COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) GENOVESE	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 05/07/2023

FATTO

La parte ricorrente espone quanto segue:

- la cliente è stata vittima di truffa il 03.10.2022 riceveva una telefonata da numero riconducibile all'intermediario resistente, presso il quale l'odierna ricorrente intrattiene un rapporto di conto corrente cointestato con il fratello;
- l'interlocutore telefonico, spacciatosi per operatore della resistente, "spaventava" la cliente "dicendole che vi erano delle intrusioni da parte di terzi sul conto e che doveva quindi disinstallare l'applicazione della banca che aveva sul suo cellulare. La invitava poi ad accedere ad un link che nel frattempo le era stato inoltrato dallo stesso numero da cui era stata chiamata il quale – si ripete – appariva come salvato in rubrica col nome della banca";
- la cliente cliccava sul link inviato e veniva indirizzata "sul sito della [resistente]";
- scaricava la nuova applicazione e "immetteva le stesse credenziali che utilizzava per accedere in quella vecchia. Inseriva numero cliente e password. Non inseriva quindi né il PIN della carta né il CVV né altro codice alcuno";
- al termine dell'operazione, l'interlocutore la chiamava nuovamente per dirle "che vi era bisogno di più tempo per far sì che la procedura di ripristino andasse a buon fine e così ha fatto anche il giorno successivo"; precisa che sia il 3, sia il 4 ottobre, l'applicazione sul cellulare della cliente risultava "bloccata, inaccessibile";

- precisa che: “non vi è stato l’inserimento del codice di sicurezza “ID”, non vi è stato il ricevimento della notifica in App, non è stato associato alcun strumento di pagamento (carta di pagamento o conto corrente) e via dicendo”;
- aggiunge: “non si comprende infatti se l’App sia stata installata sul device del truffatore che ha, pertanto, ricevuto sul proprio dispositivo i codici necessari a finalizzare l’operazione”;
- il 05.10.2022 la cliente accedeva all’applicazione con il dispositivo del fratello, cointestatario del conto, in quanto l’app risultava bloccata; si accorgeva che erano state effettuate n. 6 operazioni, che disconosceva;
- contattato il numero verde della resistente, la cliente riusciva a bloccare gli ultimi bonifici del 5 ottobre per un totale di euro 9.000,00, che venivano stornati;
- allega al ricorso la denuncia presentata il 07.10.2022;
- la cliente chiedeva immediatamente il blocco della carta e disconosceva le sei operazioni;
- evidenzia che la cliente è stata vittima di una truffa realizzata con la modalità del c.d. caller id spoofing e del vishing;
- osserva quanto segue: “la mancata adozione del sistema di protezione che consentisse di evitare la doppia autenticazione, il cambio della password e la conferma dell'operazione mediante apposito pin inviato via SMS da un numero che appariva come intestato alla banca del titolare del conto, è sicuramente addebitabile ad una mancata verifica della riconducibilità delle operazioni alla volontà del cliente che non ha mai prestato consenso all’effettuazione di tali operazioni di pagamento”;
- il 12.10.2022, il difensore inviava tramite pec il reclamo alla banca e chiedeva il rimborso di quanto fraudolentemente sottratto;
- il 17.10.2022 la banca forniva riscontro negativo, rilevando che la cliente aveva “imprudentemente digitato le credenziali di accesso all’home banking, permettendo così poi la frode a suo danno” e che aveva “incautamente rilevato il codice di attivazione del mobile token ricevuto dalla stessa mediante un sms al suo interlocutore”;
- rileva che la cliente non ha mai ricevuto tale sms e che ha inserito solamente numero cliente e password; tale circostanza veniva evidenziata con un secondo reclamo, presentato in data 01.11.2022, riscontrato negativamente il 17.11.2022;
- rileva che “è sicuramente evidente il fatto che la sig.ra (…) sia stata certamente raggirata ed avrebbe potuto prestare maggiore attenzione utilizzando maggiore diligenza. Ma questo è un discorso valevole per ogni tipo di truffa e raggiro che subisce un individuo”;
- rileva la responsabilità della banca, tenuta ad adottare tutte le misure tecniche idonee a garantire un adeguato standard di sicurezza;
- evidenzia che “tale fattispecie di Truffa rientra nell'area del “rischio professionale del prestatore dei servizi di pagamento””;
- richiama la decisione n. 12987/2022 del Collegio di Bologna;
- rileva che a seguito dei bonifici disconosciuti non veniva inviato alcun messaggio o e/mail che informava i titolari del conto dell’effettuazione delle operazioni;
- evidenzia che tale servizio è attivo e produce una serie di email ricevute prima della truffa subita in relazione a bonifici effettuati dalla cliente;
- evidenzia che, se la cliente avesse ricevuto la prima mail relativa all’effettuazione del primo bonifico disconosciuto, “sarebbe di certo riuscita ad accorgersi della truffa ed a bloccare i successivi bonifici”;
- rileva che la cliente non ha ricevuto alcuna comunicazione a seguito delle varie operazioni dei giorni 3 e 4 ottobre 2022, “operazioni comportanti un di certo anormale ed ingente flusso di denaro dal conto corrente dei Sig.ri (…) che avrebbe dovuto destare allarme ed una pronta comunicazione ai correntisti da parte dell’operatore bancario”;

- osserva: “si fa infatti presente che i due soggetti, non hanno mai effettuato operazioni di bonifico di così grande entità economica, soprattutto ravvicinate nel tempo, tramite l’applicazione del cellulare. Per i grandi importi la Sig.ra (…) è usa recarsi in banca per svolgere tali operazioni di elevato importo. L’anomalia era quindi evidente”;
- riferisce che, recatasi in banca, scopriva che altre persone erano state vittima di vishing ma ai correntisti non era stata inviata via mail nessuna raccomandazione “che raccomandasse di non rispondere ad una telefonata nella quale veniva chiesto di inserire o dichiarare i codici identificativi”.

L’intermediario resiste al ricorso ed eccepisce quanto segue:
- riepiloga le richieste della ricorrente;
- la ricorrente è cointestataria del rapporto di conto corrente al quale è collegato il servizio “Rapporti a distanza tra Banca e Cliente”, che consente ai clienti di effettuare le operazioni di inquiry e dispositive sui conti correnti personali a loro riferibili, utilizzando il telefono cellulare o internet;
- precisa che la cliente ha aderito al servizio sms alert collegato al suo telefono cellulare (lo stesso indicato nella denuncia); precisa che risulta inserito anche l’indirizzo e-mail;
- produce evidenza degli sms alert e delle notifiche push inviati e consegnati alla cliente nei giorni 3 e 4 ottobre;
- precisa che il servizio di home banking prevede l’accesso alle funzioni di inquiry e dispositive mediante un sistema di autenticazione forte, in linea con la PSD2:
  “in fase di accesso all’home banking da App (…) il sistema di autenticazione prevede:
  • per effettuare il login e le operazioni di inquiry, l’inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP (One Time Password), gemerato da Mobile Token;
  • per disporre le operazioni, dopo avere effettuato la login come sopra e inserita l’operazione, la stessa deve essere confermata mediante l’inserimento del PIN + codice OTP (One Time Password), generato da Mobile Token.
  Il codice OTP (One Time Password) è una password temporizzata valida per un solo utilizzo che viene generata in modo silente dal Mobile Token integrato nell’App (…) che il cliente ha attivato sullo strumento/device che sta utilizzando. Il testo della notifica, che appare sul device e sul quale l’utente deve fare “tap” per autorizzare, indica in chiaro quale operazione/attività si sta autorizzando.
  Il MobileToken è una soluzione digitale studiata per garantire i più elevati standard di sicurezza dei pagamenti online; esso permette di generare automaticamente delle password valide per un solo utilizzo, OTP, direttamente sul proprio smartphone (o Tablet), protegge le credenziali di accesso all’AreaClienti e tutte le operazioni dispositive e di pagamento”;
- l’attivazione del mobile token è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all’home banking, indipendentemente dall’attivazione del servizio sms alert;
- il cliente può attivare il mobile token contemporaneamente su due dispositivi ed è libero di sostituire il proprio device senza dover comunicare il nuovo modello alla banca se il numero di cellulare resta invariato;
- il 03.10.2022, alle ore 15:14:30 e alle ore 15:16:05 la banca ha inviato alla cliente una email e un sms contenenti il codice OTP necessario per l’attivazione del mobile token; riporta la schermata contenuta nel messaggio;
- rileva che “a fronte della esplicita raccomandazione contenuta nell’email e nell’sms la ricorrente non avrebbe dovuto comunicare a nessuno il codice OTP ricevuto e neppure

inserirlo in un eventuale link o pagina web non ufficiali" della banca; rileva che, alla luce dell'alert contenuto nella mail, avrebbe dovuto "dubitare/insospettirsi della telefonata ricevuta, a prescindere dal canale di provenienza";

- rileva che il sistema di autenticazione a due fattori come quello adottato dalla banca è riconosciuto come sistema forte anche dall'orientamento dei Collegi ABF; richiama la decisione n. 15779/2022 del Collegio di Milano e la decisione n. 5565/2019 del Collegio di Roma;
- evidenzia che, in presenza di un sistema in astratto valutabile come sicuro come quello adottato dalla banca 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"; richiama alcune decisioni dei Collegi ABF (cfr. pagina 3 delle controdeduzioni); richiama l'art. 7, comma 2 del d.lgs. 11/2010;
- rappresenta le iniziative della banca al fine di informare la clientela sulle possibili frodi (cfr. pagina 4 delle controdeduzioni);
- riporta il contenuto della denuncia; rileva che la telefonata e la ricezione del messaggio di phishing non vengono contestualizzate in modo preciso nel tempo/orario e che non sono supportate da alcuna prova ai sensi dell'art. 2697 c.c.; richiama la decisione n. 19822/2021 e la decisione n. 17846/2021 del Collegio di Roma;
- richiama la decisione n. 21135/2020 del Collegio di Roma in tema di "vaghezza e genericità del ricorso"; richiama altresì la decisione n. 8632/2021 del Collegio di Bologna;
- rileva "riteniamo alquanto improbabile che la ricorrente potesse avere memorizzato tra le proprie chat il n. (…) dal quale ha ricevuto la telefonata in quanto non corrisponde al n. (...) del servizio clienti (…) dal quale eventualmente la banca chiama i clienti e neppure al recapito dell'agenzia (…) presso la quale la ricorrente intrattiene i rapporti; è probabile che l'affermazione derivi da una verifica internet eseguita ex post";
- rileva che, con riguardo al canale di provenienza delle telefonate, "non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display";
- la richiesta di disinstallare l'app ufficiale per sostituirla con una nuova, non meglio identificata, scaricabile dal link riportato in denuncia, non riconducibile alla banca, avrebbe dovuto far dubitare la cliente, che avrebbe dovuto prendere tempo con l'interlocutore per verificare la genuinità delle richieste rivolgendosi al personale dell'agenzia di riferimento o chiamando il numero verde del servizio clienti;
- la cliente, prima di cliccare il link, per nulla riconducibile alla banca, avrebbe potuto/dovuto verificarlo sul web;
- relativamente al link, rileva che l'URL bit.ly rappresenta un servizio di abbreviazione di link, "per cui non è neppure dato leggere in chiaro il vero link sottostante";
- la ricorrente ammette di aver inserito le sue credenziali personali per accedere a una nuova app rivelandole così al terzo non autorizzato, "mentre del tutto ininfluente è la precisazione di non avere inserito pin e cvv della carta";
- ritiene che tale fattispecie sia riconducibile al tradizionale caso di phishing individuato dalla decisione n. 3498/2012 del Collegio di Coordinamento;
- richiama la decisione n. 18738/2021 del Collegio di Roma in tema di spoofing, "la cui diffusione negli ultimi tempi è divenuta tale per cui l'orientamento dei Collegi ABF è quello di non riconoscerla come frode sofisticata a prescindere";
- evidenzia che è noto da tempo che i malviventi si avvalgono di siti "clone" "per far abboccare alle frodi i malcapitati" e riporta uno stralcio dal sito della Polizia Postale;
- evidenzia che l'operatività disconosciuta dalla ricorrente è avvenuta con autenticazione a doppio fattore, che non risultano cambi di password, "che la ricorrente ha inserito il

codice OTP (…) ricevuto via sms (ma in parte anche via email) autorizzando l'attivazione del mobile token" e che la riconducibilità delle operazioni alla cliente è dimostrata, nei log, dal codice IdUtente in essi riportato;
- precisa che il recapito telefonico dei clienti può essere acquisito da fonti diverse dalla banca e che il fenomeno del phishing colpisce random indipendentemente dalla conoscenza dei rapporti bancari dei destinatari;
- osserva: "in tema di colpa grave a carico della signora Fortunato facciamo altresì rilevare la numerosità degli sms alert e delle notifiche push che [banca resistente] le ha inviato nei giorni in cui si è compiuta la frode, riguardanti accessi al suo home banking da sito web, a fronte dei quali la ricorrente non ha assunto alcuna iniziativa";
- dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi e che l'operazione risulta correttamente autenticata, registrata e contabilizzata, ai sensi dell'art. 10 del d.lgs. 11/2010;
- descrive le evidenze log (allegato n. 6 alle controdeduzioni) relative all'operazione disconosciuta;
- precisa che dalla disamina dei log si evince la riconducibilità delle operazioni al cliente, provata dall'id cliente, nonché la circostanza che tutte le operazioni (di attivazione del mobile token, di login e di bonifico) sono validate correttamente con un sistema di autenticazione forte, "in ossequio alla sicurezza prescritta dalla normativa PSD2", con un pin (fattore di conoscenza) e una OTP (fattore di possesso); richiama le decisioni n. 11254/2020 del Collegio di Milano e n. 3782/2020 del Collegio di Torino;
- richiama l'Opinion EBA del 21 giugno 2019 e la decisione n. 8703/2022 del Collegio di Roma;
- evidenzia che l'importo delle operazioni non può essere considerato anomale "e qualora tale somma, fosse stata considerata dal cliente "fuori norma", quest'ultimo avrebbe potuto far richiesta della modifica del plafond dispositivo dei bonifici"; richiama l'art. 24, primo comma, del d.lgs. 11/2010;
- precisa che la banca, venuta a conoscenza del disconoscimento delle operazioni il 5 ottobre, ha potuto revocare n. 3 ulteriori bonifici inseriti lo stesso giorno come riferito anche dalla ricorrente mentre non era più nei termini per bloccare/revocare le operazioni inserite nei giorni precedenti;
- riferisce che per le operazioni inserite in data 3 e 4 ottobre, la banca ha comunque avviato l'azione di recall verso la banca del beneficiario, senza esito positivo.

Con le repliche la parte ricorrente, oltre a ribadire quanto già riferito in sede di ricorso, espone quanto segue:
- ribadisce che "nessuno degli sms è pervenuto alla ricorrente che anche con questo atto conferma di non averli ricevuti";
- rileva che la cliente non poteva ricevere le notifiche push in quanto l'applicazione risultava bloccata;
- rileva che nelle controdeduzioni la banca fa riferimento all'invio di sms "ma nulla controdeduce in merito al (mancato) invio delle mail a seguito delle varie disposizioni di bonifico";
- con riguardo all'allegato 4 alle controdeduzioni "che servirebbe a provare l'inoltro di una comunicazione contenente regole e comportamenti per operare in sicurezza", evidenzia che "tale documento è privo di ogni valore probatorio" e che non vi è prova che sia stato inviato alla cliente, né vengono precisate le modalità di spedizione;
- sottolinea che la cliente ha "chiaramente esposto i fatti per come effettivamente verificatisi (…)".

Nelle controrepliche, l'intermediario, oltre a ribadire quanto già riferito in sede di controdeduzioni, espone quanto segue:

- conferma che gli sms alert riferiti alle operazioni disconosciute sono stati inviati dalla banca all'utenza cellulare della cliente, la stessa dichiarata anche nella denuncia e per la quale la ricorrente non ha dichiarato alcun malfunzionamento;
- con riguardo alla notifica via e-mail delle operazioni disconosciute, precisa che non si tratta di un servizio di default e che può essere richiesto di volta in volta dal cliente nell'operatività da sito web (riporta a titolo esemplificativo la schermata di impostazione di bonifico da sito web);
- con riguardo all'allegato 4, rileva che è uno stralcio dell'estratto conto al 30.06.2022, di cui non risulta che la cliente abbia reclamato la mancata ricezione; allega copia dell'estratto conto completo;
- riporta alcune decisioni ABF (cfr. pagine 2 e 3 delle memorie di controreplica);
- richiama la sentenza della Cassazione civile sez. I - 13/03/2023, n. 7214 "che in sintesi afferma a sostegno della irresponsabilità della Banca in tema di phishing".

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite tra il 3 ed il 4 ottobre 2022. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n.

218/2017, “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”.

3.- Orbene, il concetto di “autenticazione forte” trova la propria definizione all’art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): “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”.

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell’autenticazione forte, *dall’Opinion of the European Banking Authority on the elements of strong customer authentication under* PSD2 del 21 giugno 2019.

L’EBA ha chiarito, per esempio, che, mentre l’OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della *strong customer authentication*, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che “*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*”.

Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l’inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).

4.- La controversia ha ad oggetto il disconoscimento di sei bonifici online, di importo complessivo pari a euro 17.994,00, effettuati tra il 03.10.2022 e il 04.10.2022.

In sede di denuncia, l’odierna ricorrente ha riferito di aver ricevuto una telefonata da un numero fisso e che l’interlocutore, sedicente impiegato della resistente, le chiedeva di disinstallare l’applicazione della banca e di cliccare sul link che riceveva via sms “al fine di evitare il blocco” del conto corrente.

Riceveva un link che la conduceva a un sito internet dove inseriva le credenziali relative al suo conto:

Il messaggio cui viene fatto riferimento in sede di denuncia sarebbe stato inviato successivamente alla telefonata ricevuta dal sedicente operatore. Non è stata comunque prodotta alcuna schermata del messaggio menzionato in sede di denuncia.

5.- Quanto all’autenticazione delle operazioni, l’intermediario riferisce che l’attivazione del mobile token è resa possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) [fattore di conoscenza] e del codice OTP inviato alla cliente via SMS al cellulare collegato all’home banking [fattore di possesso].

Viene prodotto il log contenente evidenza dell'accesso con ID Utente e PIN (fattore di conoscenza) per l'attivazione del mobile token, nonché della OTP utilizzata per l'attivazione (fattore di possesso).

L'utenza telefonica destinataria del messaggio corrisponde all'utenza indicata dall'odierna ricorrente in sede di denuncia.

Per l'accesso al conto, dai log, emerge l'inserimento del PIN [fattore di conoscenza] e l'utilizzo del mobile token per la generazione dell'OTP [fattore di possesso].

Per le operazioni di bonifico, emerge che sono state autorizzate con PIN [fattore di conoscenza] e utilizzo dell'OTP generato da mobile token [fattore di possesso]. Viene prodotto il relativo log.

Si richiama l'Opinion dell'EBA del 21 giugno 2019 che ritiene integrante valido fattore di possesso un meccanismo che preveda l'utilizzo di una OTP generata (da un device) o ricevuta (su un device).

Questo Collegio ha ritenuto compliant alla SCA una modalità autorizzativa che preveda la generazione di una OTP da mobile app (con riguardo al medesimo intermediario, Coll. Roma, dec. n. 19821/2021).

6.- La parte ricorrente evidenzia che i bonifici disconosciuti sono "operazioni comportanti un di certo anormale ed ingente flusso di denaro dal conto corrente dei Sig.ri (…) che avrebbe dovuto destare allarme ed una pronta comunicazione ai correntisti da parte dell'operatore bancario".

Al riguardo, precisa che i clienti "non hanno mai effettuato operazioni di bonifico di così grande entità economica, soprattutto ravvicinate nel tempo, tramite l'applicazione del cellulare. Per i grandi importi la Sig.ra (…) è usa recarsi in banca per svolgere tali operazioni di elevato importo. L'anomalia era quindi evidente".

Questo Collegio ritiene che, anche a prescindere dall'applicabilità degli indici antifrode di cui al D.M.112/2007, se le operazioni di pagamento e di prelievo per frequenza oltre che per consistenza appaiano *ictu oculi* assolutamente non in linea con un'operatività fisiologica, esse siano da considerare "anomale". Pertanto, l'intermediario che non abbia predisposto idonei strumenti per evidenziare e/o bloccare automaticamente comportamenti che siano evidentemente anomali, ne è responsabile (Coll. Bologna, dec. n. 4852/2022; ma già, Coll. Bologna, dec. n. 11849/2017, Coll. Roma, dec. n. 3534/2014, n. 4131/2015, n. 11452/2016).

Nel caso di specie sono stati disposti ben undici bonifici per un importo complessivo di circa 27.000,00 euro (cinque dei quali per un importo totale di 9.000,00 euro che il cliente è riuscito a bloccare).

A fronte della eccezione della parte ricorrente, l'intermediario nulla ha replicato o prodotto al fine di dimostrare che queste operazioni potessero risultare in linea con la fisiologica operatività del rapporto.

Secondo la consolidata opinione della dottrina e della giurisprudenza, l'attività bancaria, in quanto attività riservata, deve sottostare al canone di diligenza previsto dall'art. 1176, comma 2, c.c. ("diligenza dell'accorto banchiere"), con conseguente adozione di tutte le cautele necessarie.

Ciò chiarito, stante il rilevato anomalo utilizzo del conto, vale dire il fatto che nel giro di poco più di un giorno sono state compiute in successione undici richieste di bonifico per un rilevante importo significativo anche ai sensi della cogente normativa sull'antiriciclaggio e

comunque che non risulta assolutamente in linea con l'operatività "storica" della ricorrente per frequenza e tipologia , l'intermediario avrebbe dovuto avvedersi di questa difformità, predisponendo sistemi automatici di rilievo e/o di blocco delle operazioni.

Nel caso di specie ciò non è avvenuto e, di conseguenza, l'intermediario non può andare esente da responsabilità e, pertanto, la domanda deve essere accolta.

Peraltro, ritenuto che all'origine della presente fattispecie si può verosimilmente ravvisare una responsabilità della ricorrente per "colpevole credulità", dall'altro lato, valutata la diligenza della banca nella prestazione del servizio, si deve valutare una concorrente responsabilità quasi paritaria dell'intermediario che non ha predisposto adeguati sistemi per proteggere più efficacemente i propri clienti.

Il danno può essere dunque quantificato in via equitativa nella misura di euro 9.000.00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 9.000,00, determinata in via equitativa.
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