Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) BARTOLINI	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) COEN	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - [redacted]

Seduta del 04/03/2022

Esame del ricorso n. 1248200/2021 del 02/09/2021

proposto da [redacted]

nei confronti di 3475 - ING BANK N.V.

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) BARTOLINI	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) COEN	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ROBERTO COEN

Seduta del 04/03/2022

FATTO

In data 13.05.2021 alle ore 12:29, il ricorrente, titolare di un conto corrente presso l'intermediario convenuto, riceveva un SMS che lo invitava a cliccare su un link allegato al messaggio stesso, che lo avvertiva di un accesso anomalo sul proprio conto.
Una volta cliccato, il *link* lo indirizzava alla pagina del sito clone dell'intermediario, ove digitava i propri dati e le credenziali di accesso.
Immediatamente, il ricorrente riceveva due SMS dallo stesso numero, che lo informavano dell'effettuazione di due operazioni con la carta di credito collegata al conto.
Subito dopo, il ricorrente veniva contattato telefonicamente da un numero fisso non conosciuto, da un soggetto che si presentava come dipendente dell'ufficio antifrode della banca e gli chiedeva la verifica dei suoi dati al fine di poter annullare le predette operazioni.
A seguito della telefonata, il ricorrente riceveva un ulteriore SMS apparentemente proveniente dalla banca, che lo informava dell'avvenuto blocco delle operazioni e lo invitava a seguire le istruzioni dell'operatore per il riaccredito delle somme e la conclusione della pratica.
Alle 16:59 il ricorrente riceveva un altro SMS che lo informava dell'esecuzione di un bonifico di € 4.976,00 verso un conto corrente lituano e, alle ore 17:08 il ricorrente veniva nuovamente contattato telefonicamente dal sedicente operatore della banca, che lo informava del bonifico anomalo, e lo rassicurava sul blocco dell'operazione.

Alle 17:10 un ulteriore SMS confermava il blocco del bonifico e invitava nuovamente il ricorrente a seguire le istruzioni dell'operatore.
In data 14.05.2021, il ricorrente si recava quindi in filiale, dove veniva informato dell'esecuzione di operazioni fraudolente pari a € 5.469,00, di cui due operazioni on-line di € 247,00 ciascuna, eseguite con carta di credito ed un bonifico estero di € 4.976,00.
In data 14/05/2021, il ricorrente presentava reclamo alla resistente per il rimborso della somma indebitamente sottratta, pari a € 5.469,00 corrispondente alle tre operazioni disconosciute, sostenendo la responsabilità della banca per avere consentito a terzi di immettersi nella propria utenza telefonica e per non avere bloccato le operazioni sospette ed, in considerazione dell'esito negativo del reclamo esperito, le medesime doglianze venivano riproposte dalla ricorrente innanzi all'A.B.F. in data 02/09/2021.
Si costituiva l'intermediario, il quale chiedeva il rigetto del ricorso, sostenendo la piena responsabilità della parte ricorrente in quanto vittima di phishing, perpetrato tramite l'invio di un SMS (c.d. "smishing"), ove gli utenti vengono invitati tramite un sms a cliccare su un *link* allo scopo di acquisire dati riservati e codici personali, autorizzativi e credenziali di un conto corrente o di uno strumento di pagamento, nonché, in via subordinata, la ripartizione del danno fra le parti, in misura proporzionale alle rispettive responsabilità ed, in particolare ai sensi dell'art. 1227, 1 e 2 comma c.c. (c.d. concorso di colpa).
Secondo l'intermediario, era onere della parte ricorrente custodire i propri dati identificativi e dispositivi, anche in considerazione della notorietà del fenomeno del *phishing*.
Inoltre, secondo la resistente gli SMS ricevuti dal ricorrente presentavano anomalie dal punto di vista ortografico e grammaticale, ed il link che il ricorrente ha seguito era chiaramente artefatto e non riferibile alla banca.
Precisava l'intermediario che era stato adottato un sistema di autenticazione forte di accesso all'Area Riservata e delle disposizioni di pagamento, in conformità alla Direttiva PSD2 vigente in materia.
Tutte le operazioni disconosciute erano state autorizzate da App in data 13.05.2021, alle ore 12:42, 12:43 e 16:59.
Precisava l'intermediario che nel caso in esame, alle 12:38 del 13.05.2021 era stata richiesta l'attivazione del Token su un nuovo dispositivo, autorizzata mediante inserimento del codice OTP tramesso via SMS al ricorrente alle ore 12:37. La modifica del dispositivo era dunque, avvenuta senza anomalie e nel rispetto della procedura di Strong Customer Authentication.
Secondo l'intermediario risulta evidente la colpa grave del cliente, che ha comunicato le proprie credenziali a terzi dando credito a messaggi e chiamate asseritamente provenienti dalla banca.

DIRITTO

Il Collegio osserva che, nel caso di specie, la parte ricorrente ha subito la truffa, successivamente all'entrata in vigore del D.lgs. n. 218/2017(di recepimento della PSD 2), ovvero successivamente al 14 settembre 2019, data di applicazione del Regolamento delegato (UE) della Commissione 2018/389, che stabilisce i requisiti dell'autenticazione forte ai sensi della PSD 2.
Ciò posto, la questione relativa alla fattispecie impone di valutare sia l'adeguatezza del sistema di protezione adottato dall'Intermediario, che l'adempimento del corretto obbligo di custodia dello strumento di pagamento da parte dell'utente (ex artt. 7 e 8 del D. Lgs. 11/2010, così come modificati alla luce del nuovo decreto precedentemente citato).

Per quanto riguarda il primo profilo, una delle più significative novità introdotte dalla suddetta normativa è il concetto della c.d. "autenticazione forte" (strong customer authentication – SCA, nella direttiva), di cui all'art. 1, c.1, lett. q-bis del D.lgs. 11/2010 (così come modificato dal D.lgs. 218/2017), secondo cui: "*q -bis) "autenticazione forte del cliente": 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*".
Orbene, l'avere o meno offerto al cliente un sistema di autenticazione forte assume rilevanza sostanziale con riferimento al caso di specie, soprattutto in considerazione dell'ulteriore novità introdotta dall'art. 12 commi 2 bis e 4 del D. Lgs. 11/2010 (così come modificato dal D. Lgs. 218/2017) ai sensi del quale: "*2 -bis Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente. (...)*
4. Qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3."
È notorio che il sistema delineato dal legislatore comunitario in materia di strumenti di pagamento è di particolare favore per il cliente soprattutto per quel che concerne l'onere probatorio. Ciò in quanto, per un verso limita la responsabilità del cliente alle sole ipotesi di dolo e colpa grave e, per altro verso, pone in capo all'intermediario l'onere di provare che l'operazione di pagamento sia stata eseguita correttamente e non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.
Il Collegio rileva che nel caso di specie sono state effettuate due operazioni on-line di € 247,00 ciascuna, eseguite con carta di credito alle ore 12:44 e 12:46 del 13.05.2021, ed un bonifico estero di € 4.976,00 verso un conto lituano, eseguito alle ore 16:59, per complessivi € 5.469,00.
L'intermediario afferma che le operazioni disconosciute sono state poste in essere previa attivazione del *token* su un nuovo dispositivo e produce i log relativi alla fase preliminare di *onboarding.*
Sulla base di tali log, l'attivazione del token è stata realizzata con l'impiego dei seguenti fattori di autenticazione: 1) codice cliente, data di nascita e PIN del cliente; 2) OTP trasmesso al ricorrente via SMS; 3) risposta alla domanda di sicurezza preimpostata.
Orbene, per le due operazioni on-line di € 247,00 ciascuna, eseguite con carta di credito, l'intermediario produce evidenza di 4 operazioni, che comprende anche tentativi non andati a buon fine – dichiarando che le operazioni sono state eseguite con le stesse modalità – non allegando i log relativi alle due operazioni disconosciute.
Sul punto, il Collegio rileva che per le operazioni per le quali non risulta dimostrata l'avvenuta autenticazione, registrazione e contabilizzazione i Collegi accolgono il ricorso, ai sensi dell'art. 10, primo comma, del D.lgs. 11/2010.
Pertanto, nel caso in esame, per le due operazioni on-line di € 247,00 ciascuna, eseguite con carta di credito, il Collegio accoglie la domanda, in quanto l'intermediario non ha allegato la prova dell'autenticazione, registrazione e contabilizzazione dell'operazione,

con la conseguenza che non rileva l'eventuale comportamento gravemente colposo del cliente.

In merito alla operazione di bonifico estero di € 4.976,00, l'intermediario produce i log relativi all'operazione di bonifico, dai quali risulta che essa è stata autorizzata mediante Token su App dell'intermediario, a seguito di "tap", su "notifica push" ed inserimento dell'impronta digitale registrata al momento dell'attivazione del Token.

Il Collegio osserva che dalla schermata dell'sms civetta ricevuto dalla parte ricorrente si evince che il messaggio si è inserito all'interno di una chat preesistente con l'intermediario, che il testo non presenta errori di ortografia ed il link contiene la denominazione invertita del gruppo di appartenenza della convenuta.

Ebbene, secondo la più recente posizione condivisa da tutti i Collegi territoriali, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvengano indici di inattendibilità o anomalia del messaggio: in tale caso, potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.

Ne deriva che, secondo il Collegio, nel caso di specie, vi è prova della condotta non gravemente colposa della parte ricorrente e quindi l'intermediario deve corrispondere alla parte ricorrente la complessiva somma di € 5.469,00.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 5.469,00. Respinge nel resto.

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
PIETRO SIRENA