

20/11/14

“TRUFFE NUOVE e VECCHIE”

Avv. Massimo Campanella

- 1. “Introduzione” 2. “Le Vecchie Truffe” ovvero le frodi on-line 3. “Truffe Nuove” ovvero le sostituzioni dei mezzi di pagamento agli sportelli bancomat 4. “L’importanza della Decisione n.3536 del 30 Maggio 2014 del Collegio di Roma A.B.F.” ed i suoi precedenti 5.”Conclusioni”**

1. “Introduzione”

Con questo breve articolo si vuole segnalare al lettore come nel contenzioso bancario, vi siano dei nuovi casi di truffe a danno dei risparmiatori, in cui sussiste un obbligo di indennizzo degli Istituti di credito, anche quando questi ultimi si rifiutino, dichiarandosi esenti da responsabilità.

In realtà tale responsabilità che è di natura contrattuale è facilmente dimostrabile, con conseguente addebito alle banche del relativo risarcimento dei danni sia patrimoniali che non patrimoniali.

2. “Le Vecchie Truffe” ovvero le Frodi on-line

Con il termine “*Vecchie Truffe*” contrapposte alle nuove di cui si dirà nel par. 3., si vuole indicare quelle ormai note sia agli utenti dei conto correnti online che alla Polizia Postale, ossia i fenomeni del phishing e del pharming, con cui, esperti di computer riescono a manipolare i conti correnti online, carpendone i codici di accesso e prosciugandone i relativi conti correnti.

Il Phishing è una truffa via internet, in cui un individuo (il phisher), attraverso l’invio casuale di messaggi di posta elettronica, (che apparentemente possono sembrare quelli inviati da siti bancari o postali) cerca di carpire dalla vittima la password di

accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito .

Tali truffe possono essere realizzate anche mediante richieste telefoniche e con l'invio di sms.

Il termine phishing deriva dal termine inglese fishing –pescare, e si riferisce all'uso di tecniche sofisticate per “pescare” dati finanziari e password di un utente.

Anche il Pharming come il phishing è una tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate .

In questo caso le tecniche possono essere ancora più sofisticate , in quanto a differenza del phishing, con i quali mediante falsi messaggi email si inducono gli utenti a fare click su dei collegamenti, i pharmer reindirizzano le vittime direttamente sul sito web falso, costringendole a consegnare i propri codici di accesso anche quando queste digitano correttamente l'indirizzo di una banca o di altro servizio online nel browser web.

Il termine pharming (avvelenamento)deriva dal nome di uno dei metodi di attacco utilizzato dai pharmer denominato: “avvelenamento delle cache DNS” dei sistemi di denominazione di internet .

Le banche rifiutano di pagare i risarcimenti per questo tipo di danni , la relativa difesa nei procedimenti instaurati consiste nel sostenere che il proprio sistema di protezione è assolutamente inattaccabile e tra i migliori in assoluto .

Tuttavia va sottolineato da un lato che le banche hanno l'onere di applicare sia le misure di sicurezza minime stabilite nel D.L. 196/03 per tutelare i dati personali del cliente, sia di attuare tutte quelle misure idonee che in base al progresso tecnico, possono ridurre al minimo i rischi .

Ed infatti nelle cause bancarie aventi ad oggetto furto delle proprie credenziali , la banca pur sostenendo che l'utente sia responsabile per aver risposto ad email di phishing, è comunque tenuta a dimostrare davanti ai Giudici di avere attuato tutte le misure idonee per ridurre al minimo i rischi , e qualora non dimostri di avere attuato misure che in altre banche sono comuni per la prevenzione delle frodi informatiche può essere condannata al risarcimento del danno, dal Giudice in un giudizio ordinario o dall'ABF nella procedura stragiudiziale di composizione delle liti .

Sull'argomento si vuole ricordare in particolare una sentenza del “ *Tribunale di Palermo, III Sez Civile , 20 Dicembre 2009*” in cui la relativa responsabilità veniva addirittura considerata quale vera e propria “responsabilità oggettiva” degli Istituti di Credito e delle Poste quando queste offrano servizi prettamente bancari .

3. “Truffe Nuove” ovvero le sostituzioni dei mezzi di pagamento agli sportelli bancomat.

Vi sono delle nuove truffe che, probabilmente per la maestria e per l'abilità dei suoi autori , farebbero arrossire persino i personaggi del principe Antonio De Curtis in arte “Totò” , stiamo parlando dei furti con destrezza che si sono moltiplicati presso gli sportelli bancomat negli ultimi due anni , sia nell'anno in corso 2014 che nel 2013, in particolare a danno di alcuni Istituti di Credito, in cui a parere degli autori delle truffe sarebbe più facile superare i limiti di prelievo giornaliero .

I protagonisti di tali truffe con scuse banali come le “è caduta la carta” e comunque carpendo la buona fede di soggetti distratti o di anziani e poveri pensionati , riuscivano con rapidità a sostituire bancomat e carte di credito che poi avrebbero utilizzato per prelievi ed acquisti, prosciugando conti correnti e relativi platfond delle carte .

Nonostante le denunce presentate alle Forze dell'ordine ed i reclami presentati agli Istituti bancari , questi ultimi si sono spesso rifiutati di rimborsare le relative somme, dichiarandosi estranei all'accaduto ed imputando alla colpa degli incauti fruitori delle carte la colpa e la responsabilità dell'accaduto .

4. “L'importanza della Decisione n.3536 del 30 Maggio 2014 del Collegio di Roma A.B.F.” ed i suoi precedenti .

Al proposito è opportuno sottolineare come sia il Collegio di Roma chè il Collegio di Milano dell'Arbitro Bancario e Finanziario , si siano pronunciati con decisioni favorevoli ai ricorrenti –utenti bancari, accogliendone i relativi ricorsi con la franchigia di €.150,00 e ciò ai sensi del D .Lgs 11/10 di recepimento della Direttiva Comunitaria 2007/64/CE sui sistemi elettronici di pagamento .

Sicuramente di grande importanza sull'argomento è “ la Decisione n.3536 del 30 Maggio 2014 “ , del Collegio di Roma-ABF , con il quale il Collegio si è pronunciato su un caso di sostituzione di carta bancomat , dettando principi importanti in materia di responsabilità bancaria in questo tipo di danno .

Il Collegio di Roma citando la Decisione n. 888/2011 del Collegio di Milano , ha sottolineato come la diligenza qualificata di cui all'art.1176 c.c. , debba essere individuata in una nozione superiore a quella del buon padre di famiglia.

Scrive nella sua decisione il Collegio di Roma : “ *L’adempimento dell’obbligazione deve avvenire con la diligenza professionale dell’accorto banchiere , pena il risarcimento dei danni secondo i normali canoni della responsabilità contrattuale* “ (*sul punto Collegio di Milano già cit.*)

Secondo il Collegio per valutare il criterio della diligenza, bisogna prendere come parametro l’adeguatezza degli strumenti adoperati(considerati gli standard esistenti), bisogna valutare quindi i presidi tecnici adottati dall’intermediario per evitare, nei limiti del possibile un uso indebito e fraudolento dello strumento di pagamento – servizio bancomat

Sempre la stessa pronuncia indica la legislazione a presidio di tale tutela che consiste principalmente:

1) Nella Legge 17 agosto 2005 n.166 che ha istituito presso il Ministero dell’Economia e delle Finanze un sistema di prevenzione delle frodi sulle carte di pagamento;

2) Nel Decreto di attuazione del predetto intervento normativo DM 30 aprile 2007 n.112, Regolamento di attuazione della L. 17 agosto 2005 n.166 recante l’Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento.

Del predetto intervento legislativo va menzionato in particolare modo l’art. 8 Rischio di frode , il quale detta con riferimento agli indicatori di rischio alcuni criteri , tra cui è il caso di ricordare “*il normale utilizzo delle somme da parte del correntista*”. Pertanto l’Istituto di Credito dovrebbe essere fornito di adeguati strumenti atti a rilevare movimentazioni anomale sui conti correnti dei propri correntisti, e sotto tale profilo devono acquistare particolare importanza i sistemi di alert con cui vengono inviati ai correntisti per il tramite di sms o di email dei messaggi sulle loro movimentazioni, in modo che gli stessi possano essere prontamente informati sulle operazioni effettuate sui loro conti correnti , ed in caso di utilizzi fraudolenti provvedere immediatamente al relativo blocco delle carte di pagamento .

L’importanza della pronuncia deve essere vista proprio in questo , nell’aver reso evidente che l’Istituto adempie alla propria obbligazione, solo quando abbia la capacità di approntare i rimedi specifici per tutelare i propri clienti, diversamente dovrà essere visto soccombente nei relativi procedimenti incardinati, con condanna alla restituzione del maltolto ed al risarcimento dei danni .

Infine altre due pronunce dell’ABF sempre in materia di Truffe su carte di pagamento , meritano di essere menzionate .

La prima è la decisione del Collegio di Roma ABF n.3562 del 4 luglio 2013 in cui viene sottolineato come la “destrezza” del furto non possa in alcun modo essere

addebitata al titolare della carta , e tale da ravvisare in ciò una sua colpa grave, potendosi ravvisare al più una colpa lieve non rilevante ai fini dell'art. 12 , III co, del D.Lgs 11 del 2010 .

Pertanto il Collegio di Roma ha accolto il ricorso, escludendo la colpa grave del ricorrente, quando l'evento sia dipeso dall'adozione da parte dell'autore del furto , di modalità tali da provocare la momentanea distrazione del titolare dello strumento di pagamento, allo specifico fine di approfittarne .

La decisione fa espresso richiamo ad altra sempre del Collegio di Roma ABF n.673 del 1/02/13 la quale testualmente afferma che :*"Fatto non contestato è, infatti , la fulmineità dell'azione furtiva, coperta da un espediente particolarmente insidioso, certamente in grado di sorprendere un soggetto medio, inducendolo ad allentare per qualche attimo la normale sorveglianza sui propri effetti personali "*

La seconda decisione , che si vuole ricordare è la n.1454 del 13 luglio 2011 del Collegio di Milano ABF, in cui il ricorrente, titolare di una carta di pagamento, adiva il Collegio poichè mentre stava effettuando alcune operazioni, la Carta veniva catturata dall'ATM .

Il lunedì successivo quando si recava in filiale per recuperare la carta di pagamento, veniva informato che ignoti avevano effettuato ben tre operazioni per un totale di 1800,00 €. circa .

In questo caso il Collegio di Milano accogliendo il ricorso, disponeva che la banca risarcisse al cliente la somma prelevata al netto della franchigia di € 150,00 ai sensi dell'art. 12 comma 3 del D.lgs n.11/2010 .

Nella motivazione il Collegio spiega che nel caso di prelievo fraudolento fatto con bancomat trattenuto allo sportello, la banca è tenuta al risarcimento sia quale proprietaria degli sportelli ATM , sia per non aver evidentemente adottato tutte le misure atte a garantire la sicurezza del servizio da eventuali manomissioni da parte di terzi, infatti la diligenza della banca ha natura tecnica dovendosi parametrare alla figura dell'accorto banchiere .

5. "Conclusioni"

Pertanto alla luce della legislazione vigente e delle decisioni dell'Arbitro Bancario e Finanziario va sostenuto che :

1) l'Intermediario è tenuto ad approntare adeguati sistemi di difesa a tutela dei sistemi di pagamento ed andrà esente da responsabilità solo qualora dimostri il dolo o la colpa grave dell'utilizzatore ;

2) che ne risponde anche nei casi di furto con destrezza (nei limiti che sono stati esaminati);

3) Che anche nel caso di cattura della carta da parte dell'ATM ed utilizzo fraudolento da parte di terzi può essere previsto l'indennizzo .

Può pertanto concludersi alla luce di quanto osservato che anche tali tipi di "danno" siano indennizzabili e suscettibili di risarcimento da parte degli Istituti Bancari .