Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MARTINO	Membro designato dalla Banca d'Italia
(BO) MUCCIARONE	Membro designato dalla Banca d'Italia
(BO) SOLDATI	Membro di designazione rappresentativa degli intermediari
(BO) CAPILLI	Membro di designazione rappresentativa dei clienti

Relatore GIOVANNA CAPILLI

Seduta del 02/02/2021

Esame del ricorso n. 0876333/2020 del 02/07/2020

proposto da DEL BIANCO BARBARA

nei confronti di 5387 - B.CA POP. EMILIA ROMAGNA

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MARTINO	Membro designato dalla Banca d'Italia
(BO) MUCCIARONE	Membro designato dalla Banca d'Italia
(BO) SOLDATI	Membro di designazione rappresentativa degli intermediari
(BO) CAPILLI	Membro di designazione rappresentativa dei clienti

Relatore GIOVANNA CAPILLI

Seduta del 02/02/2021

FATTO

Parte ricorrente riferisce: in data 01/02/19, dalla lista dei movimenti del conto corrente, si avvedeva di alcuni bonifici mai autorizzati eseguiti dal proprio conto corrente rispettivamente in data 29 e 30/01/19; l'intermediario le riferiva che i bonifici erano stati disposto mediante home banking, utilizzando il telefono cellulare della ricorrente; ha disconosciuto le operazioni e ottenuto dall'intermediario l'estinzione della propria utenza home banking, le cui credenziali erano sempre rimaste in proprio possesso; contestualmente, ha sporto querela contro ignoti; l'intermediario, dopo aver inizialmente riaccreditato le somme sottratte, ne disponeva lo storno adducendo che le operazioni erano imputabili a colpa grave della ricorrente, vittima di un episodio di phishing tramite SIM swap; infatti, in data 23/01/2019 era stata vittima di un sms "esca", asseritamente inviato dall'intermediario attraverso il numero telefonico solitamente utilizzato per le operazioni di home banking, il quale la invitava a cliccare su un link; di aver quindi cliccato su tale link e di essere stata reindirizzata su un sito identico a quello dell'intermediario, ove procedeva a digitare le proprie credenziali; i consulenti tecnici, cui si è rivolta per avere contezza dell'accaduto, hanno messo in luce una serie di criticità del sistema di sicurezza dell'intermediario, riportate nella perizia allegata (doc. 1); l'intermediario era al corrente di tale tipologia di truffa, avendo esso stesso allertato la cliente con sms del 31/01/2019; nonostante le operazioni, compiute nell'arco di due giorni, siano state di importo ingente, nessuna anomalia è stata rilevata dall'intermediario; secondo la giurisprudenza ordinaria, l'intermediario è responsabile ex art. 2050 c.c. per l'accesso non autorizzato ad un sistema

di home banking; il sistema di sicurezza predisposto dall'intermediario all'epoca dei fatti era inadeguato, in quanto per portare a termine le operazioni di pagamento erano richieste soltanto password statiche (credenziali di accesso al conto) e non anche password dinamiche (OTP inviato tramite sms); di non avere alcuna responsabilità, non avendo mai consentito a terzi l'utilizzo dell'home banking, né smarrito le proprie credenziali; tra gli obblighi dell'intermediario vi è anche quello di un adeguato monitoraggio delle operazioni compiute via internet dalla clientela e di segnalazione delle operazioni anomale; l'intermediario non ha adempiuto all'onere di provare la corretta autenticazione delle operazioni a norma dell'art. 10, D.Lgs. n. 11/2010; secondo l'orientamento dell'ABF, l'adozione di un sistema di sicurezza rafforzato non è sufficiente per affermare la colpa grave del cliente; lo stesso ABF si è pronunciato anche sull'obbligo di adeguato monitoraggio del conto; che i prestatori di servizi di pagamento, fornendo strumenti di home banking, dispongono dei dati sensibili dei clienti, cosicché hanno l'obbligo di prevenire l'illecita captazione di tali dati.

Parte resistente, riepilogati i fatti, afferma che: le evidenze informatiche prodotte e la stessa perizia allegata dal ricorrente dimostrano che, contrariamente a quanto asserito nel ricorso, il sistema di autenticazione predisposto fosse "a due fattori", prevedendo l'invio di un codice tramite sms per portare a termine le operazioni; l'accaduto è imputabile a colpa grave della ricorrente, la quale, cliccando sul link ricevuto via sms e digitati successivamente i propri dati sul sito contraffatto (tra cui anche il numero telefonico), ha consentito ai malviventi la clonazione della sua scheda sim, come confermato dai malfunzionamenti telefonici lamentati dalla stessa; la ricorrente ha inoltre colposamente ignorato quanto riferitole dalla compagnia telefonica in merito all'intervenuto blocco e riemissione della sim; le operazioni contestate si sono consumate nell'arco non di due ma di tre giornate lavorative, nei quali la ricorrente avrebbe potuto allertare l'intermediario e le autorità di pubblica sicurezza; le operazioni in questione non presentavano indici di anomalia tali da giustificare il blocco dell'intermediario, trattandosi di bonifici disposti nell'arco di più giorni, per causali legittime ed in linea con l'operatività del cliente; nel caso di specie si profila una responsabilità della compagnia telefonica, rea di aver acconsentito alla richiesta di sostituzione della SIM senza previamente accertare l'identità dell'istante.

Parte resistente chiede il rigetto del ricorso ed in subordine l'applicazione dell'art. 1227 c.c.; in ulteriore subordine chiede di tenere in considerazione che controparte dovrà sopportare la perdita nella misura di 50 euro stabilita dall'art. 12 comma 3 d. lgs. N. 11/2010.

DIRITTO

Il caso posto all'attenzione del Collegio riguarda la restituzione di somme per operazioni non riconosciute.

Parte ricorrente disconosce 5 operazioni di bonifico effettuate tra il 29 e il 30 gennaio 2019, come risulta dal verbale di denuncia, allegata in atti, sporta in data 1/2/2019, sebbene oggetto della pretesa del ricorrente sono solo 4 operazioni, in quanto il ricorrente non insiste nell'ulteriore operazione originariamente oggetto di disconoscimento, cosicché l'importo complessivamente richiesto a titolo di restituzione ammonta a € 98.984,00.

L'intermediario eccepisce che l'importo di € 11.500 relativo ad un bonifico del 29/01 sia stato stornato. Tuttavia, parte ricorrente afferma nel ricorso come l'intermediario abbia "*disposto il riaddebito delle somme inizialmente restituite, in via unilaterale e senza autorizzazione del correntista*".

In ogni caso, le operazioni risultano poste in essere sotto il vigore del 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).

Non risultano applicabili, invece, gli standard di cui alla Opinion dell'EBA del giugno 2019, da ritenersi vincolanti, secondo la stessa Autorità, a partire dal 14 settembre 2019.

A fronte del disconoscimento delle operazioni di pagamento da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, comma 1, del D.Lgs. 11/2010, che così statuisce: "*Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento 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*".

L'intermediario eccepisce che, contrariamente a quanto asserito dal ricorrente, il sistema di autenticazione delle operazioni di pagamento sia multifattoriale, prevedendo:

a) l'inserimento di nome utente e password per l'accesso all'home banking (fattore statico);

b) l'inserimento di un codice OTP, inviato tramite sms sull'utenza telefonica del cliente, per autorizzare la singola operazione di bonifico (fattore dinamico).

Di tale processo di autenticazione fornisce evidenza: nell'all. 13, dove, per ciascuna delle operazioni contestate, emerge che alcuni dati (user ID e numero di cellulare su cui ricevere gli sms OTP) coincidono con quelli dichiarati dalla stessa ricorrente (pag. 1 del ricorso): nell'all. 14, dove viene fornito il dettaglio di alcune operazioni di bonifico, di cui nelle controdeduzioni viene illustrata, a titolo esemplificativo, quella del 30/01/2019: nell'all. 15, dove, per ciascuna operazione di bonifico, è riportata la tracciatura informatica della creazione e dell'invio dei codici OTP, meglio illustrata nelle controdeduzioni con riferimento esemplificativo sempre all'operazione del 30/01.

Parte ricorrente, dal canto suo, deposita una perizia tecnica in cui viene fornita un'analisi del sistema di sicurezza predisposto dall'intermediario resistente per l'accesso all'home banking e per l'autenticazione delle operazioni. Pur dandosi atto che il sistema di autenticazione delle operazioni sia multifattoriale, se ne mette in dubbio la sicurezza, anche in raffronto con sistemi predisposti da altri intermediari.

In particolare, con riguardo alle modalità di accesso all'home banking, si contesta: i) l'insufficienza dell'autenticazione con soli user id e password, dal momento che i sistemi più aggiornati prevedrebbero anche un sistema di sicurezza aggiuntivo; ii) la circostanza che a tale portale si possa accedere attraverso qualsiasi device, il che metterebbe a repentaglio la segretezza delle suddette credenziali.

Quanto, invece, al c.d. fattore "dinamico", nella relazione peritale si lamenta: a) che l'sms contenente il codice venga fatto pervenire su un'utenza telefonica non riconducibile con certezza al correntista; b) che venga consentito l'utilizzo di qualsiasi operatore telefonico, senza verificarne il livello di sicurezza; c) che non può, per sua natura, essere calibrato rispetto al valore protetto.

Nonostante tutto quanto sopra, si deve evidenziare come dalle affermazioni della ricorrente emerga che nel caso di specie si sia verificato un caso di "SIM swap" posto che dopo un primo episodio di *sms spoofing* la ricorrente non riusciva più ad utilizzare il proprio

telefono e, contattato il proprio operatore telefonico, veniva a conoscenza che il suo numero telefonico era stato associato ad altra scheda SIM, senza specificare per quale motivo fosse avvenuta la sostituzione della SIM sulla medesima utenza.

Tale ricostruzione non è peraltro contestata dall'intermediario tanto che lo stesso ammette che i truffatori sono riusciti ad ottenere dall'operatore telefonico l'emissione di una nuova SIM ricevendo così sul proprio cellulare il messaggio contenente il codice OTP necessario per autorizzare le operazioni.

Nella situazione sopra rappresentata, quindi, deve ritenersi una carenza sostanziale di autenticazione posto che in caso di "SIM Swap" l'autenticazione anche se formalmente completa e regolare è da ritenersi solo apparente in quanto comprende l'invio di comunicazioni o OTP che vengono ricevuti direttamente dal truffatore e, quindi, non utilizzabili ai fini della corretta autenticazione; il ricorso, pertanto, deve essere accolto e riconosciuto il rimborso della somma pari ad euro 98.984,00.

PER QUESTI MOTIVI

Il Collegio - in accoglimento del ricorso - dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo di euro 98.984,00 (novantottomilanovecentoottantaquattro/00).

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
MARCELLO MARINARI