Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) CAMILLERI	Membro designato dalla Banca d'Italia
(BA) BUTA	Membro designato dalla Banca d'Italia
(BA) APPIO	Membro di designazione rappresentativa degli intermediari
(BA) CATERINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - DANIELA CATERINO

Seduta del 11/06/2019

FATTO

La ricorrente riferisce di aver ricevuto, in data 12 luglio 2018, «*n° 2 sms* [dall'intermediario] *con comunicazione di codici per completare 2 bonifici internazionali (uno in entrata ed uno in uscita)* […] *mai richiesti*». Insospettitasi per l'accaduto, avrebbe tentato di accedere al proprio *home banking* e avrebbe quindi appreso di «*un ammanco di € 14.780,00 a seguito di bonifico internazionale*» in favore di un terzo sconosciuto e dalla medesima non effettuato. Allega di aver sporto denuncia querela e di aver effettuato il disconoscimento del suddetto bonifico il giorno successivo. Riferisce che, sempre «*in data 13.07.2018, lo stesso gestore telefonico dell'utenza* [della ricorrente] *veniva avvertito, dall'ufficio frode, di 3 tentativi sospetti di bonifico, e* [la ricorrente] *provvedeva al disconoscimento anche con il gestore, che comunicava tutto all'ufficio frode*». Afferma di aver ottenuto il riaccredito delle somme già oggetto di bonifico, salvo poi rilevare una «*operazione di riaddebito della somma di € 14.780,00*», della quale lamenta la illegittimità. Allega l'inadempimento dell'intermediario, riportandosi all'orientamento di Cass. civ., n. 2950/2017.
Riferisce che l'intermediario avrebbe proposto «*la restituzione di somma pari al 50% del richiesto, adducendo di non avere responsabilità*» e che tale proposta è stata rifiutata, l'utilizzo fraudolento dovendo ritenersi imputabile esclusivamente alla banca convenuta.
Chiede pertanto di condannare l'intermediario al rimborso dell'importo di € 14.780,00.
L'intermediario dà preliminarmente atto della proposta transattiva rifiutata dal ricorrente.
Nel merito, nega ogni responsabilità, tenuto conto dell'inserimento da parte del ricorrente «*del codice OTP generato dal token O-Key in possesso esclusivo del cliente e* [dell']

ulteriore codice OTS». Deduce che l'operazione contestata è stata dunque eseguita con tecnologia multifattoriale.

Allega che, ove «*il sistema antifrode rilevi che un'azione possa essere potenzialmente fraudolenta* […] *viene inoltrata al cliente l'OTS, una ulteriore password* [dinamica] *che serve a confermare l'operazione*».

Ciò premesso, deduce che nella specie la cliente ha dato inizio a una sessione di internet banking alle 16:08 del 12 luglio 2018, previo inserimento di «*PIN e OTP corretti*». Allega che circa quattro minuti dopo i sistemi informativi hanno tracciato «*un primo tentativo di bonifico di € 14.760,00*»: il sistema ha tuttavia intercettato l'operazione come «*sospetta*» e, pertanto, l'intermediario «*ha inoltrato alla cliente un messaggio sms*», con il quale è stato fornito un codice di sicurezza ulteriore «*per completare il bonifico europeo* […] *di EUR 14.760,00*» in favore di beneficiario con cognome identico a quello della ricorrente. Deduce che presumibilmente tratta in inganno dal cognome del beneficiario, la ricorrente avrebbe erroneamente ipotizzato trattarsi di «*bonifico in entrata*». Nonostante la ricorrente abbia inserito il codice OTP e il codice OTS l'operazione non si è perfezionata «*a causa di errore dell'applicativo*».

Analoga situazione si è verificata con riferimento al bonifico disconosciuto, effettuato alle 16:17. Anche in questo caso il sistema antifrode ha rilevato il carattere sospetto dell'operazione e pertanto il codice OTS è stato trasmesso alla ricorrente, anche in questo caso con un sms del seguente tenore: «*Usa* […] *come codice di sicurezza per completare il bonifico europeo* […] *di EUR 14.781,6*».

Riferisce che un terzo tentativo di bonifico – dell'importo di 5.200,00 euro – è stato poi bloccato dal sistema antifrode. Sicché la ricorrente avrebbe «*incautamente fornito al truffatore, oltre alle credenziali personali (userid e pin, necessari per il login), almeno 3 otp corrette e le due ots*», peraltro ignorando il «*contenuto dei messaggi di allerta* [e inserendo] *i codici OTS autorizzando così il bonifico fraudolento*».

Deduce di aver apprestato sistemi di sicurezza adeguati e certificati (un canale di comunicazione cifrato, la protezione tramite firewall) nonché un *token* all'avanguardia anche dal punto di vista delle caratteristiche di sicurezza. Allega inoltre che il *phishing* è fenomeno noto, oggetto di informative alla clientela anche da parte dell'intermediario convenuto. Rileva in proposito che il consolidato orientamento dell'Arbitro ritiene sicuri i sistemi di autenticazioni multifattoriali, analoghi a quello adottato dall'intermediario medesimo e ne desume che «*l'efficace tutela offerta dal dispositivo adottato costituisce esatto adempimento dell'obbligazione dell'intermediario di tutelare l'interesse dell'utente*».

Di contro, rileva la negligenza della ricorrente e in definitiva la responsabilità della medesima per l'accaduto. Conclude, in via principale, per il rigetto della domanda del ricorrente e, in via subordinata, chiedendo al Collegio «*la ripartizione fra le parti del danno in esame, in misura proporzionale alle rispettive effettive responsabilità ed in particolare ai sensi dell'art. 177, 1 e 2 comma c.c.*».

In sede di repliche, la ricorrente nega di aver ricevuto email di *phishing* e di aver versato in «*colpevole credulità*». Allega piuttosto di essere stata «*vittima di un* phishing attack *di nuova generazione, dato dall'utilizzo di software malevoli (*malware*)*» e segnatamente vittima del c.d. *man-in-the-browser.* Deduce che «[è] *obbligo, da parte dell'istituto bancario, di predisporre opportuni accorgimenti volti a scongiurare violazioni del sistema e operazioni fraudolente e proteggere i clienti in modo concreto*».

Rileva che nel medesimo pomeriggio sono state intercettate ben 3 operazioni sospette e che, ciononostante, l'intermediario non avrebbe avvisato la ricorrente e, «*in ogni caso, non ha provveduto a bloccare le operazioni, attivando, per come dovuto, in tempo reale, misure di contrasto idonee a minimizzare il rischio di operazioni fraudolente o indebite*».

Sostiene, di contro, che la banca avrebbe dovuto avvisarla già alla prima operazione

sospetta. Si riporta all'orientamento della Corte di Cassazione e insiste per il rimborso dell'intero importo del bonifico disconosciuto.

DIRITTO

Il ricorso merita accoglimento, per le ragioni di seguito descritte.
La controversia concerne l'esecuzione non autorizzata da parte di terzi ignoti di tre operazioni *online.* Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, per come modificato 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), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.
Come è noto, ai sensi di tale disciplina è onere dell'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/10); inoltre il prestatore di servizi di pagamento, ai sensi della medesima norma, ha l'onere di provare che l'operazione di pagamento "non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione e di altri inconvenienti".
In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute, senza alcuna franchigia. Tale prova non è comunque di per sé sufficiente per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento. Va ulteriormente precisato che il termine "autenticazione" fa riferimento nel d.lgs. n. 11/2010 alla "procedura che consente al prestatore di servizi di pagamento di verificare l'utilizzo di uno specifico strumento di pagamento, inclusi i relativi dispositivi personalizzati di sicurezza" (cfr. la definizione contenuta nell'art. 1, comma 1, lett. q); e che la disciplina distingue come buona pratica la c.d. *"autenticazione forte del cliente",* intesa come *"un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".*
Non vi è dubbio che nel caso di specie il sistema di autenticazione adottato dall'intermediario sia del tipo "forte", ossia basato sull'uso di due o più elementi (nella fattispecie, è riconosciuta da ambo le parti la necessità dell'immissione del codice dinamico OTS quale ulteriore elemento per il perfezionamento dell'operazione). Dunque il sistema risulta in linea di principio conforme alle prescrizioni dell'art. 10 – *bis* d. lgs. n. 11/2010.
Tuttavia, nel caso di specie l'intermediario versa in atti, per comprovare la regolare autenticazione, registrazione e contabilizzazione, la riproduzione di alcune schermate la cui interpretazione non appare chiara ed inequivocabile. Le finestre di testo in cui si dà conto dell'asserito significato delle cifre e simboli riportati nelle schermate appaiono successivamente sovrapposte alle schermate stesse e sono del tutto autoreferenziali, non facendo riferimento alcuno a simbologie universalmente condivise; né risulta in atti una legenda originariamente riferibile ai detti schemi. La prova della corretta autenticazione, in definitiva, non appare raggiunta.
Si aggiunga che nella spiegazione fornita a supporto di dette schermate, lo stesso intermediario ammette testualmente che il sistema antifrode ha intercettato le operazioni

come “potenzialmente sospette”; ma anziché indirizzare al cliente un messaggio che desse conto di tale carattere potenzialmente sospetto, si è limitato a trasmettere una richiesta di inserimento di codici per il completamento dell’operazione, tra l’altro nel primo tentativo facilmente interpretabile come bonifico in entrata, a motivo dell’inserimento fraudolento del nominativo della ricorrente come destinataria del bonifico. Solo al terzo tentativo il sistema antifrode ha bloccato l’operazione sospetta, ma dopo che già era stato eseguito il cospicuo bonifico in uscita. Non si comprende perché il sistema non abbia bloccato l’esecuzione già dal primo tentativo di operazione sospetta, come è invece successivamente avvenuto per il terzo tentativo.
Tali elementi a parere di questo Collegio integrano gli estremi del malfunzionamento del sistema, che costituisce circostanza rilevante ai fini dell’addebito integrale della responsabilità per l’operazione all’intermediario, a prescindere dall’esame di qualsiasi profilo di colpa del cliente.
Pertanto, la richiesta della ricorrente appare meritevole di accoglimento.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l’intermediario rimborsi al ricorrente l’importo di € 14.780,00.
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
ANDREA TUCCI