*Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*", aggiornamento del 2016; e gli "*Orientamenti finali sulla sicurezza dei pagamenti via Internet*" di EBA del dicembre 2014), questo Arbitro ha statuito che la mancata adozione di un sistema di sicurezza (a doppio o) multi-fattore integri anch'essa un comportamento doloso o gravemente colposo (Coll. coord., dec. n. 6166/2013), posta l'inidoneità della sola password statica a tutelare il cliente.
Con riguardo alle caratteristiche del sistema di sicurezza predisposto dalla resistente, il ricorrente deduce l'adozione di un sistema a due fattori (così come anche previsto dal contratto versato in atti) dove, tuttavia, l'autenticazione sarebbe "doppia" solo nel senso che prevede l'inserimento per due volte degli stessi dati (quelli relativi alla carta e la password statica), disattendendo, nella sostanza, la logica sottesa all'autenticazione forte.
Nei propri scritti difensivi la resistente, inoltre, non smentisce espressamente tale affermazione né produce un asserto probatorio utile a confutarla, insistendo, per converso, sull'adozione del protocollo di sicurezza 3D Secure.
Questo Collegio ritiene che l'adozione di un servizio siffatto non sia di per sé idonea a qualificare il livello di sicurezza di un sistema, poiché esso, costituendo un mero protocollo

di trasmissione dei dati, non assurge un elemento qualificativo del livello di protezione garantito da un sistema.
L'attestata presenza di una password dinamica necessaria ai fini della autorizzazione alla disposizione di pagamento, è dunque sufficiente, di per sé, ad integrare la presenza di un elemento delle categoria della possesso ma non a soddisfare i requisiti richiesti dalla normativa di settore ai fini della configurazione di un sistema di autenticazione forte, essendo necessario, come noto, che l'utilizzo almeno di un secondo elemento (della conoscenza o dell'inerenza), posto che, in linea con quanto stabilito dalla richiamata *opinion EBA*, i dati della carta non sono idonei costituire né un elemento di possesso, né un elemento di conoscenza.
La mancata predisposizione di un sistema di autenticazione a due fattori va considerata avere rilevanza assorbente nella concreta concatenazione degli eventi, dovendo dunque il Collegio pronunciarsi per l'accoglimento della domanda.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda a parte ricorrente la somma di Euro 1.578,31.
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 SCIUTO