

**REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
TRIBUNALE ORDINARIO di COMO
SEZIONE SECONDA CIVILE**

Il Tribunale, nella persona del Giudice dott. Nicoletta Riva
ha pronunciato la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. r.g. XXXX/2020 promossa da:

CORRENTISTA (C.F. omissis), con il patrocinio dell'avv. omissis, elettivamente domiciliato in
Indirizzo Telematico presso il difensore avv. omissis

ATTRICE

contro

BANCA SPA (C.F. omissis), con il patrocinio dell'avv. omissis, elettivamente domiciliato in omissis
presso il difensore avv. omissis

CONVENUTA

CONCLUSIONI

Per parte attrice:

Piaccia all'Ecc.mo Tribunale adito, ogni contraria domanda, eccezione e deduzione
rigettate,

Nel merito in via principale:

Previe le declaratorie del caso ed accertati i fatti di causa, accertato altresì l'inadempimento contrattuale
di parte convenuta, condannare quest'ultima al risarcimento in favore di parte attrice di tutti i danni subiti
e quantificati nella somma di € 59.787,88.=, oltre interessi e rivalutazione monetaria dal dovuto al
soddisfo.

Condannare altresì parte convenuta al risarcimento in favore di parte attrice dell'ulteriore danno subito
e conseguente all'indisponibilità sul proprio conto corrente della somma di cui alle operazioni bancarie
disconosciute e che si quantifica nella somma di € 10.000,00.=, ovvero nella maggiore o minore somma
che dovesse risultare in corso di causa e/o che sarà ritenuta di giustizia ovvero da liquidarsi anche in via
equitativa ex art.1226 c.c.

Nel merito in via subordinata:

Previe le declaratorie del caso ed accertati i fatti di causa, accertato altresì l'inadempimento contrattuale
di parte convenuta, condannare quest'ultima alla restituzione in favore di parte attrice della somma di €
59.787,88.=, oltre interessi e rivalutazione monetaria dal dovuto al soddisfo.

Condannare altresì parte convenuta al risarcimento in favore di parte attrice dell'ulteriore danno subito
e conseguente all'indisponibilità sul proprio conto corrente della somma di cui alle operazioni bancarie
disconosciute e che si quantifica nella somma di € 10.000,00.=, ovvero nella maggiore o minore somma
che dovesse risultare in corso di causa e/o che sarà ritenuta di giustizia ovvero da liquidarsi anche in via
equitativa ex art.1226 c.c.

Nel merito in via ancor più subordinata:

Previe le declaratorie del caso ed accertati i fatti di causa, accertato altresì l'inadempimento contrattuale
di parte convenuta, condannare quest'ultima al risarcimento in favore di parte attrice di tutti i danni
subiti, anche ai sensi e per gli effetti di cui all'art.2043 c.c., e quantificati nella somma di € 59.787,88.=,
oltre interessi e rivalutazione monetaria dal dovuto al soddisfo.

Condannare altresì parte convenuta al risarcimento in favore di parte attrice dell'ulteriore danno subito
e conseguente all'indisponibilità sul proprio conto corrente della somma di cui alle operazioni bancarie
disconosciute e che si quantifica nella somma di € 10.000,00.=, ovvero nella maggiore o minore somma
che dovesse risultare in corso di causa e/o che sarà ritenuta di giustizia ovvero da liquidarsi anche in via
equitativa ex art.1226 c.c.

In ogni caso:

Con vittoria di spese e compensi professionali del presente giudizio e della procedura di mediazione.

Oltre rimborso forfettario ex art.2 d.m. n.55/2014, rifusi i.v.a. e c.p.a.

In via istruttoria:

Si chiede ammettersi tutti i mezzi di prova così come dedotti negli scritti di causa ed, in particolare, nella memoria ex art.183 6° comma n.2 c.p.c. del 14/04/2021 depositata in data 15/04/2021.

Per parte convenuta:

Voglia l'Ecc.mo Tribunale adito contrariis rejectis, previe le necessarie e/o più opportune declaratorie di legge e del caso, per i motivi dedotti in narrativa, anche in via gradata tra loro, e di cui alla presente causa così giudicare:

Nel merito: previe le necessarie e più opportune declaratorie di legge e del caso, rigettarsi comunque ogni domanda e/o eccezione proposta da parte attrice nei confronti della odierna convenuta, anche in via gradata tra loro, siccome inammissibile e/o improcedibile e/o improponibile, in ogni caso infondata in fatto e in diritto, anche assolvendo la stessa convenuta da ogni pretesa avversaria.

In via subordinata: Previe le declaratorie di legge e del caso, per il non creduto caso di accoglimento totale o parziale delle domande attoree, si chiede di limitare la condanna nei limiti della effettiva responsabilità che venisse accertata in capo alla convenuta, secondo la rispettiva partecipazione ex art. 1227 c.c. nella pretesa causazione dei fatti e delle conseguenze dannose e/o alla proporzione degli illeciti ex adverso contestati.

In via istruttoria: si insiste per l'ammissione di prova per testi sui capitoli di prova già dedotti nella memoria ex art. 183 6° comma n. 2) c.p.c. e che si riportano di seguito:

- 1) Vero che l'esecuzione di bonifico è possibile tramite filiale e tramite home banking?
- 2) Vero che per accedere alla home page del servizio di home banking di BANCA il cliente deve inserire il "codice titolare" - attribuito dalla Banca all'accensione del contratto - e il "codice PIN" - creato dal cliente (e quindi conosciuto solo dallo stesso) in sede di primo accesso?
- 3) Vero che dopo l'inserimento del codice titolare e del codice PIN, il sistema di home banking, per l'accesso alla sessione operativa con facoltà di inquiry e dispositive, richiede l'inserimento del codice OTP SMS, generato dall'app BANCA mobile attraverso l'O-key Smart, oppure attraverso l'invio di un sms se il cliente, come nel caso di specie, ha potato per l'O-key sms?
- 4) Vero che per poter eseguire operazioni dispositive il sistema di home banking richiede l'inserimento di un ulteriore codice OTP SMS, generato dall'app BANCA mobile attraverso l'O-key Smart, oppure attraverso l'invio di un sms se il cliente, come nel caso di specie, ha potato per l'O-key sms?
- 5) Vero che per l'esecuzione del bonifico l'infrastruttura di sicurezza informatica della Banca può chiedere l'inserimento di un ulteriore codice di sicurezza OTS SMS inviato sul numero cellulare certificato dell'utente?
- 6) Vero che, inserito anche tale ulteriore codice di sicurezza, la disposizione di bonifico viene autorizzata dal cliente ed eseguita?
- 7) Vero che - come risulta dai docc. 6 e 19 di parte convenuta, da rammostrarsi al teste - in data 8.10.2019 alle ore 14:09 l'utente entra nel servizio di home banking inserendo il codice utente e il codice PIN riconducibili alla dott.ssa CORRENTISTA (foglio tracciatura, riga 3)?
- 8) Vero che, come da procedura, viene inviato un codice OTP SMS (foglio sms, riga 2) al numero di cellulare certificato OMISSIS (foglio sms, Colonna A) e, una volta inserito il predetto codice OTP SMS, il processo di login si è completato?
- 9) Vero che - come risulta dai docc. 6 e 19 di parte convenuta, da rammostrarsi al teste - in data 8.10.2019 alle ore 14:12 l'utente dispone l'aumento dei limiti dispositive inserendo il codice OTP SMS (foglio sms, riga 4) e il codice di sicurezza OTS SMS (foglio sms, riga 3) inviati al numero di cellulare certificato OMISSIS?
- 10) Vero che - come risulta dai docc. 6 e 19 di parte convenuta, da rammostrarsi al teste - in data 8.10.2019 alle ore 14:19 l'utente esegue un nuovo login inserendo il codice Pin (foglio tracciatura, riga 67) e il codice OTP SMS (foglio sms, riga 5) inviato al numero di cellulare certificato OMISSIS?
- 11) Vero che - come risulta dai docc. 6 e 19 di parte convenuta, da rammostrarsi al teste - in data 8.10.2019 alle ore 14:24 l'utente inserisce la richiesta del primo bonifico di € 29.870,34 e, su richiesta del Sistema, inserisce sia il codice OTP SMS (foglio sms, riga 6) sia il codice di sicurezza OTS SMS (foglio sms, riga 7) inviati al numero di cellulare certificato OMISSIS e l'operazione viene presa in carico dalla Banca?
- 12) Vero che - come risulta dai docc. 6 e 19 di parte convenuta, da rammostrarsi al teste - in data 8.10.2019 alle ore 14:29 l'utente inserisce la richiesta del secondo bonifico di € 14.960,72 e, su richiesta del sistema, inserisce sia il codice OTP SMS (foglio sms, riga 8) sia il codice di sicurezza OTS SMS

(foglio sms, riga 9 - foglio tracciatura, riga 127-128) inviati al numero di cellulare certificato OMISSIS e l'operazione viene presa in carico dalla Banca?

13) Vero che - come risulta dai docc. 6 e 19 di parte convenuta, da rammostrarsi al teste - in data 8.10.2019 alle ore 14:34 l'utente inserisce la richiesta del terzo bonifico di € 14.956,82 e, su richiesta del sistema, inserisce sia il codice OTP SMS (foglio sms, riga 10) sia il codice di sicurezza OTS SMS (foglio sms, riga 138 - foglio tracciatura, riga 142-143) inviati al numero di cellulare certificato xxxx e l'operazione viene presa in carico dalla Banca?

14) Vero che il sistema a duplice fattore di protezione con codice OTS (One Time sms) e OTP (One Time Password) è quello adottato da **BANCA**?

15) Vero che il sistema di home banking può essere attivato su qualsiasi strumento informatico?

Si indicano a testimoni sui capitoli di prova i signori:

- **OMISSIS** c/o **BANCA**, in via OMISSIS

- OMISSIS c/o BANCA, Corso OMISSIS, OMISSIS (OMISSIS) per il quale si formula sin da ora istanza di prova delegata c/o il Tribunale di Torino.

Si ribadisce l'opposizione all'ammissione della prova testimoniale richiesta da parte attrice, per i motivi dedotti nella memoria ex art. 183 6° comma n. 3) c.p.c., nonché la richiesta di prova contraria nella denegata ipotesi di loro ammissione.

Si ribadisce altresì l'opposizione all'ammissione di CTU, in quanto palesemente esplorativa, nonché all'ordine di esibizione ex art. 210 c.p.c. avente ad oggetto documenti e/o informazioni che parte attrice avrebbe potuto e dovuto acquisire direttamente.

In punto spese: Con vittoria di spese diritti ed onorari di causa.

Concisa esposizione delle ragioni di fatto e di diritto della decisione

Con atto di citazione notificato in data 19 ottobre 2020 **CORRENTISTA** conveniva in giudizio, avanti il Tribunale di Como, **BANCA** spa per sentire accertato l'inadempimento contrattuale di parte convenuta con interesse ad ottenere la condanna di quest'ultima al risarcimento in suo favore di tutti i danni subiti e quantificati nella somma di Euro 59.787,88, oltre interessi e rivalutazione monetaria dal dovuto al soddisfo. Chiedeva altresì di condannare parte convenuta al risarcimento in favore di parte attrice dell'ulteriore danno subito e conseguente all'indisponibilità sul proprio conto corrente della somma di cui alle operazioni bancarie sconosciute e che si quantifica nella somma di Euro 10.000,00, con vittoria di spese e compensi professionali del presente giudizio anche della procedura di mediazione, oltre al rimborso forfettario ex art. 2 d.m. n. 55/2014, rifusi iva e cpa.

Si costituiva in giudizio, con comparsa di costituzione e risposta del 21 gennaio 2021, **BANCA** spa chiedendo il rigetto delle domande attoree ovvero la limitazione della condanna nei limiti della effettiva responsabilità accertata in capo alla convenuta secondo la rispettiva partecipazione ex art. 1227 cc.

Alla prima udienza di comparizione delle parti del 17 febbraio 2021 il giudice assegnava alle parti i termini di cui all'art. 183, VI comma, cpc, e fissava per la discussione sull'ammissione dei mezzi di prova all'udienza del 16 giugno 2021.

Alla successiva udienza il giudice, lette le istanze e deduzioni delle parti, invitava le stesse a precisare le conclusioni per l'udienza del 21 febbraio 2023.

A tale udienza, le parti precisavano le rispettive conclusioni come da fogli inviati telematicamente, ed il giudice assegnava i termini di cui all'art. 190 cpc per il deposito delle comparse conclusionali e delle memorie di replica e tratteneva la causa in decisione.

Orbene, la domanda è in parte fondata e, come tale, deve essere parzialmente accolta per le motivazioni che seguono.

Preliminarmente, in ordine alla dinamica dei fatti occorsi in data 8.10.2019, si precisa che è pacifico tra le parti perché emerge anche dalle risultanze processuali (e, in particolare, dalle memorie depositate da parte attrice, nonché dalla denuncia allegata dalla stessa e altresì dalle due relazioni tecniche depositate rispettivamente da attrice e convenuta) che i bonifici oggetto del presente procedimento sono stati disposti a nome dell'odierna attrice, e provenienti dal di lei conto, ma ciò è avvenuto per il tramite di un sistema informativo, ed informatico, differente rispetto a quello normalmente utilizzato dalla **CORRENTISTA**. Le parti sono concordi, dunque, nel ritenere che gli accessi al conto dell'attrice effettuati il giorno 8.10.2019 non sono stati eseguiti dall'indirizzo IP o, in ogni caso, dalla postazione della cliente di **BANCA**, bensì da altro soggetto ignoto (così anche relazione del Consulente Tecnico di Parte ing. OMISSIS, p.4).

Tanto premesso, preme a questo Tribunale rilevare la dinamica concreta e analizzare la giurisprudenza e la normativa specifica in materia di frode informatica bancaria.

Sul punto, questa autorità giudiziaria, considerate le risultanze processuali e, in particolare, le relazioni dei consulenti di parte (rispettivamente il dott. OMISSIS per parte attrice e l'ing. OMISSIS per parte convenuta), ritiene che, nel caso di specie si sia in presenza del fenomeno di truffa online denominato MITB, ossia "Man in the browser", una minaccia informatica che permette al cybercriminale di intercettare e manipolare il traffico internet che l'utente crede privato e protetto. In particolare, il Collegio di Coordinamento dell'ABF in data 26.10.2012, con la Decisione n. 34983 ha definito questo tipo di attacco hacker così: "Nella sua massima espressione di efficienza aggressiva, il programma malevolo, una volta annidatosi in un certo numero di computer, genera quella che in gergo suole definirsi una botnet, ossia per l'appunto una rete di macchine egualmente infettate dallo stesso virus. Il malware, [...] dotato di sofisticate capacità di elusione dei migliori antivirus, si annida in modo silenzioso nel computer della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il malware resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (targeted banks). In quel preciso istante il malware "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso (c.d. protocollo di trasferimento ipertestuale, Hyper Text Transfer Protocol) "http" e non già "https" (dove la "s" finale sta per secured, protetto)." In altre parole, il MITB è un software molto insidioso che, a differenza di altre fattispecie di phishing dove l'aggiramento dei sistemi di sicurezza avviene con sms, chiamate, email e altre false comunicazioni apparentemente riconducibili all'istituto di credito di fiducia, invece, in questo caso, l'appropriazione indebita dei codici di sicurezza avviene in maniera così subdola che, "ignaro dell'intervenuta sostituzione della pagina, l'utente è indotto a ritenere di trovarsi nel normale ambiente sicuro in cui normalmente egli opera"(Collegio di Coordinamento dell'ABF, Decisione n. 34983 del 26.10.2012).

In ordine a ciò, occorre precisare che proprio per contrastare questi fenomeni sono stati creati dei mezzi di contrasto a tali cyber-truffe prevedendo sistemi di autenticazione forte. Sul punto, la normativa tecnica di riferimento è contenuta nel Regolamento Delegato della Commissione (UE) 2018/389 e, in particolare agli artt. 8 e seguenti. In particolare, ai fini della presente decisione, si anticipa che ai sensi dell'art. 10 co 2 d. lgs. n. 11/2010: "Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per se' necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, ne' che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. 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 o della colpa grave dell'utente"; in altri termini, è onere della banca fornire la prova della riconducibilità dell'operazione al cliente.

Alla luce delle varie pronunce ABF, nonché del citato quadro normativo, è opportuno ritenere che ogniqualvolta si verifichi un accesso non autorizzato al servizio online della banca, quest'ultima, al pari di un'impresa che esercita un'attività pericolosa (ex art. 2050 c.c.), incorre in una responsabilità oggettiva aggravata; la banca, per superare la presunzione di colpevolezza, deve dunque dimostrare sia di aver adottato le misure idonee ad evitare il danno derivante dal fenomeno di phishing sia l'inescusabile colpevolezza a carico dell'utente (ex multis, Cass. Civ., sez. VI, sent. n. 9158 del 12.04.2018).

Detto ciò, nella giurisprudenza della Corte di Cassazione si è ormai cristallizzato il principio secondo cui in caso di truffa informatica cd. phishing (sia essa avvenuta attraverso la clonazione di carte di credito o attraverso fenomeni online come il MITB) incombe sul prestatore di servizi di pagamento, e dunque, sull'istituto di credito, il duplice onere di provare di aver adottato tutte le misure di sicurezza necessarie per la protezione del cliente e l'inadempimento doloso e/o gravemente colposo del cliente medesimo (così, di recente Cass. Civ., Sez. III, ordinanza n. 13204 del 15.05.2023). Invero, in ordine a ciò, già con la sentenza n. 2950 del 3.2.2017 la Suprema Corte (Sez. I) aveva stabilito che: "In tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012

Registro affari amministrativi numero 8231/11

Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

Copyright © 2012 - Ex Parte Creditoris - ISSN 2385-1376

tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo". Sul punto, per altro, viene aggiunto 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, la banca, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente."

Orbene, è opportuno ora verificare se nel caso di specie l'odierna convenuta abbia soddisfatto il doppio onere che grava sulla stessa.

Invero, per quanto concerne le misure di prevenzione e sicurezza utilizzate da **BANCA** questo Tribunale ritiene che esse fossero sufficienti e, dunque, che quanto sostenuto da parte attrice, secondo cui i sistemi adottati dalla convenuta fossero inadeguati non sia stato dimostrato né tanto meno veritiero. Resta tuttavia da sottolineare che nessun sistema ha rilevato anomalie nelle operazioni avvenute sul conto della CORRENTISTA nonostante l'indirizzo IP dal quale venivano disposte le operazioni sul conto dell'attrice non fosse quello abitualmente utilizzato dalla cliente della banca. Ancora si prende atto che, per quanto i sistemi di prevenzione e sicurezza attuati dalla convenuta non siano stati violativi di alcuna normativa italiana né internazionale posta a garanzia dei dati sensibili degli utenti di istituti di credito, tuttavia, è emerso chiaramente, anche per conoscenze dirette di questa autorità giudiziaria, che dal 2018 in poi diverse truffe informatiche hanno visto coinvolti utenti di **BANCA** per episodi simili a quella subita dall'odierna attrice.

Per quanto concerne, poi, il secondo onere probatorio a carico dell'odierna convenuta, consistente nel dimostrare che vi sono stati comportamenti incauti da parte della CORRENTISTA nei fatti occorsi in data 8.10.2019, questo Tribunale ritiene che tale onere non sia stato sufficientemente assolto dalla **BANCA**; invero, alla luce delle risultanze processuali, non solo non sono emersi comportamenti dolosi tenuti dall'attrice ma nemmeno è possibile rinvenire dei comportamenti incauti tenuti della stessa per i fatti per cui si sta procedendo.

Sul punto, si precisa, infatti, che la giurisprudenza della Corte di Cassazione nella già citata sentenza n. 2950 del 3.2.2017, innanzitutto, ha sottolineato che l'istituto di credito deve dimostrare la riconducibilità delle operazioni di pagamento alla volontà del cliente, circostanza che, nel caso di specie, non è stata in alcun modo provata; al contrario, come già segnalato, l'indirizzo IP da cui è partito il collegato al sito della banca convenuta non poteva essere noto all'istituto di credito dal momento che non era mai stato utilizzato dalla cliente CORRENTISTA. A conferma del fatto che mancasse la volontà dell'attrice di effettuare i bonifici oggetto di causa, vi è anche la circostanza che, a seguito dei fatti occorsi, appena riceveva notizia dall'odierna convenuta che le disposizioni da lei richieste non potevano essere evase in quanto il conto non aveva liquidità sufficienti, l'odierna attrice, dopo aver controllato che risultavano emessi dal proprio conto dei bonifici per un valore totale di euro 59.787,88 dalla stessa mai disposti, immediatamente denunciava il fatto presso la stazione dei Carabinieri di Erba (denuncia del 16.10.2019 presente in atti).

Ancora, secondo una più recente pronuncia della Corte di Cassazione che si allinea al già citato orientamento della medesima Suprema Corte espresso con la sentenza n. 2950/2017, "la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa solo se ricorre una situazione di colpa grave dell'utente" (Cass. Civ., Sez. 6-3, Ordinanza n. 26916 del 26.11.2020); ne deriva che l'odierna convenuta avrebbe dovuto dimostrare la presenza di dolo o di colpa grave nei comportamenti dell'attrice per potersi liberare della presunzione di responsabilità, cosa che non ha, invece, fatto.

Sul punto si precisa che, in ordine alla possibilità che l'attrice abbia agito dolosamente, la controparte si è limitata ad affermare che, tra le ipotesi plausibili di quanto accaduto il giorno 8.10.2019, vi fosse anche quella secondo cui la CORRENTISTA avrebbe voluto effettuare quei bonifici agendo con dolo. Orbene, questo Tribunale ritiene che tale tesi di parte convenuta non sia stata in alcun modo suffragata da prove o elementi di prova né sono emerse dalle risultanze processuali che possano essere utilizzate a sostegno della predetta teoria della

banca convenuta. Di talchè questo Tribunale ritiene che non si possa ravvisare alcun atteggiamento doloso nelle condotte poste in essere dall'odierna attrice in ordine ai fatti per cui si sta procedendo.

Alla stessa conclusione è possibile giungere in ordine all'asserita colpa grave della CORRENTISTA per i medesimi fatti; invero, questo Tribunale, sulla base delle corpose risultanze processuali ritiene che non vi siano elementi tali da poter ritenere che sull'attrice possa ricadere una responsabilità da colpa grave.

Sul punto si richiama una recente pronuncia della Suprema Corte (Cass. Civ., Sez. 3, Sentenza n. 18045 del 05.07.2019), la quale, ritenendo sempre che la responsabilità dell'istituto bancario “per operazioni effettuate a mezzo di strumenti elettronici con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa se ricorre una situazione di colpa grave dell'utente”, ha riconosciuto la colpa grave del cliente dal momento che quest'ultimo aveva atteso due anni prima di comunicare alla banca con cui aveva aperto il conto corrente, l'uso non autorizzato dello strumento di pagamento. Invero, secondo la Suprema Corte del 2019 l'omessa attivazione di un sistema di controllo degli estratti conto “integra quella situazione di colpa grave alla quale fa riferimento il suddetto plesso normativo, atteso che alla conoscenza dell'uso non autorizzato dello strumento deve equipararsi la possibilità di conoscenza, allorchè la sua mancanza [...] si sia protratta per un arco di tempo particolarmente prolungato ed in relazione ad un conto corrente presso il quale risultava una notevole giacenza di danaro”. In tal caso, è evidente che la colpa grave è rinvenibile nell'atteggiamento del cliente che non si è attivato in una qualsiasi forma di controllo degli estratti conto per un lasso di tempo considerevole; al contrario, nel caso di specie, la **CORRENTISTA** si è fin da subito attivata per controllare il proprio conto e, inoltre, come anticipato, preso coscienza di quanto accaduto, ha immediato sporto denuncia per i fatti oggetto del presente procedimento.

Ancora, si precisa che non è possibile paragonare il caso di specie con quello su cui ha deciso di recente il Tribunale di Milano –sez. VI con la sentenza del 15.9.2022 dal momento che in quel caso sono stati ritenuti responsabili per colpa grave i correntisti truffati dal momento che la controparte aveva dimostrato che i clienti dell'istituto bancario pur inconsapevolmente avevano cooperato con i cybertruffatori fornendo agli stessi tutti i dati (credenziali di accesso, codici OTP e OTS) utili per poter accedere ai loro conti online ed eseguire le operazioni bancarie. Orbene, diversamente, nel caso di specie non è possibile rinvenire nelle condotte della CORRENTISTA la violazione degli obblighi di diligenza, prudenza e perizia, né la convenuta ha dimostrato il contrario essendosi limitata a dire che, per ben 10 volte, la CORRENTISTA avrebbe fornito i codici necessari per la conferma delle operazioni di bonifico; quest'ultima circostanza non è mai stata allegata né provata da alcun elemento. Al contrario la CORRENTISTA ha dichiarato, sia in corso di causa sia in sede di denuncia ai carabinieri, di non aver mai ricevuto email di phishing nei giorni o mesi precedenti rispetto all'accaduto, di non aver mai comunicato a nessuno le sue credenziali e password per effettuare operazioni online sul suo conto corrente aperto con BANCA né di aver mai perso o ceduto a terzi il proprio telefono cellulare con il quale normalmente effettua l'accesso al conto online. Fra l'altro, non risulta alcuna prova contraria.

Alla luce di tutto quanto precede questo Tribunale ritiene dunque che non si possa ritenere che l'odierna attrice abbia agito con dolo o con colpa grave; ne consegue che la responsabilità ai sensi di legge e, dunque, secondo le normative sopraccitate, ricadono in capo all'istituto bancario convenuto.

Inoltre non è possibile nemmeno riscontrare un concorso di colpa dell'attrice ex 1227 c.c. dal momento che non vi sono elementi tali da poter ritenere che la stessa abbia, in effetti, cooperato o posto in essere condotte che abbiano potuto agevolare il soggetto (o i soggetti) che hanno commesso la truffa informatica di cui parte attrice è stata vittima.

Infine, per quanto riguarda, la domanda di risarcimento del danno non patrimoniale formulata da parte attrice, questo Tribunale ritiene che essa debba essere rigettata per mancanza di supporto probatorio venendo meno all'onere di allegazione che si ricava dall'art. 112 c.p.c., articolo in applicazione del quale la parte deve introdurre in giudizio i fatti che ne costituiscono il fondamento, pena la loro irrilevanza. In particolare, nel caso di specie, la CORRENTISTA ha quantificato tale danno nella somma pari ad euro 10.000,00 senza tuttavia fornire elementi tali che possano giustificare tale somma.

Sicchè, accertato che la banca per poter superare la presunzione di colpevolezza deve provare sia che ha adottato tutte le misure di sicurezza utili ad impedire frodi informatiche, sia che il proprio cliente abbia agito con dolo o colpa grave, e che la CORRENTISTA non ha agito né con dolo né con colpa grave, considerato anche che quest'ultima ha subito un danno per valore pari ad euro 59.787,88, oltre interessi e rivalutazione monetaria dal dovuto al saldo, questo Tribunale, tenuto conto anche che non

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012

Registro affari amministrativi numero 8231/11

Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

Copyright © 2012 - Ex Parte Creditoris - ISSN 2385-1376

può essere accolta la domanda di parte attrice riguardante il risarcimento del danno non patrimoniale, condanna l'odierna convenuta al risarcimento della predetta somma in favore di parte attrice. Le spese seguono la soccombenza in giudizio e, dunque, cedono a carico della banca convenuta.

P.Q.M.

il Tribunale, definitivamente pronunciando, ogni contraria istanza reietta e disattesa, in parziale accoglimento della domanda dell'attrice **CORRENTISTA** così provvede:

- 1 -accerta e dichiara l'esclusiva responsabilità civile della banca convenuta **BANCA** in ordine ai fatti occorsi il 8.10.2019 in danno dell'attrice;
- 2 -per l'effetto, condanna la convenuta banca convenuta **BANCA spa**, nella persona del suo rappresentante legale pro tempore, al pagamento in favore dell'attrice **CORRENTISTA** della somma di euro 59.787,88, oltre interessi e rivalutazione monetaria dal dovuto al saldo;
- 3 -rigetta la domanda dell'attrice **CORRENTISTA** relativa al risarcimento del danno non patrimoniale per un valore pari ad euro 10.000,00 per mancanza di prove;
- 4 -condanna, altresì, la banca convenuta **BANCA spa**, nella persona del suo rappresentante legale pro tempore, alla rifusione delle spese di lite di parte attrice che si liquidano in complessivi Euro 786,00 per anticipazioni, ed Euro 13.430,00 per compensi professionali, oltre rimborso al 15%, iva e cpa, come per legge.

Como, 24 ottobre 2023

Il Giudice
dott. Nicoletta Riva

EX PARTE