

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MAIMERI	Membro designato dalla Banca d'Italia
(BO) LOMBARDI	Membro designato dalla Banca d'Italia
(BO) PASQUARIELLO	Membro di designazione rappresentativa degli intermediari
(BO) D ATRI	Membro di designazione rappresentativa dei clienti

Relatore ETTORE MARIA LOMBARDI

Seduta del 24/01/2023

FATTO

Nel proprio ricorso, la parte, anche a mezzo della documentazione acclusa, ha riferito di essere titolare del conto corrente n. **987 acceso presso l'intermediario resistente e al quale è collegato il servizio di *home banking*; che, in data 12 aprile 2022, alle 16:15 è stata contattata sul cellulare da un interlocutore che si è presentato come operatore dell'intermediario resistente; che ha creduto all'operatore poiché era effettivamente cliente dell'intermediario resistente e il numero da cui l'operatore chiamava era lo stesso indicato dalla banca per bloccare le carte di pagamento; che il presunto operatore le ha riferito che per evitare il blocco delle carte le avrebbe inviato un sms con un link di attivazione di una presunta procedura di sicurezza; che, dopo aver ricevuto il link, ha seguito le istruzioni dell'interlocutore e ha installato sul proprio telefono l'app dell'intermediario; che l'interfaccia grafica della app era perfettamente identica a quella del sito della banca; che il presunto operatore, dopo circa venti minuti, le ha riferito che l'avrebbe chiamata il giorno successivo; che il suo telefono è rimasto bloccato per le ventiquattro ore successive; che in data 13 aprile 2022 ha effettivamente ricevuto la telefonata dallo stesso operatore, che le chiedeva di verificare che la schermata di avvio fosse la stessa del giorno precedente, dopodiché l'interlocutore le diceva che l'avrebbe richiamata il giorno seguente; che il 14 aprile 2022 un funzionario dell'intermediario l'ha chiamata e le ha riferito che il suo conto era stato svuotato mediante sessantaquattro bonifici per una somma complessiva di

64.349,59 euro; che la banca è riuscita a bloccare solo i bonifici effettuati in data 13 aprile 2022, riaccreditandole l'importo di 31.349,92 euro, mentre si è rifiutata di risarcire i bonifici effettuati in data 12 aprile 2022; che il 14 aprile 2022 ha sporto denuncia e in data 20 maggio 2022 ha inoltrato reclamo, ricevendo riscontro negativo; che le trentaré disposizioni di pagamento, al limite del massimale consentito, erano del tutto anomale rispetto al suo profilo e alle consuete modalità di accedere ai servizi, ovvero tramite sportello; che la banca l'ha avvisata solo dopo cinquantaquattro bonifici online e dopo trentasei ore dall'inizio della truffa; che non ha ricevuto alcun sms alert per i bonifici disposti e non le è stato chiesto di inserire alcuna password dinamica; che non ha autorizzato le operazioni tramite alcun sistema di autenticazione a due fattori; che non ha fornito ai truffatori le credenziali del suo *home banking* ma si è limitata a cliccare sul link che le era stato inviato tramite sms da un numero identico a quello della banca. La ricorrente ha, poi, così concluso:

Chiediamo il rimborso di euro 32.999,67 pari ai 33 bonifici da euro 999,99 ciascuno non autorizzati, fraudolentemente disposti il 12 aprile 2022, dal conto corrente della signor ██████████

Dal proprio canto, la parte resistente, nel controdedurre, ha affermato che nell'accesso all'home banking tramite la app, per effettuare il login e le operazioni di *inquiry*, il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente + pin, codice statico noto solo al cliente) + codice otp; che, per disporre le operazioni, dopo aver effettuato il login, il cliente deve confermarle inserendo il proprio pin + codice otp; che il codice otp viene generato per un solo utilizzo, in modo silente, dal mobile token integrato nella app; che l'attivazione del mobile token è possibile solo attraverso la digitazione delle credenziali di sicurezza (numero cliente + pin) e del codice otp inviato tramite sms al cellulare collegato all'home banking; che, nel caso specifico, come dichiarato in denuncia, la banca alle ore 15:59 del 12.04.2022 ha inoltrato al numero di cellulare della ricorrente un sms alert che la avvisava del fatto che stava attivando il mobile token; la ricorrente ha altresì ricevuto numerosi sms di avviso di inserimento bonifici, anche il giorno successivo, senza preoccuparsi minimamente di quanto stava accadendo; che la banca da tempo raccomanda alla propria clientela la massima attenzione e cautela nell'utilizzo dei canali telematici; la cliente, dopo aver ricevuto il primo sms in data 12.04.2022, avrebbe dovuto immediatamente contattare il servizio clienti della banca; che il sistema a due fattori adottato è riconosciuto come un sistema forte anche dall'orientamento diffuso dei Collegi ABF (cfr. Collegio di Roma, decisione n. 5565 del 2019); che la ricorrente non ha adempiuto con la necessaria diligenza ai propri obblighi di custodia poiché ha comunicato al presunto frodatore, oltre alle credenziali di sicurezza dell'home banking, anche il codice otp ricevuto via sms, consentendogli così di scaricare l'app, attivare il mobile token ed effettuare le operazioni; che, come dimostrato dai log prodotti, le operazioni sono state autorizzate tramite un sistema di autenticazione a due fattori, uno statico (pin) e uno dinamico (otp); che, quanto al contatto telefonico proveniente da un numero della banca, è possibile con pochi passaggi modificare il mittente di un numero telefonico da parte di terzi; tale modalità è nota da tempo e chiunque ha la possibilità di modificare l'identificativo del chiamante poiché sul web esistono molti servizi che permettono tale operazione; che, in sintesi, quindi, le operazioni risultano correttamente eseguite tramite un sistema di autenticazione forte e sono state rese possibili esclusivamente dalla conoscenza, in capo al frodatore, delle credenziali di sicurezza fornite dal ricorrente medesimo. Alla luce di quanto precede, la parte resistente

ha così concluso:

chiediamo a codesto spettabile Arbitro di voler respingere il ricorso nel merito in quanto infondato.

In sede di repliche, il ricorrente, nel ribadire quanto affermato in sede di ricorso, ha affermato che, dopo aver eseguito l'accesso alla app inserendo le proprie credenziali, ma senza comunicarle a terzi, ha perso completamente padronanza del suo telefono cellulare, che si è bloccato per settantadue ore; che ella dunque non ha potuto visualizzare gli eventuali sms che la banca afferma di averle inviato e non ha ricevuto né comunicato a terzi i codici OTP; che evidentemente il truffatore è riuscito a prendere pieno possesso del suo cellulare e ha potuto operare indisturbato inserendo gli otp che solo lui poteva visualizzare; che a differenza di quanto avvenuto nei precedenti citati da controparte, ella non ha mai comunicato al malfattore i codici otp proprio perché non li ha mai potuti visualizzare; che il sistema di sicurezza, completamente interno, basato solo su otp e alert comunicati via sms, non protegge i clienti dalle truffe realizzate nel caso in esame; che la banca avrebbe dovuto accorgersi delle operazioni anomale su conto corrente avuto a riguardo il suo profilo e la sua ordinaria operatività; a favore dei beneficiari indicati dal frodatore non era mai stata effettuata prima alcuna operazione; che la banca non ha attuato un sistema di monitoraggio dei movimenti anomali rendendosi dunque, anche sotto questo profilo, gravemente inadempiente ai propri obblighi e violando la diligenza del *bonus argentarius*.

DIRITTO

Parte ricorrente chiede il rimborso di trenta bonifici, dell'importo di 999,99 euro ciascuno, effettuati tutti il 12 aprile 2022 online tramite *app* collegata al servizio di *homebanking*, e la cui somma complessiva è pari a 32.999,67 euro pari alla somma chiesta in restituzione dalla stessa ricorrente.

Il Collegio osserva che, sebbene l'intermediario eccepisca che le operazioni di bonifico contestate, perfezionate online, sono state correttamente autenticate tramite l'inserimento di password statiche e dinamiche, e sebbene affermi che l'attivazione iniziale del mobile token sia avvenuta tramite l'inserimento di PIN e OTP ricevuto via sms, dai log prodotti non risulta esplicitata la presenza del PIN quale fattore di autenticazione di tale fase il 12 aprile 2022. Il PIN, infatti, risulta inserito unicamente per la disposizione dei bonifici unitamente all'OTP generato da mobile token.

Alla luce di quanto precede, pertanto, il Collegio ritiene che la procedura di autenticazione adottata dall'Istituto non sia conforme ai criteri richiesti dalla Opinion EBA, conseguendone l'accoglimento della istanza.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l’intermediario tenuto in favore della parte ricorrente alla restituzione dell’importo complessivo di euro 33.000,00 (trentatremila/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