TRIBUNALE DI NAPOLI

II sezione Civile

Repubblica Italiana

in nome del Popolo Italiano

Il Giudice Unico del Tribunale di Napoli II sezione Civile , dott. ssa Maria Carolina De Falco ha pronunciato la seguente

SENTENZA

nella causa iscritta al numero 27808 del Ruolo Generale degli affari civili ordinari contenziosi dell'anno 2018 avente ad oggetto: risarcimento danni – contratti bancari

TRA

[redacted], rappresentati e difesi giusta procura a margine dell'atto di citazione dall'avv.to Lucia Vitiello e con questa elettivamente domiciliati presso il suo studio in Napoli alla Via Santa Lucia n. 20

ATTORI

E

[redacted], in persona dei procuratori speciali, rappresentata e difesa in virtù di mandato speciale in allegato alla comparsa di costituzione dall'Avv.to [redacted] unitamente all'Avv.to [redacted] e presso lo studio di quest'ultimo in Napoli al [redacted] elettivamente domiciliata

CONVENUTA

CONCLUSIONI

Conclusioni: all'udienza del 22.02.19 le parti presenti concludevano a verbale riportandosi agli atti introduttivi e successive integrazioni. All'esito il GU all'esito assumeva la causa in decisione con i termini ex art. 190 c.p.c. per il deposito delle comparse conclusionali e memorie di replica.

MOTIVI IN FATTO E DIRITTO

Con atto di citazione regolarmente notificato alla [redacted], dedotto di essere cointestatari del conto corrente on line n. [redacted] operante prevalentemente tramite tecniche di comunicazione a distanza sul quale era attivato il servizio di "home banking", riferiva che in data [redacted]14 ricevevano sulla mail intestata a [redacted] una comunicazione

proveniente verosimilmente dalla convenuta con la quale i correntisti venivano invitati ad inviare – al fine di aggiornamento dei servizi – i propri codici di accesso al servizio home banking, pena l'inutilizzabilità del servizio.

La predetta mail riportava un link cliccando il quale compariva una schermata in tutto e per tutto (colori e loghi) riconducibili alla convenuta, tanto che secondo un ragionevole affidamento, la [redacted] inseriva i propri codici di accesso.

Solo nella giornata del [redacted].14, gli attori si avvedevano che in data [redacted]14 era stati bloccati due ordini di bonifico di euro di rilevante importo e che, senza alcuna comunicazione tempestiva ai clienti, invece dopo poco la convenuta aveva autorizzato tre ordini di pagamento in favore di tale [redacted] (IBAN n. [redacted]), medesimo beneficiario dei due bonifici rifiutati, dell'importo complessivo di euro 21.999,00.

Prontamente veniva sporta denuncia presso la Legione dei Carabinieri di Roma, cui seguiva l'apertura di un procedimento penale a carico di [redacted] che si concludeva con la sentenza n. [redacted] del Tribunale di Roma di condanna dell'imputato per frode informatica.

Chiedeva, stante la responsabilità contrattuale e/o extracontrattuale della banca per omessa predisposizione dei sistemi di sicurezza e attivazione delle cautele necessarie ad impedire accessi impropri al sistema informatico, la condanna della banca al risarcimento dei danni corrispondenti alla somma indebitamente prelevata.

Si costituiva la banca convenuta, intanto chiedendo dichiararsi l'improcedibilità del giudizio per difetto del tentativo obbligatorio di mediazione e, nel merito, declinando ogni responsabilità in ordine all'accaduto sia per aver attivato tutti i sistemi necessari alla tutela del servizio home banking (tra cui anche l'invito reiterato al correntista di non inserire mai i propri codici di accesso in alcuna richiesta di informazioni) sia per la evidente condotta colposa della cliente che aveva consentito con la sua imprudenza la violazione del sistema

Chiedeva, pertanto, rigettarsi la domanda attorea con vittoria delle spese di lite.

Ammessa la parte attrice ad attivare il tentativo di mediazione che si svolgeva con esito negativo, alle parti che ne facevano richiesta veniva consentito il deposito delle memorie ex art. 183 VI co. c.p.c., ed all'esito del deposito, in assenza di richieste istruttorie la causa, sulle conclusioni rassegnate dalle parti all'udienza del [redacted].19, veniva assunta in decisione con i termini ex art. 190 c.p.c.

In via del tutto preliminare ed in assenza di questioni in rito, solo al fine di inquadrare la vicenda oggetto di giudizio, serva premettere alcune coordinate in tema di responsabilità della banca per le ipotesi di operazioni eseguite con il sistema "home banking".

Invero, come chiarito di recente dalla giurisprudenza di legittimità, l'utilizzazione dei servizi telematici da parte dei correntisti (home banking) rientra nell'area del rischio professionale della banca e richiede una diligenza di natura tecnica specifica (Cassazione civile sez. VI, 12/04/2018, n.9158).

Dunque, 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 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.

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, 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 (Cass. 3 febbraio 2017, n. 2950).

Al fine di dare fiducia agli utenti nei sistemi che consentono le operazioni on line, poi, la banca è tenuta a dotarsi di sistemi che permettano di verificare la riconducibilità delle operazioni alla volontà del cliente, evitando i rischi prevedibili, come la possibilità che estranei possano fare uso dei codici di accesso.

Pertanto, in caso di operazione contestata dal cliente, la banca è tenuta a fornire la prova della sua diligenza, da valutarsi con il criterio dell'accorto banchiere.

Ne consegue che, secondo la corretta interpretazione del d.lgs. n. 11/2010 , qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio.

Nel contempo obbliga quest'ultimo a rifondere con sostanziale immediatezza il correntista in caso di operazione disconosciuta, tranne ove vi sia un motivato sospetto di frode, e salva naturalmente la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata, con consequenziale diritto di chiedere e ottenere, in tal caso, dall'utilizzatore, la restituzione dell'importo rimborsato. Agli istituti bancari, da considerare debitori qualificati ex art. 1176, comma 2, c.c., si richiede un elevatissimo livello di diligenza (c.d. « diligenza del buon banchiere » : Tribunale Roma sez. X, 31/08/2016, n.16221).

Come ben sintetizzato dalla giurisprudenza di merito di recente "*Nel caso di operazioni effettuate con strumenti elettronici (home banking), spetta all'istituto di credito verificare la riconducibilità delle stesse alla volontà del cliente, impiegando la diligenza dell'accorto banchiere. L'eventuale uso*

dei codici di accesso al sistema da parte dei terzi rientra nel rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure tecniche, volte a verificare la riferibilità delle operazioni suddette alla volontà del correntista. La banca non risponde del danno patito dal cliente, solo qualora dimostri che il fatto sia attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo. Di conseguenza, qualora si verifichi un accesso non autorizzato o l'impiego dei dati raccolti per finalità non conformi alla legge, il gestore risponde ex art. 2050 c.c.. Si tratta di una forma di responsabilità oggettiva "aggravata", in cui il prestatore del servizio, per andare esente da responsabilità, non deve solo dimostrare di aver adottato tutte le misure idonee ad evitare il danno (cosiddetta "prova liberatoria"), ma è tenuto a fornire la prova positiva di una causa esterna. Può trattarsi di fatto naturale, di fatto del terzo o di fatto dello stesso danneggiato che, per imprevedibilità ed inevitabilità, sfugge alla sfera di controllo dell'esercente l'attività pericolosa" (Tribunale Parma sez. I, 06/09/2018, n.1268 ; Tribunale Siracusa sez. II, 04/02/2019, n.200).

Ebbene applicando i principi suddetti alla fattispecie de qua, emerge chiaramente che le operazioni eseguite dalla banca – peraltro in successione immediata rispetto a due rifiuti di bonifico con disposizione in favore del medesimo soggetto e IBAN – in data [redacted].14 sono state autorizzate senza le dovute misure di cautela e senza assicurarsi – come doverosamente richiesto al bonus argentarius – che le disposizioni provenissero dai titolari del conto (tramite ad esempio il controllo dell'indirizzo IP normalmente utilizzato per le operazioni on line: cfr. sul punto, Tribunale Milano sez. VI, 04/12/2014 "*Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata, ai sensi dell'art. 1176, comma 2, c.c. In particolare, nel rapporto contrattuale di home banking, la banca ha la veste di contraente qualificato, che, non ignaro delle modalità di frode mediante phishing da tempo note nel settore, è tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza)*").

Peraltro, quest'ultima circostanza oltre che non disconosciuta dalla banca – che non ha neanche tentato di provare la riconducibilità dell'ordine ai correntisti – è stata definitivamente smentita dalla sentenza del Tribunale di Roma di condanna del disponente per il reato di frode informatica (cfr. decisione allegata al fascicolo d'ufficio in data 15.02.19).

Né, pervero, la banca ha provato come era suo onere di aver adottato sistemi adeguati per evitare episodi di cd. phishing, essendosi limitata a depositare alcune comunicazioni di allerta proprio per il predetto fenomeno, senza dimostrare l'invio e la ricezione da parte degli attori o altre forme di comunicazione personale.

Quanto, poi, alla dedotta condotta colposa della parte attrice [redacted] che avrebbe omesso di tenere un comportamento vigile di fronte alla mail apparentemente riconducibile alla banca di richiesta di

inserimento dei propri codici, deve ribadirsi che l'art. 10 del D.lgs. 11/10 precisa al co. 2 che " *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 e' 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 piu' 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*".

Nel caso di specie, le parti attrici hanno depositato in atti una schermata mail con provenienza "[redacted]" con la dicitura "no reply", tipica delle comunicazioni delle imprese bancarie, che invitava ai fini di aggiornamento del sistema ad inserire nel link allegato le proprie credenziali del servizio on line che ben poteva indurre in errore la titolare della posta elettronica, della cui esperienza in materia bancaria o informatica non si è dato prova da parte della convenuta.

Manca, infine, prova – secondo l'eccezione mossa dalla banca negli scritti difensivi finali – del pagamento della somma da parte del responsabile condannato in sede penale.

In definitiva, la domanda degli attori merita accoglimento con conseguente condanna, previo accertamento della responsabilità contrattuale della banca, al risarcimento dei danni in loro favore della somma di euro 21.999,00 (euro 11.000,00 + euro 1.000,00 + euro 9.999,00), oltre interessi codicistici dalla domanda giudiziale.

Quanto al riparto delle spese di lite, le stesse, liquidate secondo il valore della controversia e la complessità dell'attività svolta, seguono la soccombenza.

PQM

Il Tribunale di Napoli, in composizione monocratica, definitivamente pronunciando nella causa promossa come in narrativa, ogni contraria istanza ed eccezione disattesa, così provvede:

1) Accoglie la domanda di risarcimento dei danni avanzata da [redacted] e per l'effetto condanna la [redacted] in persona del legale rappresentante p.t. al pagamento in loro favore della somma di euro 21.999,00 oltre interessi codicistici dalla domanda giudiziale;
2) Condanna, pertanto, la [redacted] in persona del legale rappresentante p.t. alla refusione delle spese del presente giudizio in favore di [redacted] che liquidano in euro 290,00 per spese vive ed euro 3.545,00 per compensi professionali, oltre IVA e CPA e rimborso forfetario al 15% con attribuzione all'Avv.to Lucia Vitiello dichiaratosene antistatario.

Napoli, 05.06.19

Il GU

Dott.ssa Maria Carolina De Falco