**N. R.G.**

**REPUBBLICA ITALIANA**

**IN NOME DEL POPOLO ITALIANO**

**TRIBUNALE ORDINARIO di MILANO**

SESTA SEZIONE CIVILE

Il Tribunale, nella persona del Giudice dott. Laura Cosentini

ha pronunciato la seguente

**SENTENZA**

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

**E T** (C.F. ),
**D D T** (C.F. ),
elettivamente domiciliati in MILANO presso lo studio dell'Avv.
che assiste la parte per delega a margine dell'atto di citazione

PARTE ATTRICE

contro

**P I SPA** (C.F. ),
elettivamente domiciliata in MILANO
presso lo studio dell'Avv. che assiste la parte per procura generale alle liti

**CONCLUSIONI**

Per parte attrice:

Piaccia all'Ill.mo Tribunale adito, ogni contraria istanza, eccezione e conclusione disattesa:
IN VIA PRINCIPALE E NEL MERITO:
- Accertare e dichiarare la responsabilità contrattuale ed extracontrattuale della convenuta per i motivi sopra esposti, e per l'effetto
- Condannare le P I S.P.A. al risarcimento del danno patrimoniale subito dagli attori pari ad € 10.210,60, o nel maggiore o minore danno accertato in corso di causa, oltre rivalutazione

dell'importo e interessi legali dalla domanda al saldo effettivo;

- Condannare le P I S.p.A. al risarcimento danno non patrimoniale quantificato in € 1.000,00 per ciascun attore danneggiato o nella diversa misura che riterrà l'Ill.mo Giudice adito, secondo equità e giustizia.

IN VIA ISTRUTTORIA

- ammettersi prove per interpello e testi sui fatti indicati in narrativa.

Si indica, sin d'ora, quali testi

- Sig. Do T , , Milano.
- Sig.ra R C , , Milano.
- Sig.ra I D , , Rozzano (MI).

Con vittoria di spese, diritti ed onorari del presente giudizio. Salvo ogni altro diritto.
Salvis iuribus."

Per parte convenuta:

Voglia codesto Ill.mo Tribunale adito, *contrariis reiectis*,
- respingere le domande tutte avanzate dalla parte attrice nei confronti di P I S.p.A. in quanto infondate in fatto e diritto;
- con vittoria di spese;
- in via istruttoria, chiedesi, a modifica parziale dell'ordinanza di ammissione prove in data 7 marzo 2013, interrogatorio formale di parte attrice e prova per testi sulle circostanze di fatto di cui alla comparsa di costituzione e risposta del 6 dicembre 2012 - che qui di seguito si capitolano dal n. 1) al n. 23) - da intendersi precedute da "vero che", espunte eventuali espressioni valutative:

1) I signori T E e D D erano titolari del conto corrente B n. 42208231 (ora estinto), acceso in data 23 gennaio 2002 presso l'ufficio ed in relazione al quale i clienti medesimi avevano richiesto il servizio aggiuntivo di *home banking* denominato "B online" (disciplinato dalle condizioni contrattuali applicabili al rapporto all'epoca dei fatti di causa), che consente al correntista di comunicare con P I attraverso la rete telematica Internet per impartire disposizioni ed avere informazioni in riferimento al proprio conto corrente;

2) P I S.p.A., al fine di garantire la sicurezza del servizio B in parola, adotta uno tra i più efficaci sistemi di crittografia dei dati di riconoscimento del cliente e di tutti i flussi di informazioni scambiate durante le operazioni che il correntista medesimo compie nella fruizione del servizio di *home banking* (sistema del tipo a doppia chiave, pubblica/privata);

3) Con il servizio di *home banking* in discorso, il cliente accede al suo conto *online* attraverso una connessione protetta che assicura la non intelleggibilità ai terzi delle informazioni scambiate: il sistema di protezione adottato utilizza il protocollo http con crittografia SSL (*Secure Socker Layer*) a 128 *bit*;

4) Con il servizio di *home banking* in discorso, l'accesso al conto corrente *online* è possibile esclusivamente attraverso la corretta identificazione, che avviene mediante la digitazione delle proprie credenziali riservate;

5) il sistema di crittografia adottato rappresenta lo "stato dell'arte" in tema di sistemi di sicurezza per garantire la riservatezza delle informazioni trasmesse via internet e costituisce lo standard cui gli operatori professionali prudentemente si adeguano;

6) tale tecnologia consente altresì all'utente di sincerarsi in ogni momento, durante la navigazione in internet, che il soggetto con il quale ci si sta interfacciando sia realmente quello desiderato, attraverso la verifica dell'esattezza dell'indirizzo elettronico evidenziato nella barra degli indirizzi e della bontà del certificato di protezione;

7) L'adozione del suddetto protocollo è riscontrabile nella presenza della sigla http://, che costituisce sempre il prefisso dell'indirizzo del sito internet al quale è applicato (e che diventa "https://" nel momento in cui si accede alla connessione protetta, momento a partire dal quale appare, nella pagina *web*, un simbolo a forma di lucchetto);
8) L'adozione del citato protocollo testimonia il fatto che P ha predisposto un sistema di protezione tale da garantire al cliente di poter fruire in sicurezza del servizio di *home banking*, avendo effettuato le necessarie registrazioni ed avendo ricevuto le prescritte certificazioni da parte degli enti a ciò preposti (unitamente alla presente memoria si depositano alcune delle certificazioni rilasciate dalle competenti autorità alla convenuta, le quali dimostrano che P , durante il periodo in cui si sono svolti i fatti allegati a fondamento della domanda, aveva predisposto un sistema di sicurezza per l'esercizio dell'internet banking conforme alle normative internazionali - v. doc. 1);
9) A presidio della corretta identificazione del correntista nelle fasi di accesso e di operatività del servizio di *home banking* B (come previsto all'art. 2, sezione VI delle condizioni contrattuali applicabili al rapporto all'epoca dei fatti di causa – v. doc. 2) sono posti quattro elementi: 1) l'identificativo dell'utente (*user ID*); 2) la parola chiave (o *password*); 3) il codice dispositivo segreto (*PIN*); 4) la cifra di controllo, atta a richiedere ed ottenere l'attivazione del codice dispositivo;
10) La parola chiave - come l'identificativo utente - è definita dal correntista in fase di registrazione e può da questi essere successivamente modificata ogniqualvolta ritenga di farlo; il *PIN* e la cifra di controllo sono generati dal sistema informatico di P con procedura protetta in occasione dell'attivazione del servizio;
11) Il cliente titolare del servizio B che intenda effettuare un'operazione per via telematica (per es. consultare il saldo del proprio conto corrente) non deve fare altro che accedere, tramite Internet, al sito di P , entrare nell'area B *online* ed immettere negli appositi spazi i propri dati di riconoscimento *user ID* (codice identificativo personale) e *password* (parola chiave);
12) qualora voglia effettuare un'operazione dispositiva a valere sul proprio conto corrente, oltre ad accreditarsi mediante l'inserimento delle due credenziali pre-citate, all'atto della conferma della disposizione impartita il cliente deve farsi nuovamente riconoscere inserendo quattro dei dieci caratteri del codice dispositivo segreto (*PIN*), richiesti ogni volta in una composizione differente e selezionati a caso (*at random*), nell'occasione, dal sistema;
13) Per assicurarsi che il codice dispositivo sia effettivamente segreto, quindi conosciuto esclusivamente dal cliente titolato ad avvalersene, P invia il suddetto codice (composto di dieci caratteri alfanumerici e generato, come accennato, da una procedura informatica che lo determina in una composizione non conoscibile al personale di P , neanche ai più alti livelli della gerarchia aziendale) al domicilio indicato dal cliente, in busta sigillata (e non "attivo");
14) Avendo richiesto e ricevuto (in busta sigillata) il codice dispositivo riservato necessario per effettuare operazioni dispositive *online*, la cliente T , seguendo le istruzioni recapitate da P nella casella di posta elettronica personale, si recava presso l'ufficio postale di radicamento del conto corrente ove otteneva l'attivazione di tale codice;
15) A partire dal momento dell'attivazione del codice dispositivo, la signora T è stata abilitata ad impartire per via telematica operazioni dispositive a valere sul conto corrente;
16) P I S.p.A. invia le comunicazioni relative al servizio B esclusivamente all'indirizzo di posta elettronica attribuito al cliente in fase di registrazione;
17) Non esiste, per i clienti B , la possibilità di indicare un indirizzo elettronico (diverso da quello attribuito in fase di registrazione) per ricevere da P comunicazioni *online* relative al proprio conto corrente;
18) Nei giorni dal 10 al 13 settembre 2009, pervenivano a P I S.p.A. tre richieste di ricarica *online* di carta prepagata P , una richiesta di ricarica telefonica e nove richieste di postagiro, tutte a valere sul conto corrente postale bancoposta n. 422082321 intestato all'odierna attrice, come specificato nella lista operazioni che si produce (doc. 2);

19) Gli ordini di operazioni dispositive di cui al punto che precede venivano impartiti attraverso il sistema telematico da parte di soggetto accreditatosi mediante la digitazione delle chiavi di accesso del correntista (soggetto che appariva quindi legittimato ad operare sul conto intestato all'odierna attrice), che è stato altresì in grado di fornire correttamente i caratteri del codice dispositivo segreto richiesti dal sistema;
20) La signora T E non ha adottato adeguati sistemi di protezione dell'apparecchiatura utilizzata per fruire del servizio B ;
21) in data 11.09.2009, (come evincesi anche dal doc. 2 precit.) sono stati anche rimborsati buoni postali fruttiferi dematerializzati intestati alla cliente, con relativo accredito sul conto corrente della signora T ;
22) il postagiro è una operazione che avviene in tempo reale, con disponibilità immediata sul conto del beneficiario, il quale può immediatamente utilizzare la somma appena accreditata;
23) Le operazioni di ricarica telefonica vengono effettuate verso un gestore di telefonia mobile e P non ha alcuna possibilità di risalire all'eventuale beneficiario della ricarica, dati in possesso esclusivo del gestore telefonico.
A tal fine si indicano a testi: Ra P , Ro P , C S , domiciliati per l'incombente presso B sistemi e canali di pagamento Roma, con riserva d'altri.
Si dichiara di non accettare il contraddittorio su eventuali nuove domande ed eccezioni di controparte."

## SVOLGIMENTO DEL PROCESSO

Con atto di citazione notificato in data 8.6.2012, i fratelli T E e T D D chiamavano avanti a questo Tribunale P I s.p.a., lamentando che, nel periodo dal 10.9.09 al 15.9.09 sul conto corrente B agli stessi cointestato, erano state effettuate plurime operazioni di addebito per il complessivo importo di € 10.216,60, operazioni dagli stessi non disposte e di cui si erano avveduti accedendo al conto il 18.9.09, quando verificavano l'impossibilità di operazione d'acquisto tramite carta bancomat per insufficienza del saldo; effettuato immediato disconoscimento delle suddette operazioni e proceduto il 19.9.2009 a tempestiva denuncia penale, vanamente esperiti tentativi di conciliazione, chiedevano accertarsi la responsabilità contrattuale ed extracontrattuale di P , cui contestavano la mancata adozione di misure di sicurezza e protezione idonee a prevenire la sottrazione e il fraudolento utilizzo dei dati personali necessari per accedere al servizio *home banking* (denominato "*B Online*"), ascrivendo ciò a violazione degli artt.31 e 33 del Codice della Privacy (D.lgs. 196/2003), ovvero a responsabilità ex art.2050 c.c..

Costituitasi in data 6.12.12, P I chiedeva il rigetto della domanda e negava la propria responsabilità, affermando che il sistema di sicurezza dalla stessa adottato doveva reputarsi conforme allo stato dell'arte e idoneo a garantire piena tutela ai propri clienti avverso potenziali truffe informatiche, e imputando l'evento alla negligenza dei clienti, che avrebbero incautamente rivelato a terzi i propri dati di accesso, o si sarebbero avvalsi, per l'esecuzione di operazioni in via telematica, di apparecchi sprovvisti di adeguati software di protezione.

Concessi termini per memorie ex art.183 c.6 c.p.c., all'udienza del 7.3.13 il Giudice ammetteva CTU in punto verifica dei sistemi di sicurezza adottati da P , dandone incarico all'Ing G C , che assumeva l'incarico all'udienza del 3.4.13 e depositava relazione finale il 18.10.13. All'udienza del 16.9.14, sulle conclusioni precisate come in epigrafe, il giudice tratteneva la causa in decisione, dando termini di giorni 45 per memorie conclusionali e ulteriori 20 per memorie di replica.

## MOTIVI DELLA DECISIONE

Fondate si reputano le domande svolte dagli attori, nei limiti e sulla base delle argomentazioni che seguono.

Non sembra in primo luogo possa essere posto in discussione che le 13 operazioni dispositive che compaiono in addebito sul conto corrente dei fratelli T nei giorni dal 10 al 15 settembre 2009 (unitamente all'addebito delle relative commissioni), siano operazioni dagli stessi non volute, imputabili all'operato truffaldino di soggetti terzi; non solo in tal senso vi è tempestiva denuncia penale degli interessati (del 19.9.09), ma la stessa modalità e tempistica delle operazioni, tutte avvenute on line, e la maggior parte ripetute nella stessa giornata (9 nella stessa data del 11 settembre), per importi pari al massimale consentito per singola operazione, sono indici evidenti di siffatto procedere delittuoso, che la stessa convenuta peraltro non pare contestare nello specifico, negando piuttosto di poterne essere ritenuta responsabile.

Ciò detto vengono in esame le approfondite verifiche condotte dal nominato CTU, il quale, sul presupposto che le operazioni suddette siano state effettuate utilizzando i codici di accesso nella disponibilità del solo correntista, mostra di escludere che ciò sia avvenuto, o in esito alla violazione da parte di soggetto esterno dei sistemi interni di sicurezza di P , ovvero tramite accesso al computer del correntista.

Quanto al primo profilo, inerente i sistemi interni di sicurezza di P (ossia quei canali di diretta custodia informatica di P necessari alla verifica di correttezza dei dati immessi dal cliente durante le fasi di accesso al sistema "*home banking*"), il CTU riscontrava che "*i sistemi delle P. I furono effettivamente e palesemente violati in ottobre 2009*", rilevando tuttavia che, in merito a evento successivo ai fatti di cui è causa, era in ogni caso da escludere che "*tale attacco -fosse stato- preceduto da altri, silenti, che avessero avuto accesso a codici identificativi di titolari di conto corrente*", osservando che "*questo fatto, se accaduto, avrebbe avuto dimensione ben diversa da quella di cui si sta trattando*", ossia si sarebbe esplicato in contemporanea su un numero ben maggiore di rapporti di conto corrente e con risonanza ben più ampia, e di ciò si rileva non esservi prova.

Quanto al secondo profilo, parimenti il CTU esclude quanto ipotizzato dal CT di P che "*il PC di controparte fosse totalmente controllato da ignoti*", affermazione che ritiene indimostrata. Ove invero si fosse trattato del c.d. "*attacco di man in the middle -MITM*", dispositivo che, frapponendosi tra il computer del privato e quello della banca, "*imbroglia l'elenco telefonico di internet e fa indirizzare a un suo computer le richieste che l'utente indirizza alla banca*" (pag.8 relazione iniziale CTU), lo stesso sarebbe stato "*ragionevolmente arginato dal fatto che i due interlocutori utilizzino il protocollo cifrato HTTPS, che prevede che il server remoto invii al PC dell'utente un documento elettronico che contiene la firma univoca del mittente e che non è contraffabile ...il PC dell'utente può accorgersi della falsificazione e interrompere il contatto*" (pag.7 relazione finale CTU). Ove invece si fosse trattato di "*attacco di man in the browser –MITB, virus che si insinua nel programma che si usa per accedere a internet... e che intercetta i dati mentre vengono digitati*", ciò avrebbe indirizzato un'operazione di bonifico digitata dal cliente verso un conto complice "*presentando a video dati congruenti con quanto digitato dall'utente*", il che tuttavia si sarebbe tradotto in fattispecie diversa da quella denunciata, perché avrebbe dato luogo a "*operazioni diverse da quelle disposte dal cliente ovvero all'assenza di quelle disposte da lui*"; in presenza invece di operazioni mai digitate dal cliente, il CTU ne deduce che "*le transazioni truffaldine non furono*

*generate da un dispositivo automatico che, insinuatosi nel PC del cliente o inseritosi nelle comunicazioni, modificasse al volo le disposizioni impartite verso la banca*".

Escluse le suddette ipotesi, il CTU conclude invece affermando che i due correntisti siano stati vittima di "*phishing*", ossia di quella tecnica informatica illecita finalizzata alla sottrazione fraudolenta dei dati personali di accesso ai conti correnti online, da utilizzare per compiere atti dispositivi in danno dei legittimi titolari, di cui carpiscono l'identità informatica; la modalità è ascrivibile per lo più all'ingannevole invio di mail, apparentemente provenienti dall'istituto di credito con il quale è in corso il rapporto, che contengono l'invito al titolare di accedere al conto on line, con ciò comunicandone i dati di accesso personali e riservati, onde scongiurare temporanei asseriti problemi.

In merito a tale tecnica di frode informatica, il CTU rappresenta trattarsi di fenomeno sorto ben prima delle operazioni di cui è causa, e che da tempo era stato oggetto di attenzione da parte delle banche, che si erano progressivamente attivate adottando politiche a protezione dei propri clienti; in particolare, come da indagini di cui riporta le fonti di conoscenza, afferma il CTU che *"sin dal 2003 si stavano diffondendo nel mondo bancario delle tecniche specificamente messe a punto per prevenire gli attacchi dei programmi spia e del phishing...sulla base della constatazione che il pirata utilizzava i codici sottratti in un momento diverso da quello della sottrazione ...e che se fosse stato possibile abbinare a una transazione bancaria un codice legato, non solo all'utente, ma anche all'istante in cui la transazione era svolta, anche se tutti i codici fossero stati rubati dal pirata, sarebbe stato impossibile per lui riutilizzarli una seconda volta in un secondo momento"*. Nascevano così le c.d. "*password usa e getta ...tecnicamente OTP "One Time Password", valido per pochi secondi da quando compare... al disporre di un'operazione il sistema chiede di introdurre l'OTP, che è generata in quell'istante... il sistema controlla che l'OTP immessa sia corrispondente a quella che quell'utente doveva immettere in quell'istante... se difforme, la transazione è rifiutata... in questo modo il ladro informatico, per operare la truffa, dovrebbe rubare anche il dispositivo generatore delle OTP, cosa impossibile per via informatica*".

Dalle verifiche condotte dal CTU è emerso che dal 2005 in avanti le principali banche, in contesto europeo, asiatico e statunitensi, iniziarono ad adottare il sistema di autenticazione OTP nel servizio bancario on line, e che già nel 2007, come da rapporto allegato alla CTU, in Italia erano svariate le banche che avevano proceduto in tal senso, e in particolare si erano già attivate quelle che, come P , avevano massima diffusione in territorio italiano (M , Banca N , U , Banca I , I , C , A , ed altre).

Si reputa con ciò che nel 2009, epoca delle operazioni di pirateria informatica di cui è causa, fosse gravemente in difetto P I per non essersi ancora adeguata agli standard di sicurezza dei sistemi informatici, non avendo adottato, nel servizio di "*home banking*", quel *"sistema di autenticazione basato su OTP, che all'epoca dei fatti costituiva uno standard consolidato per la tutela dei Clienti di banche dal phishing e dai programmi spia*".

Di ciò P dovrà rispondere ai sensi dell'art.1176 comma 2 c.c., secondo cui "*nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata*". Si stima invero che nel rapporto contrattuale di "Servizio B OnLine" stipulato tra la banca e il cliente privato, nel quale P garantiva "*la sicurezza del sistema ...mediante idonei sistemi di crittografia dei dati di riconoscimento dell'utente*" (art.2 Sez.VI Condizioni contrattuali), fosse la banca il contraente qualificato che, non

ignaro delle modalità di frode mediante *phishing* da tempo note nel settore, era tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza informatici, altrettanto noti, idonei a contrastare il fenomeno; non poteva invece ascriversi a mancata diligenza del cliente il fatto di non essere stato al corrente di tali modalità di frode, e conseguentemente di non essersi accorto che possibili mail di apparente provenienza di P fossero in realtà frutto di pirateria informatica e celassero l'intento truffaldino di carpire dati riservati.

A tale ultimo proposito, si reputa che la mail 21.9.09 destinata a E T (doc.5 attori), che verosimilmente era stata veicolo della truffa informatica perpetrata, non presentasse palesi evidenze di contraffazione, ciò in particolare agli occhi di un cliente comune, di cui non è provata alcuna qualificata competenza nel settore informatico, nè tanto meno nel settore dell'informatica bancaria; trattasi invero di mail inviata alla T presso l'account fornitole da P mail, dichiaratamente proveniente dall'"Assistenza Clienti B Online" e da un indirizzo mail "B @ .it" di non immediata riconoscibilità truffaldina, riportando il logo di quel "Servizio B OnLine" (B ), che compare nella stessa documentazione contrattuale rilasciata ai correntisti (doc.3 convenuta).

Parimenti e peraltro si rileva che, quella stessa procedura predisposta da P per "*Analisi indicatori di frode*" (documento menzionato dal CTU come di provenienza del CT di parte convenuta) si rivelava inadeguata nel caso di specie ("*È curioso constare come tale sistema non ha rilevato la situazione palesemente anomala illustrata nella mia bozza ...pur utilizzando criteri che nel caso in oggetto avrebbero potuto scattare*" –pag.5 CTU definitiva); non veniva segnalata, ad esempio, "*l'operazione disposta da un conto corrente con un indirizzo IP differente dall'operazione precedente, anche se eseguita in una giornata differente*", differenza che pure emergeva più volte se si guarda alla "Lista operazioni T " fornita da P (in Cartella Verbali/Documenti P 13.5.2013); tale mancato riscontro è quindi parimenti fonte di responsabilità da parte di P , atteso che, ove tempestivamente intervenuto, avrebbe se non altro interrotto il procedere truffaldino, limitando l'entità dell'importo sottratto dal conto.

Affermata la responsabilità contrattuale di P , la convenuta sarà tenuta a risarcire il danno riportato dagli attori, danno che, sotto il profilo patrimoniale, va individuato nell'importo di € 10.210,60, pari al totale dell'importo sottratto dal conto degli stessi in esito alle disposizioni truffaldine accertate; trattandosi di debito risarcitorio e quindi debito di valore, l'importo andrà annualmente rivalutato a decorrere dal 15.9.2009 (data ultima delle operazioni dispositive) sino alla presente pronuncia di liquidazione del danno.

Parimenti fondata si stima la richiesta degli attori di risarcimento del danno non patrimoniale dagli stessi riportato, valutandosi l'inevitabile sofferenza e preoccupazione degli stessi, in esito alla truffa informatica subita, nel constatare la perdita dell'intera provvista accreditata sul conto, danno che si liquida in via equitativa in € 800,00 ciascuno al valore attuale.

Le spese seguono la soccombenza e si pongono pertanto a carico della parte convenuta, liquidandosi le spese sostenute dagli attori ex D.M. n.55/14. Parimenti a carico della parte convenuta vanno poste le spese di CTU, come liquidate con decreto 18/21.10.13.

P.Q.M.

Il Tribunale, definitivamente pronunciando in contraddittorio delle parti, ogni diversa o ulteriore domanda ed eccezione reietta:

1. condanna P I s.p.a. a risarcire a E e D D T , in solido tra loro,
   - danni patrimoniali liquidati in € 10.210,60, oltre interessi legali sulla somma come annualmente rivalutata dal 15.9.2009 alla data della presente pronuncia, e interessi legali sull'importo totale dalla presente pronuncia sino al saldo,
   - danni non patrimoniali liquidati in € 1.600,00, oltre interessi legali dalla presente pronuncia sino al saldo;
2. condanna P I s.p.a. a rifondere a E e D D T , in solido tra loro, le spese di procedimento, liquidate in € 230,00 per esborsi ed € 4.835,00 per compensi professionali, oltre 15% rimborso spese generali, CPA e IVA di legge;
3. pone a carico definitivo di P I s.p.a. le spese di CTU, come liquidate in decreto 18/21.10.2013.

Milano, 4 dicembre 2014

Il Giudice
dott. Laura Cosentini