

# Chiudere la falla del phishing – frodi e rischi nei sistemi di pagamento non bancari

di Ross Anderson, Professore di Security Engineering alla Università di Cambridge.

Traduzione in italiano, su autorizzazione dell'autore, di Agatino Grillo (disponibile in <http://www.agatinogrillo.it/pdf/phishingnonbanks-it.pdf>, 113 K); versione originale in lingua inglese: "Closing the Phishing Hole – Fraud, Risk and Nonbanks" (disponibile sul sito di Ross Anderson <http://www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf>, 105 K).

Versione del 5 luglio 2007.

## Indice

<b>SINTESI</b> .....	<b>1</b>
<b>INTRODUZIONE – FRODE E PHISHING</b> .....	<b>2</b>
<b>I CONTROLLI SULLE FRODI E DEL PERCHÉ FALLISCONO</b> .....	<b>4</b>
<b>IMPLICAZIONI PER LA NORMATIVE BANCARIA</b> .....	<b>6</b>
<b>IMPLICAZIONI PER LA CONCORRENZA</b> .....	<b>7</b>
<b>TRACCIARE IL DENARO O TRACCIARE LE PERSONE?</b> .....	<b>9</b>
<b>IMPLICAZIONI PER I CONTROLLI DI ANTIRICICLAGGIO</b> .....	<b>11</b>
<b>I DIRITTI DEI CONSUMATORI</b> .....	<b>12</b>
<b>CONCLUSIONI</b> .....	<b>13</b>

## Sintesi

I truffatori online usano una gran varietà di servizi di pagamento non bancari per riciclare i proventi delle loro attività criminose. Per lungo tempo si è ritenuto che la tracciabilità fosse la soluzione migliore per contrastare tale fenomeno ma le esperienze "investigative" di questi anni hanno rivelato che la "revocabilità" dei pagamenti fraudolenti è una misura più efficace. Tuttavia mentre nel sistema bancario i pagamenti fraudolenti possono essere facilmente tracciati e se necessario recuperati con una certa probabilità di successo viceversa se i fondi rubati sono stati usati per acquistare beni finanziari trasferibili, come permette ad esempio il sito eGold, il recupero diventa molto più difficile. Ciò suggerisce che molti dei benefici che si pensa di ottenere da una nuova e più severa regolamentazione del comparto non bancario possono essere in realtà più efficacemente ottenuti da una maggiore trasparenza sui rischi di controparte. In questo saggio mi occupo, inoltre, di temi più ampi come ad esempio in che modo i centri finanziari offshore, se adeguatamente regolati, possono procurare benefici al sistema finanziario globale garantendo maggiore concorrenza e come, ugualmente, anche i sistemi di pagamento non bancari possono giocare un utile ruolo per la concorrenza. Un ulteriore tema è la confusione tra i controlli di identificazione e quelli di tracciabilità, confusione dovuta alle nuove procedure di conformità adottate dopo l'11 settembre; la mia tesi è infatti che ci sia stata troppa enfasi sulla identificazione a discapito della tracciabilità. Le attuali regole del FATF, Financial Action Task Force (Gruppo d'azione finanziaria contro il riciclaggio di capitali, GAFI) impongono a mio avviso oneri non necessari e non fanno abbastanza per facilitare il rapido recovery dei beni rubati. La regolamentazione futura dei servizi di

pagamento non bancari deve tener conto di tutto ciò. In particolare ritengo che meccanismi di pagamento anonimi o non verificati possono essere accettati per strumenti finanziari a basso valore purché i fondi che eventualmente risultassero rubati possano essere rapidamente tracciati e recuperati. Occorre inoltre essere cauti sulle responsabilità. Molti sistemi di pagamento non bancari impongono ai propri clienti contratti vessatori nei quali le società che erogano il servizio di pagamento si proclamano, in caso di contenzioso con i clienti, giudice e giuria – rischiando una corsa verso il basso a danno dei consumatori dei quali vengono messi in discussione il diritto alla protezione e che spinge verso un vero e proprio “moral hazard” cioè verso una sorta di opportunismo contrattuale che peggiora i rischi operativi. Solo i fornitori di servizi di pagamento possono contrastare in modo efficace le frodi, solo loro hanno accesso a tutti i dati e dunque la capacità di migliorare i propri sistemi. La protezione del consumatore infine non può ignorare la resilienza nei sistemi di pagamento cioè la capacità di resistere agli attacchi e garantire in tempi rapidi il ripristino delle condizioni normali.

## Introduzione – frode e phishing

A cominciare dal 2000 circa è aumentata la consapevolezza che la gestione dei rischi dell’information security fosse ormai un tema a confine tra tecnologia e politica. I sistemi spesso falliscono non tanto per ragioni tecnologiche ma perché gli incentivi economici sono sbagliati; infatti di solito le persone che gestiscono i sistemi non sono le stesse che devono rispondere dei danni che eventuali errori possono causare: anzi i sistemi sono spesso progettati per esternalizzare in modo deliberato il rischio. Questo ha portato allo sviluppo di una nuova disciplina, la security economics (o economia della sicurezza) che conta oggi oltre 100 ricercatori attivi e due conferenze annuali<sup>1</sup>. Una questione che mi è stata posta dalla Federal Reserve quando mi ha chiesto di preparare questo discorso è stata: cosa può dire un economista della sicurezza sulle frodi online e sui rischi operativi nell’ambito dei servizi di pagamento non bancari<sup>2</sup>?

Dal 2004 circa il crimine online è diventato un grande business. Prima il tipico “hacker” era un teenager birichino che tentava di infettare i computer o di penetrare nelle reti informatiche per impressionare i suoi amici; ed anche se c’erano delle truffe online si trattava di episodi sporadici e non continui. Tutto ciò adesso è cambiato. Ora la gente scrive virus informatici non per diletto ma per profitto. I computer infettati diventano parte di reti di centinaia di macchine note come “botnet” affittate per inviare spam, condurre attacchi di tipo “denial of service” ed ospitare siti web fraudolenti. Ma il cambiamento veramente importante è rappresentato dall’emergere di una vera e propria economia criminale che permette ai cattivi di specializzarsi, commerciare tra loro e scambiarsi servizi. La crescita maggiore nel crimine online riguarda il phishing, nel quale le vittime sono agganciate da email fraudolente che chiedono loro di autenticarsi con le proprie credenziali su un sito web che sembra autentico ma che in realtà ruba le loro password. Questo fenomeno è cominciato nel 2003 con un mezza dozzina di attacchi denunciati<sup>3</sup>. Si trattava di attacchi rozzi e “ingordi”: gli attaccanti chiedevano ogni sorta di informazioni personali tra cui anche il PIN per il bancomat il che insospettiva immediatamente i consumatori. Dal 2004 gli autori del phishing hanno reso il gioco sempre più sofisticato usando email e siti web sempre più verosimili e migliorando l’aspetto psicologico. Nel 2006 le perdite dovute al phishing sono arrivate a 35 milioni di sterline nel solo Regno Unito ed hanno raggiunto cifre a nove zeri negli USA. La crescita di questo

---

<sup>1</sup> Una recente indagine sul tema è disponibile in “The Economics of Information Security – A Survey and Open Questions”, Ross Anderson, Tyler Moore, Softint 2007 (Jan 19–20, Toulouse); in <http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf>

<sup>2</sup> Un’altra questione era: “il gioco d’azzardo online sarà la killer application che renderà popolari i servizi di pagamento non bancari?”; tuttavia oggi il gioco d’azzardo si sta spostando su Second Life, al punto che l’FBI ha già effettuato delle “perquisizioni” virtuali: <http://www.reuters.com/article/technologyNews/idUSN0327865820070404?>

<sup>3</sup> R Clayton, “Techno-Risk”, Cambridge International Symposium on Economic Crime 2003, in <http://www.cl.cam.ac.uk/~rnc1/talks/030910-TechnoRisk.pdf>

fenomeno criminale continua ad un tasso fenomenale con la lista degli “obiettivi” che adesso comprende non soltanto grandi banche ma anche servizi di pagamento come PayPal e grandi venditori come Amazon.

Però, sebbene sia più facile per i criminali costruire una copia del sito web di una banca piuttosto che costruire una finta filiale bancaria in un centro commerciale, l’infrastruttura necessaria per un attacco phishing efficace non è ancora alla portata di tutti. Ma questo è proprio il punto in cui interviene la nuova economia criminale. Oggi un ingegnere del software americano scrive un malware che poi sarà usato da una botnet romena per prendere il controllo di migliaia di computer; questi sono poi affittati ad un phisher russo che crea un falso sito che usa per mandare spam massiccio ai clienti della banca. Infine, una volta ottenuto il denaro, questo è spostato su conti correnti compromessi che sono venduti a terzi mentre ci sono anche organizzazioni che reclutano veri e propri “muli”<sup>4</sup>. In tal modo le numerose bande criminali prelevano il denaro dai conti correnti compromessi, li trasferiscono su altri conti compromessi o sui conti dei “muli” ed alla fine li accredita su istituzioni non bancarie come eGold o Western Union. Alla fine del giro il denaro rubato è ritirato dal sistema dei pagamenti per mezzo di operatori specializzati in “versamento di assegni” e conversione in contanti (cash-out) che possono appartenere a tutt’altra banda. Come con la fabbrica di spilli di Adam Smith, la specializzazione del lavoro porta i criminali ad ottenere una grande produttività.

Ci sono delle varianti come il “pharming” nel quale l’inganno non è effettuato direttamente sul cliente ma sulla infrastruttura; per esempio possono essere acquistati e configurati home router per dirigere i clienti delle banche verso pagine web contraffatte invece di quelle reali.

Negli ultimi anni è stato fatto molto lavoro dal punto di vista delle difese tecnologiche contro il phishing ed il pharming ma c’è ormai una crescente consapevolezza che la tecnologia può agire solo fino ad un certo punto<sup>5</sup>. Per prima cosa c’è il classico argomento della security-economics per cui ciascuno vuole che sia qualcun altro a risolvere il problema; ad una recente conferenza nel Regno Unito il governo voleva che i cittadini si assumessero maggiori responsabilità per la propria sicurezza online mentre le banche incolpavano il governo e gli ISP e tutti contemporaneamente erano anche ansiosi di tirarsi fuori in ogni modo dal problema<sup>6</sup>. Questo “scarico” di responsabilità è endemica; essa è stata analizzata e formalizzata da Hirshleifer e Varian come segue: la sicurezza di un sistema è determinato dalla somma degli sforzi dei suoi difensori in funzione del massimo o del minimo sforzo di ognuno. Nel secondo caso (il minimo sforzo) dunque il risultato finale in termini di difesa reale può rivelarsi assai lontano dall’optimum sociale<sup>7</sup>.

In secondo luogo, i meccanismi standard di sicurezza previsti nei comuni PC sono poco adatti alle necessità reali. Il protocollo SSL/TLS è stato progettato nella metà degli anni 90 per spostare i costi di conformità sugli utilizzatori<sup>8</sup>, ed ancora una volta la ragione fondamentale è stata di natura economica; le aziende erano in competizione per il dominio in mercati con forti “effetti di network” (come Microsoft e Netscape che a quel tempo si fronteggiavano nel mercato dei browser) ed erano spinti ad investire più nella usabilità dei loro prodotti piuttosto che nella loro sicurezza. Il SET, un protocollo alternativo che avrebbe fornito molta più sicurezza rispetto al phishing, fu inoltre osteggiato dalle banche a causa dei suoi più alti costi infrastrutturali e dai consumatori dato che esso eliminava il rimborso in caso di frode e spostava la responsabilità della transazione su di loro.

---

<sup>4</sup> I “muli” sono spesso persone anziane con scarsa istruzione, reclutati per mezzo di avvisi di “lavori casalinghi” che credono di poter guadagnare onestamente il 10% spostando i fondi che vengono accreditati nei loro conti bancari su conti di “esportatori” esteri

<sup>5</sup> Un recente libro è M Jakobsson, S Myers, “Phishing and Countermeasures”, Wiley 2007

<sup>6</sup> Si veda per esempio Ross Anderson, “TK Maxx and banking regulation”, in <http://www.lightbluetouchpaper.org/2007/03/30/tk-maxx-and-banking-regulation/>

<sup>7</sup> Si veda Jack Hirshleifer, “From weakest-link to best-shot: the voluntary provision of public goods”, in Public Choice v 41, (1983) pp 371–386; e Hal Varian, “System Reliability and Free Riding”, in Economics of Information Security, Kluwer 2004 pp 1–15

<sup>8</sup> Don Davis, “Compliance Defects in Public-Key Cryptography”, Proc. 6th Usenix Security Symposium (San Jose, CA, 1996), pp. 171–178

Terzo, gli uffici marketing delle banche sono spesso difficili da distinguere rispetto ai phisher. Forse il peggior esempio viene da una grande banca del Regno Unito che ha inviato un vero e proprio spam per pubblicizzare i propri nuovi servizi usando URL non registrati dalla stessa banca. Le sue pagine web avvisavano correttamente i propri clienti di non rispondere alle email o cliccare sui link o rivelare proprie informazioni personali e lo stesso spam aveva un warning simile alla fine. La madre di un nostro studente ricevette questo spam ed avvisò il dipartimento di sicurezza della banca che le confermò che si trattava di un phishing. Lo studente successivamente contattò l'ISP per riferire dell'abuso e scoprì che la URL ed il servizio erano veri – sebbene forniti alla banca da una terza parte. Quando l'ufficio frodi di una grande banca non è in grado di distinguere il proprio spam dal phishing cosa si può ragionevolmente aspettare dai clienti di una banca?<sup>9</sup>

Quarto, la tecnologia usata per l'attacco ha avuto a disposizione molto tempo per essere sviluppata. Nelle ultime versioni del phishing, note come "vishing", ai clienti della banca veniva chiesto di telefonare ad un call center bancario che era in realtà gestito da malfattori. Il software di risposta automatica era programmato non solo con gli stessi script che usava il servizio "vero" ma anche con le stesse voci. Progettare una vera sicurezza che permetta non solo alla banche di riconoscere i propri clienti ma anche ai clienti di riconoscere le vere banche è sicuramente difficile. E in ogni caso rimarrebbe il problema fondamentale della sicurezza della piattaforma. Ecco un'altra argomentazione economica: Windows Vista rappresenta un passo avanti enorme per proteggere i contenuti video ma non offre nulla di nuovo per proteggere i numeri delle carte di credito dei clienti.

Per tutte queste ragioni non è ragionevole aspettarsi che l'integrità del sistema di pagamento possa basarsi esclusivamente sui meccanismi di autenticazione e dunque sul front-end. Si deve dare per scontato che, in ogni caso, una parte dei conti correnti dei clienti possa cadere sotto il controllo di criminali. I controlli di back-end sono dunque fondamentali: per limitare l'esposizione, per intercettare le frodi in corso, per rallentare la velocità delle transazioni fasulle e per recuperare i fondi rubati velocemente. A livello filosofico abbiamo bisogno di spostare la nostra attenzione dalla "integrità del sistema di pagamento" alla sua resilienza. Il vecchio sistema resisteva contro occasionali insider disonesti che cercavano di rubare grandi quantità di denaro e di solito fallivano. Gli insider occasionali disonesti esistono ancor oggi ma adesso abbiamo a che fare con un gran numero di conti correnti di clienti compromessi e dobbiamo assicurarci che il sistema di pagamenti sappia opporsi e gestire anch'essi.

## **I controlli sulle frodi e del perché falliscono**

Il primo sistema di e-banking per i consumatori, inaugurato nel 1984 dalla Bank of Scotland, aveva controlli molto severi: i clienti potevano spostare il denaro tra i conti ma effettuare pagamenti solo a terze parti su conti che avevano precedentemente indicato per iscritto. Così per pagare una bolletta elettrica un cliente doveva recarsi presso la filiale della banca, riempire un modulo indicando la sua compagnia elettrica, il suo numero cliente ed il limite di pagamento mensile. C'erano (serve dirlo?) poche frodi. Così i controlli furono via via resi meno severi e poi praticamente eliminati durante il periodo dell'entusiasmo per la bolla delle dotcom.

Ma ci devono essere, oltre ai controlli istituzionali, anche controlli generali di sistema. Le banche hanno una lunga tradizione nella cooperazione con le forze dell'ordine per il recupero dei soldi rubati dai truffatori. Se un programmatore, per esempio, inseriva una transazione non autorizzata nella coda dei messaggi SWIFT, disponendo un pagamento ad un complice all'estero, presumibilmente le procedure bancarie di quadratura avrebbero pizzicato l'anomalia il giorno lavorativo seguente dopodiché un senior manager avrebbe contattato la banca del beneficiario e fatto in modo che il complice venisse arrestato quando avesse cercato di incassare il contante. Le poche truffe di successo si basavano su una qualche modalità di portare fuori i beni attraverso il

---

<sup>9</sup> SA Mathieson, "Gone phishing in Halifax – UK bank sends out marketing email which its own staff identify as a fake", Infosecurity News, 7 ottobre 2005

sistema bancario stesso; nel noto caso della “Security Pacific” Rifkin usò i bonifici bancari per acquistare diamanti da un broker russo mentre in un altro caso che conosco i colpevoli si fecero dare un prestito di garanzia per una compagnia fantasma.

La SWIFT e le frodi sui bonifici di cui ci preoccupavamo 20 anni fa sono state adesso industrializzate e l’industria bancaria stessa deve industrializzare le misure per gestire tali fenomeni. Negli ultimi tre anni l’inondazione degli attacchi di phishing ha causato, nel Regno Unito, una riorganizzazione dell’asset recovery che è ormai una sorta di vera e propria linea produttiva. Mentre una volta era necessario l’intervento di un senior management ora gli storni delle transazioni sono decise dallo staff di front-line dell’ufficio antifrode della banca e sostenute da un network di reciproci indennizzi tra le banche.

La domanda fondamentale è se il sistema bancario sta rispondendo in maniera corretta allo stress imposto dal phishing e, più in generale, se esso può evolversi correttamente in risposta alle nuove minacce<sup>10</sup>. La security economics insegna che ciò dipenderà in larga misura dal fatto che ci siano appropriati incentivi.

Nel 2006, in UK, una singola banca ha accumulato 30 dei 35 milioni di sterline di perdite dovute al phishing. Secondo gli investigatori, i phisher hanno scelto come bersaglio questa banca proprio a causa dei suoi scarsi controlli interni e soprattutto per il suo scarso operato in tema di asset recovery: di fatto essa riesce a recuperare solo il 60% circa del denaro rubato rispetto al 75–95% dei suoi concorrenti. Non ho cifre precise per quanto riguarda gli USA ma le esperienze riportate dagli investigatori suggeriscono un pattern simile: rapida crescita delle frodi, con perdite concentrate sulle banche che richiedono ai propri clienti online pochi controlli e che hanno team di asset recovery meno efficaci.

Negli ultimi due anni i phisher hanno virato in massa verso i sistemi di pagamento non bancari come eGold (con Western Union che insegue al secondo posto). Si era inizialmente pensato che ciò fosse dovuto allo status offshore di eGold ed alla difficoltà di citare in giudizio e dunque individuare la destinazione dei soldi rubati. Ma negli ultimi anni (a causa delle ingiunzioni, dell’azione di IRS contro l’azienda madre, delle pressioni contro i siti di pedopornografia e del flusso continuo di citazioni<sup>11</sup>), eGold è diventata più reattiva. Di conseguenza ci sono stati alcuni spostamenti in questo tipo di business, specialmente verso Webmoney<sup>12</sup> e verso le banche degli stati baltici dalle quali i trasferimenti verso la Russia sono facili: tuttavia eGold rimane ancora la prima scelta.

Secondo gli investigatori, il vero motivo del successo di eGold è che i pagamenti di eGold non sono revocabili. Sebbene la polizia cerchi di tracciare gli operatori dei siti pedopornografici o coloro che usano tali sistemi per riciclare il denaro sporco, fin’ora chi si occupa di asset recovery non è mai riuscito a recuperare il denaro rubato e trasmesso attraverso questi sistemi non bancari. Per il crimine organizzato la tracciatura anche poco tempo dopo il reato è di poca rilevanza; in molte giurisdizioni i criminali possono usare documenti contraffatti (o veri ma ottenuti da pubblici ufficiali corrotti) per comparire e ritirare il contante mentre anche all’interno dei paesi meglio regolati essi non hanno difficoltà nel trovare persone disponibili, come i tossicodipendenti, per convertire i fondi in contante e successivamente scomparire. La finalità dei phisher quando selezionano un sistema di pagamenti non è tanto volta a nascondere l’identità dei loro galoppini di basso livello che effettuano praticamente la conversione in contanti quanto nel mettere in difficoltà gli uffici antifrode delle banche rallentando il processo di asset recovery.

---

<sup>10</sup> Un chiaro indicatore si ha nel nuovo campo dei sistemi biologici nel quale la robustezza si può evolvere; si veda H Kitano, “Self-extending symbiosis”, *Biological Theory* 1(1) 2006 pp 61–66

<sup>11</sup> B Grow, J Cady, S Rutledge, D Polek, ‘Gold Rush’, *Business Week*, 9 gennaio 2006; in [http://www.businessweek.com/magazine/content/06\\_02/b3966094.htm](http://www.businessweek.com/magazine/content/06_02/b3966094.htm)

<sup>12</sup> B Grow, B MacWilliams, “WebMoney and its Customers”, *Business Week*, 9 gennaio 2006; in [http://www.businessweek.com/magazine/content/06\\_02/b3966104.htm](http://www.businessweek.com/magazine/content/06_02/b3966104.htm)

## Implicazioni per la normative bancaria

Nel “vecchio” mondo delle banche che usano ancora la carta, un assegno o una cambiale potrebbero non essere onorati se non sono presenti fondi in modo sufficiente o se i fondi apparentemente disponibili sono il frutto di una frode (come avviene in truffe quali l’ordine di merci mai pagate, eccetera). Di conseguenza i pagamenti in entrata sono considerati “salvo buon fine” cioè effettivamente contabilizzati solo dopo che sono realmente incassati ed anche in quest’ultimo caso possono essere successivamente revocati. I meccanismi di risk-management si sono evoluti; in UK differenti banche avevano regole differenti per trattare pagamenti “salvo buon fine” (da tre a dieci giorni di ritardo). Le merchant bank di Londra hanno fatto utili per secoli “accettando” (quindi in realtà: garantendo) cambiali emesse dai commercianti. I mercati gestivano bene il rischio; in effetti il rischio finiva con l’essere assunto dai fornitori di “trust service” più capaci. Un po’ di tempo fa ho acquistato un’auto ed ho pagato alla mia banca £40 per avere un “assegno circolare” cioè un assegno per cui la mia banca garantiva al venditore dell’auto che ci fosse realmente la disponibilità del controvalore in denaro. Il mercato ha allocato questo particolare rischio alla mia banca; io sono stato un loro cliente per oltre 20 anni ed essa dunque può fornire una assicurazione sul “buon fine” dei miei assegni nella maniera più efficiente e a buon mercato di chiunque altro.

Tuttavia, durante l’ondata di innovazione scatenata dal boom delle dotcom, sono comparsi intermediari che a tutti gli effetti vendevano “assegni circolari” a prezzi inferiori a quelli di mercato dato che, sfruttando il loro status offshore, compravano “garanzie di pagamento” con denaro rubato. Se questo continuerà allora, a parte gli effetti sulla criminalità, ciò distruggerà i mercati esistenti che assicurano il rischio; se eGold può vendervi un “assegno circolare” per £20 quando la Lloyds’ Bank ve ne chiede £40 allora ovviamente la gente userà eGold per comprare le loro auto ed il mercato bancario degli assegni circolari crollerà.

Mantenere la resilienza del sistema finanziario dipende dall’allocazione dei rischi a quelle parti che meglio sono capaci di gestirli. Sarebbe meglio che ciò fosse fatto in modo trasparente dai meccanismi di mercato; in questo caso l’allocazione iniziale dei rischi sarà almeno meno critica. Ma se il mercato fallisce e ciascun attore cerca di scaricare la responsabilità agli altri allora ciò può portare ad una gara verso il basso nella quale la fiducia si perde.

Come possiamo assicurare che il sistema dei pagamenti elettronici rimanga affidabile come il sistema basato sugli assegni e cambiali cartacei ha fatto per molti anni? In un mondo dove ogni pagamento bancario può essere stato ordinato senza il mandato del titolare del conto – ed un piccolo ma significativo numero di questi casi è effettivamente accaduto – la strategia naturale del regulator è di insistere che per default tutti i pagamenti elettronici effettuati dai correntisti dovrebbero essere considerati provvisori fino a che sia passato abbastanza tempo perché sia verificato che essi siano effettivamente solvibili (almeno 90 giorni, ma PayPal ne richiede 180).

I pagamenti provvisori sono sufficienti per la grande maggioranza delle transazioni di basso valore tra gli individui e per quei business che trattano tra loro con frequenza. Ci sarà naturalmente una domanda di mercato per strumenti di pagamento irrevocabili – “assegni circolari digitali”. Molto probabilmente, per piccoli importi e buoni clienti, il pagamento irrevocabile comporterà solo un piccolo extra di seccature (come la richiesta di un SMS di conferma dalla banca di qualcuno) fino a quando il rischio di credito è supportato da un assessment automatico e il pagante ha una buona reputazione. I trasferimenti ai sistemi di basso valore quali borsellini elettronici possono anche essere gratuiti. Molto probabilmente però i pagamenti garantiti verso entità che sono note per essere condotte con spirito “speculativo” richiederanno un maggior sovrapprezzo e le garanzie costeranno ancora di più per i pagamenti in tempo reale rispetto alla compensazione nel giorno successivo. Questo creerà un incentivo perché gli operatori dei pagamenti non bancari conoscano e sorvegliano i loro clienti in modo più efficace.

## Implicazioni per la concorrenza

C'è un parallelo interessante tra i servizi di pagamento non bancari ed i centri finanziari offshore sui quali un'interessante inchiesta è apparsa recentemente sull'*Economist*<sup>13</sup>. I centri offshore possono essere un problema non solo a causa della criminalità finanziaria ma anche a causa della evasione fiscale e dei rischi sistemici di grandi flussi finanziari non regolamentati nei quali esoterici strumenti finanziari rendono i rischi meno trasparenti. Tuttavia la competizione che essi offrono sul fronte fiscale, regolatorio e dei servizi aiutano ad impedire che i governi dei grandi paesi diventino troppo grandi ed inefficienti e forniscono ai centri finanziari convenzionali anche uno sprone alla competizione. In modo simile i sistemi di pagamento non bancari possono garantire una utile concorrenza alle loro controparti regolate. Negli anni 90, quando il commercio elettronico su Internet prese il via, in molti paesi le aziende di carte di credito addebitavano esorbitanti commissioni anche ai piccoli business; in UK le commissioni arrivavano fino all'8%; occorre, attraverso la concorrenza, riuscire a garantire un giusto equilibrio costi/ricavi per le transazioni con carte di credito. Anche i grandi business dovevano pagare oltre il 2% di commissione. Si potrebbe pensare che si trattava di un ragionevole sovrapprezzo per il rischio di controparte che doveva essere accettato dal sistema delle carte a causa delle innumerevoli "contestazioni" sulle transazioni con carte di credito, ma si trattava in realtà di una mossa delle banche britanniche per garantirsi economicamente nel caso i commercianti spedissero beni di scarsa qualità o non spedissero nulla. Dato che tali pratiche oligopolistiche rappresentavano una seria minaccia potenziale allo sviluppo dell'e-commerce, l'arrivo di fornitori di servizi di pagamento non bancari come PayPal fu salutare. Il takeover di PayPal da parte di eBay è stato istruttivo da questo punto di vista; l'acquisizione ha portato significative sinergie grazie ai sistemi ed alla reputazione di eBay: in pratica un sistema di pagamento collegato direttamente a eBay può fornire garanzie alle controparti in modo più efficiente rispetto a terzi parti quali emittitori di carte o banche acquirenti.

Un altro esempio viene dai pagamenti basati sul telefono; il sistema MTN MobileMoney in Sud Africa è stato sviluppato da MTN, un fornitore di servizi per telefoni cellulari e fornisce un pagamento rapido basato sul telefono ad una frazione del costo degli assegni o dei bonifici. Questa è una buona notizia per la popolazione che rapidamente si urbanizza nel paese: molti di loro non sono clienti di una banca e non hanno neanche una residenza fissa (in questo caso, il sistema opera con un accordo di "agenzia" con una banca convenzionata che fornisce la copertura legale).

L'emergere delle compagnie di pagamento collegate ad aziende tecnologiche non è un fenomeno nuovo. La Western Union fu fondata nel 1851 come compagnia telegrafica; dieci anni dopo si collegò alla "US West and East Coasts", nel 1866 introdusse la telescrivente e nel 1871 grazie all'uso dello "stock ticket" (identificatore delle transazioni di pagamento) inaugurò un servizio di "money transfer". La Western Union alla fine del 19esimo secolo era ormai diventata principalmente una compagnia di servizi finanziari ed anche se le banche "ordinarie" cominciarono immediatamente ad utilizzare il telegrafo esse non poterono competere con una azienda tecnologica leader nell'innovazione<sup>14</sup>.

Naturalmente i servizi di pagamento non bancari non si limitano alla Western Union ed ai suoi successori su Internet come PayPal ed eGold. Hawala, hundi, fei chien ed altri sistemi di pagamento tradizionali sono stati in uso per generazioni prima dell'11 settembre ed offrivano un prezzo terribilmente competitivo rispetto al sistema bancario esistente con un trasferimento di \$5000 da New York a Islamabad al costo di \$5-10. Il 7 novembre del 2001 il Presidente degli USA ha dichiarato che i sistemi informali di trasferimento del denaro dovevano essere posti sotto il microscopio per impedire flussi di fondi legati al terrorismo o al crimine; il Patriot Act (s373) ha avuto la mano pesante sul business della trasmissione di denaro non regolamentato e da quel momento la pressione per implementare controlli contro il riciclaggio di denaro ha spinto il loro costo in alto fino a circa \$100 che è all'incirca la somma che chiede anche il sistema bancario

---

<sup>13</sup> J Ramos, "Places in the Sun", *The Economist*, 22 febbraio 2007

<sup>14</sup> T Standage, "The Victorian Internet", Walker and Company, 1998

convenzionale di commissioni (ciò è stato negativo per la concorrenza: dal 2002 il livello delle rimesse degli emigrati dagli USA al Pakistan attraverso il sistema bancario regolato è raddoppiato). Anche il Regno Unito ha adottato misure simili (anche se meno drastiche) richiedendo ai money remitters la registrazione presso la dogana dal 12 novembre 2001.

Gli studiosi del sistema hawala hanno recentemente espresso delle riserve sulla efficacia della regolamentazione dalla mano pesante sostenendo che un approccio “dolce” che richieda il coinvolgimento degli operatori e la fiducia tra le parti produca migliori risultati dal punto di vista del rafforzamento delle regole<sup>15</sup>. Per esempio, gli operatori hawala mantengono a lungo le registrazioni nei paesi occidentali dove le loro operazioni sono legali ma li distruggono subito dopo la transazione nel sud Asia dove il loro business è fuori legge. L’India, che nel 1973 ha reso illegale hawala, ha depenalizzato i divieti ora soggetti al solo al Codice Civile dal 2000; ed il Pakistan, che precedentemente obbligava al monopolio di una banca per i servizi di pagamento, ha annunciato che alcuni operatori hawala avranno una licenza (gli operatori hawala sono in realtà migliori di quanto si pensi nel tracciare e revocare le transazioni ma tutto dipende dalle registrazioni che devono essere mantenute).

Esistono anche sistemi di pagamento alternativi che non sono né tradizionali né web-based e quindi occorrono meccanismi ad hoc. Un buon esempio è relativo alla Repubblica Democratica del Congo dove a seguito del collasso del governo e delle infrastrutture commerciali la gente ha cominciato ad usare carte telefoniche prepagate come contante. Quando alcuni criminali presero un ostaggio in Katanga fu richiesto alla sua famiglia a Kinshasa di pagare il riscatto acquistando \$50 in carte telefoniche e cedendo loro i relativi codici di abilitazione. Nei paesi che non hanno sistemi bancari che funzionano la loro interfaccia con i settori informali è fondamentale per la regulation. I bonifici convenzionali e gli strumenti negoziabili sono largamente usati per regolare i pagamenti non bancari aggregati che danno alcuni utili poteri ai regolatori. PayPal insiste molto sul fatto che essa è di utilità per il sistema bancario: essa può essere usata per verificare gli intestatari dei conti inviando una piccola somma di denaro ai loro conti bancari dopo di che l’intestatario deve confermare di controllare quel conto rinviando a sua volta indietro a PayPal la somma e i riferimenti del pagamento. In questo modo PayPal evita la faticosa raccolta di milioni di fatture commerciali dei clienti dei conti utili. MTN fa qualcosa di simile; i clienti possono operare entro centri limiti sui conti aperti sulla base dell’identità dichiarata; se vogliono modificare questi limiti devono presentarsi presso una filiale bancaria con un documento di identità e qualcosa che dimostri che il loro indirizzo sia valido (ad esempio una bolletta pagata).

Ci possiamo quindi aspettare che continuerà ad esserci un mix fra sistemi di pagamento non bancari. Alcuni saranno di tipo tradizionale alcuni fortemente basati sulla tecnologia ed altri ad-hoc. Il fine ultimo dal punto della regolamentazione dovrebbe essere lo stesso di quello relativo ai centri finanziari offshore: avere i vantaggi competitivi che producono i sistemi alternativi e contemporaneamente impedire che essi siano troppo facilmente sfruttabili dalla criminalità. Per citare “The Economist”:

Due decenni fa c’erano principalmente depositi passivi del contante rivolti a grandi aziende, individui ricchi e disonesti. Alcune giurisdizioni ancor oggi presentano questa tripartizione nei loro commerci e dovrebbero essere posti fuori dal business. Ma i migliori di loro – per esempio Jersey e Bermuda – sono diventati sofisticati centri finanziari gestiti molto bene secondo le loro leggi, con valide expertise in certe nicchie come le assicurazioni o la finanza strutturata. Questo rapporto spiega che, nonostante le iniziative internazionali volte a ridurre i crimini finanziari siano benvenute, la maggior parte delle preoccupazioni dell’OFC sono artificiali. Gli ordinamenti giuridici di tutti i tipi, sia nominalmente onshore sia pubblicamente offshore, sono positivi per il sistema finanziario globale.

La domanda chiave è: che tipo di regole dobbiamo cercare di imporre ai servizi di pagamento non bancario e come possiamo imporle in un mondo globalizzato? Ho già sostenuto che la tracciabilità

---

<sup>15</sup> N Passas, “Informal Value Transfer Systems, Terrorism and Money Laundering”, US DoJ report 208301, gennaio 2005

dei pagamenti ed in particolare la revocabilità dei pagamenti non autorizzati sono fondamentali. Nel seguito analizzerò gli aspetti relativi alla privacy, alla identità ed alla protezione dei consumatori.

## Tracciare il denaro o tracciare le persone?

Garantire l'anonimato ai clienti onesti non è, in linea di principio, in antitesi con il tracciamento rapido ed il recupero dei fondi rubati. I sistemi di "digital-cash" possono gestire molto bene la tracciabilità – ciò che serve è semplicemente un database delle transazioni più recenti per evitare di raddoppiare le spese<sup>16</sup> (la moneta elettronica inventata da Chaum e commercializzata dalla sua azienda Digicash è considerata da molti ingegneri come il modo corretto di fare e-cash ma la sua diffusione è stata ostacolata dai problemi di brevetto – problemi che presumibilmente scompariranno quando i brevetti di Chaum non saranno più validi). Ci sono state molte pubblicazioni su come l'anonimato può essere reso opzionale in tali sistemi così che l'identità dell'intestatario di un conto sia rivelata solo se viene commesso un crimine<sup>17</sup>.

La modalità ad-hoc per mezzo del quale l'anonimato è stato garantito da eGold e da alcuni altri – conti trasferibili che erano vagamente collegabili alla reale identità dei sottoscrittori – hanno fatto nascere alcune discussioni molto interessanti. I banchieri tradizionali credono che sia importante "conoscere il proprio cliente"; i banchieri londinesi preferiscono insistere sulle referenze personali mentre i loro colleghi di Zurigo vogliono assolutamente vedere un passaporto – anche se il conto stesso viene presentato al mondo esterno come un anonimo conto cifrato.

Dopo l'11 settembre c'è stato un forte irrigidimento della legge più per quanto riguarda l'identità che per quanto riguarda i flussi di denaro. Sono stati gli USA a spingere perché tutti gli esseri umani fossero forniti di documento di identità con foto. Ciò ha provocato ostilità anche tra i più affidabili tra gli alleati degli americani. Il partito conservatore britannico progetta di affrontare le prossime elezioni (e sembrerebbe destinato alla vittoria) con una piattaforma elettorale che comprende l'opposizione alla già approvata carta identità obbligatoria mentre una indagine dell'Home Office rivela che 15 milioni di persone potrebbero rifiutarsi, in ogni caso, di accettarla<sup>18</sup>. Negli stessi USA, l'efficacia del programma US-VISIT è stata ripetutamente messa in discussione<sup>19</sup>.

Grazie alla pressione del Financial Action Task Force (FATF), i clienti delle banche in tutto il mondo nel giro di pochi anni hanno dovuto affrontare un vero e proprio "identity circus" – che obbliga anche un banchiere privato che conosce i propri clienti da più di trent'anni a chiedere loro copie delle fatture del gas o dell'elettricità come prova del loro effettivo indirizzo di residenza. Ciò è ridicolo dato che i banchieri privati conoscono i loro clienti molto meglio che la compagnia del gas; questo è un classico esempio di risk management che è stato trasformato in due diligence che a sua volta produce "moral hazard". Un manager bancario corrotto potrebbe infatti pensare che, avendo un bel pacchetto di bollette del gas messe da parte, gli potrebbe convenire aprire conti correnti fasulli per riciclare denaro. Le bollette del gas sono abbastanza facili da falsificare specialmente adesso che in UK ci sono oltre 400 aziende del gas molte delle quali forniscono bollette online. Inoltre le norme sono oppressive nei confronti di chi vorrebbe essere ligio alla legge come una donna sposata i cui conti di casa sono indirizzati presso il marito o gli studenti che arrivano dall'estero per frequentare l'università. La situazione peggiore è per le persone del terzo mondo; ci sono milioni di persone che vivono in capanne in Africa e non hanno un indirizzo di residenza comprovato da contratti con le compagnie del gas o dell'elettricità e che tuttavia hanno bisogno di servizi finanziari per riuscire a sfuggire alla povertà. I vecchi metodi erano in molte circostanze molto più efficaci. Quando aprivo per la prima volta un conto bancario avevo bisogno

---

<sup>16</sup> D Chaum, "Achieving Electronic Privacy", Scientific American, agosto 1992, pp 96–101, in [http://www.chaum.com/articles/Achieving\\_Electronic\\_Privacy.htm](http://www.chaum.com/articles/Achieving_Electronic_Privacy.htm)

<sup>17</sup> R Davies, "Electronic Money, or E-money, and Digital Cash", in <http://www.ex.ac.uk/~RDavies/arian/emoney.html>

<sup>18</sup> R Winnett, D Leppard, "Millions to rebel over ID cards", Sunday Times, 8 aprile 2007, in <http://www.timesonline.co.uk/tol/news/uk/article1626768.ece>

<sup>19</sup> Si veda per esempio EPIC, "United States Visitor and Immigrant Status Indicator Technology", at <http://www.epic.org/privacy/us-visit/>

delle referenze di due correntisti bancari già registrati. Ultimamente il mondo online sta scoprendo i benefici del “social network” come sono adesso definiti; i social network possono essere mappati e i pattern sospetti di relazioni essere individuati. Un approccio troppo rigido all’identificazione dei clienti ha dunque portato a sostituire un sistema che funzionava con uno che è più facilmente ingannabile dai criminali. Oggi fortunatamente la spinta verso l’identificazione obbligatoria sta esaurendo le forze dal punto di vista politico anche perché è essa è inefficace nei paesi in via di sviluppo dove sono disponibili migliori meccanismi di controllo. In questi paesi la situazione è peggiorata dal fatto che i documenti di identità o non esistono o possono essere facilmente contraffatti. In India di solito le persone non hanno documenti; in Pakistan è facile ottenere documenti di identità sotto falso nome da impiegati governativi corrotti. Il problema del Pakistan è così grave che l’UAE ha predisposto un sistema di riconoscimento dell’iride nei suoi porti ed aeroporti per controllare le identità dei passeggeri in arrivo per mezzo di un database di persone espulse (la maggior parte di loro prostitute dal Pakistan). Fino ad oggi oltre 73.000 passeggeri sono stati individuati come facenti parte della lista dei sospetti<sup>20</sup>.

La pressione politica verso l’obbligo di avere documenti di identità danneggia direttamente anche alcuni servizi di pagamento non bancari; per esempio, Western Union ha tentato a lungo di ottenere l’identificazione dei destinatari dei pagamenti ma con il solo risultato di ricevere un danno reputazionale in Nigeria e dovunque la gente raccoglie fondi usando false identità grazie alla complicità di ufficiali governativi corrotti<sup>21</sup>.

Adesso che sono passati cinque anni dall’impeto regolatorio post undici settembre è tempo di riflettere e valutare cosa sia esagerato e cosa sia insufficiente. L’enfasi sulla carta d’identità si è esaurita e non la si ritiene ormai più una panacea. Quindi il framework esistente non ha sufficientemente facilitato la cooperazione nell’asset recovery. Il più applicabile dei 25 criteri del FATF è l’obbligo per ciascun paese di criminalizzare il riciclaggio dei proventi dei crimini più seri ma, in ogni caso, la campagna del FATF è arrivata alla naturale conclusione in tutti i paesi compresa la Birmania che ora è conforme<sup>22</sup>. Tuttavia il furto da parte di un phisher di \$4.000 dal conto di un cliente potrebbe di per sé non essere considerato un crimine serio. La più applicabile tra le 40 raccomandazioni del FATF è la numero 38 che recita “Ci dovrebbe essere una autorità che adotta azioni efficienti e veloci in risposta alle richieste dei paesi stranieri di identificare, congelare, sequestrare e confiscare i beni riciclati, i profitti del riciclaggio di denaro o anche indica quali sono i reati ed i poteri e gli strumenti da usare nella persecuzione di questi reati e nel recupero dei beni”. Anche in questo caso si potrebbe sostenere che il phishing non è di per sé uguale al riciclaggio di denaro sporco e che “azioni efficienti e veloci” può essere interpretato in alcuni paesi come relativo ad un periodo di settimane o mesi piuttosto che ore. Così non sono d’accordo con le conclusioni del rapporto 2006 del FATF e non credo che le sue regole siano adeguate per i nuovi sistemi di pagamento<sup>23</sup>. Il problema fondamentale è che abbiamo permesso che la regolamentazione delle banche fosse guidata dalla preoccupazione di rafforzare le leggi, le strategie e le tattiche mentre il fattore economico è quello realmente importante. Non solo il crimine è correlato all’economia – esso diminuisce via via che i paesi diventano più ricchi – ma anche per quel che riguarda i conflitti sociali ed il terrorismo l’economia è il vero fattore chiave. Ricerche innovative di Paul Collier e Anke Hoeffler per la Banca Mondiale hanno esaminato le cause scatenanti delle guerre civili<sup>24</sup> ed i dati indicano in modo inoppugnabile che si tratta quasi sempre di una causa economica. I problemi, i conflitti e le lamentele sono presenti ovunque ma per dare inizio ad una guerra civile deve esserci un qualche modo per pagare e rifornire i combattenti. Possiamo trovare le radici del conflitto

---

<sup>20</sup> J Daugman, “United Arab Emirates Deployment of Iris Recognition”, in <http://www.cl.cam.ac.uk/~jgd1000/deployments.html>

<sup>21</sup> N Passas, op. cit.

<sup>22</sup> FATF, “Annual Review of Non-Cooperative Countries and Territories”, 2005–6

<sup>23</sup> FATF, “Report on New Payment Methods”, 13 ottobre 2006

<sup>24</sup> Anke Hoeffler, Paul Collier, “Greed and Grievance in Civil Wars”, 2004, Oxford Economic Papers 56: 663-595; si veda anche “Breaking the Conflict Trap: Civil War and Development Policy”, OUP 2003

irlandese nella volontà degli irlandesi-americani di finanziare l'IRA mentre la guerra civile in Sri Lanka è stata innescata dalle donazioni dei Tamil negli USA, India e UK (dopo l'11 settembre per un certo periodo la guerra civile irlandese è cessata e quella dello Sri Lanka è diventata silente a seguito della ridotta tolleranza del terrorismo da parte degli USA). Pertanto dato che il terrorismo islamico è ancora foraggiato da facoltosi e mal consigliati finanziatori nella penisola arabica, occorrerebbe tracciare il denaro così come si tracciano le persone: dobbiamo riequilibrare gli sforzi e ripristinare l'equilibrio tra i due tipi di tracciamento. Occorrono maggiore trasparenza finanziaria e tracciabilità delle transazioni e meno raccolta di bollette del gas. A riguardo può essere istruttivo notare che PayPal non ha obiezioni sulla identificazione sebbene ciò limiti cosa gli utilizzatori "non verificati" possono fare mentre considera i pagamenti provvisori in linea di principio per almeno 180 giorni; inoltre non permette ai clienti di ritirare il contante nelle cosiddette "regioni send-only" cioè in quei paesi con legislazioni insufficienti.

## Implicazioni per i controlli di antiriciclaggio

Al momento i costi di compliance che le istituzioni finanziarie sostengono sono considerevoli per quanto riguarda le misure contro il riciclaggio di denaro sporco. Oggi tali controlli sono largamente indirizzati solo verso i terminali finali del traffico, la pizzeria, il gelataio e gli altri posti dove il contante potrebbe essere reinserito nel sistema bancario. C'è poca attenzione, invece, sia al processo di layering (stratificazione) cioè al processo che permette al denaro sporco di essere spostato da un conto all'altro sia al processo di output cioè alla fase in cui il denaro viene trasformato in beni non contabilizzati (sebbene l'attenzione verso l'ultimo punto sia recentemente cresciuta).

Il phishing ci costringe a prestare maggiore attenzione al processo di output. Qualsiasi meccanismo che permette ad un bonifico di essere tramutato in un bene al portatore può essere usato, dai criminali, per interrompere la catena dell'asset-recovery ed è così assai probabile che sia usato anche dai criminali online prima o poi. Occorre rendere i pagamenti ed il rischio di controparte trasparenti così da spostare il focus del controllo dell'antiriciclaggio dalla fase di input ad una visione più bilanciata di input e output. Ci si può augurare inoltre che nuovi meccanismi di revoca propriamente progettati renderanno il tracciamento più semplice anche rendendo il processo di layering più facilmente accessibile agli investigatori. Una maggiore attenzione al tracciamento del denaro, a scapito di quello sulle persone, ha senso anche nel contesto del crescente interesse per il recupero dei proventi del crimine in generale e non solo del crimine online. Nel 2000 in UK il rapporto governativo sul "Recovering the Proceeds of Crime"<sup>25</sup> ha portato al "Proceeds of Crime Act" del 2002 da cui è nata la "Asset Recovery Agency (ARA)". Gli obiettivi di ARA sono diversi; in primo luogo deve sequestrare il denaro dei criminali già condannati; in seconda battuta, nel caso il procedimento penale non avesse avuto successo, deve intentare una azione civile per tentare il recupero dei beni; infine, se i criminali sono residenti nel Regno Unito, deve torchiarli dal punto di vista fiscale per quanto riguarda i proventi del crimine.

L'idea è buona ma finora essa non ha funzionato per la frode. La maggior parte dei 14 milioni di sterline di beni congelati nel 2004 è relativa ai proventi del traffico di droga; la stessa ARA stima che i tre business criminali che generano maggiori profitti in UK siano la frode (perdite e costi per 14 miliardi di sterline), le droghe illegali (6,6 miliardi) ed i furti di veicoli (900 milioni)<sup>26</sup>. Sulla base di queste cifre, l'asset recovery nei confronti dei truffatori rimane piuttosto deludente. Spostando gli sforzi da una lenta tracciabilità delle persone ad una rapida revocabilità dei trasferimenti dei fondi può dunque solo aiutare. La nostra proposta è di limitare i pagamenti non revocabili sia ai grandi pagamenti esplicitamente garantiti (come gli assegni circolari) dove i mercati potrebbero creare pressione perché i sottoscrittori conoscano effettivamente i loro clienti sia

---

<sup>25</sup> UK Cabinet Office, "Recovering the Proceeds of Crime", in [www.cabinetoffice.gov.uk/strategy/downloads/su/criminal/crime.pdf](http://www.cabinetoffice.gov.uk/strategy/downloads/su/criminal/crime.pdf)

<sup>26</sup> J Earl, "The Work of the Assets Recovery Agency", NAO Fraud conference, in [www.nao.org.uk/conferences/fraud/ConferenceSlides.pdf](http://www.nao.org.uk/conferences/fraud/ConferenceSlides.pdf)

ai sistemi a basso valore come il borsellino elettronico ed i pagamenti telefonici che hanno poco interesse dal punto di vista dell'antiriciclaggio.

## I diritti dei consumatori

Un ostacolo al recupero dei proventi del crimine è rappresentato dal fatto che spesso perdite ricadono su persone che non hanno le risorse economiche per condurre le operazioni di recupero dei propri beni. Un trend particolarmente preoccupante a questo riguardo è l'azione congiunta delle banche in Europa per far ricadere le responsabilità della frode su clienti e commercianti. Questo fenomeno è iniziato molti anni fa quando le regole relative alla risoluzione delle frodi agli ATM (bancomat) erano diverse sulle due sponde dell'Atlantico. Negli USA, la prima sentenza relativa ad un caso di "prelievo fantasma" si concluse a favore del cliente<sup>27</sup> portando alla "Regulation E" che limitava la responsabilità della clientela per le transazioni elettroniche che non risultavano effettivamente autorizzate. Nel Regno Unito i primi casi "giudiziari" hanno avuto un esito opposto e le banche per anni hanno continuato con dichiarazioni del tipo "i nostri sistemi sono completamente sicuri e dunque se il vostro PIN è stato utilizzato da qualcun altro ciò si deve solo alla vostra incuria". Questo atteggiamento ha creato ovviamente un "moral hazard", un effetto economico perverso, spingendo di fatto le banche a curarsi di meno della sicurezza dei loro ATM ed in ultima analisi ha prodotto una valanga di frodi ai bancomat nel biennio 1992 – 1994 il che, in ultima analisi, ha obbligato ad una revisione dell'UK Banking Code. Si potrebbe pensare che tale scarico di responsabilità possa almeno aver creato un vantaggio competitivo alle banche britanniche rispetto alle banche americane in quanto esse avrebbero speso meno per la sicurezza o per i rimborsi delle frodi. In realtà questo ragionamento è errato. Le banche britanniche spendono molto più denaro in sicurezza perché effettuano molte più in "due diligence" invece che in attività volte alla riduzione del rischio ed alla fine sono soggette a molte più frodi a causa del "moral hazard". Questa curiosa anomalia è uno dei motivi che ha causato così tanto interesse per l'economia dell'information security<sup>28</sup>. Quanto sostengo è stato provata sperimentalmente. Due anni fa le banche del Regno Unito hanno introdotto le carte di credito dotate di chip EMV e con PIN obbligatorio: ebbene immediatamente esse sono ritornate alla dottrina dell'infallibilità e della sicurezza "assoluta" e ricominciato a rifiutare i reclami dei clienti; come previsto c'è già stato un aumento esponenziale delle frodi. Contemporaneamente le banche hanno anche scaricato la responsabilità per le frodi dovute allo shopping elettronico con carta di credito "virtuale" sui commercianti. Infine, più recentemente, lo sviluppo dell'electronic banking ha portato molte istituzioni finanziarie ad imporre ai loro clienti termini e condizioni contrattuali che scaricano nei loro confronti il rischio di frode; i clienti che accettano di usare una password per operare con la propria banca via telefono o online di fatto accettano che, in caso di contenzioso, l'onere della prova sia a loro carico. Bohm, Brown e Gladman hanno analizzato<sup>29</sup> i contratti proposti dalle banche. Il programma 'Verified by VISA' in pratica cerca di trasferire la responsabilità nei casi di truffa con carta di credito nello shopping online dai commercianti agli issuer ed ai clienti.

L'esempio più recente di "scarico di responsabilità" è la proposta di direttiva EU per i servizi di pagamento<sup>30</sup> che nei fatti rischia di livellare verso il basso (cioè secondo il modello del Regno Unito) la protezione dei consumatori in Europa. In tal modo le banche potranno imporre le loro condizioni nella risoluzione delle controversie e quindi, di fatto, essere sia giudici che giurie nelle dispute con i propri clienti. C'è ancora una speranza che il Parlamento Europeo emenda ciò prima che la direttiva diventi legge ma l'industria bancaria europea è molto più coesa che in America e nel passato è stata a tutti gli effetti una lobby.

---

<sup>27</sup> Judd v Citibank, 435 NYS, 2d series, pp 210–212, 107 Misc.2d 526

<sup>28</sup> Hal R. Varian, "Managing Online Security Risks", New York Times, primo giugno 2000; in <http://www.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html>

<sup>29</sup> N Bohm, I Brown, B Gladman "Electronic Commerce: Who Carries the Risk of Fraud?" JILT 2000 (3)

<sup>30</sup> Proposal for a Directive on Payment Services (PSD), in [http://ec.europa.eu/internal\\_market/payments/framework/index\\_en.htm](http://ec.europa.eu/internal_market/payments/framework/index_en.htm)

Come tutto ciò riguarda i regulator USA ed il contesto dei servizi di pagamento non bancari? Molto semplicemente le società non bancarie hanno un incentivo nell'arbitraggio del rischio che li porta a scaricare le responsabilità adottando il modello europeo. L'esempio classico è eGold: se la tua passphrase viene usata tu sei l'unico responsabile; tutte le spese sono autorizzate in via presunta e nessun pagamento può essere revocato<sup>31</sup>. Il meno criticabile sembra essere PayPal, il cui user agreement per i clienti USA propone varie alternative per la risoluzione delle dispute ma solo sotto i \$10.000; negli altri casi il foro competente è quello della California (con le spese legali pagate dal vincitore); il suo agreement per i clienti europei specifica invece che il foro competente è nel Regno Unito o che in alternativa le parti si appelleranno al britannico Financial Ombudsman Service: ma il primo è costoso ed il secondo è notoriamente a favore delle banche. Per essere più gentile PayPal dichiara che essa considera le eventuali perdite del cliente dovute sempre a transazioni non autorizzate ed in questo esso è un service provider modello. Tuttavia se PayPal in modo errato ritenesse che un cliente è colluso in una truffa allora revocare l'addebito per il cliente potrebbe rivelarsi molto più difficile che con una banca. Sembra inevitabile che via via che i servizi di pagamento si diffonderanno essi diventeranno sempre più soggetti alle frodi online e che dunque i reclami da parte di onesti cittadini diventeranno una costante; sempre più spesso arriveranno proteste del tipo "Non ho autorizzato tale pagamento" oppure "Sono stato truffato – Pensavo di pagare \$2 per un parchimetro a Baltimora ed invece mi sono stati addebitati \$2.000 di fiches per un casino online a Macao". Anche le tecnologia alla base dei reclami cambieranno nel tempo – quest'anno il tema dominante potrebbe essere la truffa sulle transazione ACH (Automated Clearing House – trasferimento elettronico di fondi) nei prossimi cinque anni<sup>32</sup> invece le transazioni RFID. In ogni caso però devono essere previsti mezzi adeguati ed efficienti per gestire e risolvere i reclami dei clienti altrimenti non solo si perderà la loro fiducia ma avremo anche incentivi economici insufficienti per contrastare la criminalità e migliorare i sistemi. In definitiva solo i fornitori dei servizi di pagamento possono contrastare con successo le frodi online; solo essi infatti hanno accesso a tutti i dati ed anche la capacità di migliorare i sistemi. Se le banche e gli operatori finanziari non bancari non faranno il possibile tutti gli sforzi saranno inutili.

## Conclusioni

Le società umane hanno sempre avuto leggi per rendere difficile ad un ladro di scappare con i beni rubati o il denaro. In generale un ladro non dovrebbe mai poter acquisire un titolo legittimo sul bene sottratto alla sua vittima. Nel passato ci sono sempre state regole per dare certezza sulla proprietà: nell'Inghilterra medioevale se rubavi il mio cavallo e lo vendevi al vicario in un mercato, regolato tra il crepuscolo e l'alba, il vicario acquisiva sì un titolo legittimo sull'animale ma questo non estingueva il mio diritto che tu fossi impiccato e che denaro frutto della vendita fosse sequestrato e mi fosse assegnato come rimborso. Il riciclaggio di danaro era più difficile; a parte alcuni casi speciali<sup>33</sup>, il denaro rubato poteva sempre in linea di principio essere recuperato. Per questa ragione, le transazioni che necessitavano di pagamento certi hanno a lungo usato degli intermediari che assicuravano il rischio di controparte, fossero essi "accepting houses" (società specializzate nell'accettazione di carte commerciali) che sottoscrivevano i debiti dei commercianti o fossero venditori che scontavano le fatture o anche banchieri che vendevano assegni circolari ai loro clienti. Così per lungo tempo, fino a quando tali rischi sono stati trasparenti e trasferibili, il mercato ha selezionato le figure economiche che meglio erano capaci di gestire questi rischi il che di solito significava una istituzione finanziaria ben conosciuta alla parte che doveva fidarsi. Questo apparato di risk management è stato largamente analizzato in termini piuttosto generali da studiosi di legge ed economia, ma non è mai diventato una parte formale della regolazione bancaria. Negli ultimi

---

<sup>31</sup> eGold, Terms of Use, in <http://www.e-gold.com/unsecure/terms.htm>

<sup>32</sup> RJ Anderson, "RFID and the Middleman", Financial Cryptography 2007, in [www.cl.cam.ac.uk/~rja14/Papers/rfid-fc07.pdf](http://www.cl.cam.ac.uk/~rja14/Papers/rfid-fc07.pdf)

<sup>33</sup> Come nei casi in cui un truffatore si sia rifugiato in un paese senza controlli e si sia messo sotto la protezione della criminalità

dieci anni la crescita dei servizi di pagamento elettronici ha indebolito questo sistema. La rapida globalizzazione ha creato infatti forti incentivi a tali figure economiche perché cerchino in ogni modo di liberarsi dei propri rischi di controparte; la confusione in ambito regolatorio e negli arbitrati hanno portato inoltre le istituzioni finanziarie a riscrivere i loro contratti per scaricare i rischi sui loro clienti (o gestori delle carte o commercianti) là dove era possibile; ed i nuovi schemi di pagamenti non bancari sono stati definiti fuori dai tradizionali regulatory framework. Mentre alcuni di tali servizi di pagamento hanno operato in modo corretto trasformandosi in grandi aziende dotate di buona reputazione altri hanno approfittato della situazione: in ogni caso come era inevitabile anche le aziende migliori hanno ridotto la tradizionale protezione dei consumatori. L'arbitrato delle terze parti è stato via via sostituito da un approccio del tipo “abbi fiducia in noi – ti rimborseremo se sarai derubato”. Tutto ciò rischia di farci tornare al mondo della regolazione bancaria del diciottesimo secolo; siamo di fronte ad una corsa verso il basso e forse anche ad una nuova bolla speculativa, versione elettronica dello scandalo South Sea. La reazione iniziale dei regolatori al problema è stata confusa dagli avvenimenti dell'11 settembre ed in particolare dalle pressioni dei governi per misure di sicurezza e controllo basato sull'identificazione delle persone per mezzo di carte di identità ed anche di strumenti biometrici. Indipendentemente dai costi e benefici di tale programma di “identificazione” esso è stato realizzando a spese dei controlli per tracciare i fondi rubati. Seguire il percorso del denaro e dare un nome al sospetto non sono prassi intercambiabili e passare da un approccio all'altro richiede costi sensibili. Adesso che, in tutto il mondo, la spinta verso l'identificazione ad ogni costo delle persone non è più considerata una priorità imprescindibile, abbiamo bisogno di tornare a seguire il denaro. Un ulteriore punto di attenzione è il tentativo in molti paesi (specialmente in Europa) di portare la responsabilità delle transazioni non autorizzate dalla parte che si fida alla parte che asserisce di aver concesso l'autorizzazione. La bozza di direttiva EU sui servizi di pagamento deve essere messa a confronto con la “Regulation E” che ha servito bene l'industria bancaria USA ed i suoi clienti per una generazione. Il rischio è che spostando la responsabilità della frode dalle banche ai commercianti ed ai clienti, gli sforzi di asset recovery saranno indeboliti così come gli incentivi per rendere sicuri i sistemi di pagamento.

In conclusione, suggerisco ai regolatori di insistere seriamente sulla “revocabilità” dei pagamenti elettronici. Regole chiare negli USA si propagheranno inevitabilmente all'esterno verso i paesi meglio regolati (inclusi i centri off-shore ben regolati); i pagamenti verso paesi con controlli inadeguati dovrebbero essere irrevocabili e così richiedere un “risk premium”. Questo renderebbe i servizi finanziari non bancari meno attraenti come veicoli per “trucchetti” finanziari; se eGold avesse accettato solo assegni circolari i phisher non avrebbero usato questo canale così spesso. In questo contesto è opportuno muoversi rapidamente verso una regolazione “leggera” degli operatori del sistema dei pagamenti non bancari; ciò garantirà ed incoraggerà la competizione, sosterrà i diritti dei consumatori, proteggerà il sistema dei pagamenti contro la criminalità e soprattutto ci porterà in una nuova fase per quanto riguarda al sicurezza delle informazioni: una fase nella quale l'attenzione si sposterà dalla protezione dell'integrità del sistema dei pagamenti all'assicurazione della sua resilienza in caso di attacco.

**Ringraziamenti:** ho avuto utili discussioni con un gran numero di persone tra cui Richard Clayton, Nick Bohm, Steven Murdoch, Johann Bezuidenhout, Matthew Pemble, Nikos Passas, Sharon Lemon, Andy Auld, Keith Mularski and Rafal Rohozinski.

La redazione di questo studio è stato, grazie a loro, un originale progetto di ricerca.