## COLLEGIO DI BOLOGNA

composto dai signori:

| | |
|---|---|
| (BO) MARINARI | Presidente |
| (BO) BERTI ARNOALDI VELI | Membro designato dalla Banca d'Italia |
| (BO) MUCCIARONE | Membro designato dalla Banca d'Italia |
| (BO) SOLDATI | Membro di designazione rappresentativa degli intermediari |
| (BO) D ATRI | Membro di designazione rappresentativa dei clienti |

Relatore ROBERTO D ATRI

Seduta del 20/12/2022

## FATTO

Parte ricorrente riferisce di essere titolare di un conto corrente, con servizio di internet banking, in essere presso la convenuta; in data 14.3.2022, alle ore 17:06, riceveva un sms, nella stessa chat dove pervenivano i messaggi genuini contenenti i codici OTP provenienti dall'intermediario, che la informava di una richiesta di autorizzazione di spesa per euro 251,78, invitando a cliccare in un link se non era stata lei ad autorizzarla; dopo aver cliccato sul link, si apriva una pagina web identica a quella della banca, dove inseriva codice utente, password e numero di cellulare; mentre restava in attesa di ricevere per SMS l'OTP da inserire, effettuava un accesso al conto direttamente dal suo computer per completare il quale riceveva sul proprio cellulare, nella stessa chat dove aveva ricevuto il messaggio c.d. civetta, il codice OTP; alle 17:31, mentre era collegata con l'home banking nel proprio computer, riceveva una telefonata da un sedicente operatore dalla banca al quale comunicava l'ulteriore codice OTP nel frattempo pervenuto con SMS; gli SMS con gli OTP di login non riportano la raccomandazione contenuta negli altri SMS in cui si dice di non condividere il codice con nessuno; non riceveva alcun alert relativo all'accesso al proprio internet banking di un dispositivo diverso, pur essendoci contemporaneamente due dispositivi collegati, probabilmente da città diverse; il sedicente operatore richiedeva poi

l'ulteriore codice OTP che sarebbe pervenuto con SMS, necessario per bloccare il conto; l'SMS pervenuto indicava che il codice serviva per attivare l'App, ma la ricorrente non era a conoscenza che l'installazione di questa App avrebbe sostituito il sistema fino a quel momento utilizzato che prevedeva la ricezione degli OTP dispositivi su SMS; dato che quest'ultimo messaggio riportava l'indicazione di non condividere il codice con nessuno, si rifiutava di comunicarlo per telefono; il sedicente operatore la invitava a bloccare il conto in autonomia: effettuava il login dal finto portale, con inserimento di password e codice OTP; alle 17:42 riceveva sul cellulare un sms che la avvisava che l'App era stata attivata su un dispositivo IPhone; si rendeva così conto di essere vittima di una truffa e riagganciava il telefono; alle 17:46, dopo aver prima chiamato il proprio consulente bancario, telefonava al numero verde della banca e veniva invitata ad installare l'App necessaria per poi bloccare il conto; il blocco del conto avveniva alle 17:51, dopo che il truffatore aveva già disposto alle ore 17:44 un bonifico istantaneo di € 4.582,82; solo in seguito apprendeva che il truffatore, grazie all'applicazione scaricata sul proprio cellulare, era in grado di generare in autonomia i codici OTP; a pochi minuti di distanza, l'App veniva installata su ben due dispositivi, senza che questo facesse scattare alcun sistema di sicurezza in grado di bloccare eventuali disposizioni di conto corrente; di non essere a conoscenza che attraverso l'App fosse possibile disporre dei bonifici istantanei, ciò in quanto il contratto sottoscritto nel 2017 non prevedeva questa modalità di pagamento; l'intermediario convenuto, nei giorni successivi, al fine di riattivare il conto corrente inviava la nuova "password" dell'e-banking mediante l'app, applicazione che però era ancora in possesso anche del truffatore, ed il nuovo "codice utente" mediante mail, codice che ero lo stesso identico codice utente già inserito nel falso sito internet e quindi già conosciuto dal truffatore; questo a conferma che i sistemi di sicurezza della convenuta non sono tali da prevenire le frodi.

L'intermediario controdeduce che le informazioni sull'App sono contenute nella Proposta di Modifica Unilaterale Contratto Inbank del 30.09.2019 inviata al cliente tramite Internet Banking; il numero di cellulare è certificato e indicato nel documento di sintesi; nel caso specifico la App è stata associata al cellulare del truffatore, grazie alla collaborazione della cliente che ha fornito allo stesso tutti i codici, statici e dinamici; la ricorrente è stata vittima di sms *spoofing*, mista a *vishing*; il messaggio truffaldino peraltro presenta errori grammaticali, non arriva con dicitura della banca ma "Sistemalosicuro", nel link di rinvio indicato nel messaggio "civetta" non compare la denominazione dell'intermediario ed il dominio .me è il dominio di primo livello nazionale del Montenegro; la ricorrente ammette di aver fornito al truffatore tutti i codici necessari per portare a termine la truffa; la ricorrente, accortasi della truffa, per bloccare l'attivazione dell'app da parte del truffatore avrebbe dovuto inviare un SMS come indicato nel messaggio di alert ricevuto; l'attivazione dell'invio di bonifici SCT Instant è avvenuta con decorrenza dicembre 2021, a seguito di Proposta di Modifica Unilaterale del 30.09.2021 inviata al cliente tramite Internet Banking; l'attivazione dell'app sul cellulare della cliente comporta l'automatica disabilitazione della precedente app abilitata dal truffatore, che risulta pertanto impossibilitato a ricevere qualsiasi tipo di codice ed a disporre operazioni.

La ricorrente replica che i documenti prodotti dall'intermediario evidenziano la contemporanea presenza sul medesimo e-banking di due utenti distinti riconducibili ai seguenti due indirizzi IP 37.183.38.227 (quello della ricorrente) e 176.245.62.201 (quello del truffatore); il sistema di controllo degli accessi della banca non provvedeva a bloccare l'accesso di un nuovo dispositivo mai registrato prima e soprattutto non dava alcuna comunicazione né alcun alert alla ricorrente dell'accesso al proprio internet banking da parte di un dispositivo diverso rispetto a quello dalla stessa generalmente utilizzato per accedere al proprio conto online; si contestano i LOG depositati dall'intermediario in quanto non si

comprende il loro contenuto, la loro fonte e neanche il dispositivo al quale i dati indicati dovrebbero riferirsi; la ricorrente non ha mai ricevuto le proposte di modifiche unilaterali indicate dall'intermediario nelle controdeduzioni né la banca prova di averle inviate; la ricorrente ha agito con estrema diligenza essendosi immediatamente attivata sia per bloccare il proprio conto corrente sia per impedire al truffatore di effettuare ulteriori disposizioni di pagamento; la ricorrente ha comunicato al truffatore solo il primo codice OTP pervenuto, che gli ha permesso di accedere all'e-banking.

L'intermediario si riporta al contenuto delle proprie controdeduzioni e chiarisce tra l'altro che il sistema di controllo della banca non poteva bloccare l'accesso del nuovo dispositivo in quanto era stato precedentemente autorizzato, anche se non volutamente, dalla ricorrente, fornendo al truffatore i codici necessari; gli accessi non sono stati effettuati in contemporanea, sicuramente con un lasso temporale limitato, ma non in contemporanea; i log prodotti risultano leggibili in combinazione con la Relazione tecnica allegata alle controdeduzioni; la ricorrente ha ricevuto le Proposte di Modifica unilaterale attraverso l'area Inbank, come si evince dai documenti allegati.

**Conclusioni:**

*Il ricorrente*

che l'Ill.mo Arbitro Bancario e Finanziario di Bologna, Voglia accogliere il ricorso e, conseguentemente, disporre e/o condannare [illegible] (c.f. [illegible]), con sede legale in [illegible] alla via [illegible] n. , a provvedere all'immediato rimborso/restituzione della somma di € 4.582,82 (importo del bonifico disconosciuto), oltre spese della presente procedura, in favore dei ricorrenti.

*L'intermediario*

Per tutto quanto sopra esposto, si chiede, in via principale, di rigettare la domanda formulata nei confronti della resistente in quanto infondata in fatto e in diritto e, comunque, non provata e, in via secondaria, di accertare e dichiarare il concorso di colpa del ricorrente nella determinazione del danno, con ogni conseguente statuizione, per tutte le ragioni esposte e vista la condotta gravemente colposa del ricorrente di natura non solo omissiva, ma (soprattutto) fattiva, al punto da avere consentito e, comunque, facilitato il compimento dell'operazione oggi disconosciuta.

**DIRITTO**

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.

Parte ricorrente chiede il rimborso di un bonifico istantaneo, disposto fraudolentemente in data 14.03.2022 alle ore 17:44, di importo pari ad euro 4.582,82.

Circa il bonifico istantaneo, parte ricorrente fa presente che il contratto di conto corrente, sottoscritto nel 2017, non prevedeva la possibilità di effettuare i bonifici istantanei; afferma inoltre di non essere stata messa a conoscenza che attraverso l'App fosse possibile disporre i suddetti bonifici. È in atti il contratto di conto corrente bancario sottoscritto il 27.2.2017 che non prevede tale disposizione. Infatti, l'intermediario evidenzia che detto servizio è stato introdotto per effetto di una modifica unilaterale del contratto datata 30.9.2021, con decorrenza dicembre 2021 ed allega copia della "Proposta di modifica unilaterale del contratto di conto corrente" datata 30.09.2021, inviata alla ricorrente tramite internet Banking, non avendo però la ricorrente controfirmato la missiva 27.2.17 in atti. L'intermediario aveva anche disposto, per gli utenti di internet banking, un massimale per bonifico per le persone fisiche di € 5.000,00.

Sulla proposta di introduzione della modalità di pagamento tramite bonifico istantaneo il Collegio di Coordinamento, nella decisione n. 15627/2021, ha affermato il seguente principio di diritto: *"Le modifiche introdotte dal D.Lgs. 218/2017 all'art. 126-sexies del T.U.B. attraverso la soppressione del previgente comma 5 e l'introduzione del comma 4-bis, non hanno carattere innovativo, poiché ribadiscono la necessità di un giustificato motivo alla base delle proposte unilaterali di modifiche contrattuali relative ai servizi di pagamento, ove il cliente è un consumatore, a conferma della previsione già precedentemente in essere in forza dell'abrogato comma 5. La proposta al consumatore di introduzione della modalità di pagamento tramite bonifico istantaneo, ai sensi dell'art.126-sexies, comma 4-bis, del T.U.B., può essere validamente formulata se corredata da una informazione completa e corretta delle relative caratteristiche. Tale non è quella che si limiti a evidenziare il costo del bonifico istantaneo, a conferma implicita della nuova opportunità offerta al destinatario, senza indicazione della caratteristica della irrevocabilità della operazione, determinativa dell'aumento del rischio in capo all'ordinante".*

Nel caso di specie, si evidenzia che la proposta sopra riprodotta descrive le caratteristiche del bonifico istantaneo precisando che *"il bonifico SCT Instant viene eseguito immediatamente, con accredito alla banca del beneficiario in un tempo massimo pari a 20 secondi"* e che *"non può essere revocato".*

Nella suddetta Proposta del 30.09.2021 veniva anche indicato che i bonifici SCT Instant potevano essere disposti "*solo accedendo al sito internet*" e che solo "*in un secondo momento, a partire dalla data che Le sarà comunicata dalla Banca, potrà disporre ordini di Bonifico SCT Instant anche attraverso la App … (installata sul suo smartphone o tablet) e presso gli sportelli della banca*".

Il punto è se la ricorrente ne ha avuto notizia.

Benvero è che l'intermediario allega di aver trasmesso la Proposta di modifica unilaterale del 30.9.2019 mediante notifica sull'app della ricorrente e ne fornisce evidenza: tuttavia, le predette autenticazioni non sembrano con certezza costituire la prova della ricezione del documento richiamato, perché i log riguardano documenti del 2.10.2021 e l'intermediario precisa che si riferiscono all'invio di un documento "*rapporto CC*" e a un documento "*rapporto VB.*

In conclusione, non sembra asseverata la ricezione delle modifiche, avvenute mediante caricamento sul sito e sul profilo della ricorrente, non mediante autonome comunicazioni dirette.

Invero, se è preliminare la disamina circa la variazione contrattuale, negata nella ricezione dalla ricorrente, giacchè essa si costituisce come radicale negazione della operazione, quand'anche residuassero dubbi al riguardo, soccorre la disamina sulla autenticazione delle operazioni, giacchè è onere dell'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata (art. 10, dlgs. 11/2010). In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute. Invero, qualora non sia stata adottata la c.d. autenticazione forte (SCA), il cliente risponde soltanto in caso di frode (cfr. art. 12, comma 2-*bis* dlgs. n. 11/2010).

L'intermediario ha trasmesso una Relazione Tecnica, denominata "Raccolta dati di dettaglio", dove è presente la legenda dei codici contenuti nelle tracciature informatiche nonché la spiegazione delle tracciature con l'illustrazione dei relativi Log. Allega anche la descrizione dei due fattori di autenticazione utilizzati nel servizio di internet banking. Epperò, dalle richiamate evidenze non pare evincersi l'utilizzo del fattore di conoscenza, ovvero *la password*, che è uno dei due fattori di autenticazione indicati dall'intermediario stesso.

Tanto esime il Collegio dalla indagine sulla colpa grave della ricorrente, incorsa in una truffa insieme di *spoofing* e *vishing* e conduce all'accoglimento del ricorso.

## 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 4.583,00 (quattromila e cinquecentoottantatrè/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