Fabio Di Resta -
Avvocato – LL.M. – già Docente universitario Master Data Protection Officer di II livello Università Roma Tre – Dipartimento di Giurisprudenza – Presidente Centro europeo per la privacy (EPCE)

L'evoluzione del furto di identità digitale dal phishing alla sim swap fraud: analisi dei profili di responsabilità degli istituti di credito

The evolution of identity theft from phishing to sim sawp fraud : Analysis of the bank liabilities

Sommario: Il furto di identità in questi anni ha subito certamente una crescita esponenziale come confermato anche dalle più note indagini pubblicate in materia. Il fenomeno del furto di identità sotto un profilo legale non trova una puntuale definizione, sotto il profilo penalistico viene inquadrato in diversi modi, dalla frode informatica alla sostituzione di identità digitale. L'aspetto che viene analizzato in questo articolo è relativo ai furti di identità perpetrati nei confronti dei correntisti bancari, analizzando nello specifico i profili di responsabilità bancaria per servizi di home banking. Si può ritenere che la posizione della giurisprudenza in tema di risarcimento del danno era monolitica fino a tutto il 2009 disconoscendo le responsabilità degli istituti credito e basandosi principalmente su argomentazioni relative alla negligenza del correntista come parte contrattuale oppure alla mancanza di prove di inadempienza dell'istituto bancario. Tale approccio si basava su un principio di parità delle parti contrattuali, correntista e istituto di credito, tuttavia, nel corsi degli anni che seguono il 2009 vi sono stati cambiamenti estremamente rilevanti. Infatti, la giurisprudenza, giovandosi anche di normative più favorevoli come la normativa privacy e la normative sui servizi di pagamento nel mercato interno, ha affermato dapprima in forma più timida, per poi consolidarsi, i principi del riconoscimento del risarcimento dei danni a favore del correntista che sia stato vittima di un furto di identità. Il riconoscimento del correntista come parte debole contrattuale porta con sé un disciplina di favore che vede l'onere della prova liberatoria necessariamente a carico degli istituti di credito.

Abstract: In the last years it has been a consistent increase of identity theft cases as demonstrated by a number of statistical surveys published on this subject. So far, in our legal system there is not a legal definition of identity theft, but several applicable provisions, especially in respect of criminal law. In this article identity theft will be analysed with regard to the home banking services linked with the bank liability.

In this regard, it should be considered that the position of courts until the end of the year 2009 was essentially to refuse any compensation to the bank account holders which were victim of identity thefts, the courts refused to recognise compensation mainly on arguments based on neglect behaviours of bank account holder (as a user of home banking service), such as for instance the loss or communication to third parties of the password to access the home banking service, and the lack of evidences of the banks' negligence provide by the user. This approach was based on the principle of equal position of the contractual parties, bank account holder and bank; however, during the years after 2009 relevant changes have been on this position of courts. Lastly, in the recent years courts recognised compensation to the victims of the identity thefts through legislations on data protection and on the payment services in the internal market (Directive 2007/64/EC on Payment Services transposed into Italian law). The bank account holder is consider by this legislation as a weak contractual party with the consequence that the bank should be obliged to give the evidence of the exact contractual performance.

Il furto di identità digitale come mostrano le indagini più note, è un fenomeno in forte crescita e che può essere realizzato tramite diverse azioni semplici o più complesse. Vi è da premettere che il termine furto di identità appartiene al linguaggio comune e non giuridico, per quanto interessa questo approfondimento il fenomeno verrà analizzato sotto il profilo del diritto civile e della legislazione applicabile al settore bancario volto ad individuare le responsabilità dei danni cagionati al correntista danneggiato.

In primo luogo occorre anche evidenziare che i professionisti che assistono frequentemente i clienti vittime di furti di identità si accorgono che purtroppo si tratta di un fenomeno dagli effetti devastanti per loro, non solo perché viene violata la loro identità personale e la propria riservatezza, ma soprattutto perché i tempi per recuperare questa identità sottratta possono richiedere anche alcuni anni e occorre comunque un monitoraggio continuato per un certo periodo dovuto al rischio di nuove azioni.

Tra le più note azioni illegali volte a sottrarre telematicamente i dati al correntista vi è sicuramente *phishing* (che potrebbe essere tradotto come abboccamento) nel quale il correntista forniva inconsciamente a terzi i propri dati personali tramite email fasulle, inclusi password e nome utente, ma il phishing nel tempo è diventato sempre più sofistica, sia migliorando il testo delle email sia diventando

più capzioso, ci si riferisce il particolare alle tecniche di *phishing* mirato nelle quali i truffatori acquisiscono informazioni personali di dettaglio profilando la vittima in vari modalità, non ultimo l'utilizzo dei social network per carpire informazioni più specifica, in tal modo i truffatori riescono a spacciarsi per amici o colleghi della vittima acquisendo informazioni sempre più delicate fino a realizzare la truffa (c.d. *spear phishing*).

Inoltre, accanto a questa tattica illegale che può essere considerata la più tradizionale si sono sviluppato frodi, come il *pharming* nelle quali il frodatori tramite l'IP dell'indirizzo *internet* dirottano l'utente su un sito civetta carpendo i dati personali, oppure il *vishing* che sfrutta la tecnologia *internet*, spesso realizzata tramite sistemi *voip*, *call center*, lo *smishing* nel quale i frodatori ottengono le password tramite semplici sms.

Infine, solo per citare i più diffuso ci sono le tecniche di *Man In The Middle (MITM)* o *Man In The Browser (MITB)*, con la prima il truffatore durante la sessione di lavoro sul PC si insinua nel canale di comunicazione tra l'utente e l'istituto di credito, riuscendo a carpire le credenziali di autenticazione dell'utente e compiendo azioni dispositive di denaro su conti correnti di terzi, nel *MITB* l'azione illegale compiuta è molto simile all'altro ma sfrutta la debolezza del *browser*.

Dopo questa breve rassegna delle tattiche finalizzate a carpire i dati dei correntisti, appare opportuno passare agli aspetti legali. Sino a quasi tutto il 2009 poteva considerarsi consolidato l'orientamento della giurisprudenza di merito che asseriva la mancanza di responsabilità da parte degli istituti di credito in casi di frodi telematiche relative ai servizi di home banking.

Invece, dal 2010 in poi si cominciava ad intravedere qualche timida apertura alla responsabilità degli istituti di credito. Da una parte vi erano alcuni organi giudicanti che asserivano che l'illecita captazione delle credenziale fosse da ritenersi ipso facto un indice di una mancanza di cautela del correntista (App. Trento, n. 69 del 8 marzo 2011) senza disporre nomina di alcun consulente tecnico, dall'altra vi erano stati invece arresti giurisprudenziali di merito nei quali si riteneva che sebbene la CTU (Consulente tecnico d'ufficio) asserisse che il "sistema all'epoca adottato dalla convenuta (codice dispositivo segreto composto da dieci caratteri) non era sufficientemente efficace nella prevenzione delle frodi informatiche, tanto da essere sostituito un paio di mesi dopo", tuttavia, non vi era nessuna prova nemmeno indiziaria che si fosse realizzata la specifica frode del phishing (Tribunale di

Milano, 28 gennaio 2013). Pronuncia questa che verrà esaminata meglio più avanti.

Già da questi brevi richiami di alcuni dei più rilevanti arresti giurisprudenziali appare chiaro come gli orientamenti che spostano l'onere della prova sul correntista considerano quest'ultimo e l'istituto di credito sullo stesso piano, equiparazione molto pericolosa e sfavorevole per il correntista oltre ad essere chiaramente non raffigurare correttamente la situazione contrattuale tra le parti (correntista e istituto di credito).

Invero, un'impostazione questa poco condivisibile e contrastante con le normative più recenti in materia, laddove il correntista dovrebbe essere considerato come parte debole del contratto, essendo lo stesso qualificabile appunto come consumatore, per contro l'istituto di credito che opera nel proprio ambito professionale deve attenersi invece ad un livello di diligenza elevata appunto denominata diligenza del buon banchiere.

Interpretando le vicende del furto di identità occorse ai correntisti in chiave di parte debole, infatti, gli organi giudicanti di merito già dalla fine del 2009 hanno avuto modo di affermare una sostanziale inversione dei tendenza, tenendo appunto conto del disequilibrio contrattuale tra correntista/parte debole da parte e istituto di credito come titolare del trattamento/professionista dall'altra parte.

Così il Tribunale di Palermo nella pronuncia del 20 dicembre 2009 (deposita il 12 gennaio 2010) affronta il punto critico del sistema dell'onere probatorio ed asserisce che: "Nel caso di specie gli attori hanno provato l'esistenza del rapporto obbligatorio in forza del quale agiscono ed allegato l'inadempimento della convenuta, dal canto suo le (omissis) nulla hanno dimostrato in ordine al corretto adempimento delle proprie obbligazioni". Pertanto, seconda la tesi accolta dal giudicante il correntista è tenuto a fornire la prova delle fonte dell'obbligazione contrattuale, la quale non presenta di solito difficoltà coincidendo con contratto di conto corrente bancario, tuttavia, la prova dell'inadempimento merita invece maggiore attenzione. Prescindendo dalla prova del danno sempre presente, il giudicante si trova a dover individuare il concreto significato di inadempimento, il quale si fa talvolta perfino coincidere con la prova della vulnerabilità del sistema informatico bancario, prova molto difficile da dimostrare lato correntista. D'altro canto, la prova dell'inadempimento dell'istituto bancario non può neppure consistere nel dimostrare inequivocabilmente che il sistema informatico è inidoneo perché per

verificare le vulnerabilità del sistema informatico della banca occorrerebbero in tal caso conoscenze tecniche specialistiche nonché supportare costi troppo elevati per il correntista.

Orbene, dopo questo breve *excursus* argomentativo sulla questione dell'inadempimento, la soluzione adottata in concreto dal Tribunale di Palermo del 2009 appare pienamente condivisibile laddove si afferma che: "In applicazione dei predetti principi, le (omissis) avrebbero dovuto adottare tutte le misure di sicurezza, tecnicamente idonee e conosciute in base al progresso tecnico, a prevenire danni, come quelli verificatisi in capo agli attori, non essendo sufficiente la non violazione di norme di legge, posto che la diligenza richiesta deve essere valutata con maggior rigore, atteso che la prestazione inerisce all'esercizio di un'attività professionale."

La tesi sopra descritta in ordine alle responsabilità dell'istituto fondate sulla normativa privacy trova pieno conforto in numerose pronunce di merito relative alle frodi telematiche subite dai correntisti, laddove, come già accennato si afferma in primo luogo che: "L'art. 31 del d.lgs. n. 196/2003 impone che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico […] Va, quindi, applicata nel caso di specie la previsione di cui all'art. 15 del d.lgs. 196/2003[…] Le […], non impedendo a terzi estranei di introdursi illecitamente nel proprio sistema hanno provocato un danno al proprio cliente" (Tribunale di Nocera, 15 settembre 2011; in senso conforme, Tribunale di Palermo, 12 Gennaio 2010; Giudice di Pace di Lecce, 4 dicembre 2013).

Anche la recente pronuncia del Tribunale di Milano del 4 dicembre 2014, sez. VI, accoglie questa impostazione, in tal caso il correntista lamentava plurime operazioni non autorizzate sul proprio conto corrente, il quale presumibilmente vittima di phishing, aveva comunicato il disconoscimento delle stesse alla banca, constata l'impossibilità di addivenire ad una conciliazione, ricorreva al Tribunale chiedendo di essere risarcito per i danni patrimoniali ed extrapatrimoniali subiti per effetto della mancata adozione delle misure di sicurezza idonee a prevenire un utilizzo fraudolento dei dati personali del correntista. Nel corso del giudizio veniva nominato un CTU, lo stesso nella relazione tecnica asseriva quanto segue:

- l'esclusione del *Man In The Browser (MITB)*, in tale attacco in terzo malintenzionato frapponendosi tra il computer del privato e quello della banca utilizza un "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", trattandosi invece di operazioni mai digitate dall'utente non può configurarsi il fenomeno informatico in questione;

- l'esclusione anche di altre ipotesi, come anche il *Man In the Middle (MITM)*, portano a concludere che si trattava di *phishing*.

- il fenomeno di phishing è noto da tempo, sin dal 2003 gli istituti di credito avevano messo a punto misure di sicurezza volte a prevenire tale fenomeno, a tale riguardo l'istituto avrebbe potuto adottare una password "usa e getta" ovvero una *One Time Password (OTP)*, inoltre, sin dal 2007 numerose erano le banca che avevano adottato tale dispositivo.

Questi assunti del CTU condivisi dall'organo giudicante portano ad asserire che il sistema informatico adottato all'epoca dei fatti da parte del noto istituto di credito non era adeguato allo standard di sicurezza, pertanto, anche tenuto conto dell'elevato livello di diligenza (art. 1176, co. 2, c.c., c.d. debitore qualificato) cui sono tenuti gli istituti, la banca veniva condannata al pagamento dei danni patrimoniali e non patrimoniali. La pronuncia in esame può essere vista come un *leading case* sia relativamente alle conoscenze tecniche che emergono dalla stessa, come la nozione tecnica di recente conio *Man In The Browser*, ma soprattutto perché si definisce in modo puntuale il parametro dell'utente medio/cliente comune per valutare la diligenza del correntista.

Più nel merito, si richiamano alcuni assunti della pronuncia:

- la maggior parte delle 13 operazioni di trasferimento del denaro erano avvenute l'11 settembre 2009, l'istituto convenuto era pertanto in forte ritardo nell'adottare le migliori soluzione sui servizi di *home banking*;

- al correntista "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 essersi accorto che possibili mail di apparente provenienza [della convenuta, n.d.r.] fossero in realtà frutto di pirateria informatica e celassero l'intento truffaldino di carpire dati riservati", inoltre, il fatto che la email "che verosimilmente era stata veicolo di della truffa informatica perpetrata, non presentasse palesi evidenze di contraffazione, ciò agli occhi di un cliente comune, di cui non è provata alcuna qualificata competenza".

Ne segue una maggiore certezza per il correntista vittima di frode telematica da *phishing*, non è sufficiente solo analizzare l'idoneità del sistema rispetto agli standard di mercato ma occorre anche che il messaggio di phishing, estendibile alle diverse sue varianti tecniche, sia apparentemente genuino e non riconoscibile rispetto all'utente medio. E' in questo che si coglie l'aspetto più innovativo dell'arresto che ci occupa, nell'approccio del "cliente comune" ossia dell'utente medio non dotato di specifica competenza in ambito informatico né tantomeno nell'"informatica bancaria". Analogamente anche il Tribunale di Firenze appena un mese prima nel pronunciamento del 3 novembre 2014, condannando al risarcimento l'istituto bancario asserisce proprio che l'approccio dell'utente medio è il parametro in base al quale valutare la diligenza dei comportanti del correntista e non degli esperti informatici.

Peraltro, in questo senso si era anche pronunciato il Tribunale di Parma (depositata il 23 luglio 2013) asserendo che nel caso di phishing la banca è tenuta ex art. 1176 c.c. a implementare tutti i presidi necessari al fine di evitare le conseguenze prevedibili illecite intrusioni da parte del proprio sistema informatico. Dall'altra parte, si asserisce che non è sufficiente che l'istituto di credito fornisca prova che l'autenticazione al sistema informatico sia avvenuta correttamente, ossia che l'azione dispositiva di trasferimento sia stata autorizzata con il corretto inserimento dei codici dispositivi.

Invece, "la presunzione di responsabilità contrattuale della parte inadempiente, imposta dall'art. 1128 c.c., può considerarsi superata solo qualora la banca assolva all'onere probatorio posto a suo carico di dimostrare che le credenziali fornite al cliente sono entrate in possesso di terzi per una condotta colposa del cliente".

Pertanto, in base a questa impostazione dell'organo giudicante è l'istituto bancario che deve dimostrare in caso di phishing che vi sia stata una condotta negligente del correntista, impostazione che appare convincente e necessaria tenuto conto che il correntista altro non è che un semplice utente medio. Conclude inoltre il giudicante che "a prescindere da comportanti negligenti dei clienti, deve addossarsi a quest'ultima la conseguente responsabilità ove […] essa non abbia messo a disposizione del proprio clienti idonei accorgimenti tecnici […] o, più semplicemente, ad esempio, quello di conferma dell'ordine impartito (o ricevuto) via Sms".

Peraltro verso, invece, corre l'obbligo di richiamare una importante e recente pronuncia del Tribunale di Roma depositata il 31

agosto 2016, l'organo giudicante si trovava ad affrontare il tema del trattamento illecito dei dati in ambito di *home banking*, infatti, il nesso causale secondo ai sensi degli art. 11, 15 e 31 del Codice della Privacy, derivava dall'omessa adozione dei misure idonee di sicurezza il cui contenuto concreto è determinato in base ad una fonte contrattuale.

Si trattava di una frode molto complessa, non meramente telematica, i frodatori non solo carpivano le credenziali di accesso al sito di *home banking*, ma avendo acquisiti i dati anagrafici dell'utente riuscivano a riprodurre la carta di identità falsa del correntista vittima (si tratta invero di un acquisto non particolarmente difficile da compiere).

Tramite tale carta di identità si recavano presso un *Dealer* telefonico e sostituivano la *SIM Card* del correntista, in tale modo i frodatori ottenevano la *SIM* con il numero telefonico del correntista registrata sul sistema di home banking. A questo punto i frodatore possedevano tutto, credenziali di accesso al sito e *SIM card* del correntista tramite il quale l'istituto comunicava una password "usa e getta", realizzavano in tal modo la frode.

La frode in oggetto è nota almeno dal 2011-2012 in ambito bancario nel nostro Paese, in particolare, il rapporto di ABI LAB titolata *Sicurezza e frodi informatiche in banca* pubblicata nel giugno 2013 si specificava che: "Un'analisi più approfondita merita, invece, la modalità di generazione di *OTP* via *SMS*, scelta come tecnologia di 2° fattore dal 28,6% del campione; più specificatamente, il 75% delle banche ne rende obbligatorio l'utilizzo a tutta la clientela, mentre il restante 25% lascia la scelta a discrezione del cliente. Particolare attenzione è stata rivolta nei confronti di tale tecnologia nel corso degli ultimi mesi, poiché a essa sono associabili i primi (limitati) casi di frode che hanno visto nel 2012 anche il coinvolgimento del *device mobile* nello scenario di attacco messo in atto dai frodatori. Per in dettaglio, in cinque delle banche che ricorrono all'*OTP* via *SMS* come 2° fattore (e soprattutto in fase di autorizzazione di una disposizione), sono stati registrati degli episodi di intercettazione illecita di *SMS*, che ha portato in un numero ristretto di casi alla realizzazione di transazioni fraudolente con una conseguente perdita di denaro per l'utente […] l'intercettazione o inoltro fraudolento degli *SMS* è stato possibile grazie alla disabilitazione illecita dell'utenza telefonica della vittima e all'associazione della stessa di una *SIM Card* attivata dal frodatore".

Nel contesto internazionale tale frode viene denominata come Sim Swap Fraud ovvero frode nella quale viene scambiata la *SIM* (meglio sarebbe dire disabilitata appunto), purtroppo, la complessità

della frode lasciava in molti casi la vittima se non sfornita di tutela in forti difficoltà trovandosi in un vicolo cieco tra l'istituto di credito che negava le proprie responsabilità spostale eventualmente a carico del dealer telefonico.

Più spesso l'istituto di credito cercava direttamente di imputare il danno occorso ad una omessa cautela nella custodia delle credenziali di autenticazione, ma poteva persino spingersi a suggerire al correntista che doveva tutelarsi non con l'istituto di credito ma con il *Dealer* telefonico (negozio di telefonia presso il quale veniva sostituita la *sim card*) oppure con il gestore di telefonia che mediante protocolli di identificazione del cliente, ai quali non erano imposti gli alti standard di sicurezza previsti per il sistema bancario, avevano consentito a terzi la disabilitazione della sim e quindi il compimento della frode.

La difesa degli istituto di credito pertanto poteva essere efficace e sostenere la violazione degli obblighi di custodia del correntista, il quale era anche negligente perché si sarebbe affidato ad un gestore di telefonia non altamente affidabile nei termini sopra descritti; ma queste argomentazioni sono evidentemente carenti sotto l'aspetto del rischio di impresa, infatti, è l'istituto di credito che definisce una strategia di sicurezza informatica del proprio sistema scegliendo l'architettura di sicurezza del proprio sistema informativo, scegliendo per esempio se adottare un *token OTP* (dispositivo fisico generatore delle password usa e getta appunto *One Time Password/OTP*) oppure dando preferenza ad una maggiore usabilità sfruttando per esempio il cellulare del correntista e quindi comunicare le proprie password anche temporanee tra il dispositivo telefonico.

Tuttavia, le normative italiane recepiscono chiaramente un principio di *favor* per il correntista, in base al Titola V del Codice della Privacy (artt. 31 e seguenti) le misure di sicurezza devono essere in linea con il "progresso tecnologico" ossia con i migliori standard di sicurezza del settore bancario, riferibili a qualsiasi titolare del trattamento e quindi anche ai titolare del trattamento che offrono servizi di home banking, i quali in caso non adottino adeguate misure di sicurezza sono da ritenersi soggetti negligenti per aver consentito a terzi di accedere ai dati personali identificativi, economici e quant'altro contenuto nel profilo di home banking del correntista.

Il legislatore nella ratio dell'art. 31 del Codice della Privacy, in combinato disposto con l'articolo 15, ha considerato che l'interessato, tanto più quando è parte contrattuale debole, non può farsi carico dei costi economico-sociali volti a prevenire gli accessi non autorizzati al

sistema informatico dell'istituto di credito titolare del trattamento, né in generale può farsi carico dei rischi d'impresa generati dall'esercente l'attività bancaria equiparata all'attività pericolosa, rimanendo a carico in capo a quest'ultima onere della prova degli eventi interruttivi del nesso causale o quanto meno di aver adottato soluzioni in linea con gli standard di mercato.

Più nel merito, richiamando l'art. 2050 c.c., non volendo accedere all'interpretazione della responsabilità oggettiva, il legislatore ha invero inserito una presunzione di colpa a carico del titolare (l'istituto di credito nel caso specifico) il cui superamento richiede la dimostrare di avere appunto adottato le migliori soluzioni del mercato (*rectius* misure di sicurezza idonee) volte a ridurre al minimo il rischio generato dall'attività, c.d. modello della responsabilità aggravata per colpa presunta, rimanendo del tutto eventuale e residuale la dimostrazione che l'interessato non abbia o meno adottato le minime cautele volte teoricamente a neutralizzare i rischi connessi all'attività.

In tale contesto, l'organo giudicante romano recepisce questo orientamento ed asserisce che "In tema di ripartizione dell'onere della prova, al correntista abilitato a svolgere operazioni "online" che, alla stregua degli artt. 15 del d.lgs. n. 196 del 2003 e 2050 c.c., agisca per l'abusiva utilizzazione (nella specie, mediante illegittime disposizioni di bonifico) delle sue credenziali informatiche, spetta soltanto la prova del danno siccome riferibile al trattamento del suo dato personale, mentre l'istituto creditizio risponde, quale titolare del trattamento di dato, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico mediante la captazione dei codici d'accesso del correntista, ove non dimostri che l'evento dannoso non gli sia imputabile perché discendente da trascuratezza, errore o frode del correntista o da forza maggiore (Cfr. Cass, Sez. 1, Sentenza n. 10638 del 23/05/2016). Viene così a configurarsi un sistema di responsabilità di tipo "semioggettivo", atteso il rinvio all'art. 2050 cod. civ. contenuto nell'art. 15 del codice della privacy, e considerato che il modello di responsabilità è coerente con quello delineato finanche a livello comunitario dall'art. 23 e dal considerando n. 55 della direttiva comunitaria n. 95/46-CE, relativamente alla tutela delle persone fisiche con riguardo al trattamento dei dati personali."

L'interpretazione del Giudicante è pienamente condivisibile per in linea con la lettera della legge, l'onere della prova ai sensi dell'art. 2050 c.c. deve essere necessariamente posto a carico dell'Istituto di credito, altrimenti i rischi di impresa sarebbe distribuiti sui correntisti che sono invece parte debole del rapporto contrattuale, è giusto quindi

che il titolare del trattamento debba dimostrare di aver adottato tutte le misure volte a ridurre al minimo i rischi generati dall'attività.

La recente sentenza del Tribunale di Roma che condanna pertanto i due istituti di credito convenuti, afferma in piena coerenza, con quanto asserito dalla recente Cassazione, che i correntisti vittime di frodi sono tutelati come interessati e quindi come consumatori parti deboli di rapporto contrattuale, in caso di mancanza di prove sull'adeguatezza dei sistema e salvo la dimostrazione del dolo o colpa grave del correntista l'istituto di credito deve essere condanno alla restituzione del danno patrimoniale subito e degli altri danni dimostrati dall'attore.

Normative e documenti di riferimento

d.lgs. 196/2003, artt. 11, 15 e 31

d.lgs. 11/2010, artt. 7 e 12

Codice civile, artt. 1128, 1176 e 2050

Provvedimento Banca d'Italia del 5 luglio 2011, attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti e obblighi delle parti)

ABI LAB, Sicurezza e frodi informatiche in banca, giugno 2013.