[redacted]

TRIBUNALE DI BERGAMO

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

Il Giudice Unico di Bergamo, dott.ssa Laura Giraldi, ha pronunciato la seguente

SENTENZA

nella causa civile iscritta al n. [redacted] R.G.

promossa da

[redacted] (C.F. [redacted]), residente ad [redacted], rappresentato e difeso dall'avv [redacted] per delega in atti;

-attore-

contro

[redacted] (C.F [redacted]), in persona del legale rappresentante *pro tempore*, con sede legale i[redacted], rappresentata e difesa dall'avv. [redacted] per delega in atti;

-convenuta-

OGGETTO: risarcimento danni.

CONCLUSIONI

Per parte attrice: come da atto di precisazione delle conclusioni depositato il 04/10/2022.

Per parte convenuta: come da atto di precisazione delle conclusioni depositato il 07/10/2022.

MOTIVI IN FATTO ED IN DIRITTO

Con atto di citazione notificato in data 21/01/2022, il Signor [redacted] conveniva in giudizio la [redacted] chiedendo il rimborso della somma di euro 7.400 illecitamente sottratta da terzi soggetti a seguito di frode informatica

dal proprio conto corrente [redacted] acceso presso la Banca odierna convenuta. L'attore esponeva che in data 10/01/2020, a seguito di una chiamata da parte di un operatore del Nucleo Antifrode che lo invitava a controllare gli avvisi relativi alle proprie disposizioni bancarie ricevuti via SMS sul proprio cellulare, si avvedeva della presenza di una operazione non autorizzata effettuata dal proprio conto corrente. A sostegno della propria domanda l'attore deduceva la responsabilità dell'intermediario che, non avendo adottato misure di protezione adeguate ad impedire la commissione di frodi, aveva consentito a terzi di introdursi illecitamente nel sistema elettronico di pagamento cagionandogli un danno.

Si costituiva in giudizio [redacted] contestando integralmente le avverse difese e chiedendo il rigetto delle domande formulate in quanto infondate in fatto ed in diritto. La convenuta deduceva di aver posto in essere tutte le misure di sicurezza e prevenzione richieste dalla normativa di settore tramite l'adozione di un sistema di autenticazione c.d. forte e che la sottrazione della somma dal conto corrente lamentata dell'odierno attore doveva essere ricondotta a colpa grave del Signor [redacted] in relazione alla gestione, conservazione ed utilizzo degli strumenti di sicurezza fornitegli dalla banca.

Precisate le rispettive conclusioni, la causa passa ora in decisione.

La domanda dell'attore deve essere accolta.

I dati incontestatamente risultanti in atti sono i seguenti.

[redacted] è titolare del conto corrente bancario [redacted] acceso nell'anno [redacted] presso la filiale di [redacted] con operatività anche da remoto tramite *home banking* (docc. 2 parte attrice e 3 e 4 parte convenuta).

In data 9.1.2020 alle ore 6.42.32 la il sistema operativo della banca ha inviato all'attore sul suo cellulare ([redacted]) un sms di attivazione del *mobile token* contenente il codice di sicurezza da digitare per l'attivazione, sms ricevuto alle 6.55.16; in particolare il

messaggio indicava "hai chiesto l'attivazione del Mobile token, inserisci il codice riservato******* non comunicarlo mai a nessuno, personale BNL incluso. Info BNL****'

Disponendo l'attore di servizio di *sms alert*, alle ore 11.47 il sistema operativo della banca informava il [redacted] anche dell'esecuzione del bonifico di euro 7.400.

In data 11.1.2020 alle ore 18.30 il [redacted] riceveva poi una telefonata da tale [redacted] presentatosi come operatore del Nucleo Antifrode Internet di Roma, che gli comunicava la rilevazione di un avviso di operazione anomala uscita dal conto corrente del [redacted], avviso che effettivamente l'attore rinveniva relativo al bonifico di euro 7.400 : il messaggio indicava 'è stato inserito un ordine di bonifico [redacted] importo 7.400 euro, in data 9.1.2020 da mobile [redacted].

Tali i dati incontestati.

Dalla registrazione del servizio SMS Alert (doc.1 di parte convenuta) risultano infatti i due avvisi inviati al numero di cellulare del [redacted]

Assume l'attore di non aver mai attivato il servizio di *home banking* per l'operazione in questione e tanto meno di aver mai inserito le relative credenziali e di averle fornite a qualcun altro.

Dalle registrazioni della banca relative all'operazione in questione (doc.2 di parte convenuta) risultano regolarmente effettuati tutti i passaggi per la disposizione bancaria oggetto di contestazione: alle ore 6.43.32 è stato effettuato infatti Accesso con PIN, alle ore 6.43.35 la Verifica a due fattori con OTP da Mobile Token, alle ore 6.43.44 altro Accesso con Pin da altro telefono), alle 6.43.58 Accesso con Id utente e Pin per attivazione del Mobile Token, alle ore 6.44.07 la Scelta del Nick Name, alle ore 6.45.09 l'Attivazione del Mobile Token ed alle 6.45.10 il Mobile Token era attivato.

Successivamente alle ore 11.39.38 è stato effettuato un nuovo accesso con Pin, alle 11.39.43 è stata effettuata la verifica a due fattori con OTP da Mobile Token ed infine alle 11.47.38 è stato eseguito il bonifico con inserimento del Pin e OTP da Mobile Token.

Nella materia che qui interessa rilevano in primo luogo gli obblighi cui le parti del rapporto bancario sono tenute in forza del d.lvo 11/10, artt. 7 e 10, come modificato dal d.lgs 218/17.

In particolare l'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di utilizzare il predetto in conformità con i termini che ne regolano l'emissione e l'uso, di comunicare senza indugio lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza e di adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate.

Ai sensi dell'art. 10 citato è onere del prestatore di servizi di pagamento (la banca), laddove il cliente neghi di aver autorizzato l'operazione di pagamento, provare che essa 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. Inoltre quando l'utente neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato al prestatore di servizi di pagamento non è di per sé sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave agli obblighi contrattuali.

Sempre ai sensi della citata norma ' E' onere del prestatore di servizi di pagamento compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo e della colpa grave dell'utente'.

Orbene, nella specie, non vi è dubbio che la banca convenuta ha fornito adeguata prova della corretta autenticazione, registrazione e contabilizzazione dell'operazione in questione.

L'autenticazione effettuata rientra peraltro in quelle di tipo 'forte' così come imposte dalle direttive comunitarie PSD1 e PSD2 che, al fine di favorire la concorrenza con l'ingresso di nuovi intermediari sul mercato finanziario e di stimolare sistemi di pagamenti diversi

dal contante e dal cartaceo, prescrivono requisiti di sicurezza per l'autenticazione dell'ordinante, dell'importo e del beneficiario per i pagamenti *on line*, requisiti meglio precisati dalla European Banking Autority(EBA).

In effetti nel caso in esame l'identificazione dell'ordinante risulta essere stata effettuata tramite l'utilizzo di codici statici (pw e Pin già noti al cliente) e dinamici (OTP generata al momento dell'operazione).

Dalla sequenza delle operazioni registrate come sopra descritte può tuttavia registrarsi un'anomalia: l'avviso tramite *sms* nel quale si richiedeva l'inserimento del codice riservato risulta infatti inviato al cliente alle ore 6.42 e dunque prima ancora che l'accesso con PIN fosse avvenuto; pertanto pur volendo ritenere (anche se non indicato dalla banca) che l'*alert* fosse legato all'accesso via internet tramite App BNL allorchè inserite le credenziali del cliente, nella specie l'accesso ancora non era avvenuto. Inoltre tale accesso risulta effettuato con due diversi dispositivi: alle ore 6.43.32 con Iphone ed alle ore 6.43.44 con Android.

A prescindere dal rilievo che precede -che consentirebbe di ricondurre il caso anche all'ipotesi di cui al primo comma dell'art.10 d.lvo 11/2010, come modificato dal d.lgs 218/17citato-, si osserva che l'attore in questa sede ha negato di aver effettuato l'accesso via internet tramite App o pc, di aver inserito le proprie credenziali o di averne consentito l'uso a terzi soggetti.

Ai sensi dunque del secondo comma del medesimo art. 10 d.lvo 11/2010, lo svolgimento dell'operazione tramite l'utilizzo del *mobile token,* seppur con la dovuta autenticazione, non dimostra che l'operazione è stata autorizzata dall'utente medesimo né che questi ha agito in modo fraudolento e che ha tenuto un comportamento gravemente colposo rispetto agli obblighi contrattuali di custodia ed uso di cui all'art.7.

D'altra parte clausole contrattuali, nel caso di specie non espressamente invocate, non possono in alcun modo derogare alle citate disposizioni normative.

Vertendosi in ipotesi di responsabilità contrattuale spetta peraltro al cliente solo allegare gli obblighi cui è tenuta la banca in virtù del rapporto costituitosi ed il relativo inadempimento, mentre spetta a quest'ultima la prova di aver dato corretta esecuzione al rapporto ovvero, per indicazione normativa, che ciò non è stato possibile per effetto di dolo o colpa grave del cliente.

E che la mera autenticazione del cliente e dell'ordine non è sufficiente a fornire la prova richiesta si evince dalle stesse finalità delle direttive sopra citate.

Le direttive PSD1 e PSD2 sono state infatti introdotte con il precipuo scopo, tra gli altri, di stimolare l'utilizzo di strumenti elettronici e innovativi di pagamento per ridurre il costo di inefficienti strumenti quali quelli cartacei e il contante e dunque sviluppare sistemi di pagamento elettronico sicuri, efficienti, competitivi ed innovativi per consumatori, imprese ed esercenti. La evidente riduzione degli sportelli bancari cui il cliente si può rivolgere per compiere operazioni quotidiane ne è piena conferma. In tale ottica dunque la finalità e necessità di garantire la fiducia degli utenti nella sicurezza del sistema implica che la possibilità di sottrazione dei codici del correntista attraverso tecniche fraudolente, rientra nel rischio d'impresa del prestatore dei servizi di pagamento laddove l'utilizzazione dei codici da parte di terzi non sia attribuibile al dolo del titolare od a comportamenti talmente incauti da non poter essere fronteggiati dallo stesso anticipatamente (Cass. 2950/2017, 9158/2018,26916/2020,16417/22). Ne consegue che, anche prima dell'entrata in vigore del d.lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, l'erogatore di servizi, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuto a fornire la prova della riconducibilità dell'operazione al cliente (Cass., 03/02/2017, n. 2950).

L'onere della prova delle condotte esimenti della responsabilità del prestatore dei servizi di pagamento è dunque a carico dello stesso.

Nella specie allora parte convenuta affida tale prova all'omessa dovuta considerazione da parte del cliente degli *sms* già sopra indicati i quali, se oggetto di opportuna e tempestiva attenzione da parte dell'attore, avrebbero consentito di impedire l'operazione.

L'assunto non può tuttavia essere condiviso.

Ed infatti il primo messaggio è stato ricevuto dal [redacted] alle ore 6.55 del 9.1.2020 allorchè, per quanto sopra esposto, già era avvenuto l'accesso completo all'[redacted]d al conto dello stesso. Tuttavia a seguito di tale messaggio non risulta essere stato tempestivamente eseguito il bonifico né inviato messaggio ulteriore.

Pertanto seppur il [redacted] si fosse effettivamente reso conto dell'invio del messaggio, la mancanza di successiva comunicazione dell'operazione nell'arco di pochi minuti, non avrebbe necessariamente indotto lo stesso ad attivarsi per verificare i propri movimenti o segnalare l'anomalia.

L'invio poi del successivo *sms alert,* non preceduto da alcun altro messaggio nei minuti precedenti, nella medesima giornata alle ore 11.47.49 a fronte dell'esecuzione dell'ordine alle ore 11.47.38 implicava una reazione immediata del cliente per poter eventualmente revocare l'ordine già eseguito. Peraltro la banca non ha precisato in quale spazio temporale, secondo le condizioni contrattuali, avrebbe potuto essere bloccato o revocato il bonifico in questione (atteso che data contabile e data valuta corrispondono -doc.6 di parte attrice).

Deve peraltro ritenersi che la mancata visualizzazione di un sms alert sul proprio cellulare non può costituire condotta gravemente colposa, ma al più una negligenza: l'afflusso continuo di messaggi sui dispositivi mobili, variabile da soggetto a soggetto e da periodo a periodo, impedisce frequentemente una costante e tempestiva verifica da parte dell'utente; nè l'attivazione di un servizio di comunicazione degli accessi *on line* nella propria banca può comportare un tale obbligo permanente di monitoraggio del proprio cellulare da parte del titolare (ed infatti non vi sono indicazioni in tal senso nei documenti

negoziali prodotti) la cui inosservanza giungerebbe a determinare perfino un aggravamento di colpa a carico del cliente. Tanto più poi che nel caso di specie, come sopra esposto, al primo sms non era immediatamente seguito altro indicante l'esecuzione dell'operazione e solo dopo cinque ore ne era seguito altro indicante l'operazione già eseguita

La domanda deve dunque essere accolta e la banca convenuta deve essere condannata a risarcire all'attore il danno subito e corrispondente all'importo sottratto di euro 7.400 rivalutato ad oggi e con applicazione degli interessi di cui a Cass.1712/95 in euro 8.319.

Su tale somma sono poi dovuti interessi dalla data della presente sentenza al saldo.

In considerazione della soccombenza, le spese processuali liquidate in euro 6.000 oltre rimborso forfettario ed accessori di legge devono essere rifuse dalla convenuta all'attore.

P.Q.M.

definitivamente pronunciando, ogni altra istanza ed eccezione disattesa, così provvede:

1) accertata la responsabilità contrattuale della convenuta, condanna la stessa a risarcire all'attore il danno subito e liquidato ad oggi in euro 8.319 oltre interessi legali dalla data della presente sentenza al saldo,
2) condanna la convenuta a rifondere all'attore le spese processuali liquidate in euro 6.000 oltre rimborso forfettario ed accessori di legge.

Così deciso in Bergamo il 17.1.2022.

Il Giudice