COLLEGIO DI BOLOGNA

composto dai signori:

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

Relatore MARCO CORRADI

Seduta del 11/07/2023

FATTO

Parti ricorrenti, quali cointestatario e cointestataria di un rapporto di c/c, riferiscono che:

- all'epoca dei fatti, la cointestataria era la sola ad aver abilitato le credenziali per accedere al conto corrente in modalità on line.
- Nel mese di marzo 2022 sul conto corrente erano stati disposti due bonifici ordinari, mai autorizzati, per un importo pari ad € 36.227,21.
- Il 14 marzo 2022, il cointestatario riceveva sulla propria utenza mobile il seguente sms proveniente dalla banca: "*effettuare il nuovo aggiornamento [nome intermediario] per evitare il blocco dei suoi servizi*". Lo stesso, non potendo procedervi in considerazione del fatto che non aveva le credenziali per accedere all'home banking, ne dava avviso alla cointestataria.
- Il successivo 21 marzo 2022, questa volta all'utenza telefonica della cointestataria, perveniva un ulteriore sms con il quale la banca comunicava di aver già limitato l'operatività del conto corrente per mancanza dell'adeguata verifica del cliente.

- La cointestataria cliccava sul link contenuto nel messaggio sms ed era, così, reindirizzata su di una pagina web del tutto identica a quella dell'intermediario. Immediatamente dopo, era contattata telefonicamente dal numero clienti della banca e l'interlocutore, qualificatosi operatore dell'intermediario, la informava che il questionario di adeguata verifica non era ancora stato aggiornato a causa di un malfunzionamento all'app ma che, comunque, bisognava procedervi.
- L'operatore chiedeva, quindi, di installare un aggiornamento dell'app attraverso un link inviato con un sms che aveva come mittente la banca e che subito dopo lo stesso operatore chiedeva di cancellare. Dopo aver condotto una serie di tentativi volti a ripristinare il corretto funzionamento dell'app, l'operatore comunicava alla cointestataria che il malfunzionamento continuava a persistere e le chiedeva di disinstallare l'app e di attendere una sua chiamata nei giorni successivi.
- Alle ore 14:42 dello stesso 21 marzo, prima che la telefonata con il sedicente operatore si concludesse, la cointestataria riceveva un primo sms che confermava di "*aver certificato il numero*" e, poi, un secondo sms con cui l'appuntamento con l'"operatore" era fissato per le ore 17:00 del giorno 22 marzo. Alle ore 13:41 del 22 marzo, la stessa riceveva sul proprio cellulare un nuovo messaggio che le comunicava il rinvio dell'appuntamento alle ore 17:00 del 23 marzo.
- Il 23 marzo 2022, la cointestataria riceveva una nuova chiamata dal medesimo operatore che nel corso della quale le comunicava che l'intervento di aggiornamento dell'app si era concluso correttamente.
- L'operatore, durante le conversazioni telefoniche, non aveva mai chiesto alla cointestataria di comunicare le credenziali di accesso al conto corrente.
- Il 24 marzo 2022, la cointestataria contattava telefonicamente il servizio clienti dell'intermediario e, così facendo, apprendeva che sul conto corrente non vi era la giacenza che avrebbe dovuto esservi, e cioè di circa € 40.000,00, bensì la sola di € 2.887,60.
- Lo stesso giorno, la cointestataria sporgeva denuncia per truffa presso la competente stazione dei carabinieri e, al contempo, proponeva reclamo all'intermediario.
- Successivamente, erano stati informati dal direttore della filiale che la truffa era stata perpetrata per il mezzo di un *malware* ed erano stati invitati a ripristinare sui propri dispositivi elettronici le impostazioni di fabbrica al fine di scongiurare nuovi attacchi informatici.
- L'intermediario, nonostante le numerose richieste nei suoi confronti rivolte, non forniva la documentazione inerente alle disposizioni di bonifico non autorizzate ed alla cronologia degli accessi all'*home banking*, né dava evidenza dei messaggi sms *alert* inviati.
- La truffa era stata realizzata, evidentemente, con sistemi di intrusione informatica altamente sofisticati tali da consentire ai truffatori di entrare in possesso delle credenziali di accesso all'*home banking* e dei codici necessari per l'esecuzione delle operazioni fraudolente.
- Sul dispositivo mobile non era pervenuto alcun messaggio contenente l'OTP, per cui è ragionevole pensare che la ricezione ne era stata impedita da un'intrusione informatica capace di deviare i messaggi da remoto. Prova ne è che sul numero di telefono certificato, nonostante fosse stato attivato il servizio di *alert*, nessun avviso era stato ricevuto in occasione dei due bonifici disconosciuti.

- Sotto altro profilo, la frode aveva avuto buon esito perché era stata consumata in concomitanza della fase di aggiornamento del questionario di adeguata verifica, nel corso della quale l'intermediario aveva tenuto comportamenti tutt'altro che chiari, anzi piuttosto confusionari.
- Peraltro, benché la banca avesse sollecitato l'aggiornamento del questionario tramite SMS ed e-mail, un malfunzionamento dell'app non aveva mai consentito loro di completare autonomamente il questionario.
- A partire dall'anno 2018 dal conto corrente erano stati ordinati solo due bonifici di importo irrisorio. Invece, il 21 e il 22 marzo, erano stati ordinati due bonifici per un importo complessivo di € 36.227,21. L'intermediario, quindi, avrebbe potuto impedire l'esecuzione degli stessi, allorquando si fosse dotato di un meccanismo in grado di rilevare le operazioni anomale, come tali sono state quelle di che trattasi.
- Il primo bonifico era stato disposto alle ore 18:53 del 21 marzo 2022, mentre il secondo alle ore 18:07 del successivo giorno 22. Le operazioni dispositive erano, quindi, avvenute oltre l'orario limite di ricezione delle ore 17:00 e, pertanto, sicuramente contabilizzate il giorno successivo alla data del loro rispettivo compimento. La banca, tuttavia, non si era attivata al fine di richiamarli.
- In ogni caso, entrambi i bonifici erano stati eseguiti oltre il termine ultimo previsto per l'aggiornamento del questionario di adeguata verifica e, conseguentemente, l'operatività del conto corrente avrebbe dovuto essere inibita.
- I bonifici disconosciuti presentavano, del resto, chiari indici di anomalia (superamento del limite annuo di uscite attese; causali dei bonifici estremamente generiche; IBAN del beneficiario del secondo bonifico corrispondente ad una carta prepagata).
- La banca aveva assunto un atteggiamento ostativo rispetto alle richieste di informazioni e di consegna documenti avanzate in fase di reclamo, opponendo dinieghi con motivazioni del tutto pretestuose. Ciò aveva comportato l'impossibilità di poter esercitare per diversi mesi il diritto di presentare il ricorso e la necessità di dover sopportare spese per l'assistenza legale e per le indagini tecniche.

L'Intermediario, in sede di controdeduzioni, eccepisce che:

- il ricorso è irricevibile nella parte in cui sono spiegate domande in tema di *privacy* e di antiriciclaggio, poiché materie queste che esulano dalla competenza dell'ABF.
- Si era prontamente attivato, a seguito della segnalazione dei clienti, per l'ottenimento della restituzione delle somme oggetto di frode ma di non esservi riuscito per via del fatto che la banca corrispondente aveva eccepito l'incapienza dei conti dei beneficiari.
- I ricorrenti sono intestatari di un conto corrente al quale è collegato il servizio "Rapporti a distanza tra Banca e Cliente" che consente l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione "forte" tale per cui è necessario:

  - per effettuare il *login* e le operazioni di *inquiry*, inserire le credenziali di sicurezza (numero cliente + PIN) + codice OTP generato da *Mobile Token* integrato nell'app che il cliente ha attivato sul proprio *device*;

- per disporre le operazioni, dopo avere effettuato il *login* e inserita l'operazione, la conferma mediante l'inserimento del PIN + codice OTP;
- per l'attivazione del *Mobile Token*, la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'*home banking*.

- La cointestataria il 21 marzo 2022 aveva ricevuto sul suo cellulare il seguente messaggio: "*gentile cliente la invitiamo ad effettuare il nuovo aggiornamento […] per evitare il blocco dei suoi servizi*". In tale messaggio era contenuto il seguente link: "*http://linkeu.info*". Non solo. Dopo poco tempo, la stessa era stata contattata da un sedicente operatore che l'aveva invitata a disinstallare l'app ufficiale e ad installare un'altra app (non autorizzata dalla banca), inviandole il seguente SMS: "*scarica e installa la nuova app sms sicura*" con un link: "*https://is.gd/***bancasicura*". La ricorrente aveva riferito di aver seguito le indicazioni dell'interlocutore cliccando sul citato link e, così facendo, installato l'app.
- A fronte della richiesta di disinstallare la app ufficiale, la ricorrente avrebbe, quindi, dovuto insospettirsi e non avrebbe dovuto comunicare a nessuno le credenziali dell'*home banking*.
- Dalle verifiche effettuate non era emerso alcun malfunzionamento o compromissione dei sistemi, tanto che le operazioni risultano correttamente autenticate, registrate e contabilizzate.
- Dai log allegati, si evince che le operazioni sono state validate correttamente con un sistema di autenticazione "forte a due fattori", uno statico (PIN - fattore di conoscenza) ed uno dinamico (OTP – fattore di possesso).
- Aveva, comunque, inviato al cellulare della cointestataria le relative notifiche *push* e gli sms *alert*, inviando, precedentemente all'esecuzione delle operazioni, anche le notifiche riguardanti l'attivazione del *Mobile Token*.
- Senza la comunicazione del codice riservato, non sarebbe stata possibile, da parte di soggetti terzi, l'attivazione del *Mobile Token*, a seguito della quale erano state poi avviate, sempre da soggetti terzi, tutte le attività finalizzate alla successiva esecuzione delle operazioni fraudolente.
- Per quanto riguarda i limiti previsti per l'esecuzione on line dei bonifici ordinari, sul sito ufficiale era riportata la seguente informazione: "*l'importo massimo per la singola operazione online è di 50.000,00 euro, pari anche al limite massimo dispositivo giornaliero sulla Banca via Internet*".
- Nessuna assistenza di tipo professionale era espressamente richiesta ai fini della presentazione di un ricorso ABF e, pertanto, non può essere oggetto di valutazione la domanda accessoria di rimborso di spese legali eventualmente sostenute dai ricorrenti.

Parti ricorrenti, in sede di repliche, eccepiscono che:

– il richiamo all'"*attività della Banca di ricertificazione del Questionario Cliente*" non travalica la competenza dell'Arbitro, atteso che nessuna specifica domanda era stata formulata al riguardo. Nella narrativa del ricorso, il comportamento tenuto

dall'intermediario in occasione dell'aggiornamento del questionario cliente era stato descritto con il solo intento di fornire all'arbitro adito tutti gli elementi utili ai fini del decidere.

- La cointestataria non avrebbe potuto avvedersi dell'inattendibilità delle informazioni ricevute dal sedicente operatore dal momento che il *modus operandi* della banca in materia di antiriciclaggio era risultato sovrapponibile a quello adottato dal truffatore.

- La cointestataria era stata indotta ad eseguire il download dell'app, che si sarebbe poi rivelata non essere dell'intermediario, perché il falso operatore era, evidentemente, a conoscenza del mancato aggiornamento del questionario cliente e, così, gli era stato agevole sostenere che fosse necessario effettuare un download di aggiornamento.

- Il sistema di sicurezza adottato dalla banca era conforme agli standard della PSD2 solo nella fase di prima configurazione dell'app. Per ogni operazione successiva, il rispetto degli standard imposti dalla PSD2, invece, è solo apparente. Una volta carpite alla vittima le chiavi della conoscenza ed una sola OTP necessaria alla configurazione dell'app su di un proprio dispositivo, i truffatori hanno, difatti, libero accesso al conto corrente on-line della vittima.

- I log della banca riportano le attività eseguite sull'app ma nulla attestano sulla riconducibilità delle stesse alla ricorrente.

- Il primo bonifico era stato inserito immediatamente dopo l'attivazione di un nuovo *mobile token* e ciò avrebbe dovuto imporre all'istituto di predisporre appositi *alert* o blocchi di operatività.

- Peraltro, dalla sequenza dei dati dei log, si evince che il 21 marzo 2022, alle ore 14:23, era registrato il primo accesso all'app con OTP da Mobile Token, l'unico riconducibile alla cointestataria, geolocalizzato nell'area geografica di residenza della stessa. Dopo nove minuti, vi era un secondo accesso all'app per l'attivazione del *Mobile Token* sul dispositivo del truffatore da cui erano stati eseguiti i bonifici disconosciuti, geolocalizzato in Sardegna. Il giorno successivo, dopo un primo accesso geolocalizzato in Sardegna, erano stati eseguiti una serie di accessi da un differente IP, geolocalizzato a Napoli, località dalla quale sarebbe stato eseguito il secondo bonifico disconosciuto.

- La schermata prodotta dalla resistente in ordine alla trasmissione dei messaggi SMS e delle notifiche *push* non offre alcuna prova del fatto che gli stessi sono stati ricevuti effettivamente sul dispositivo della ricorrente. Viceversa, la circostanza della mancata ricezione dei messaggi SMS e delle notifiche *push* è attestata dalla copia forense eseguita sul telefono cellulare della cointestataria, dalla quale risulta che su tale dispositivo non era mai stato visualizzato né il messaggio contenente il codice OTP né i messaggi sms *alert*.

- Le notifiche *push* non erano state visualizzate sul dispositivo della cointestataria bensì su quello in uso al truffatore.

- L'intermediario non aveva dato prova delle attività eseguite per il recupero delle somme sottratte.

L'intermediario, in sede di contro repliche, evidenzia che:

- in presenza di un sistema valutabile come sicuro e in assenza di particolari anomalie di sistema, si deve presumere che ci sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento.

- Le operazioni disconosciute erano state inserite ed autorizzate con le credenziali di sicurezza della cointestataria, come dimostrato dai log allegati alle controdeduzioni.

- Comunicare le proprie credenziali configura un incauto comportamento del titolare degli strumenti di pagamento ed una condotta gravemente colposa.

- La cointestataria ha dichiarato, difatti, di avere disinstallato la app ufficiale ed installato un'altra app non autorizzata dalla banca.

- Dalle verifiche effettuate non era emerso alcun malfunzionamento o compromissione dei sistemi, tanto che le operazioni risultano correttamente autenticate, registrate e contabilizzate.

- La cointestataria aveva ricevuto il messaggio di attivazione del *Mobile Token* e, a seguito della ricezione di tale messaggio, non si era insospettita, considerato che non era stata lei a richiedere l'attivazione del *Mobile Token*. Sicché, da subito, avrebbe ben potuto richiedere il blocco dei canali diretti ed evitare, così facendo, l'esecuzione delle successive operazioni in frode.

- Di non poter interferire con l'autonomia dispositiva della clientela.

- Senza le credenziali di sicurezza non sarebbe stato possibile in alcun modo attivare il *Mobile Token*. Tale attivazione aveva consentito ai soggetti terzi di poter operare liberamente sul conto ed eseguire le operazioni dispositive.

- Dai log allegati alle controdeduzioni, si evince che le operazioni sono state validate correttamente con un sistema di autenticazione "forte a due fattori", uno statico (PIN - fattore di conoscenza) e uno dinamico (OTP – fattore di possesso).

- Aveva inviato al cellulare del cointestatario le relative notifiche *push* e gli sms *alert*, e, precedentemente all'esecuzione dell'operazione, anche il messaggio riguardante l'attivazione del *Mobile Token*.

DIRITTO

Il Collegio, in primo luogo, rilevato che i richiami di parte ricorrente in tema di *privacy* e di obblighi di adeguata verifica sono finalizzati esclusivamente a rappresentare compiutamente il contesto fattuale nell'ambito del quale si è consumata la truffa, non può

che respingere l'eccezione di incompetenza per materia sollevata dall'intermediario resistente.

Venendo al merito, occorre sottolineare che le operazioni contestate sono state poste in essere sotto il vigore del D.lgs. 27 gennaio 2010, n. 11, 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.

Orbene, ai sensi del primo comma dell'articolo 10 del citato D.lgs. 11/2010 è onere dell'intermediario provare che l'operazione sia 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, pena, in difetto, sopportare integralmente le conseguenze delle operazioni disconosciute. Non solo. A mente del secondo comma del medesimo articolo 10, la sussistenza di tale prova non è comunque, di per sé, sufficiente per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento, restando in capo all'intermediario l'ulteriore onere di provare la frode, il dolo o la colpa grave dell'utente.

Dalla documentazione allegata dall'intermediario si evince che:

- alle 14:23 del 21 marzo 2022 è stato effettuato un primo accesso all'app, mediante PIN e OTP, dal *device* ("*Galaxy Tab S3*") e dall'indirizzo IP "151.44.21.147", in dotazione della cliente;

- alle 14:32 del medesimo giorno è stato effettuato un secondo accesso all'app, **mediante il solo PIN**, da un diverso *device* ("*realme C21-Y*") e da un diverso indirizzo IP ("37.159.72.239"). All'interno di tale sessione è stato attivato il *Mobile token* sul nuovo *device*.

- alle 14:36, sempre del 21 marzo, è stato effettuato un terzo accesso dal nuovo *device,* mediante PIN e OTP e, in quella stessa sessione, è stato effettuato, alle 14:38, il primo dei due bonifici disconosciuti, autorizzato mediante PIN e OTP.

- alle 13:37 del successivo giorno 22, è stato effettuato l'accesso all'app, mediante PIN e OTP, dal *device* del truffatore ("*realme C21-Y*");

- all'interno di tale sessione, alle 13:38, è stato effettuato il secondo bonifico, autorizzato mediante PIN e OTP.

Il Collegio, deve rilevare che dai log prodotti dall'intermediario si evince che il primo accesso effettuato dal device "*realme C21-Y*", presumibilmente in uso al truffatore, è stato effettuato con l'inserimento del solo PIN, ma non anche di un secondo fattore di autenticazione.

A tale proposito, pare appena il caso di ricordare che la normativa vigente prevede l'autenticazione forte del cliente (*Strong Customer Authentication* - SCA), cioè l'esistenza di una procedura per convalidare l'identificazione di un utente basata sull'uso di due o più elementi di autenticazione (cd. "autenticazione a due fattori"), appartenenti ad almeno due categorie tra le seguenti:

- **conoscenza** (qualcosa che solo l'utente conosce, come una *password* o un PIN);
- **possesso** (qualcosa che solo l'utente possiede, come un *token*/chiavetta, o uno *smartphone*);
- **inerenza** (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale).

Orbene, nella fattispecie, il primo accesso dal device del truffatore è stato autenticato, come già sopra detto, solo con l'inserimento dell'elemento di conoscenza (PIN) ma non anche con un secondo fattore (possesso/inerenza). Tale circostanza, impone di ritenere non autenticate tutte le operazioni successivamente compiute, a cominciare da quella di attivazione del mobile token, grazie alla quale il truffatore ha poi autonomamente potuto disporre i bonifici disconosciuti.

Ne consegue, inevitabilmente, che le operazioni di bonifico di che trattasi devono ritenersi non autorizzate e, per l'effetto, l'intermediario tenuto - ai sensi dell'art. 11, D.lgs. 11/2010 – al rimborso delle corrispondenti somme.

Avuto riguardo, alla richiesta dei ricorrenti di ristoro delle spese di assistenza difensiva, si rammenta che, secondo le più recenti posizioni condivise dai Collegi e in linea con l'orientamento già espresso nella pronuncia del Collegio di coordinamento n. 3498/2012, il rimborso delle spese legali è ammesso soltanto a condizione:

- della necessità dell'ausilio di un professionista a causa della complessità della controversia;
- della prova dell'effettivo esborso di tali spese da parte del ricorrente.

Nel caso concreto, il Collegio rileva, da un lato, che è sicuramente dimostrato che i ricorrenti si siano avvalsi nell'intero snodo procedimentale, che va dal reclamo al ricorso, dell'ausilio di un difensore, dall'altro, che ne sussista, a fronte delle fatture e della pro-forma agli atti, l'obbligo in capo ai ricorrenti del pagamento.

Fermo quanto sopra, il Collegio è dell'avviso che, nella fattispecie, il comportamento tenuto dall'intermediario resistente (con particolare riferimento al difetto di autenticazione del primo accesso dal device del truffatore), legittimi il risarcimento delle spese di assistenza difensiva, richieste dai ricorrenti, difatti, a titolo di danno.

La particolare complessità della controversia e l'onere defensionale profuso (risultato assolutamente funzionale alla gestione del procedimento), consentono al Collegio di stimare il pregiudizio in via equitativa nella misura di € 1.500,00.

PER QUESTI MOTIVI

Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 36.227,00 (trentaseimila duecento ventisette/00), oltre interessi legali dalla data del reclamo, nonché dell'importo di euro 1.500,00 (mille e cinquecento/00) a titolo di risarcimento del danno.

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