Ex Parte Creditoris
Rivista di Informazione Giuridica

Sentenza, Tribunale di Napoli, Giudice Paolo Andrea Vassallo, n. 10743 del 30.11.2022

www.expartecreditoris.it

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

IL TRIBUNALE ORDINARIO DI NAPOLI

SECONDA SEZIONE CIVILE

in persona del dr. Paolo Andrea Vassallo ha emesso la seguente

SENTENZA

nella causa civile di primo grado iscritta al n. xxxxx del R.G.A.C.C. dell'anno 2019, trattenuta in decisione nell'udienza del 13/09/2022, tenutasi secondo le modalità di trattazione scritta ex art. 221, co. 4, D.L. D.L. 19 maggio 2020, n. 34 rimessa al Giudice per la decisione all'esito della scadenza dei termini di cui all'art. 190 c.p.c. e vertente

TRA

CORRENTISTI,

- ATTORI -

E

BANCA,

- CONVENUTA -

Svolgimento del processo - Motivi della decisione

1.1. La domanda attorea è manifestamente infondata. La presente controversia scaturisce dalla contestazione, da parte degli attori **CORRENTISTI**, di due bonifici effettuati on line sul loro conto (...) con la **BANCA**, di cui sono contestatari.

1.2. I fatti rilevanti, nella loro storicista, sono pacifici è non hanno richiesto attività istruttoria. In particolare in data 29 novembre 2018 **CORRENTISTA N.1**, ricevette una email proveniente da un indirizzo mail: omissi@omissis.it del seguente testo "Ogg.: li tuo account e in attesa. Gentile cliente. Questo è un messaggio automatico del nostro sistema di sicurezza per informarti che hai 48 ore per confermare le informazioni del tuo account perché non siamo in grado di convalidare le informazioni dell'account.

Una volta aggiornati i record del tuo account, tenteremo di nuovo di convalidare le informazioni e la sospensione dell'account verrà revocata. Questo ti aiuterà a proteggere il tuo account in futuro. Questo processo non richiede più di 3 minuti. Per continuare a confermare i dettagli del tuo account clicca sul link sottostante e segui le istruzioni. Clicca qui per convalidare il tuo account. I migliori saluti. I. Security Department" (cfr. fasc. att. All. 10 Comunicazione di **CORRENTISTA N.1** del 29/11/2018 ore 20:17 ad I. contenente il messaggio di posta elettronica del 29/11/2018 delle ore 7:03).

1.3. A seguito della ricezione di tale email il **CORRENTISTA N.1** si collegava ad un link che conduceva a una richiesta di trasmissione delle credenziali del conto, le quali, una volta inserite, davano l'accesso al conto medesimo e alla possibilità di effettuare bonifici.

Il sistema di accesso al conto e di autorizzazione alle operazioni dispositive era il seguente. Unitamente al contratto di conto corrente era stato concluso dall'attore un contratto di internet banking cui era associato un generatore di password c.d. fisico (token o chiavetta di plastica). Per accedere online al conto corrente, il titolare delle credenziali doveva inserire password c.d. statiche (fisse) e password c.d. dinamiche (variabili), e precisamente: il codice titolare, che è il numero riportato sul contratto internet banking (password statica); il codice PIN, che è il codice creato dal titolare del conto, a sua scelta, in sede di primo accesso (password statica); il codice generato dal token o chiavetta (password dinamica: codice detto OTP, e cioè one time password). Effettuato l'accesso online al conto corrente, per eseguire una disposizione di. pagamento (un bonifico) il cliente doveva inserire una password c.d. dinamica, e cioè: altro codice generato dal token o chiavetta (altro codice OTP) (cfr. documenti A e B prodotti dalla I.S. unitamente alla seconda memoria ex art. 183 comma 6 c.p.c.).

1.4. Venivano dunque effettuati sul conto dell'attore due bonifici istantanei, il primo di Euro 12.345,00 avente quale beneficiario "omissis" effettuato alle ore 15.30 circa e il secondo di Euro 12.444,00 beneficiario "**omissis**" alle ore 19.20 circa. Per effettuare dette disposizioni di pagamento venivano inseriti, quindi, oltre al codice titolare, ed al codice PIN, il codice OTP per accedere, ed altro codice OTP per disporre il bonifico. Inoltre poiché si trattava di operazioni provenienti da IP (l'identificativo del computer) differente da quelli in passato usati dall'avv. **CORRENTISTA N.1** venivano inviati sul numero di utenza telefonica certificata dell'avv. **CORRENTISTA N.1** due ulteriori codici a mezzo SMS (c.d. codice OTS, e cioè on time password via SMS) necessari per autorizzare definitivamente le operazioni (cfr. fasc, att. All. 01. verbale di ricezione di querela/denuncia del 30/11/2018 "preciso che per ciascuna operazione sono pervenute dal gruppo I.S. due SMS all'interno del quale vi erano due codici di sicurezza da me inseriti, come richiesto dalla procedura truffaldino" e documento O prodotto dalla I.S. unitamente alla seconda memoria ex art. 183 comma 6 c.p.c.).

2.1. Tali essendo i fatti pacifici accaduti va osservato che la fattispecie sottoposta all'attenzione del Tribunale ricade nel c.d. fenomeno del "phishing". Purtroppo i casi di truffa come quello che qui ci occupa non sono infrequenti. La giurisprudenza ha avuto modo già da parecchi anni di affrontare la materia e nel tempo è andato elaborandosi un orientamento che ormai possiamo definire consolidato, essendo stato ribadito in diversi precedenti della Corte di Cassazione (cfr. da ultimo Cass. Sez. I, 3/2/2017, n. 2950; Cass. Sez. VI, 12/4/2018, n. 9158; Cass. Sez. III, 5/7/2019, n. 18045).

2.2. La soluzione propugnata dalla Suprema Corte - che, come si vedrà, è da ritenersi oggi parzialmente superata dalla normativa sopravvenuta - discende dall'applicazione dei principi fondamentali sul riparto dell'onere prova in materia contrattuale, in forza dei quali spetta al debitore convenuto dimostrare di avere correttamente adempiuto oppure dimostrare l'impossibilità della prestazione derivante da causa a lui non imputabile.

2.3. Tale principio generale ha trovato una sua specificazione con riguardo all'utilizzazione di servizi di pagamento che si avvalgono di mezzi elettronici, in quanto si è ritenuto che spetta all'istituto bancario dimostrare di avere adottato tutte le misure idonee a garantire la sicurezza del servizio, secondo un criterio di diligenza di natura tecnica che tenga conto dei rischi tipici della sfera professionale di riferimento ed assuma parametro la figura dell'"accorto banchiere".

2.4. Questo sistema di riparto dell'onere probatorio certamente amplia la sfera di rischio della Banca, ma ciò risulta del tutto giustificabile nella prospettiva generale del sistema, poiché, come spiega la Suprema Corte nelle sentenze sopra citate: "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

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

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" (cfr. Cass. 2950/2017 cit.).

2.5. Questi principi giurisprudenziali, sebbene affermati in pronunce molto recenti, riguardano però casi antecedenti all'entrata in vigore del D.Lgs. n. 11 del 2010 attuativo della direttiva europea n. 2007/64/CE in materia di servizi di pagamento.

2.6. Per l'inquadramento delle finalità legislative e delle novità introdotte dal D.Lgs. n. 11 del 2010 in materia di utilizzo non autorizzato dei sistemi di pagamento elettronici, si può richiamare l'autorevole opinione del Collegio di Coordinamento dell'Arbitro Bancario Finanziario (decisione del 26/10/2012 n. 3498), secondo cui: - l'obiettivo del legislatore era di rendere l'ambiente informatico-finanziario improntato a criteri di maggior sicurezza e affidabilità; - tale obiettivo è stato conseguito, da un lato, imponendo agli intermediari, nella loro qualità di prestatori di servizi di pagamento, specifici obblighi di precauzione, primo fra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati e, dall'altro lato, istituendo un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori; - nel concreto, tali speciali disposizioni prevedono: 1) che in caso di disconoscimento di un'operazione di pagamento, è onere dell'intermediario dimostrare che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema (cfr. art. 10); 2) che la responsabilità dell'utente resta circoscritta ai casi di comportamento fraudolento o all'inadempimento gravemente colposo agli obblighi che l'art. 7 del decreto pone a suo carico, cioè gli obblighi di utilizzare lo strumento di pagamento in conformità ai termini del servizio e di denunciare tempestivamente lo smarrimento o ogni altro uso non autorizzato dello strumento. Ove una simile responsabilità non possa affermarsi, l'utilizzatore non sopporterà le conseguenze dell'uso fraudolento, o comunque non autorizzato, del mezzo di pagamento (cfr. art. 12); - logicamente l'onere probatorio relativo alla colpa grave dell'utente incombe sull'intermediario prestatore del servizio; - le predette disposizioni determinano un evidente squilibrio nel rapporto fra prestatore e utilizzatore dei servizi di pagamento, che però si giustifica per il principio del rischio d'impresa, essendo razionale far gravare sull'intermediario i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, in quanto il costo dell'assicurazione di detti rischi può essere computato nella determinazione dei prezzi di vendita dei beni o di fornitura del servizio alla generalità degli utenti.

2.7. In conclusione, come si può vedere, dall'entrata in vigore del D.Lgs. n. 11 del 2010 discende un aggravamento degli oneri probatori posti a carico dell'Istituto di credito: mentre in precedenza per liberarsi dalla responsabilità era sufficiente dimostrare di avere adottato tutti i sistemi di sicurezza ragionevolmente esigibili, ora occorre anche la dimostrazione di una colpa grave dell'utente per non avere utilizzato correttamente lo strumento di pagamento elettronico o per non aver protetto le credenziali di accesso al sistema.

2.8. Nel nostro caso, gli attori sostengono che il sistema di sicurezza di **BANCA** non sia adeguato, non essendo riuscito ad evitare che essi fossero vittima di phishing.

Tuttavia la convenuta ha dimostrato di offrire un elevato grado di sicurezza ai propri clienti, fornendo un sistema di autenticazione a due fattori, ossia composto dal codice utente, dalla password di accesso statica e dalla password one time, generata dal token.

2.9. Tale sistema è ritenuto, da svariate pronunce dell'Arbitro Bancario Finanziario, "il più sicuro" (cfr. decisione n. 10118/2016; decisione n. 2660/2017; decisione n. 142/2017). Tale valutazione viene

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

condivisa anche in questa sede non potendosi ravvisare alcuna negligenza in capo alla Banca, né alcuna falla nei sistemi di sicurezza.

2.10. Come detto, però, ciò non è sufficiente per esonerare la convenuta dalla responsabilità per i danni denunciati dall'attrice, dovendosi verificare se le concrete modalità del fatto consentano di muovere a quest'ultima qualche addebito di negligenza.

2.11. Invero, trova qui applicazione il comma 4 dell'art. 12 del D.Lgs. n. 11 del 2010, in forza del quale le perdite conseguenti a operazioni di pagamento non autorizzate gravano sul cliente solo se egli abbia agito in modo fraudolento o non abbia adempiuto per colpa grave ai suoi obblighi imposti dall'art. 7 di attenersi ai termini del servizio e proteggere le credenziali di accesso.

3. Le regole di diligenza proprie dei vari contesti di riferimento rappresentano la "cristallizzazione" dei giudizi di prevedibilità ed evitabilità ripetuti nel tempo, non essendo la evitabilità dell'evento dannoso altro che la possibilità dell'uomo coscienzioso ed avveduto, dell'homo eiusdem professionis et condicionis, di cogliere che un certo evento è legato alla violazione di un determinato dovere oggettivo di diligenza, che un certo evento è evitabile adottando determinate regole di prudenza. In definitiva, ciò che l'ordinamento rimprovera all'agente è di non aver osservato lo standard di diligenza richiesto dalla situazione concreta e con riferimento alle qualità soggettive dell'incolpato; di non avere cioè attivato quei poteri di controllo e di impulso che doveva e poteva attivare, in quel contesto spazio-temporale, al fine di scongiurare l'evento lesivo.

3.1. Essendo questo il parametro normativo di riferimento per valutare la fondatezza della pretesa attorea, diviene determinante l'analisi delle modalità specifiche attraverso le quali è stata praticata con successo la truffa.

3.2. Orbene si può dare per assodato, siccome risulta pacifico tra le parti oltre che documentale, che ignoti truffatori si siano impossessati abusivamente delle credenziali e dei codici operativi dell'avv. P. mediante lo stratagemma del phishing descritto in precedenza, cioè inducendolo ad inserirle in un sito internet fasullo.

3.3. L'attore è tuttavia incappato in tale sito fasullo predisposto dai truffatori collegandosi ad un link inviatogli per email da un indirizzo palesemente non riconducibile in alcun modo alla Banca, e cioè omissis@omissis.net, dove non compaiono né logo della banca né altri elementi identificativi della Banca e che risulta addirittura contenente errori di ortografia ("Il tuo account I. e senza accento in attesa"), oltre che, per certi versi, anche poco comprensibile ("hai 48 ore per confermare le informazioni del tuo account perché non siamo in grado di convalidare le informazioni dell'account"). L'avv. P. sulla base del collegamento indotto da per email ha quindi compilato i campi di login sulla pagina fasulla digitando anche il codice OTP (One Time Password). Ciò senza sapere che il malvivente gli stava "rubando" le credenziali di accesso. Il malvivente, entrato in possesso di tutti e 3 i codici di accesso (nome utente, password e codice OTP) è riuscito pertanto ad effettuare l'accesso al portale della Banca ufficiale ed all'account dell'attore. Non solo: come risulta denunziato dallo stesso avv. P. (cfr. fasc, att. All. 01. verbale di ricezione di querela/denuncia del 30/11/2018) per ciascuna operazione all'attore sono pervenute dal gruppo I.S. due SMS all'interno del quale vi erano due codici di sicurezza inseriti dall'attore (codici OTS on time password via SMS) per effettuare i bonifici truffaldini.

3.4. Il caso in esame rientra dunque tra le ipotesi di phishing più comuni e ormai note alla clientela, anche senza particolari conoscenze informatiche, già all'epoca degli accadimenti. Le operazioni di bonifico di pagamento impartite sul conto dell'attore sono state autenticate regolarmente mediante i codici da egli stesso fomiti e non risulta ipotizzabile alcuna anomalia nel sistema di sicurezza della banca. L'aver abboccato alla e-mail palesemente ingannevole dei truffatori - sia per la sua riconoscibile anomala provenienza che per il suo contenuto - che non poteva essere confusa con un messaggio

autentico della Banca costituisce certamente una grave colpa da parte dell'attore, tenuto conto altresì della professione (avvocato) e del grado di istruzione dello stesso.

3.5. La domanda risarcitoria va in definitiva rigettata. Le spese di lite seguono la soccombenza e sono liquidate in dispositivo, con limitazione al minimo di scaglione delle fasi di istruttoria e di decisione secondo il Decreto 10 marzo 2014, n. 55 pubblicato in GU n.77 del 2-4-2014 nella misura aggiornata sulla base del D.M. n. 147 del 13 agosto 2022, pubblicato sulla G.U. n. 236 del 08/10/2022 e in vigore dal 23 ottobre 2022.

P.Q.M.

il Tribunale definitivamente pronunciando, ogni diversa domanda ed eccezione respinta, così provvede;
1) RIGETTA le domande proposte da **CORRENTISTI**;
2) CONDANNA **CORRENTISTI**, in solido, alla refusione delle spese di lite in favore della **BANCA**, che liquida in Euro 3.387,00 per compensi di avvocato, oltre rimborso forfettario ex art. 2 Decreto 10 marzo 2014, n. 55, Iva e Cpa come per legge e se dovute.
Conclusione
Così deciso in Napoli, il 30 novembre 2022.

Depositata in Cancelleria il 30 novembre 2022.

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