Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) SANTAGATA DE CASTRO	Membro designato dalla Banca d'Italia
(NA) FEDERICO	Membro designato dalla Banca d'Italia
(NA) SICA	Membro di designazione rappresentativa degli intermediari
(NA) GIGLIO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - GIUSEPPE GIGLIO

Seduta del 11/06/2019

FATTO

La ricorrente, titolare di una c/c acceso presso l'intermediario convenuto afferma che in data 5 novembre 2018, alle ore 09:42, riceveva un messaggio di posta elettronica al proprio indirizzo mail che leggeva solo alle ore 17:20, recante l'informazione di una operazione sospetta effettuata sul proprio conto corrente bancario nonché un link da utilizzare per annullarla.
Poiché la mail riportava il logo dell'intermediario convenuto e la medesima grafica, procedeva ad aprire il suddetto collegamento e, a seguito di tale operazione, sullo schermo appariva una pagina che all'aspetto era perfettamente identica alla pagina ufficiale della banca; non essendo richiesta altra attività procedeva a chiudere il *browser*; subito dopo accedeva all'app mobile dell'intermediario convenuto, accorgendosi della presenza di un bonifico per una somma pari a € 14.950,00 a favore di un IBAN spagnolo e recante come beneficiario "Antoni O".
Resasi conto che si trattava di un'operazione fraudolenta, contattava immediatamente il numero verde della parte resistente al fine di disconoscerla e farne disporre l'immediata revoca, ma l'operatore telefonico le suggeriva di presentare denuncia querela e recarsi il mattino successivo direttamente in filiale per procedere al disconoscimento, operazioni che provvedeva ad effettuare.
A seguito del disconoscimento, alla ricorrente veniva riaccreditato l'intero importo oggetto della transazione non autorizzata (€ 14.950,00), tuttavia a distanza di pochi giorni tale somma le veniva nuovamente addebitata.

In data 21 novembre 2018 l'ufficio reclami della convenuta trasmetteva lettera mediante la quale dichiarava genericamente che l'operazione risultava eseguita con i corretti codici di accesso alla Banca online – benché illegittimamente acquisiti da parte di terzi attraverso una probabile frode informatica – e che la banca non aveva pertanto responsabilità nell'accaduto, aggiungendo che il tentativo di ottenere la restituzione di quanto sottratto aveva avuto esito negativo.

Si è rivolta quindi all'ABF tramite legale e deduce la cliente di essere stata vittima di una truffa informatica perpetrata attraverso la semplice apertura di un link ipertestuale che ha consentito l'esecuzione di un bonifico internazionale di considerevole importo, circostanza che fa sorgere dubbi sulla la sicurezza dei sistemi informatici della parte resistente, unitamente al fatto che l'effettuazione di ogni operazione dovrebbe richiedere l'utilizzo di un codice OTP generato dal token, che nel caso di specie non è stato mai utilizzato.

Nonostante abbia immediatamente denunciato l'accaduto al numero verde, non è stato possibile revocare il bonifico; l'intermediario convenuto avrebbe dovuto allertarla in considerazione dell'importo della movimentazione truffaldina, assolutamente sproporzionato ed anomalo rispetto ai normali movimenti operati sul suo conto corrente; sostiene poi che la parte resistente non ha assolto all'onere della prova su di essa gravante ex art. 10 del D.Lgs. n.11/2010, essendosi la convenuta limitata ad affermare, senza documentarlo né provarlo, che i bonifici contestati sarebbero stati disposti con digitazione della password temporanea prodotta dal dispositivo O-Key in dotazione della ricorrente;

l'intermediario non ha nemmeno allegato alcuna evidenza attestante i presidi di sicurezza a governo di siffatta modalità di pagamento on line anzi, l'inadeguatezza degli stessi sarebbe confermata dalla comunicazione inviata alla ricorrente in data 4 febbraio 2019, con cui l'intermediario avvisava della sostituzione del "attuale sistema tecnologico del servizio a distanza con il più avanzato sistema "MyKey", dismettendo il dispositivo O-Key fisico , cioè la chiavetta di plastica che oggi i clienti utilizzano per accedere ed autorizzare operazioni tramite il servizio a distanza". A giudizio della ricorrente, laddove le misure di sicurezza già in uso fossero state adeguate non vi sarebbe stato alcun motivo di implementare ulteriori misure.

La circostanza che il tentativo di riottenere la restituzione di quanto sottratto abbia avuto esito negativo fa presupporre che si sia trattato di un bonifico istantaneo, della cui esistenza ella non era a conoscenza ne' era stata informata dell'intermediario convenuto né ha rinvenuto contrattualmente riferimenti. Tale strumento deve considerarsi sostanzialmente differente dal bonifico europeo proprio in quanto non reversibile e pertanto più rischioso, cosicché ella è stata esposta a sua insaputa e resa vulnerabile ad operazioni come quella di cui è stata vittima senza che l'intermediario adottasse tutte le misure idonee a garantire la sicurezza del servizio.

Costituitosi ritualmente, l'intermediario ha chiesto di respingere il ricorso, eccependo:

la responsabilità della ricorrente nell'effettuare l'operazione disconosciuta e la legittimità del conseguente addebito in c/c in quanto la stessa è stata realizzata mediante inserimento del codice OTP - generato dal token in esclusivo possesso della ricorrente - e confermato a mezzo di un ulteriore codice OTS ricevuto sul cellulare della stessa: è quindi assolutamente da escludere la circostanza affermata dalla ricorrente secondo cui un semplice click sul link abbia potuto generare l'operazione di bonifico.

In particolare: 1) per accedere al sito dell'intermediario al fine di effettuare bonifici on line è richiesto l'inserimento di 2 password statiche (codice titolare + codice PIN) oltre un OTP generato da un token in possesso della cliente; 2) una volta collegatosi al servizio on line è necessario per l'utente inserire nuovamente un OTP per autorizzare una disposizione; 3) se il sistema antifrode intercetta un'operazione potenzialmente fraudolenta di bonifico invia

un ulteriore codice OTS: nel caso di specie la prima volta il codice non è stato correttamente inserito e pertanto il bonifico non è stato eseguito, mentre la seconda volta il codice OTS è stato corretto e pertanto il bonifico europeo è stato eseguito;
che la tracciatura informatica dell'operazione e le dichiarazioni della ricorrente consentono di affermare che la stessa è stata vittima di phishing, avendo fornito incautamente al truffatore userid, PIN, OTP e OTS, che sono strettamente personali e non devono essere comunicate a terzi - come specificato sul sito istituzionale dell'intermediario nonché nel contratto relativo allo strumento di pagamento, al fine di contrastare il fenomeno del phishing – così contravvenendo all'art. 7 del D.Lgs 11/2010 e di fatto cooperando alla realizzazione della truffa;
di aver messo a disposizione della propria clientela un sistema di sicurezza a più fattori ed in particolare le caratteristiche tecniche del dispositivo che genera l'OTP nonché del codice stesso fanno sì che tale soluzione sia assolutamente sicura, circostanza avvalorata dal fatto che non risulta si siano mai verificate violazioni della sicurezza del token consegnato ai clienti;
che i tentativi esperiti per la restituzione della somma relativa all'operazione disconosciuta non sono andati a buon fine;
di aver adottato anche ulteriori accorgimenti di sicurezza a protezione dell'infrastruttura tecnologica.
Sottolinea infine che se è vero che a seguito del citato regolamento europeo gli standard di sicurezza saranno implementati, non vuol dire che gli attuali standard non siano elevati;
che unitamente all'estratto conto di settembre 2017 la cliente era correttamente informata della nuova modalità di bonifico istantaneo, diversamente da quanto sostenuto.
In sede di repliche, la ricorrente contesta la ricostruzione operata, osservando ed evidenziando:
a) che in base al dettato dell'art. 10 comma secondo, del D. Lgs. n. 11/2010, "Quando l'utente 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, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è' di per se' necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, ne' 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. E' onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente";
b) il grave comportamento dell'intermediario, che "nonostante ci fossero stati almeno tre evidenti segnali di anomalia" nell'esecuzione dell'operazione disconosciuta, "che facevano emergere in maniera chiara il tentativo di frode", ha comunque proceduto al completamento dell'operazione, senza ritenere opportuna alcuna ulteriore verifica che l'autrice della disposizione fosse realmente la sua cliente, quantomeno contattandola telefonicamente, soprattutto considerando sia che in oltre sei anni (il contratto di c/c è stato sottoscritto il 15/05/2012) ella non ha mai trasferito alcuna somma tramite operazioni bancarie online ne' si è mai avvalsa del dispositivo O-Key sia che l'importo del bonifico corrispondeva al limite massimo trasferibile ed era considerevole in relazione ai fondi disponibili complessivamente sul c/c (€ 25.564,78)
d) in merito ai sistemi di sicurezza, nelle proprie controdeduzioni l'Intermediario si limita ad elencare tutta una serie di elementi di natura tecnica che dovrebbero garantire l'adeguatezza dei livelli di protezione della soluzione di internet Banking: tuttavia diverse decisioni ABF evidenziano come "La messa a disposizione dell'innovativo strumento di generazione della password non può essere considerata di per sé prova (presuntiva) della

violazione degli obblighi di custodia in senso lato gravanti sul cliente";
e) la rapida evoluzione tecnologica genera un continuo innalzamento del livello di vulnerabilità dei sistemi informatici, che necessitano quindi di costanti implementazioni di sicurezza. Evidentemente l'esigenza di introdurre nuovi standard con il Regolamento UE 2018/389 deriva proprio dall'esponenziale aumento delle frodi, circostanza che conferma che il sistema di sicurezza dell'intermediario non è stato adeguato.

DIRITTO

La parte ricorrente, titolare di un c/c acceso presso l'intermediario convenuto, lamenta l'esecuzione fraudolenta di un'operazione di bonifico effettuata on line, tramite il servizio di home banking, per un importo di € 14.950,00, di cui chiede la restituzione, oltre agli interessi legali.
La ricorrente ha prodotto la nota di contestazione importi presentata in sede di reclamo, contente l'evidenza dell'operazione contestata, consistente in un bonifico istantaneo in area SEPA, disposto on line, effettuato su un sito internet spagnolo in data 5.11.2018 per un importo di € 14.950,00 di cui chiede il rimborso:
Dalla denuncia presentata si evince che la ricorrente, in data 5.11.2018, riceveva una mail che sembrava essere apparentemente inviata dall'intermediario convenuto e la informava della presenza di un'operazione di bonifico sospetta operata sul conto corrente e conteneva un *link* che provvedeva a cliccare: una volta effettuata tale semplice operazione, riscontrava sul c/c la presenza di un'operazione di bonifico di € 14.950,00 da lei mai effettuata.
Parte ricorrente allega anche la mail ricevuta, probabilmente di phishing, contenente un *link*, e precisa in denuncia di non aver assolutamente utilizzato il token dopo l'accesso al *link*.
La mail è stata inviata nella mattina del giorno dell'operazione fraudolenta, ma la ricorrente sostiene di averla letta solo nel pomeriggio dopo le 17,00.
L'intermediario afferma che per compiere la transazione contestata è stato necessario utilizzare il codice OTP e pertanto rileva di aver messo a disposizione un sistema di sicurezza a più fattori.
In particolare afferma che l'operazione è stata possibile nel seguente modo:
1) per accedere al sito è richiesto l'inserimento di 2 password statiche (codice titolare + codice PIN) oltre un OTP generato da un token in possesso della cliente;
2) una volta collegatosi al servizio on line è necessario per l'utente inserire nuovamente un OTP per autorizzare una disposizione;
3) nel caso specifico il sistema antifrode ha intercettato un'operazione potenzialmente fraudolenta di bonifico e ha inviato un ulteriore codice OTS tramite sms sul cellulare della ricorrente: la prima volta il codice non è stato correttamente inserito e pertanto il bonifico non è stato eseguito, mentre la seconda volta, pur intercettando l'operazione come sospetta, il codice OTS è stato correttamente inserito e pertanto il bonifico europeo è stato immediatamente accreditato.
I tentativi di recupero non hanno avuto esito positivo.
La resistente allega il log della sessione di *internet banking* aperta alle 17:19 del 5/11/2018 a seguito di login confermato con PIN e OTP corretti.
La resistente allega altresì il log il log della tracciatura delle 2 operazioni di bonifico di cui la prima non è andata a buon fine (per errato OTS) e la seconda invece è stata inoltrata (cfr. all. 3 cdz.):
1) bonifico di € 14.951,60, NON andato a buon fine (OTS).

2) bonifico di € 14.9500, andato a buon fine (OTS ok):
Il numero di invio degli sms corrisponde a quello della denuncia.
Agli atti il Collegio ha riscontrato la comunicazione effettuata dalla resistente in occasione dell'invio dell'estratto conto nel settembre 2017 - avente ad oggetto la proposta di modifica unilaterale - da cui è possibile constatare il rispetto dei limiti di utilizzo per i bonifici istantanei in uscita in area SEPA, il cui importo massimo è di € 15.000,00.
Tutto ciò premesso, evidenzia il Collegio che dalle risultanze istruttorie, la ricostruzione dell'attrice secondo cui avrebbe subito la frode telematica solo attraverso l'apertura di un link, è stata smentita dalle tracciature informatiche depositate, per cui sono rilevabili profili di negligenza della istante sulla custodia delle credenziali di accesso al conto.
Di converso giova evidenziare che l'intermediario, per sua stessa ammissione, per ben 2 volte ha valutato l'operazione potenzialmente sospetta, come risulta dalla circostanza che per completare la stessa sia stato necessario l'inserimento anche del c.d. codice OTS.
Avendo riscontrato potenziali anomalie e/o sospettato si potesse trattare di una operazione in frode, l'intermediario (che ha deve attenersi alla diligenza dell'accorto banchiere), avrebbe dovuto in qualche modo verificare che la disposizione fosse realmente attribuibile alla cliente.
Ciò non ha fatto, per cui anche in capo alla convenuta rinviene il Collegio profili di responsabilità.
Per quanto esposto, la gradazione delle rispettive responsabilità al 50% è quella ritenuta equa nel caso di specie dal Collegio.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto al risarcimento del danno per l'importo di € 7.475,00, oltre interessi legali alla data del reclamo.
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
GIUSEPPE LEONARDO CARRIERO