IL COLLEGIO DI COORDINAMENTO

composto dai signori:

Dott. Giuseppe Marziale.....	Presidente - Presidente del Collegio ABF di Roma (designato dalla Banca d'Italia)
Prof. Avv. Antonio Gambaro……	Membro effettivo - Presidente del Collegio ABF di Milano (designato dalla Banca d'Italia)
Prof. Avv. Enrico Quadri……..	Membro effettivo - Presidente del Collegio ABF di Napoli (designato dalla Banca d'Italia)
Avv. Emilio Girino…… ……. ……..	Membro effettivo - Componente del Collegio ABF di Milano (designato da Confindustria di concerto con Confcommercio, Confagricoltura e Confartigianato) [Estensore]
Dott. Dario Purcaro…….	Membro effettivo - Componente del Collegio ABF di Milano designato dal Conciliatore Bancario Finanziario (per le controversie in cui sia parte un professionista/imprenditore)

nella seduta del 12/09/2012, dopo aver esaminato

- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria tecnica,

FATTO

Con ordinanza assunta nella seduta del 5 luglio 2012, il Collegio di Milano aveva ritenuto di rimettere al Collegio di Coordinamento la decisione dell'odierna controversia, ponendo a base della rimessione la seguente testuale motivazione: "*il Collegio di Roma in casi strettamente analoghi ha accolto il ricorso anche in presenza di sistemi di autenticazione a due fattori, mentre sino ad oggi questo Collegio [di Milano: n.d.r.] era orientato a non accogliere tali ricorsi*".

E' agevole evincere dalla suddetta motivazione come il tema controverso investa i confini della responsabilità dell'intermediario in caso di frodi informatico-finanziarie perpetrate mediante forzatura dei sistemi di pagamento elettronici.

Il caso specifico vede coinvolta in qualità di ricorrente un'azienda agricola, indubbiamente qualificabile come microimpresa nel senso di cui all'art. 1 comma 1°, 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.

Questi i fatti contestati in reclamo ed egualmente riproposti nel ricorso.

In data 26 maggio 2011 la ricorrente, in persona di uno dei titolari, stipulava con la resistente un contratto di conto corrente bancario e contestualmente il correlato contratto di "Multicanalità integrata" per il servizio di *home banking*, all'attivazione del quale riceveva 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.

Il successivo 10 ottobre la ricorrente accedeva al servizio di *home banking* per effettuare un bonifico ma, dopo aver inserito le credenziali di accesso e la password monouso secondo le usuali modalità, non riusciva a portare a termine l'operazione. Nel corso di un successivo accesso, avvenuto qualche ora dopo, apprendeva che era stato disposto un bonifico mai autorizzato di euro 9.101,18 in favore di una sconosciuta società ungherese. 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 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 (11 ottobre). In conseguenza di ciò, il titolare 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 il giorno 11

ottobre 2011, 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 computer e 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.

In data 18 ottobre 2011, la ricorrente sporgeva reclamo confermando la fraudolenza del pagamento sopradescritto, in quanto privo di autorizzazione della scrivente, 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 il 3 novembre 2011 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.

Il 22 novembre 2011 la ricorrente, tramite avvocato, nel ritenere la resistente responsabile del danno patito, rinnovava la richiesta di rimborso della somma

sottratta unitamente agli interessi decorrenti dalla data del bonifico contestato ed alle spese legali quantificate in 300,00 euro. Ad avvalorare tale domanda, la ricorrente sosteneva 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.

In assenza di replica alle proprie doglianze, la ricorrente presentava ricorso all'ABF Collegio Milano il 17 febbraio 2012. Dopo aver ripercorso i fatti per come sopra narrati, in punto di diritto la ricorrente poneva l'accento sulla normativa di riferimento, in primo luogo l'art. 8 del d.lgs. 11/2010, già richiamato nella nota del 22 novembre, 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 ricorente, 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 delle transazioni 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 non protetta - con indirizzo "http", come da allegato D al ricorso – 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 così quantificato: la somma capitale di 9.101,18 euro, le commissioni addebitate per l'operazione, gli interessi maturati dal 10 ottobre 2011, la rivalutazione monetaria e l'integrale pagamento delle spese di lite pari a 1.032 euro.

Nelle controdeduzioni depositate il 20 aprile 2012, la resistente, dopo aver premesso di aver adottato ogni presidio per la prevenzione di frodi informatiche, notava come nel caso di specie non avesse rilevato alcuna anomalia nei tracciati relativi all'immissione delle credenziali né di accesso né di disposizione, dovendosi imputare l'uso illegittimo dei codici unicamente all'acquisizione degli stessi da parte di terzi con l'evidente "concorso" della ricorrente, vuoi sotto il profilo della scorretta conservazione e custodia delle chiavi di autenticazione, vuoi per l'inadeguata protezione del software utilizzato per disporre l'operazione contestata. Soggiungeva la resistente come non rispondesse al vero l'affermazione della ricorrente circa la mancata informazione sui servizi alert e-mail o SMS, in quanto previsti tra le condizioni economiche del citato contratto di Multicanalità integrata sottoscritto dalle parti. Concludeva dunque la ricorrente per la dichiarazione di infondatezza e conseguente reiezione del ricorso.

DIRITTO

Come superiormente osservato nell'enunciazione in fatto, l'oggetto del contendere impone di tracciare con la maggior esattezza possibile il confine di responsabilità degli intermediari bancari e finanziari nel caso di frodi, perpetrate da terzi ai danni della clientela, nell'ambito della prestazione di servizi di pagamento regolati dal cit. d. lgs. 11/2010.

Notoriamente siffatto decreto, nel dare attuazione alle direttive comunitarie in materia, ha inteso rendere l'ambiente informatico-finanziario improntato a criteri di maggior sicurezza e affidabilità e ciò in ragione vuoi del crescente impiego dello strumento di pagamento elettronico da parte del pubblico degli utilizzatori vuoi del parallelo (e prevedibile) espandersi degli attacchi sferrati dalla nuova criminalità in questo stesso, sempre più affollato ambiente di operatività finanziaria. L'obiettivo è stato conseguito, da un lato, imponendo agli intermediari, nella loro qualità di prestatori di servizi di pagamento, specifici obblighi di precauzione, primo fra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati (ossia diversi dal loro legittimo titolare: cfr. art. 8, comma 1° lett. a) del cit. d. lgs. 11/2010), e, dall'altro lato, istituendo un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori. Regime e *favor* che si sostanziano nelle seguenti concatenate proposizioni precettive (art. 10 d.

lgs. cit.): a) in caso di disconoscimento di un'operazione di pagamento, è onere dell'intermediario dimostrare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; b) l'apparentemente corretta autenticazione non è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca; c) la responsabilità dell'utilizzatore resta dunque circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento agli obblighi che l'art. 7 del decreto pone a suo carico e che poi si limitano all'utilizzazione dello strumento di pagamento in conformità ai patti contenuti nell'accordo quadro che regola il servizio e alla tempestiva denuncia di furto, smarrimento, distruzione o altro uso non autorizzato dello strumento. Ove una simile responsabilità non possa affermarsi (e logicamente il correlato onere probatorio incomberà sull'intermediario prestatore del servizio), l'utilizzatore non sopporterà le conseguenze dell'uso fraudolento, o comunque non autorizzato, del mezzo di pagamento se non nei limiti, eventualmente stabiliti dall'intermediario, di una "franchigia" non superiore a 150 euro (art. 12, commi 1° e 3° d. lgs. cit.).

L'evidente squilibrio che le predette disposizioni determinano nel rapporto fra prestatore e utilizzatore di un servizio di pagamento trovano una loro giustificazione, per così dire, "social-commerciale", nitidamente ricostruita in una pronuncia del Collegio di Roma, ad avviso del quale "*la disciplina è evidentemente ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi. Si tende, in altri termini, a "spalmare" sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento, sì da evitare che esso gravi esclusivamente e direttamente sul singolo pagatore*" (Collegio Roma, dec. n. 1111/2010).

Naturalmente, la concreta traduzione del principio non può prescindere da una corretta applicazione del limite che le norme regolatrici vi appongono e che, al netto di ogni ulteriore considerazione, si riduce allo stabilire se l'intermediario

abbia adottato tutti i migliori accorgimenti della tecnica nota per scongiurare questo genere di rischi e quando (esclusa ovviamente la condotta fraudolenta del cliente di per sé tale da precludere l'operatività di qualsivoglia presidio) l'eventuale negligenza del cliente possa ricadere o meno nella nozione di colpa grave al cui ricorrere il cit. art. 8 esclude ogni responsabilità dell'intermediario.

In tale prospettiva il Collegio di Milano, ispirandosi al principio di ragionevole esigibilità della prestazione calato nel pur peculiare ed asimmetrico rapporto fra cliente e intermediario, ha costantemente affermato la responsabilità di quest'ultimo nel caso di mancata adozione dei più avanzati accorgimenti tecnici di prevenzione (cfr. fra le molte Collegio Milano, decc. nn. 111/2012 e 113/2012), mentre l'ha esclusa in tutto o in parte là dove il cliente, pur debitamente informato (con adeguata evidenza e trasparenza) della disponibilità di siffatti strumentari di sicurezza, ometta di avvalersene (cfr. dec. 528/2012).

Ma la fattispecie più problematica si colloca nel mezzo dei due estremi ora evocati, realizzandosi là dove l'intermediario abbia messo a disposizione del cliente i predetti strumentari avanzati, il cliente se ne sia avvalso e nondimeno una fraudolenta intrusione ad opera di terzi sia avvenuta o comunque sia stata denunciata.

Ora, lo strumentario avanzato di sicurezza è stato individuato, almeno per quanto specificamente attiene al caso che ci occupa (pagamenti disposti mediante sistemi di *internet banking*), nella messa a disposizione dei cc.dd. *token* o *OTP* (*one time password*), vale a dire congegni in grado di generare mutevoli password monouso che, aggiungendosi alla password fissa nota solo all'utente, concorrono a formare un sistema di autenticazione a "due fattori" (altri dice a "tre fattori" includendovi anche lo *username*, per quanto più "visibile" e catturabile): sistema come tale di difficilissima, (quasi) impossibile forzatura e dunque ritenuto coerente alle indicazioni promananti dal provvedimento della Banca d'Italia adottato il 5 luglio 2011 ove si prevede che gli intermediari si attrezzino adeguatamente per identificare, valutare, misurare, monitorare e mitigare le minacce di natura tecnologica, individuando un insieme di misure di sicurezza e di controlli appropriati, in grado di assicurare gli obiettivi di confidenzialità, integrità, disponibilità dei sistemi informativi e dei dati ad essi associati. Ne consegue, secondo la predetta lettura del Collegio milanese, che, una volta che il sistema OTP sia stato chiaramente offerto al cliente e questi se ne sia avvalso, l'eventuale

intrusione fraudolenta di un terzo soggetto debba ricadere nella pur ristretta area di rischio che la legge pone a carico dell'utente. Secondo il Collegio di Milano, la pressoché totale invulnerabilità del sistema a "due fattori" garantita dai sistemi OTP appare 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, 1462/2012).

Siffatto orientamento riposa sull'assunto per il quale, allo stato attuale dell'arte tecnologica, 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 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 dell'Arbitro partenopeo ponendo una speciale enfasi sul principio di diritto ricavabile dalle anzidette norme del d. lgs. cit. 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 più 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 degli intermediari, quanto ad affermarlo secondo un nuovo stilema di giudizio aggiornato all'evoluzione del fenomeno criminale e alla sua nuova capacità offensiva.

Nel caso specifico oggetto dell'odierno ricorso, la fattispecie appare invero, sul piano tecnico, ancor più complessa di quelle sin qui analizzate dai Collegi – motivo che ha propriamente indotto lo stesso Collegio milanese ad operarne la rimessione a questo Collegio di Coordinamento.

Nello specifico, la ricorrente risulta essere stata vittima di un'aggressione informatica costruita attraverso un software particolarmente insidioso. A differenza che nelle fattispecie "classiche" sin qui note, dove l'aggiramento dei presidi di sicurezza e la circonvenzione del cliente ha luogo attraverso metodi ormai noti (e-mail civetta, false comunicazioni di scadenza, invito all'aggiornamento di database e 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 – come si noterà – 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 ineccepibile 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, la

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 della vittima 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 callidamente 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.

Non appare ragionevolmente ravvisabile, in siffatto contesto, 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 ci occupa, 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 video-schermata mischiata 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 ad avviso di questo Collegio, 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 un momento 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. – questo Collegio non può non rimarcare come 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 questo Collegio di Coordinamento 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, da parte del cliente, la mancata individuazione della presunta offerta in un siffatto contesto (cfr. Coll. Milano, dec. n. 2622/2011)

L'assenza di qualsivoglia colpa, e certamente di una colpa grave, in capo alla ricorrente, esclude che nella specie la ricorrente debba sopportare conseguenza alcuna, ulteriore e diversa dalla sopramenzionata franchigia contrattuale di 150 euro, operando in tal senso l'inequivoco disposto dell'art. 12 cit.

Né varrebbe in proposito obiettare, come la banca resistente obietta, 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. Tale obiezione non persuade per almeno tre ordini di motivi.

In primo luogo, 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 resistente 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 si trascuri 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 consente di superare l'eccezione di estraneità invocata dalla resistente risiede nel descritto principio di distribuzione

del rischio, enunciato nel sopradetto pronunciamento del Collegio romano, 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 questo Collegio di Coordinamento ritiene 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 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 (si ponga mente soltanto all'obbligo per le imprese e i professionisti di operare i pagamenti tributari *on line* e non più allo sportello). Siffatta promozione e siffatta imposizione, sulla cui opportunità questo Collegio non intende né ha titolo per esprimersi, comporta obiettivamente un sensibile beneficio economico per gli stessi intermediari consentendo loro significativi ed evidenti risparmi rispetto ad una tradizionale operatività di sportello. Un tale beneficio deve dunque trovare, come trova, nel dettato normativo, 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).

Da quanto precede discende in 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. Dal che consegue l'obbligo per la resistente di ristorare il danno patito dalla ricorrente calcolato in misura pari all'ammontare dell'operazione disconosciuta (euro 9.101,18) diminuito della franchigia, prevista nella misura massima di legge (euro 150) dall'art. 11 delle condizioni speciali che regolano il servizio per come risultanti dalla documentazione versata in atti dalla stessa ricorrente, dunque per un importo pari a euro 8.951,18.

In sede di ricorso la richiesta della ricorrente si è estesa anche al riconoscimento delle commissioni pagate per l'operazione non autorizzata, degli interessi al tasso convenuto e della relativa rivalutazione nonché delle spese legali sostenute. Al riguardo questo Collegio di Coordinamento reputa opportuno svolgere alcune considerazioni di chiarimento dato il rilievo che il tema assume in via generale nei procedimenti celebrati dall'Arbitro Bancario Finanziario.

Quanto alle commissioni, nessun dubbio sul fatto che le stesse, addebitate per l'esecuzione di un'operazione non autorizzata, vadano senz'altro stornate.

Quanto agli interessi e alla rivalutazione, questo Collegio ritiene di aderire al costante orientamento giurisprudenziale per il quale il debito risarcitorio, in quanto debito di valore e non di valuta, rende perfettamente lecito e compatibile il riconoscimento cumulato di entrambe le voci e che le stesse siano calcolabili anche in via equitativa. Rientrando nel potere decisionale dell'Arbitro accertare il diritto al risarcimento, il riconoscimento dei predetti accessori diviene una logica conseguenza.

Per quanto viceversa attiene alla refusione delle spese legali, le "Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari" (in breve "Reg. ABF") non contemplano alcuna espressa previsione al riguardo, e ciò in coerenza alla natura alternativa del procedimento instaurabile – e di norma instaurato – senza il ministero di un difensore. Ciò non toglie tuttavia che, là dove sia dimostrato che la parte ricorrente si sia avvalsa, nell'intero snodo procedimentale che va dal reclamo al ricorso, dell'ausilio di un difensore sopportandone il relativo costo, quest'ultimo possa e debba prendersi in considerazione, in caso di accoglimento del ricorso che si concluda con l'accertamento di un diritto risarcitorio, non già quale autonoma voce di rimborso non prevista dal Reg. ABF, bensì quale componente del più ampio pregiudizio patito dalla parte ricorrente.

In tale valutazione, il Collegio giudicante deve naturalmente attenersi a criteri di estrema prudenza, che includono l'accertamento dell'effettivo sostenimento dell'onere defensionale, della sua funzionalità alla gestione del procedimento, della ragionevolezza e coerenza dell'importo richiesto rispetto al valore e alla complessità della controversia, risultando pertanto l'importo di tale componente di pregiudizio stimabile anch'esso in via equitativa.

Nel caso specifico, consta agli atti del procedimento l'intervento operato in via stragiudiziale dal legale della ricorrente e l'esposizione della fattura di onorario per un importo omnicomprensivo di 1032,00 euro, misura che questo Collegio reputa del tutto equa e coerente ai parametri di valore e complessità del litigio.

Ne consegue che il sopraindicato indicato importo risarcitorio deve maggiorarsi del predetto onere defensionale, delle commissioni nonché degli interessi e rivalutazione, il tutto stimato secondo un prudente ed equitativo apprezzamento che induce ad elevare e consolidare il debito risarcitorio complessivo che la resistente sarà tenuta ad onorare nei confronti della ricorrente a 10.500,00 euro.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e, per l'effetto, dispone che l'intermediario corrisponda alla ricorrente, a titolo risarcitorio, la somma di Euro 10.500,00 comprensiva di interessi e rivalutazione.
Dispone inoltre che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e al ricorrente di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE MARZIALE