ISSN 1825-9871

Università degli Studi di Napoli Federico II
Facoltà di Giurisprudenza

INNOVAZIONE E DIRITTO

Responsabilità degli intermediari bancari e finanziari e sistemi di internet banking: aggressione informatica e protezione del cliente.*

di Marilena Rispoli Farina

ABSTRACT

The paperanalyses the regulatoryprotection of clients whoasusers of paymentserviceswerevictims of IT attackthrough the lenses of banking ADR decisions (so called: Arbitro Bancario Finanziario).

The paperunderlines case law more favourable to the clients and pays a carefulattention to an up-to-date ADR decision (Collegio di Coordinamento, Decision n. 3498 of 28th October 2012) establishingthatany user adhering to a more insidiousform of IT message(so called Man-in-the-brower) wascharged of neglicencewhile the financialintermediarywaslegallyresponsible for anydamagescaused to the client.

SINTESI

L'articolo pone in evidenza l'emergere di un orientamento più favorevole al cliente che sia stato vittima di un'aggressione informatica, nell'applicazione della disciplina sui servizi di pagamento. L' orientamento prevalente dell'Arbitro Bancario Finanziario ha finora sanzionato la condotta dell'utilizzatore del servizio di pagamento che subisca un'aggressione informatica sotto forma di phishing.*Una più recente decisione del Collegio di Coordinamento (Decisione*

n.3498 del 28 ottobre 2012) ha considerato colpa lieve (e non colpa grave) l'avere

* Articolo sottoposto a revisione

n.3498 del 28 ottobre 2012) ha considerato colpa lieve (e non colpa grave) l'avere

aderito ad un messaggio informatico particolarmente insidioso (Man in the browser) con conseguente ricaduta sull'intermediario della responsabilità per i danni derivanti dall'operazione fraudolenta posta in essere a carico del cliente.

SOMMARIO:1.Premessa - 2.- Gli obblighi di comportamento del cliente.– 3. Responsabilità della banca e del cliente. nelle operazioni *on line* -4 Distribuzione del rischio e onere della prova nelle operazioni contestate 5.- Il cd principio di inversione dell'onere della prova. .Portata e fondamento –- 6 Le decisione dei collegi in tema di phishing 7. Il caso del *Man in the browser* e la decisione del Collegio di coordinamento.

1. Premessa

La problematica relativa alla responsabilità degli intermediari in casi di frodi informatiche, realizzate mediante forzatura dei sistemi di pagamento elettronici, con particolare riguardo al cd "phishing, "è stata poco approfondita in sede dottrinale [1]. Si deve in particolare alla

* I contenuti del presente scritto esprimono opinioni personali e non sono riconducibili in alcun modo all'Arbitro Bancario Finanziario di cui l'Autore fa parte.

1)Il **phishing** è un tipo di *truffa* effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando la posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS .La prima menzione registrata del termine phishing è sul newsgroup di Usenet *alt.online-service.america-online* il 2 gennaio 1996, malgrado il termine possa essere apparso precedentemente nell'edizione stampata della rivista per hacker *2600*. Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese) probabilmente influenzato da *phreaking* e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente. La parola può anche essere collegata al linguaggio leet, nel quale la lettera f è comunemente sostituita con ph. ^ *"phish, v." OED Online, March 2006, Oxford University Press.* su *Oxford English Dictionary Online.* URL ^ Ollmann, Gunter, *The Phishing Guide: Understanding and Preventing Phishing Attacks* su *Technical Info.* URL consultato il 10 luglio 2006.^ *Spam Slayer: Do You Speak Spam?* su *PCWorld.com.* URL consultato il 16 agosto 2006.^ *"phishing, n." OED Online, March 2006, Oxford University Press.* su *Oxford English Dictionary Online.* URL consultato il 9 agosto 2006.^ *Phishing* su *Language Log, 22 settembre 2004.* URL^ Anthony Mitchell, *A Leet Primer*, TechNewsWorld, 12 luglio 2005.^ *Know your Enemy: Phishing* su *The Honeynet Project & Research Alliance.* URL consultato l'8 luglio 2006.^ F.Cajani, G. Costabile, G. Mazzaraco, *Phishing e furto d'identita digitale. Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008^ Tribunale di Milano, sentenza del 10.12.2007 - est. Gamacchio (Giudice per l'udienza preliminare): cfr. R. Flor, *Frodi identitiarie e diritto penale*, in *Riv. giurisp. econ. az.*, 2008, 4, p. 184; A. Sorgato, I*l reato informatico: alcuni casi pratici*, in *Giur. pen.*, 2008, 11, p. 40^ L. Fazzo,«Ecco come noi hacker romeni vi svuotiamo i conti bancari», in *Il Giornale*, 11 dicembre 2007^ Tribunale di Milano, sentenza del 29.10.2008, est. Luerti (Giudice per l'udienza

giurisprudenza dell'Arbitro bancario e finanziario il merito di aver adottato numerose decisioni sul tema, in concomitanza con l'entrata in vigore del Dlgs n.11 del 2010, che ha dato attuazione alla Direttiva sui servizi di pagamento[2] e che ha introdotto, agli artt.7-12.[3], un'articolata disciplina della prestazione dei servizi di pagamento, soffermandosi in particolare sugli obblighi cui sono tenuti, da un lato, gli intermediari, dall'altro i clienti. Il decreto ha dettato apposita disciplina della responsabilità del prestatore di servizi di pagamento per le operazioni non autorizzare (art.11).

2.- .- *Gli obblighi di comportamento del cliente*.–Vi è da rilevare che, in una prima fase di applicazione della nuova normativa, i Collegi ABF, affrontando la soluzione di controversie relative a phishing, hanno sanzionato il comportamento dei clienti, che avendo incautamente "abboccato" al phishing si sono resi colpevoli di non aver diligentemente adempiuto agli obblighi di custodia e conservazione degli strumenti di pagamento, sanciti in particolare all'art.

preliminare) in *Corr. Mer.*, 2009, 3, pp. 285 e ss. con nota di F. Agnino, *Computer crime e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*^ L. Ferrarella , Soldi trasferiti online. «È riciclaggio», in *Corriere della Sera*, 7 gennaio 2009^ F. Tedeschi, Lotta al cybercrime. Intervista esclusiva al magistrato a caccia delle nuove mafie^ AMATO G., DESTITO V., DEZZANTI G., SANTORIELLO C., I reati informatici, Cedam, 2010 S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer Forensics e indagini digitali*, Experta, 2011.

[2] Si tratta della direttiva 2007/64/CE del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE e 2006/48/CE, che abroga la direttiva 97/5/CE, pubblicata nella G.U.C.E., 5.12.2007, L139. Per un'illustrazione degli obiettivi e dei principali contenuti della PSD si rinvia a MAIMERI, I Rulebook della SEPA: natura e funzioni, in *Quaderni di Ricerca Giuridica e della Consulenza Legale della Banca d'Italia* n. 63,Roma, Dicembre 2008, 123 ss.;O. TROIANO, *La nuova disciplina privatistica comunitaria dei servizi di pagamento: realizzazioni e problemi della Single Euro Payments Area, in Quaderni di Ricerca Giuridica e della Consulenza Legale n. 63,* cit., 41 ss.;MANCINI, *I sistemi di pagamento retail verso la Single Euro Payments Area (SEPA),* in *Quaderni di Ricerca Giuridica della Consulenza Legale* n. 63,cit., 243 ss.Cfr. anche MODIANO*, Le banche italiane verso la SEPA e la direttiva sui servizi di pagamento,* in *Bancaria*, 2008 10, 12;O. TROIANO, *Contratti di pagamento e disciplina privatistica comunitaria (proposte ricostruttive con particolare riferimento al linguaggio e alle generalizzazioni legislative*), in *Banca borsa*, 2009, I, 520 ss.;GRANIERI, *Le liberalizzazioni nel sistema dei servizi di pagamento e l'impatto della direttiva comunitaria sull'industria delle carte di credito. Alcune riflessioni preliminari*, in *Alcune riflessioni preliminari*, in MANCINI, PERASSI (a cura di), *Il nuovo quadro normativo comunitario dei servizi dipagamento. Prime riflessioni,* Roma, 2006, 97 ss. RISPOLI FARINA-SANTORO-SCIARRONE ALIBRANDI TROIANO (a cura di), *Armonizzazione europea dei servizi di pagamento e attuazione della direttiva 2007/64/CE*, Milano, 2009.

[3] Il d.lgs. 27 gennaio 2010, n. 11 pubblicato sulla *G.U.* 13 febbraio 2010, n. 36, entrato in vigore il 1 marzo 2010, attua nel nostro ordinamento la direttiva 2007/64/CE. Il d.lgs. n. 11/2010 ha modificato in parte la disciplina del t.u.l.b., inserendo nello stesso il nuovo Titolo V-*ter,* rubricato «Istituti di Pagamento» (Titolo II della Direttiva), il Capo II-*bis* sui «Servizi di pagamento» nel Titolo VI – «Trasparenza delle condizioni contrattuali» (Titolo III della Direttiva), nonchè nuove disposizioni riguardanti diritti ed obblighi dei destinatari della disciplina *de quo* e delle loro controparti contrattuali (Titolo IV della Direttiva), che compongono un *corpus* normativo autonomo, ed attribuendo alla Banca d'Italia il compito di emanare la disciplina di dettaglio..

Per un *Commento* al dlgs, n.11, si veda MANCINI RISPOLI FARINA. SANTORO SCIARRONE ALIBRANDI TROIANO (a cura di*), La nuova disciplina dei servizi di pagamento, Torino* ,Giappichelli, 2011.

7 del Dlgs n.11 del 2010 di attuazione della direttiva sui servizi di pagamento. Questi sono individuati e si concretizzano nella fase di attuazione del rapporto :a) nell'utilizzare lo strumento di pagamento in conformità a quanto prestabilito nel contratto quadro; b) nel comunicare senza indugio al prestatore del servizio di pagamento lo smarrimento, il furto l'appropriazione indebita o l'uso non autorizzato dello strumento appena ne venga a conoscenza. In via preliminare, l'utilizzatore, appena ricevuto lo strumento di pagamento, deve adottare tutte le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentano l'uso.[4] L'obbligo di custodire in condizioni di sicurezza i codici personalizzati, come rileva la Relazione illustrativa al decreto, è stato ritenuto applicabile alle operazioni on line. D'altro canto rileva l'art. 8 del d.lgs. 11/2010, il quale pone a carico del prestatore dei servizi di pagamento l'obbligo di assicurare che i dispositivi personalizzati non siano accessibili a soggetti diversi dall'utilizzatore. La banca, predisponendo misure di protezione idonee ad evitare l'accesso fraudolento di terzi ai depositi dei clienti o a neutralizzarne gli effetti, deve adempiere all'obbligo di custodia dei patrimoni dei clienti con la diligenza professionale richiesta dall'art. 1176 c.c., diligenza che, parametrata alla specificità del servizio di *home banking*, implica l'adeguatezza agli standard esistenti dei presidi adottati per la inviolabilità delle transazioni *on-line* da attacchi di pirateria informatica.[5]

Va precisato tuttavia che, richiamando i principi in tema di onere della prova, i Collegi hanno ritenuto che il rischio di frode informatica mediante *phishing* non possa essere posto a carico del cliente, a meno che l'intermediario non dimostri che sia a lui imputabile un difetto di prudenza o di diligenza nella conservazione e custodia dei propri dati personali. Tale negligenza, peraltro, non può essere dedotta dalla semplice constatazione che le operazioni fraudolente sono state disposte con l'utilizzo delle credenziali del cliente. È necessario piuttosto che la banca dimostri una vera e propria condotta negligente del cliente, contestando in primo luogo le sue affermazioni in merito all'utilizzo di un *computer* adeguatamente protetto e all'assenza di una

[4] si veda PIRONTI, *Commento all'art.7* in MANCINI –RISPOLI FARINA –V. SANTORO- SCIARRONE ALIBRANDI –O.TROIANO (a cura di), *La nuova disciplina dei servizi di pagamento,* Torino ,Giappichelli, 2011,cit,,115.

[5] si vedano TROIANO PIRONTI , *Commento all'art.8,* in MANCINI RISPOLI FARINA. SANTORO SCIARRONE ALIBRANDI TROIANO (a cura di*), La nuova disciplina dei servizi di pagamento, Torino* ,Giappichelli, 2011,119 ss.

qualsivoglia responsabilità in merito alla divulgazione dei suoi dati personali [6]. Numerose decisioni hanno così affermato che rispondendo al messaggio di phishing, trasmettendo i propri dati personali (codici, password etc) i clienti abbiano violato l'obbligo di custodia dei dati personali di cui all'art.7 del dlgs.n.11.Hanno altresì rilevato che non siano state adottate le m isure idonee a garantire la sicurezza degli strumenti (pc; siti protetti, etc).

3.- *Responsabilità della banca e del cliente nelle operazioni* on line.-Più in generale va detto che si è creato un consolidato orientamento dell'ABF, relativo all'utilizzazione di canali di pagamento *online* da parte degli intermediari, per il quale si è posto l'accento sugli obblighi di diligenza e custodia del cliente che debbono estendersi a tutto ciò che rientra nella sua sfera di controllo, ivi compresa la dimostrazione di avere adottato tutti gli accorgimenti necessari ad evitare il verificarsi di episodi di utilizzo fraudolento degli strumenti di pagamento. In particolare, il cliente ha l'obbligo di diligente custodia della carta e dei codici identificativi, dovendo anch'egli essere consapevole della delicatezza dei mezzi telematici e della possibilità che, attraverso di essi, siano perpetrate frodi di varia natura. Dall'altro, molta attenzione è posta sugli obblighi dell'intermediario che, nell'offrire tali servizi, deve adempiere il proprio compito di custodia dei patrimoni dei clienti con la diligenza professionale e qualificata richiesta dall'art. 1176, comma 2, c.c. predisponendo misure di protezione adeguate rispetto agli standard esistenti, anche sotto il profilo dei presidi tecnici adottati [7].Conformemente alla disciplina del decreto, è stata riconosciuta, ad esempio, la responsabilità del cliente nel caso in cui i codici e la carta siano stati conservati unitamente, oppure nel caso questi abbia comunicato a un terzo il numero della propria carta di credito. Il cliente, in sintesi , deve attuare tutte le cautele del caso nei confronti di comunicazioni anomale che richiedono fraudolentemente la digitazione dei propri codici identificativi personali.. È stata riconosciuta la responsabilità dell'intermediario, altresì, per non avere predisposto sistemi automatici di blocco delle operazioni anomale realizzate tramite internet, dovendo ritenersi tali, ad esempio, una serie di ricariche telefoniche su numeri diversi, per un importo elevato, nel giro di poche ore. Analogamente, l'intermediario è stato ritenuto

[6] V. Collegio di Roma, dec. n. 289/2010.

[7] Sul punto v., Cass., 12 giugno 1996, n. 5409; Cass., sez. I, 24 settembre 2009 n. 20543; sul consolidato orientamento dell'ABF, v. *ex multis*, Collegio di Milano, decisione n. 87/2010; Collegio di Napoli, decisione n. 688/10; Collegio di Milano, decisione n. 1407/2010.

responsabile nel caso in cui non era stato adottato un terzo livello di protezione, quali le serie numeriche casuali generate da dispositivi elettronici, ovvero per non avere previsto l'invio di sms di avviso dell'esecuzione dell'ordine [8] .Secondo orientamenti consolidati della giurisprudenza, la diligenza che la banca deve impiegare nel consentire al cliente l'utilizzo di strumenti di pagamento online, deve avere riguardo non solo all'attività di esecuzione di contratti bancari in senso stretto, ma deve anche essere «in relazione ad ogni tipo di atto od operazione che sia comunque oggettivamente esplicato presso una struttura bancaria e soggettivamente svolto da un funzionario bancario. Tale diligenza va valutata, non alla stregua di criteri rigidi e predeterminati, ma tenendo conto delle cautele e degli accorgimenti che le circostanze del caso concreto suggeriscono» [9].In alcuni casi, tuttavia, la violazione degli obblighi di diligenza da parte dell'intermediario non vale ad escludere la colpa concorrente del cliente, ex art. 1227 c.c. [10]. Laddove quest'ultimo non dimostri di avere custodito con la necessaria diligenza i codici di accesso al conto online, è ragionevole ritenere che una condotta più accorta avrebbe impedito il verificarsi dell'evento fraudolento. Circa la valutazione del sistema di sicurezza dell'intermediario, va fatto riferimento altresì agli standard di sicurezza indicati dalla Banca d'Italia nelle diposizioni attuative del d.lgs. n. 11/2010 (in particolare, del Titolo II). Come richiesto dal c.d. schema di "conformità estesa", la banca deve adottatore per l'operatività online una metodologia a due fattori, scelti fra i seguenti tre: qualcosa che l'utente conosce (ad esempio, password/pin); qualcosa che l'utente possiede (es.: smart card, token, one time password, sim cellulare); qualcosa che l'utente è (ad esempio, caratteristiche biometriche). Tali fattori di autenticazione «devono essere tra loro indipendenti in maniera che la compromissione dell'uno non comprometta anche l'altro fattore». Sebbene le modalità "non hardware" di generazione delle one time password siano riportate conclusivamente nella elencazione di cui al documento appena citato, va evidenziato come esse certamente offrano minori garanzie di sicurezza. Inoltre, a prescindere dagli accorgimenti tecnici di protezione, il documento prevede, altresì, che le transazioni siano continuativamente monitorate per riscontrare eventuali anomalie che possano essere indice di attività illecite di frode o riciclaggio. Per altro verso, la predisposizione da parte dell'intermediario di presidi di sicurezza rafforzati ma che riguardino solo determinate operazioni di pagamento (quali, ad esempio, ricariche online, pagamento bollettini ecc.) o siano "facoltativi" richiedono anzitutto un'adeguata e riscontrabile

[8] Cfr. BANCA D'ITALIA, *Sintesi dell'attività*, cit., p. 4.

[9] V. Cass., sez. I, 24 settembre 2009 n. 20543; ma anche Cass., sentenze nn. 13777/07, 11382/02, 6756/01.

[10] Cfr. Collegio di Milano n. 46/2010; n. 87/10; Collegio di Roma n. 33/2010.

informazione ai clienti. I sistemi non obbligatori, inoltre, evitano di rendere cogente e operativo un livello di protezione idoneo ad evitare accessi fraudolenti [11]. La disciplina di base del decreto integrata dalle Disposizioni dell'Autorità di vigilanza che hanno completato il quadro delineato dalle norme della direttiva. [12] costituisce per gli intermediari un indiscutibile quadro di riferimento.

4.- *Distribuzione del rischio e onere della prova nelle operazioni contestate.* Una delle questioni più rilevanti ai fini della soluzione dei casi di utilizzo fraudolento di strumenti di pagamento attiene alla distribuzione del rischio e all'onere della prova nelle ipotesi di operazioni realizzate tramite un conto corrente con funzionalità *online* [13]. Si ritrovano sovente, nelle condizioni contrattuali degli intermediari coinvolti, anacronistiche disposizioni relative alla prestazione del servizio di *internet banking*, secondo la quale sono rimesse a carico del cliente le conseguenze dannose rivenienti "dall'utilizzo illegittimo dei codici, nonché dal loro smarrimento o sottrazione". È evidente come tale disposizione non offra adeguata soluzione al problema della distribuzione tra i due contraenti del rischio e delle responsabilità connesse agli eventuali utilizzi fraudolenti dello strumento di pagamento (come segnalato ampiamente anche dalla dottrina che si è occupata del tema). Tali regole delineano uno schema piuttosto articolato in cui il confine tra la responsabilità del cliente e quella della banca è segnato da due elementi: la tempestiva notifica all'emittente della perdita o del furto della carta e/o dei codici personali, nonché di addebiti erronei o non autorizzati o di ogni altra irregolarità nella gestione del conto, da un lato; la "colpa" (di fatto, presunta) dell'utente nella custodia dei codici, dall'altro.

Trattandosi, inoltre, di responsabilità contrattuale, l'onere di provare la non imputabilità dell'inadempimento, ad avviso dei Collegi ABF, grava sull'intermediario che con il contratto ha assunto l'obbligo di assicurare al proprio cliente il corretto svolgimento del servizio. Non fornirebbe, infatti, alcun riscontro probatorio in tal senso, la mera affermazione che le operazioni eventualmente disconosciute siano avvenute previa corretta utilizzazione dei dati

[11] Sul punto, v. decisione del Collegio di Napoli del 29/11/2011; Collegio di Milano, decisione n. 1411/11.

[12] Si veda Il Provvedimento *Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi a pagamento (Diritti ed obblighi delle parti*). (11A10113) (GU Serie Generale n.176 del 30-7-2011).

[13] Per alcune considerazioni critiche sul regime di responsabilità, v. TROIANO, CUOCCI, *Commento* sub *art. 11,* in AA.VV., *La nuova disciplina dei servizi di pagamento*, cit., p. 137 ss.; TROIANO, CUOCCI, PIRONTI, *Commento* sub *art. 12,* in AA.VV., *La nuova disciplina dei servizi di pagamento*, cit., p. 143 ss.

identificativi (*user-id*, *password*, numero e scadenza della carta) ivi compreso il c.d. codice di sicurezza della carta (CVV2). Tale circostanza, infatti, non autorizza a ritenere che la frode sia riconducibile ad un comportamento, commissivo o omissivo, del titolare dello strumento di pagamento e ad integrare quindi le ipotesi di dolo o colpa grave, previste dal d.lgs. n. 11/2010 e necessarie per imputare al cliente le operazioni disconosciute o compiute in maniera fraudolenta [14].

Come accennato il d.lgs. n. 11/2010, pur recependo in larga parte gli indirizzi già affermatisi nella prassi contrattuale, assicura una tutela più incisiva dell'utente di servizi di pagamento, in specie se consumatore. Il complessivo quadro normativo avvalora pertanto l'idea, già elaborata in dottrina, di una c.d. responsabilità da *status* in capo all'intermediario che – in considerazione della propria elevata professionalità – sarebbe tenuto ad adottare le misure e gli standard di sicurezza più idonei a garantire la clientela.

Per altro verso, la complessità nella definizione dell'assetto contrattuale per l'utilizzazione di strumenti di pagamento emerge, con tutta evidenza, per quanto attiene sia alla valutazione del comportamento del cliente, sia della banca, nonché degli assetti organizzativi adottati a tutela della sicurezza delle transazioni.

Ai fini della determinazione del rimborso, si può fare riferimento al principio di cui all'art. 1711 c.c. in considerazione della evidente mancanza di un ordine imputabile al cliente mandante, con il conseguente addossamento all'intermediario delle operazioni disconosciute.

Infine, nell'ambito delle controversie relative all'utilizzo fraudolento di strumenti di pagamento, notevole rilevanza assumono, le circostanze fattuali che caratterizzano la fattispecie; in tal senso, rilevano, ad esempio: 1) l'unicità dell'episodio contestato; 2) il lasso temporale – più meno breve – di perpetrazione della frode; 3) il dato statistico sulla movimentazione della carta; 4) la sussistenza di operazioni non contestate che intervallano la sequenza di operazioni asseritamente fraudolente.

5.- *Il cd principio di inversione dell'onere della prova .Portata e fondamento Il* decreto n. 11, va infatti precisato, riafferma un importante principio, contenuto nell' art.59 della Direttiva e poi traslato nel dlgs n.11del 2010 di attuazione della stessa, per il quale (Art. 10, comma 2.) "Quando l'utilizzatore 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

[14] Così, sul punto, Collegio di Roma, decisione n. 561/2010.

pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo né 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".Pertanto, ai fini di escludere la propria responsabilità per i danni derivanti dall'uso non autorizzato dello strumento di pagamento, la banca (il prestatore dei servizi di pagamento) non può simpliciter affermare, come ha fatto di regola prima della introduzione della nuova disciplina, che essendo stata l'operazione compiuta adoperando i codici del cliente, e constando un sistema di protezione, si debba presumere che i sistemi di sicurezza non siano stati diligentemente custoditi dal cliente.[15]

La nuova disciplina dei servizi di pagamento prevede come si è detto, una sorta di inversione dell'onere della prova a carico del prestatore del servizio di pagamento che deve *dimostrare i*l dolo o la colpa grave del cliente nell'utilizzo dello strumento di pagamento, con particolare riguardo alla violazione degli obblighi di custodia sanciti dal decreto. Si discute del fondamento di tale principio. La dottrina, e la giurisprudenza dell'Abf hanno in merito ricordato che il principio di distribuzione del rischio, nel regime dei servizi di pagamento appare decisamente squilibrato *a* favore dell'utilizzatore del servizio di pagamento. Tale assetto avrebbe il suo fondamento nella maggior capacità economica dell'intermediario di sostenere il rischio connesso all'impiego di strumenti la cui sicurezza assoluta non è stata sin qui raggiunta (e probabilmente non verrà mai raggiunta dato l'inarrestabile evolversi della tecnologia civile e la naturale "rincorsa" della tecnologia criminale nella stessa direzione), grazie ad una distribuzione dei relativi costi sull'intero pubblico dell'utenza.[16] Principio che il Collegio di Coordinamento

[15] Sulle norme sopra richiamate v. PIRONTI, *Commento* sub *art. 7*, in AA.VV., *La nuova disciplina dei servizi di pagamento*, cit., p. 113 ss.; TROIANO, *Commento* sub *art. 10*, in AA.VV., *La nuova disciplina dei servizi di pagamento*, cit., p. 159 ss.

[16] La problematica è stata posta più volte all'attenzione della giurisprudenza ordinaria.Vale ricordare la sentenza del 2 ottobre 2012 del Tribunale di Verona, che ha esaminato diversi profili di interesse in materia di *home banking,* con particolare riferimento alla responsabilità della banca in caso di frodi informatiche (c.d. phishing) ed agli obblighi di controllo delle parti.(In *Dirittobancario, it, 2013*) Per quanto attiene il primo profilo, il Tribunale di Verona ha ritenuto fondata la responsabilità della banca in ragione della mancata adozione delle misure necessarie a garantire al cliente la sicurezza del servizio.I n tal senso, nel caso di specie, la banca si era limitata a predisporre la consegna, al momento dell'attivazione del servizio di home banking, di un codice utente e di una password di accesso da modificare al momento del primo accesso .Come evidenziato dal Tribunale, numerosi erano i dispositivi più sicuri che la banca avrebbero potuto offrire al cliente, fra cui il servizio di "sms-alert" e la c.d. chiave elettronica o token, ovvero altri che richiedono l'inserimento, oltre che del codice identificativo e del pin, o di una password, al momento di accedere al servizio, anche di un'ulteriore password, al momento di effettuare le singole disposizioni (c.d. password dispositiva), prevedendo spesso anche che quest'ultima credenziale sia cambiata periodicamente dall'utente.

dell' ABF ha di recente (si veda la decisione n 3498 del 2012) ritenuto di pienamente condividere, soggiungendo che l'addossamento del rischio all'intermediario (il cui estremo confine si colloca all'altezza della colpa grave dell'utente) appare sempre più giustificato dalla

Per quanto attiene il secondo profilo, il Tribunale ha evidenziato come, in difetto di una specifica previsione normativa o contrattuale, non sia configurabile un obbligo in capo alla banca di monitorare in via continuativa i movimenti di conto corrente, finalizzato a vagliarne entità e frequenza sì da prevenire eventuali frodi informatiche. Una simile attività di controllo appare infatti inesigibile stante l'impossibilità per la banca di operare una selezione tra la miriade di flussi di dati elettronici che affluiscono ad essa nell'arco delle ventiquattro ore. Al contempo, pur dovendosi riconoscere al servizio di home banking un'indubbia funzione informativa per il cliente – il quale può verificare, praticamente in tempo reale, le movimentazioni che vengono registrate nel conto, avvedendosi di eventuali errori o ritardi ai propri danni e ponendovi rimedio dandone tempestivo avviso all'istituto di credito – deve escludersi l'esistenza di un simile obbligo di controllo per il correntista e, conseguentemente, la sussistenza di un eventuale concorso di responsabilità laddove, in ipotesi di frodi informatiche, questo controllo non venga dallo stesso cliente esercitato.Si veda anche la sentenza n. 14533 del 4 dicembre 2014, del Tribunale di Milano, analogamente concernente la responsabilità della banca nella prestazione del servizio di home banking, con particolare riguardo all'ipotesi in cui il cliente sia vittima di "phishing" , individuato come "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 e la cui modalità sono per lo più ascrivibili 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".
Nel caso di specie, il cliente lamentava il fatto che, già dal 2005, le principali banche, in contesto europeo, asiatico e statunitensi, avevano iniziato ad adottare il sistema di autenticazione OTP (One Time Password, con password valida per pochi secondi) nel servizio bancario on line, e che già nel 2007 in Italia erano svariate le banche che avevano proceduto in tal senso.A fronte di tali circostanze il Tribunale ha ritenuto che nel 2009, epoca delle operazioni di pirateria informatica oggetto di controversia, la banca fosse gravemente in difetto 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 dal phishing e dai programmi spia.Laddove quindi nel contratto la banca si era assunta l'obbligo di garantire la sicurezza del sistema mediante idonei sistemi di crittografia dei dati di riconoscimento dell'utente, la stessa, non ignara delle modalità di frode mediante phishing da tempo note nel settore, era tenuta ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza informatici, altrettanto noti, idonei a contrastare il fenomeno. Diversamente, non poteva 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 Poste fossero in realtà frutto di pirateria informatica e celassero l'intento truffaldino di carpire dati riservati.*(*in *Diritto Bancario*,it ,2014

forte e incessante promozione all'uso di tali strumenti da parte degli intermediari bancari, in un più generale contesto che sempre più ne impone l'adozione (si ponga mente, fra tante nuove ipotesi, soltanto all'obbligo per le imprese e i professionisti di operare i pagamenti tributari on line e non più allo sportello). dei relativi costi sull'intero pubblico dell'utenza.

La decisione n 3498 del 2012 del Collegio di coordinamento ha ritenuto di pienamente condividere tale impostazione, soggiungendo che l'addossamento del rischio all'intermediario (il cui estremo confine si colloca all'altezza della colpa grave dell'utente) appare sempre più giustificato dalla forte e incessante promozione all'uso di tali strumenti da parte degli intermediari bancari, in un più generale contesto che sempre più ne impone l'adozione (si ponga mente, fra tante nuove ipotesi, soltanto all'obbligo per le imprese e i professionisti di operare i pagamenti tributari on line e non più allo sportello). Poichè siffatta promozione comporta obiettivamente un sensibile beneficio economico per gli stessi intermediari, ha affermato il Collegio,consentendo loro significativi ed evidenti risparmi rispetto ad una tradizionale operatività di sportello, appare equo trovare un correlato *pendant* proprio nel trasferimento, in capo allo stesso intermediario che gode di quel beneficio, altresì del rischio portato dall'impiego dello strumentario tecnologico da cui quello stesso beneficio deriva (con i soli estremi limiti, beninteso, della frode del dolo o della colpa grave ascrivibile all'utilizzatore)".

6.- *Le decisione dei Collegi Abf in tema di phishing* .La decisione in parola, (che affronta tuttavia una ipotesi peculiare di phishing denominata *Man in the browser*)rappresenta l'evoluzione di orientamenti precedenti dei Collegi Abf , che vanno distinti a seconda che la banca adotti o meno dei presidi di sicurezza per così dire rafforzata, ovvero di strumenti di protezione dei siti e degli strumenti di pagamento che non possano impedire del tutto le intrusioni, possano quanto meno renderle molto difficili. Infatti i Collegi hanno rilevato che non è da escludere – in considerazione dell'adozione del *token* e in mancanza di ulteriori elementi di fatto – che il ricorrente sia rimasto vittima di una frode informatica, probabilmente effettuata tramite l'installazione inconsapevole sul proprio PC di *malware* in grado di catturare le credenziali per l'accesso al conto *on line*, ma non ritiene che sia il cliente a dovere chiarire se e di che tipo di frode si tratti.

In relazione a tali casi, in cui pure la banca adottava un sistema di autenticazione a due fattori con un generatore OTP, si segnalano alcuni precedenti, in particolare la decisione n.822/ 2014

del collegio di Milano il quale ha assunto deliberati di accoglimento delle richieste di rimborso dei clienti per operazioni non autorizzate.

Va allora ricordato che, precedentemente, secondo il Collegio di Milano, la pressoché totale invulnerabilità del sistema a "due fattori" garantita dai sistemi OTP appariva tale da fondare la presunzione di una colpa grave in capo al cliente, precisamente consistente nel non aver custodito con la dovuta diligenza il dispositivo in questione (cfr., fra le moltissime,Collegio Milano, decc. nn.2103/2012, 2658/2011, 462/2012).

Siffatto orientamento riposa sull'assunto per il quale, allo stato attuale dell'evoluzione delle tecnologia, l'autenticazione a due fattori con metodo OTP risulterebbe la più sicura possibile sicché diviene giocoforza concludere che, ove tale sistema risulti adottato, l'intrusione non si sia resa possibile se non attraverso la cooperazione, pur involontaria, del cliente, traducentesi nella mancata custodia dei codici e dei dispositivi di autenticazione ovvero nell'ingenua trasmissione degli stessi a terzi. Detto orientamento è stato, in tempi più recenti (cfr. dec. 1583/2012), non pienamente condiviso dal Collegio di Napoli, il quale, pur ammettendo la spiccata capacità protettiva del sistema OTP, ha escluso l'automatismo deduttivo cui si ispira invece il pensiero del Collegio milanese, per concludere che l'impiego dell'OTP non vale di per sé a lasciar irreversibilmente presumere una negligenza comportamentale del cliente, bensì a indurre l'Arbitro ad una valutazione più rigorosa della sua condotta.

Il Collegio di Roma ha, a sua volta, ripreso la lettura del Collegio di Napoli ponendo una speciale enfasi sul principio di diritto ricavabile dalle anzidette norme del d. lgs. citato

La ripartizione dell'onere probatorio, per come delineata nell'impianto normativo, non consentirebbe, secondo l'Arbitro romano, di pervenire all'automatismo affermato dal Collegio di Milano, dovendosi al contrario apprezzare, oltre al meccanismo offerto, anche l'intero sistema di controlli approntato dall'intermediario, e potendosi con ciò concludere che la cattura dei codici ad opera di terzi non autorizzati ben possa avvenire in presenza di un pur diligente comportamento da parte del Cliente (Cfr. Collegio Roma, decc. nn.2264/2012, 2660/2012, 1910/2012).

In particolare, in un caso nel quale il sistema di sicurezza approntato dall'intermediario contemplava un'autenticazione mediante l'uso di un lettore di *smartcard*, non azionabile dunque in difetto della carta, mentre il cliente aveva "abboccato" ad un contestuale *phishing* operato da terzi mediante la proiezione di una finestra a comparsa (c.d. *pop-up*)che richiedeva l'inserimento delle credenziali (OTP comprese), il Collegio romano è giunto ad affermare una colpa

concorrente dell'intermediario desumendola dalla accertata ripetitività di simili intrusioni, come tali testimoni di una inadeguatezza o lacunosità dei presidi di sicurezza predisposti.Questo progressivo spostamento del metro valutativo nella direzione di una ampia ed efficace protezione del cliente si spiega alla luce della parallela evoluzione dei metodi di aggressione informatica, la cui sofisticazione induce a porre in discussione non già il più generale principio di ragionevole esigibilità delle contromisure di sicurezza da predisporsi a cura intermediari, quanto ad affermarlo secondo un nuovo stile ma di giudizio aggiornato all'evoluzione del fenomeno criminale e alla sua nuova capacità offensiva.

7.-- *Il caso del Man in the browser e la decisione del Collegio di coordinamento.*

Il caso specifico affrontato dal Collegio di coordinamento, vede coinvolta in qualità di ricorrente un'azienda agricola, indubbiamente qualificabile come microimpresa nel senso di cui all'art. 1 comma1°, lett. t) del d. lgs. 27 gennaio 2010 n. 11 attuativo della Direttiva 2007/64/CE in materia di servizi di pagamento, meglio nota quale Direttiva PSD. La Direttiva citata, infatti ha inteso predisporre più incisive forme di tutela per il cliente consumatore e per la microimpresa.[17]. L'art. 126-*bis* , disposizione contenuta nel Capo II-*bis* del Testo Unico bancario –che detta disposizioni di carattere generale[18] –nell'operare la definizione del campo di applicazione oggettivo e soggettivo della disciplina di trasparenza per i servizi di pagamento ha esteso l'applicazione delle norme in questione alle micro-imprese, oltre che ai consumatori nonché la possibilità di deroga alla disciplina predisposta, se l'utente non è un consumatore o una micro-impresa (artt. 30, 1°, 2° co., PSD).

La questione affrontata, di cui pare utile rappresentare le caratteristiche principali, concerne la stipula con la resistente di un contratto di conto corrente bancario e contestualmente il correlato contratto di "Multicanalità integrata" per il servizio di *home banking*, all'attivazione del quale al cliente vengono consegnate le credenziali per l'accesso al servizio (codice utente e password di accesso per accedere a tutti i servizi bancari sia via internet che via telefonica) unitamente alla chiavetta elettronica generatrice di password monouso per l'effettuazione di operazioni dispositive.

[17]RISPOLI FARINA, *Note a margine della disciplina di trasparenza dei servizi di pagamento*,in M. Campobasso - V. Cariello - V. Di Cataldo F. Guerrera - A. Sciarrone Alibrandi *Liber amicorum* Pietro Abbadessa, 3 Banche - SOCIETÀ, BANCHE E CRISI D'IMPRESA, III, Banche - Mercati finanziari - Crisi d'impresa, UTET GIURIDICA,Torino, 2014, 2395.

[18] Riflette la formula "Regole generali" del Capo I, del Titolo III della direttiva PSD. Si veda SCIARRONE ALIBRANDI, *sub* art. 126-*bis*, in PORZIO, BELLI, LOSAPPIO, MARILENA RISPOLI FARINA, SANTORO, *Testo Unico Bancario*, *Commentario*, 2010, cit., 1079.

Nell'utilizzazione del servizio di *home banking* per effettuare un bonifico, dopo aver inserito le credenziali di accesso e la password monouso secondo le usuali modalità, la cliente constatava che esso risultava bloccato. Nel corso di un successivo accesso, avvenuto qualche ora dopo, apprendeva che era stato disposto un bonifico mai autorizzato di notevole valore a favore di una sconosciuta società estera. Nell'immediatezza dell'accaduto, il titolare della ricorrente provvedeva ad informare la resistente tramite numero verde chiedendo il blocco del pagamento senza, tuttavia, ottenerlo.

L'indomani il titolare contestava quanto accaduto presso la locale filiale della resistente dove veniva informato che quanto occorso poteva costituire un caso di frode. Nelle circostanze il personale provvedeva a bloccare la chiavetta elettronica e a richiedere la formalizzazione di una denuncia penale. Nello stesso giorno, come richiestogli, il titolare sporgeva denuncia querela presso la locale stazione dei Carabinieri.

Ripresentatosi negli uffici della banca la cliente doveva tuttavia apprendere dal direttore di filiale l'impossibilità di effettuare il blocco del bonifico contestato che risultava quindi andato a buon fine nella mattinata medesima. In conseguenza di ciò, la cliente integrava la denuncia alle forze dell'ordine rilevando come la resistente non avesse provveduto al blocco del pagamento fraudolentemente disposto a danno della propria azienda. Sempre nello stesso il giorno, la vicenda veniva sottoposta all'area sicurezza della resistente, la quale evidenziava come l'operazione di bonifico, in quanto richiesta ed attuata utilizzando una configurazione del computer, un provider ed un indirizzo informatico non abituali per la ricorrente, fosse stata preceduta dalla richiesta da parte dei preposti sistemi di sicurezza, di inserimento della risposta alla domanda segreta impostata direttamente dal cliente/ricorrente e fosse stata confermata e disposta mediante password monouso generata dalla chiavetta elettronica della ricorrente. Risultava dunque plausibile che il cliente fosse stato vittima di una frode informatica perpetrata con l'ausilio di qualche malware annidato nel suo computere specializzato non solo nel furto delle credenziali di servizi *on-line*, ma anche nella cattura di schermate del PC, nella modifica di pagine web per l'acquisizione fraudolenta di *password* e perfino nel controllo remoto del computer della vittima.

Oltre al blocco della chiavetta elettronica, l'area sicurezza della resistente consigliava al cliente l'attivazione del servizio di alert e-mail o sms mediante il quale avrebbe potuto ricevere su posta elettronica o su cellulare un messaggio in occasione di eventi dispositivi sul proprio conto corrente.A pochi giorni di distanza, la ricorrente sporgeva reclamo confermando la fraudolenza

del pagamento sopradescritto, in quanto privo di autorizzazione, ribadendo di non conoscere il beneficiario ed evidenziando come le credenziali di accesso al sistema di *home banking* fossero in possesso solo di persone espressamente autorizzate.Nell'invitare la resistente a fornire una spiegazione plausibile dell'accaduto, la ricorrente si riservava ogni azione volta al ristoro del danno subito.

La resistente riscontrava il reclamo ed imputava l'esecuzione del pagamento contestato ad una probabile truffa attuata tramite la captazione di certificato e *password* da parte di terzi direttamente dal computer della ricorrente probabilmente mediante la emissione di una falsa schermata di verifica. Dal momento che la falsa schermata nulla aveva a che vedere con la resistente, trattandosi invece di software malevolo probabilmente annidato nel computer della ricorrente, non risultava imputabile alla banca alcuna azione od omissione riconducibile all'evento denunciato e nessuna richiesta di rimborso poteva essere accolta.

Reiterata la richiesta sostenendo come, ai sensi del contratto di "Multicanalità integrata", il cliente non fosse tenuto a sopportare l'eventuale perdita derivante da operazioni di pagamento non autorizzate, salvo che avesse agito in modo fraudolento, con dolo o colpa grave, e come invece fosse dovere della banca assicurare che le chiavi di autenticazione per l'utilizzo di uno strumento di pagamento non fossero accessibili a soggetti diversi dal cliente legittimato. Inoltre, in base al disposto del Codice Privacy espressamente richiamato dal citato contratto, il soggetto titolare del trattamento dei dati personali, nel custodirli, avrebbe dovuto adottare idonee e preventive misure di sicurezza tali da ridurre al minimo i rischi di accesso non autorizzato ed altresì risarcire i danni cagionati in conseguenza dell'inadempimento a tale obbligo

Nel successivo ricorso, presentato in assenza di replica alle proprie doglianze, la ricorrente, in punto di diritto poneva l'accento sulla normativa di riferimento, in primo luogo l'art. 8 del d.lgs. 11/2010, il quale pone a carico del prestatore dei servizi di pagamento l'obbligo di assicurare che i dispositivi personalizzati non siano accessibili a soggetti diversi dall'utilizzatore. La banca, predisponendo misure di protezione idonee ad evitare l'accesso fraudolento di terzi ai depositi dei clienti o a neutralizzarne gli effetti, avrebbe dovuto adempiere all'obbligo di custodia dei patrimoni dei clienti con la diligenza professionale richiesta dall'art. 1176 c.c.,diligenza che, parametrata alla specificità del servizio di *home banking*, implica l'adeguatezza agli standard esistenti dei presidi adottati per la inviolabilità delle transazioni *on-line* da attacchi di pirateria informatica.

In secondo luogo, secondo la ricorrente, il Provvedimento di Banca d'Italia del 5 luglio 2011 precisava che i prestatori di servizi di pagamento hanno l'obbligo di assicurare che "*le soluzioni tecniche adottate per l'esercizio dell'attività siano presidiate gestendo i rischi associati alle tecnologie utilizzate, tra i quali attacchi da parte di soggetti esterni o tentativi di frode*". Nell'individuare le caratteristiche che uno strumento di pagamento deve rispettare per essere maggiormente sicuro, il Provvedimento menziona l'obbligo dell'intermediario di "*mettere a disposizione dell'utilizzatore un canale di comunicazione differente da quello usualmente utilizzato per le transazioni attraverso cui l'utilizzatore viene tempestivamente informato delletransazioni effettuate (es. SMS, e-mail, pagine web riservate, etc.)*". Pur avendo richiamato tale normativa nei contratti stipulati con la ricorrente, risultava evidente come la resistente avesse palesemente violato gli obblighi di protezione e sicurezza così individuati. La circostanza, infatti, che da una pagina web protetta -con indirizzo "https"- fosse stato possibile il "reindirizzamento" ad una pagina nonprotetta - con indirizzo "http",– non faceva che confermarne la violazione, non avendo la resistente introdotto alcun meccanismo in grado di disabilitare i link ad indirizzi non protetti. Inoltre, la banca non si era premurata di mettere a disposizione il diverso canale di comunicazione richiamato dalla normativa né di informare il cliente della possibilità di attivarlo. Alla luce di tali considerazioni unitamente alla circostanza della tempestiva attivazione della ricorrente nell'informare la resistente dell'accaduto e alla inerte reazione di quest'ultima, il comportamento della banca, a dire della ricorrente, non poteva che qualificarsi come inadempiente con conseguente obbligo di risarcimento del danno. In stretta correlazione agli obblighi descritti, la ricorrente rilevava la responsabilità della resistente, ex art. 11 del d. lgs. 11/2010, per le operazioni di pagamento non autorizzate e il conseguente obbligo di rimborso dell'importo sottratto, con la sola franchigia di 150 euro e salve le ipotesi di dolo e colpa grave del cliente: ipotesi in alcun modo ravvisabili nel comportamento tenuto dalla ricorrente la quale, oltre ad essersi dotata di *antivirus* aggiornati e di appositi *firewall*, nell'accedere al servizio di *home banking* si era limitata ad eseguire le consuete operazioni di autenticazione. Risultava a questo punto evidente il tentativo della resistente di sottrarsi alla propria responsabilità con l'affermazione, non suffragata da prova alcuna, che l'evento fosse imputabile ad un malware presente nel computer della ricorrente. Con riguardo infine, all'onere probatorio, la ricorrente sottolineava come fosse onere della banca dimostrare che il danno fosse stato cagionato da dolo o colpa grave del cliente ma che tali profili non erano stati minimamente evidenziati dalla resistente, essendosi questa limitata a riconoscere nella ricorrente la vittima di una frode informatica. Pertanto, chiedeva la ricorrente il risarcimento

del danno subito quantificato: nella la somma capitale, più le commissioni addebitate per l'operazione, gli interessi, la rivalutazione monetaria e l'integrale pagamento delle spese di lite

Nello specifico, la ricorrente risulta essere stata vittima di un'aggressione informatica attraverso un software particolarmente insidioso. A differenza che nelle fattispecie "classiche" e più note, dove l'aggiramento dei presidi di sicurezza e la circonvenzione del cliente ha luogo attraverso metodi ormai noti (emailcivetta, false comunicazioni di scadenza, invito all'aggiornamento di databasee così via) che il cliente, dispiegando un minimo di diligenza, è oggettivamente in grado di schivare (anche e non secondariamente per l'accresciuta campagna di informazione che i media e gli stessi intermediari hanno da tempo ormai attuato),viceversa, nel caso in esame, la *captatio* ha avuto luogo attraverso un meccanismo decisamente assai più subdolo, noto da tempo alla scienza informatica ma non altrettanto al pubblico dell'utenza *on line*, capace di sorprendere la buona fede anche di un pur normalmente attento fruitore del servizio.

La ricostruzione tecnica, che emerge in modo efficace dagli atti del procedimento, evidenzia come la ricorrente sia stata indubitabilmente vittima di un software malevolo (*malware*), molto probabilmente derivato dal c.d. malware *Zeus*, che la letteratura informatica riporta siccome scoperto nel 2007, diffusosi nel 2009 e 2010, debellato dalle autorità statunitensi ma rieditato in altre consimili forme,grazie alla messa in rete dei codici sorgente (codici necessari per l'esecuzione, manipolazione e la riprogrammazione del malware) disposta dalle stesse autorità.Il principio operativo di tale meccanismo di intrusione viene definito in gergo *man in-the-browser* a significare l'interposizione che questo genere di malware è in grado di operare fra il sistema centrale dell'intermediario e quello del singolo utente.

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 – riconducibile alla più ampia categoria dei cc.dd. *trojan* ("cavalli di Troia") e dotato di sofisticate capacità di elusione dei migliori antivirus – si annida in modo silenzioso nel computer dellavittima 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). Ignaro dell'intervenuta sostituzione della pagina, l'utente è indotto a ritenere di trovarsi nel normale ambiente sicuro in cui normalmente egli opera. A quel punto il malware attiva una finestra a modulo, che pare sempre provenire dal sito dell'intermediario in cui si trova (crede di trovarsi)l'utente, ove è richiesta una conferma di sicurezza con l'invito a compilare i campi del modulo con i propri dati e il codice generato dal dispositivo OTP: procedura che gli intermediari stessi talora attivano per controlli di sicurezza (specie come quando, nel caso in esame, l'accesso abbia luogo da una macchina diversa da quella abitualmente utilizzata dall'utente e come tale segnalata al server della banca da un differente indirizzo di provenienza: c.d. IP, *Internet Protocol*), il che rafforza nell'utente il convincimento della piena regolarità della situazione e della normalità del controllo automaticamente disposto dal sistema.

L'utente, con ciò doppiamente ingannato, compila quindi i campi del modulo che il malware prontamente trasmette all'intruso. Questi, così chiaramente interpostosi nell'operazione, ha modo di captare tutti i fattori di autenticazione e di utilizzarli in tempo reale, nel mentre l'utente viene ulteriormente ingannato da un messaggio di attesa che, qualche minuto dopo, si conclude con la segnalazione dell'impossibilità di procedere all'operazione e con l'invito a ritentare in un secondo momento. Lo schema dianzi descritto appare propriamente replicato nel caso in esame (sul fatto che di frode si sia trattata v'è pacifica convergenza di vedute fra le parti contendenti), che ha visto la ricorrente, una volta acceduta al sito dell'intermediario, cadere in questo infido e impercettibile tranello.

La tentata operazione di bonifico che la ricorrente intendeva porre in essere non avrà seguito in quanto la schermata di cattura, formulata col descritto "illusionismo informatico", la indurrà a comunicare i propri dati e il codice monouso generato dall'OTP, salvo poi vedersi, dopo qualche minuto, comunicare dalla stessa schermata l'impossibilità di procedere e l'invito a provare in un momento successivo.

Di fronte ad un a fattispecie così peculiare il Collegio di coordinamento ha sostenuto che non appare ragionevolmente ravvisabile, alcun elemento tale da poter riqualificare siccome colposa,

e tanto meno siccome gravemente colposa (ai fini di cui all'art. 12 comma 2° d. lgs. cit.), la condotta dell'utilizzatore del servizio.

Per quanto non possa negarsi che il cliente sia caduto nella tagliola ed abbia materialmente permesso l'esecuzione dell'operazione fraudolenta cooperandovi involontariamente, non è chi non veda la profonda differenza strutturale fra i dianzi citati metodi "tradizionali" di *phishing* e il descritto fenomeno del *man-in-the-browser*. Nel primo caso, il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet. Nel caso che si è descritto invece, il subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino, posto che l'unica "differenza"consta, come si è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale "http" e non già come un "https" protetto. Ma va da sé che una simile variazione, che compare solo nella stringa di intestazione della videoschermata confusa ad almeno cinquanta o sessanta ulteriori caratteri, barre e altri segni di punteggiatura informatica, sfugge normalmente all'attenzione di chiunque si accosti ad una pagina della rete e più che mai sfugge a chi si accosti alla pagina di un sito bancario per compiere un'operazione, dunque in un momento in cui l'attenzione dell'utente è concentrata sul contenuto della schermata e non certo sugli incomprensibili codici che la circondano e che fanno parte del normale apparato di contorno anche delle innocue consultazioni in rete.

Per altro verso, l'esclusione di una colpa grave, ma finanche di una colpa lieve è, nel caso di specie, ulteriormente comprovata dalla più che tempestiva attivazione della ricorrente che, accortasi qualche ora più tardi dell'intervenuta operazione non autorizzata, ha provveduto ad informarne telefonicamente la banca per il blocco del bonifico, ha sporto il giorno successivo denuncia all'autorità di P.S.,contestualmente formalizzando il reclamo e il disconoscimento.

Circostanze queste documentalmente comprovate e che la banca resistente non ha comunque minimamente contestato. Neppure può scorgersi colpa alcuna della ricorrente nel non aver attivato il servizio di *SMS alert* che avrebbe forse consentito di individuare l'operazione in un lasso temporale anteriore al suo compimento. Non si può non rimarcare come siffatto servizio

non costituisca che una tutela *ex post*, che come tale non vale ad esonerare l'intermediario dall'approntamento di presidi di protezione avanzati, atti a prevenire il compimento stesso dell'operazione fraudolenta.

Così come non può sottacersi che l'efficienza del servizio di SMS alert dipenda da tutta una serie di variabili che in parte sfuggono al controllo dell'utente (funzionalità della linea telefonica) in parte presupporrebbero una condotta talora obiettivamente inesigibile, ossia la costante e ininterrotta sorveglianza del proprio cellulare (si pensi al solo caso in cui l'utente, per libera scelta o per necessità, abbia il telefono spento nel momento in cui perviene il messaggio e non lo riaccenda se non in unmomento successivo nel quale la segnalata operazione irregolare non potrebbe comunque più essere impedita). Ma, ad escludere ulteriormente ogni negligenza comportamentale del ricorrente in tal senso – e, parallelamente, ad affermare una carenza organizzativa della resistente come tale rilevante ai fini di cui all'art. 8 del d. lgs. cit. –la messa a disposizione di strumenti accessori al rafforzamento della sicurezza non possa valere a tramutare in colpa grave il fatto che il cliente non se ne sia avvalso ove – come altrove (in relazione allo stesso dispositivo OTP) sancisce il Collegio di Milano secondo un orientamento che il Collegio di Coordinamento ha ritenuto ritiene di pienamente condividere e far proprio – la disponibilità di tali strumenti non sia resa nota con adeguata, enfatica evidenza al cliente e tale modalità di comunicazione non può certo ritenersi assolta, come consta nel caso di specie, ove la messa a disposizione venga genericamente menzionata nel documento di sintesi o nel foglio informativo.

Una siffatta enunciazione non può ritenersi tale da integrare un'offerta sufficientemente stimolante all'uso del servizio, vuoi per l'assenza di qualsivoglia evidenza specifica, vuoi per il contenuto dell'enunciazione che non attira l'attenzione dell'utente sui benefici ritraibili in termini di sicurezza, vuoi infine perché la mera indicazione nel foglio informativo o nel documento di sintesi, non accompagnata da un'efficace stimolazione dell'utente nel senso di indurlo ad acquisire il dispositivo al preciso fine di minimizzare il rischio di incidenti informatici, non può qualificarsi quale offerta utile al fine di dimostrare il dispiegamento della miglior diligenza possibile da parte della banca resistente. E'ragionevole in effetti opinare che una semplice e indistinta menzione, inclusa nel coacervo di prezzi di altri servizi, non possa considerarsi una vera e propria raccomandazione all'utilizzo così come è altrettanto ragionevole e scusabile, daparte del cliente, la mancata individuazione della presunta offerta in un siffatto contesto (cfr. Coll. Milano, dec. n. 2622/2011).

Come conclusione della articolata motivazione il Collegio di coordinamento ha rinvenuto l'assenza di qualsivoglia colpa, e certamente di una colpa grave, in capo alla ricorrente, escludendo che nella specie la stessa debba sopportare conseguenza alcuna, ulteriore e diversa dalla sopramenzionata franchigia contrattuale di 150euro, operando in tal senso il disposto dell'art. 12 del dlgs n.11.

A completare il discorso così articolato , non è stato considerato possibile l'obiezione, sollevata dalla banca della l'estraneità della stessa ai fatti causativi dell'evento dannoso, che la resistente imputa – correttamente sul piano tecnico-fattuale – alla probabile presenza del malware nel sistema del ricorrente.

L' obiezione non è apparsa persuasiva, in primo luogo, perchè la presenza del malware non è di per sé indice di una negligenza di custodia da parte dell'utente vuoi in ragione della natura particolarmente sofisticata del suddetto programma malevolo, della sua inerzia rispetto al normale funzionamento del sistema e della sua spiccata capacità di aggirare antivirus e firewall, vuoi a motivo del fatto che una delle caratteristiche proprie del servizio di *home banking* è la sua attivabilità da qualsivoglia postazione informatica, anche diversa da quella di proprietà dell'utente (un Internet café, il computer messo a disposizione da un hotel o prestato da un amico o collega e così via), sicché non può escludersi la presenza del virus in tali diverse macchine e del pari non può affermarsi alcuna grave negligenza dell'utente né nell'essersene avvalso né nel non aver posto in essere l'obiettivamente inesigibile, spesso impossibile (e fors'anche, data la descritta capacità offensiva del virus, inutile) cautela di operarne una preventiva "disinfestazione". In secondo luogo, è e rimane, nel nuovo impianto legislativo, obbligo specifico del prestatore del servizio introdurre cautele volte a prevenire l'accesso non autorizzato ai dispositivi di pagamento dell'utilizzatore. Posto che, come si è dianzi osservato, la tipologia di malware era da tempo nota alla tecnica informatica, era ed è onere della banca adottare strumenti in grado di respingere simili offensive o quanto meno fornire precise indicazioni volte a sventarle (quale, ad esempio, la specifica avvertenza, formulata con massima, enfatica evidenza, di verificare costantemente la presenza del corretto acronimo di protocollo *https* nella stringa operativa ovvero di porsi in contatto con il servizio clienti nel caso in cui il computer riportasse un segnale di conferma di credenziali, accortezze non provate dalla, ma neppure menzionate nelle difese della, banca resistente). Né il Collegio ha omesso di trascurare che il cennato Provvedimento attuativo della Banca d'Italia 5.7.2011 prevede l'obbligo dell'intermediario di dar corso a fasi di verifica teorica e pratica della vulnerabilità dei presidi di

sicurezza con relativa revisione periodica del processo stesso nonché di definire un adeguato insieme di presidi di sicurezza logica e fisica per i sistemi informativi, un efficace processo di controllo interno, un appropriato piano di continuità operativa e una gestione dei rapporti contrattuali con i fornitori esterni coerente con i suddetti vincoli: in breve un preciso obbligo di costante ed effettivo monitoraggio dell'efficienza del sistema di sicurezza che, come tale, non può non tenere in debita considerazione l'evoluzione dei metodi di aggressione e la costante ricerca di soluzioni protese ad ovviarne o arginarne le offensive. Con che nuovamente l'obbligo organizzativo previsto dal citato art. 8 torna ad assumere piena e dirimente valenza.

Ma il terzo e più decisivo argomento che il Collegio ha evidenziato e che consente di superare l'eccezione di estraneità invocata dalla resistente risiede nel descritto principio di distribuzione del rischio, enunciato in precedenti decisioni dell'Arbitro per il quale lo squilibrio di responsabilità promanante dal dettato normativo del d. lgs.11/2010, si spiega in considerazione dell'incomparabilmente maggior capacità economica dell'intermediario di sostenere il rischio connesso all'impiego di strumenti la cui sicurezza assoluta non è stata sin qui raggiunta (e probabilmente non verrà mai raggiunta dato l'inarrestabile evolversi della tecnologia civile e la naturale "rincorsa" della tecnologia criminale nella stessa direzione), grazie ad una redistribuzione dei relativi costi sull'intero pubblico dell'utenza.

Principio che è stato considerato pienamente condivisibile,soggiungendo che l'addossamento del rischio all'intermediario (il cui estremo confine si colloca all'altezza della colpa grave dell'utente) appare vieppiù giustificato dalla forte e incessante promozione all'uso di tali strumenti posta in essere dal mondo bancario, in ciò aiutato anche da un sistema legislativo che sempre più ne impone l'adozione .).Ne è derivato quindi che essendo di tutta evidenza che la ricorrente, immune nella specie da qualsivoglia colpa grave per quanto sopra ampiamente chiarito, non sia tenuta a sopportare le conseguenze dell'accaduto ma sia piuttosto la resistente a dover ristorare il danno patito dalla ricorrente calcolato in misura pari all'ammontare dell'operazione disconosciuta diminuito della franchigia, prevista nella misura massima di legge (euro 150) dall'art. 11 delle condizioni speciali che regolano il servizio.

L'orientamento, decisamente ancor più favorevole che in passato nei confronti dell'utente, che pur prestando adeguata attenzione, non è in grado di cogliere una frode così sofisticata che è stato assunto dal Collegio di coordinamento non ha mancato di influenzare il Collegi.

Si guardi di recente la decisione del collegio di Napoli del 21 aprile 2014 che ribadisce che, in assenza di elementi circonstanziali probatori addotti dalla banca, atti a dimostrare la colpa grave

(nell'accezione più volte ribadita da questo collegio) del cliente dell'utilizzazione dello strumento di pagamento, la banca è tenuta al rimborso dell'operazione fraudolenta, ai sensi dell'art.11 del lgs.n.11 del 2010, che stabilisce l'obbligo "immediato" di rimborso dell'importo dell'operazione non autorizzata. Mette conto ricordare che è qualificabile come colpa grave quella "straordinaria ed inescusabile imprudenza e negligenza", caratterizzata non solo dall'omissione della diligenza media del buon padre di famiglia, ma anche da "quel grado minimo di diligenza osservato da tutti" (Cass. 13 ottobre 2009, n.21679; Cass. 18 maggio 2009, n. 11459; Cass. 19 novembre 2001, n. 14456.

Seppure quindi la decisione del collegio di Coordinamento si è occupata di una ipotesi di Phishing particolarmente sofisticata ed insidiosa, e quindi di quasi impossibile riconoscibilità anche da parte di un cliente accorto ed informato, essa ha preso posizione su punti discussi della disciplina delle operazioni di pagamento on line ,che vanno dagli obblighi di continuo monitoraggio dei canali di trasmissione e delle strutture, da parte degli intermediari, del valore della previsione di sistema di SMS che le decisioni ABF hanno affrontato e risolto non sempre in maniera uniforme.

Si tratta di un passaggio importante nell'ottica sia di assicurare il rispetto delle disposizioni in materia di trasparenza e di correttezza delle relazioni tra intermediari sia affermando principi sia per migliorare le relazioni tra banche e clienti.