Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) DE CAROLIS	Presidente
(BA) TUCCI	Membro designato dalla Banca d'Italia
(BA) SEMERARO	Membro designato dalla Banca d'Italia
(BA) STEFANELLI	Membro di designazione rappresentativa degli intermediari
(BA) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MASSIMIANA COSTANTINO

Seduta del 20/06/2019

FATTO

Dopo aver esperito infruttuosamente il reclamo in data 23.11.2018, parte ricorrente, in data 25.02.2019, ha proposto ricorso, nel quale, in qualità di intestataria di un conto corrente presso l'intermediario resistente, rappresenta che, in data 18/07/2017, veniva disposto da parte di ignoti un bonifico *on line*. In particolare, riferisce di non conoscere il beneficiario né di aver mai incautamente smarrito o divulgato a terzi i codici di accesso all'*home banking* o il dispositivo generatore del "*Codice O-Key*". In data 21/07/2017 inviava alla resistente modulo di disconoscimento del bonifico e chiedeva lo storno immediato della somma fraudolentemente sottratta. Peraltro, la resistente riscontrava la lettera rappresentando che il danno subito dalla ricorrente era addebitabile esclusivamente al proprio comportamento nonostante, con *e-mail* del 19.07.2017 (quindi prima che la ditta disconoscesse il bonifico), avesse segnalato come "*sospetta quindi potenzialmente rischiosa*" l'operazione. In data 26/07/2017, la ricorrente sporgeva denuncia alle competenti autorità. Ciò premesso, ritiene pertanto configurarsi una responsabilità contrattuale della banca per non aver adottato ogni misura necessaria a garantire la sicurezza dell'*home banking*. Richiama gli art. 1218 c.c. e 10 e 11, comma 1, D.Lgs. n. 11/2010 nonché gli artt. 2043 e 2050 c.c. Chiede quindi all'Arbitro di condannare la parte resistente al pagamento di € 1.575,00, oltre a interessi, rivalutazione monetaria e spese legali. L'intermediario si è costituito, facendo pervenire le proprie controdeduzioni, nelle quali innanzitutto eccepisce che, come si evince dal file *excel* prodotto in atti, alle 11.30 del 18.7.2017 è stata regolarmente aperta una sessione con inserimento del nome utente

e del Pin e, alle 11.35, è stato disposto il bonifico con digitazione della *password OTP*. Sostiene che la cliente sia incorsa in una classica ipotesi di *phishing*: infatti, dai sistemi informatici risulterebbe che l'operazione sia stata posta in essere regolarmente, mediante inserimento dei codici di accesso e della password OTP generata dal *token O-Key*. Inoltre, rileva che non emergono circostanze di fatto *"idonee a evidenziare un'aggressione informatica operata a danno del ricorrente attraverso un* malware *particolarmente sofisticato e tale da escludere ogni colpa*" in capo alla ricorrente. Esclude pertanto qualsiasi violazione dei propri sistemi e, difatti, la ricorrente non avrebbe offerto prove in tal senso. Circa i sistemi di sicurezza adottati, richiama diversi precedenti ABF sull'idoneità dei sistemi "*a più fattori*" e specifica che, nel caso di specie: a) il canale di comunicazione del servizio è cifrato (protocollo *https*), protetto da certificato emesso da apposita *Certification Authority*; b) l'infrastruttura è protetta da un *cluster di firewall* che consente la comunicazione dei soli protocolli http e https; c) l'infrastruttura è regolarmente assoggettata a verifiche di sicurezza (*Network Vulnerability Assessment e/o Web Application Penetration Test*); d) il sistema di gestione per la sicurezza delle informazioni è certificato ISO/IEC 27001, *standard* che costituisce il riferimento internazionale per la sicurezza delle informazioni; e) al cliente viene consegnato il dispositivo elettronico *O-Key (*associato univocamente al codice di accesso) che genera *password* dinamiche di 6 cifre aventi le seguenti caratteristiche: algoritmo standard di sicurezza (3DES o AES) con chiave/seme conosciuto solo dai *server* del gruppo bancario; durata limitata; visualizzazione sullo schermo per soli 16 secondi; annullamento immediato dopo il suo utilizzo; riconoscimento e validazione del codice da parte del *server*. Aggiunge di aver tempestivamente contattato la ricorrente al fine di segnalare la natura sospetta dell'operazione, prima, con telefonate (senza esito positivo, verosimilmente a causa del guasto alle linee telefoniche di cui la ricorrente pure ha dato atto) e, poi, con un'*email* inviata in data 19/07/2017 all'indirizzo di posta elettronica specificato pure sul timbro della società. Evidenzia che la ricorrente ha disconosciuto l'operazione del 18/7 soltanto il 21/07 e che tale ritardo ingiustificato ha reso non possibile il recupero delle somme.

DIRITTO

Come desumibile dalla narrativa, parte ricorrente chiede all'Arbitro di: "*1) Condannare la Banca … al pagamento in favore della ditta … della somma complessiva di € 1.575,00 oltre al pagamento degli interessi e della rivalutazione monetaria, per i motivi di fatto e di diritto esposti nel file denominato "Reclamo e messa in mora" (che si allega) e nel file denominato "Esposizione della vicenda oggetto di ricorso e dei motivi del ricorso" (già allegato); 2) Condannare la Banca …alla rifusione delle spese, competenze ed onorari (da liquidarsi allo scrivente e all'Avv. …) del presente procedimento*." L'intermediario chiede, in via principale, il rigetto del ricorso. In subordine, chiede la ripartizione fra le parti del danno in misura proporzionale alle rispettive effettive responsabilità. La questione sottoposta al Collegio concerne il disconoscimento di un bonifico *on line* del valore di € 1.575,00, effettuato il 18/07/2017, che il ricorrente asserisce di non aver mai disposto. In via preliminare, si evidenzia che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, precedentemente alle modifiche operate dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. I principi che regolano la materia sono, dunque, quelli fissati da detto decreto nonché dal relativo Provvedimento attuativo della Banca d'Italia del 5.7.2011, applicabili al caso di specie. Alla luce di tali disposizioni, come applicate da questo Arbitro, due sono i passaggi ineludibili in materia (cfr. art. 10 D.lgs. 11/10). In primo luogo è onere dell'intermediario "*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" (cfr. art. 10 comma 1, D.lgs. 11/10), prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento (art. 10 comma 2). È onere dell'intermediario, inoltre, fornire la prova di aver predisposto idonei presidi a tutela della sicura operatività con gli strumenti di pagamento. Per quanto attiene quest'ultimo profilo, nel caso di specie, si rileva innanzitutto che non è in discussione, quanto ai sistemi di sicurezza adottati dall'intermediario, l'esistenza di un sistema multifattoriale. Lo stesso ricorrente afferma di utilizzare password OTP generate dalla chiavetta O-key (token), essendo dunque dotato di un sistema di "autenticazione forte", così come previsto dalla normativa in materia (sul punto v. l'art. 12 degli Orientamenti finali sulla sicurezza dei pagamenti via internet, adottati il 19 dicembre 2014 dall'Autorità Bancaria Europea). In secondo luogo, occorre, tuttavia, rilevare che, con riferimento al sistema di autenticazione adottato, l'intermediario si limita ad affermare che l'adozione di un dispositivo di sicura efficacia come il token escluda la possibilità di accessi non autorizzati e pone l'accento sulla colpa grave del cliente, per essersi accorto tardivamente dell'operazione contestata e ipotizzando che la cliente sia incorsa in una classica ipotesi di *phishing*. Al riguardo, rileva il Collegio che il disconoscimento dell'operazione è avvenuto il 21/07/2017. Effettivamente, non è del tutto chiaro quando la ricorrente abbia avuto effettiva contezza della medesima: in una lettera del 14/12/2017, dichiarava di aver avuto conoscenza dell'operazione fraudolenta solo il 21/07, a seguito di contatto dall'intermediario. Sono però agli atti un'*email* datata 19/7 con cui la resistente informava la società della natura sospetta dell'operazione e un'altra email del 21/7 con cui la prima comunicazione veniva "inoltrata" ad un nuovo indirizzo. Tra l'altro, in relazione all'operazione contestata, non vi è evidenza dell'invio di alcun avviso o *alert*. Ad ogni buon conto, la circostanza dirimente per le sorti dell'odierno ricorso è rappresentata da fatto che lo stesso intermediario al fine di dare prova dell'autenticazione, corretta registrazione e contabilizzazione dell'operazione disconosciuta, si limita a produrre alcune tabelle excel convertite in PDF denominate "tracciatura", senza peraltro corredarle con una "*legenda*" esplicativa o particolari spiegazioni sulle relative modalità di lettura. Sul punto si rammenta che questo Arbitro (cfr., Collegio di Bologna, decisione n. 6837/17, nonché Collegio di Bari, decisioni n. 4688/19 e n. 13408/2019), ha ritenuto non sufficiente, ai fini della prova dell'autenticazione, la produzione di semplici griglie in formato Excel. Infatti le tabelle prodotte dall'intermediario non risultano di immediata e univoca interpretazione, atteso che l'attribuzione di significato alle sigle, abbreviazioni e codici numerici che compaiono nei detti fogli riposa sulla mera affermazione dell'intermediario. Pertanto, ad avviso di questo Collegio, non può ritenersi fornita la prova che l'operazione di cui trattasi sia stata autenticata, correttamente registrata e contabilizzata e che, in relazione alla stessa, non si siano verificati malfunzionamenti del sistema ovvero altre anomalie, così come richiesto dal citato art. 10, comma 1, del D. Lgs. vo 11/2010. Diversamente, assume rilievo, in proposito, la circostanza per cui lo stesso intermediario ha segnalato alla ricorrente che l'operazione contestata doveva considerarsi "sospetta e quindi potenzialmente rischiosa". Alla luce di quanto sopra esposto, il ricorso appare meritevole di accoglimento con conseguente diritto della ricorrente al rimborso della somma oggetto del bonifico contestato, oltre alla corresponsione degli interessi legali dalla data del reclamo al saldo, e altresì della somma di € 200,00 a titolo di rimborso delle spese sostenute per assistenza professionale.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 1.575,00, oltre gli interessi legali dalla data del reclamo al saldo, e altresì la somma di € 200,00 a titolo di spese per assistenza professionale.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS