



Frauds: some facts

DIREZIONE V:
Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali

UCAMP:
Ufficio Centrale Antifrode Mezzi di Pagamento

Newsletter n° 4 - Luglio 2013

In questo numero:

Frodi con le carte di pagamento

♦ **Le transazioni non riconosciute. Categorie merceologiche anno 2012**

p. 1

E-payment e My Bank: una soluzione innovativa per lo sviluppo del commercio elettronico
(Emanuele Cecala, ABI)

p. 3

L'importanza della prevenzione nelle tlc
(Fabrizio Testoni, Fraud Manager, H3G Italia)

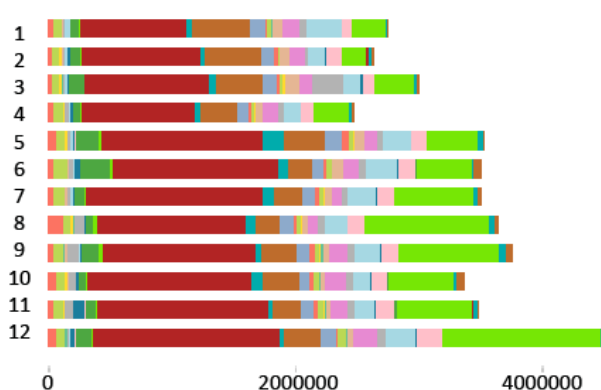
p. 5

Formazione ed Eventi

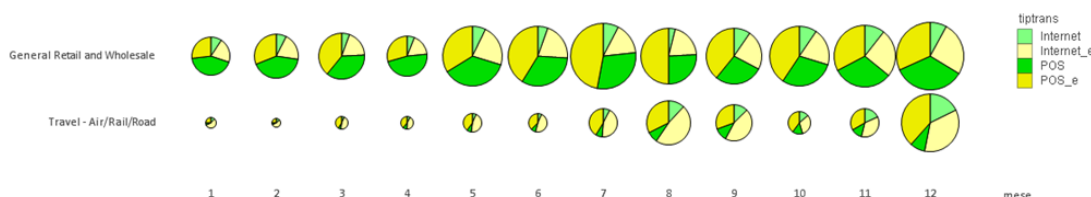
p. 7

Le transazioni non riconosciute

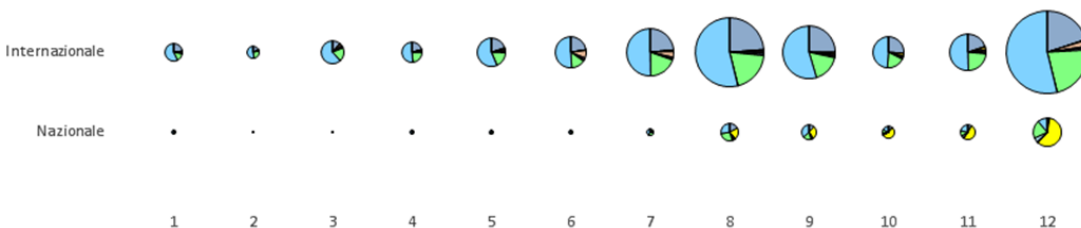
Dall'osservazione dell'andamento mensile delle transazioni non riconosciute per gruppi di categorie merceologiche emerge il forte aumento del gruppo Travel/Rail/Road che raggiunge, nel mese di dicembre, livelli paragonabili al gruppo General retail, il più ampio (comprende decine di categorie) e quindi storicamente più colpito. L'aumento si verifica in particolare a partire dalla metà dell'anno e mostra dei picchi nei mesi di agosto e dicembre, mesi in cui sono più frequenti viaggi aerei per turismo.



Focalizzando l'analisi su queste due gruppi (grafico sottostante), si nota immediatamente quanto sia stato elevato l'aumento del gruppo Travel/Rail/Road e come quest'ultimo si caratterizzi per una peculiare composizione per canale/nazione: sono molto più rilevanti le transazioni internazionali (aree gialle) e le transazioni su internet in generale (verde chiaro e giallo chiaro).



Nel grafico seguente viene rappresentata la composizione del gruppo Travel/Rail/Road distinguendo per nazionalità (nazionale/internazionale) e per singola categoria merceologica (la composizione delle torte).



Dal grafico si possono trarre le seguenti considerazioni: il fenomeno si concentra prevalentemente all'estero, e solo nell'ultima parte dell'anno interessa anche l'Italia; le categorie rilevanti all'estero sono quelle che riguardano le compagnie aeree e le agenzie di viaggio (tonalità di azzurro e verde); in Italia, oltre alle già citate categorie, vi è una presenza importante della categoria Bus/Charter/Tour (giallo).





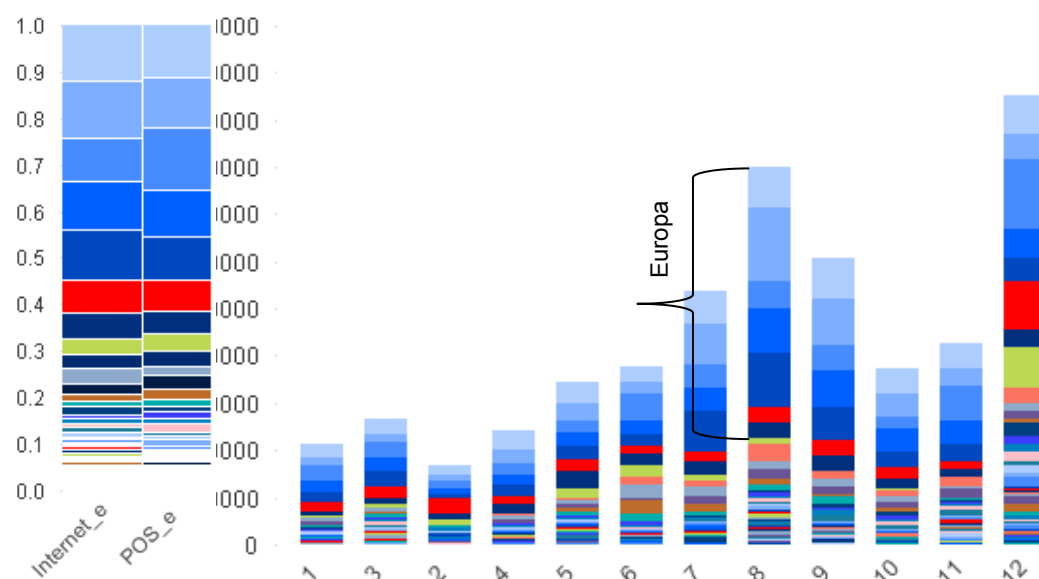
DIPARTIMENTO DEL
TESORO

MINISTERO DELL'ECONOMIA E DELLE FINANZE

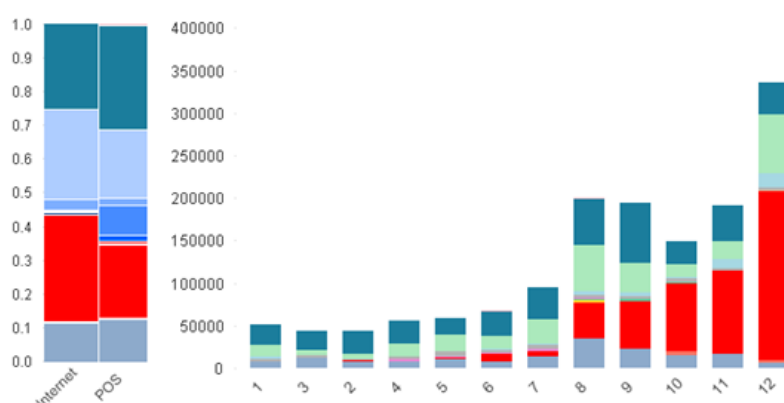
Frauds: some facts

Numero 4

Pagina 2 di 7



I due grafici analizzano la componente internazionale. Nel primo grafico a sinistra vengono messe a confronto le nazioni dove il fenomeno è avvenuto rispetto al canale di pagamento (dati 2012). Si può notare come non vi siano differenze sostanziali (la distribuzione è la stessa) di comportamento dei frodatori rispetto al mezzo, internet o POS. Il dettaglio mensile per paese della componente internazionale, la più **rilevante, viene riportato nel grafico seguente che mostra l'andamento del fenomeno. Le barre di tonalità azzurra** rappresentano i paesi europei, quella in rosso, gli Stati Uniti. Una tale preponderanza dei paesi europei non è comune a tutte le altre categorie merceologiche ma rappresenta un fenomeno peculiare. Il valore medio di ogni singola transazione ha un andamento piuttosto stabile per i primi 9 mesi dell'anno (circa 350€) per poi scendere a 280€ e risalire a dicembre a 450€.



Anche in Italia la composizione per canale è simile: i frodatori agiscono sulle stesse categorie indipendentemente dal canale internet o POS (grafico a sinistra). Molto diversa è invece la composizione per categorie merceologiche:

nella seconda metà dell'anno, oltre alle tre categorie già osservate nella componente internazionale, viene colpita con sempre maggiore intensità la categoria dei Trasporti (Bus lines/charter/tour in rosso nel grafico). Questo riguarda quasi esclusivamente l'**alta velocità ferroviaria**, sia sul canale POS che internet. Il fenomeno treni ad alta velocità sul canale POS si concentra **esclusivamente** nella provincia di Roma. Il valore medio delle transazioni sulle tre categorie relative a voli e viaggi aumenta sensibilmente nei mesi di agosto e dicembre.



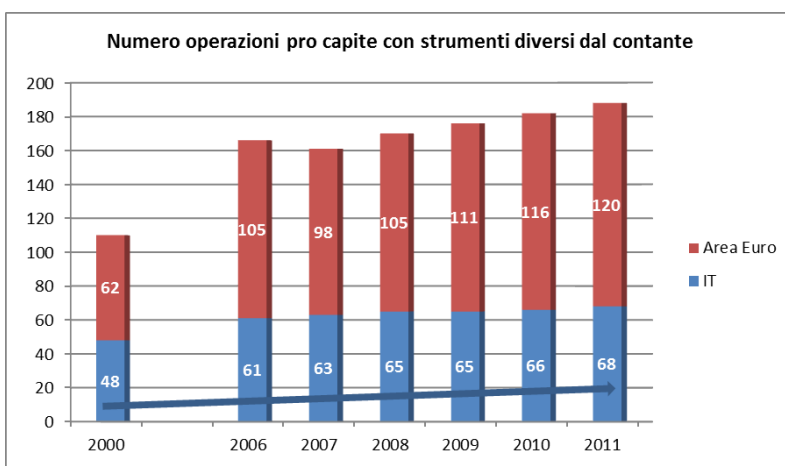
E-payment e My Bank: una soluzione innovativa per lo sviluppo del commercio elettronico Dr. Emanuele Cecala - Ufficio Sistemi e Servizi di Pagamento - ABI

Con il termine inglese "E-payments" si indicano tutti quei pagamenti elettronici (bonifici in internet, carte di pagamento, addebiti preautorizzati, prelievi bancomat) che si contrappongono ai pagamenti disposti attraverso i canali tradizionali (operazioni di prelievo e bonifici da sportello, assegni e incassi commerciali non automatizzati).

Tali pagamenti ormai da diversi anni, e sempre con maggiore intensità, svolgono un ruolo di primo piano nell'intero sistema economico-finanziario, nazionale e transfrontaliero, in virtù delle loro caratteristiche di economicità, trasparenza ed efficienza.

Il contesto di riferimento: il ricorso a strumenti e-payments da parte degli italiani cresce

Negli ultimi anni si è registrata nel nostro Paese, in linea con quanto avvenuto a livello europeo, una crescita nell'uso di strumenti di pagamento elettronici (pari a +6,7% nell'ultimo anno di osservazione, il 2012) a fronte di una riduzione



di quelli "tradizionali" (-3,9% nel 2012). La dinamica più sostenuta ha riguardato gli strumenti innovativi, soprattutto nella componente eseguita attraverso canali telematici: nel 2012 sono stati effettuati 344 mln di pagamenti in Internet (+22,9%); le operazioni online con carte di credito e prepagate sono cresciute del 25,9% e i bonifici online del 22,7% (*Relazione sulla gestione e sulle attività della Banca d'Italia 2012*, 31/05/2013). Nel 2011 sono state regolate 68 operazioni pro capite con strumenti alternativi al contante contro 188 dell'Area Euro (*Relazione annuale della Banca d'Italia*, 31/05/2013), proseguendo il trend degli ultimi anni.

Il quadro normativo europeo e nazionale

L'uso dell'e-payment è stato ed è sostenuto anche grazie a una legislazione, europea e nazionale, favorevole. A livello comunitario, a partire dalla **Direttiva sui Servizi di Pagamento (PSD)** sono stati molteplici gli interventi normativi volti a disciplinare e favorire l'uso di strumenti di pagamento elettronici. **L'Agenda digitale europea**, una delle sette iniziative faro della strategia Europa 2020 – che fissa obiettivi per la crescita nell'Unione europea – ha inserito tra le aree di intervento prioritarie la realizzazione di un mercato digitale unico. Tra gli strumenti che la Commissione ha individuato per raggiungere questo traguardo è stato inserito anche il completamento dell'Area unica di pagamenti in euro (SEPA) al fine di "agevolare le fatturazioni e i pagamenti elettronici". La stessa Commissione Europea, dopo aver presentato nell'aprile 2011 l'**Atto per il mercato unico**, in cui identificava dodici leve per stimolare la crescita e rafforzare la fiducia, nell'ottobre 2012 ha proposto un'altra serie di azioni (**Single Market Act II**) per sviluppare ulteriormente il mercato unico e attingere al potenziale non ancora sfruttato per favorire la crescita: tra le





DIPARTIMENTO DEL
TESORO

MINISTERO DELL'ECONOMIA E DELLE FINANZE

Frauds: some facts

Numero 4

Pagina 4 di 7

azioni chiave individuate ha inserito lo sviluppo di un mercato unico digitale, in cui ovviamente anche i pagamenti elettronici devono svolgere un ruolo di primo piano. A conferma di questo ruolo è intervenuto anche il **Green Paper**, col quale la Commissione europea si è posta l'obiettivo di individuare gli ostacoli alla piena armonizzazione dei pagamenti sia tradizionali che innovativi e di indicare alcune possibili modalità per risolvere tali ostacoli. Anche nei provvedimenti più recenti, la Commissione ha dimostrato la volontà di muoversi verso una legislazione sempre più "al passo coi tempi". Lo scorso mese di maggio è stata emanata la proposta di **direttiva europea sui conti di pagamento** con l'obiettivo di garantire un mercato più concorrenziale sui servizi dei conti di pagamento toccando temi quali l'accesso ai conti, la mobilità bancaria e la trasparenza delle spese. In questi ultimi giorni, infine, la Commissione europea ha adottato la proposta di revisione della direttiva relativa ai servizi di pagamento (**PSDII**) con cui, tra l'altro, mira a promuovere l'emergere di operatori nuovi e lo sviluppo di pagamenti innovativi via internet e tramite dispositivo mobile in Europa, a beneficio della competitività dell'Unione nel mondo. Le iniziative legislative e operative europee come sempre hanno riflessi anche sul contesto nazionale, già di per sé estremamente vivace, sia dal punto di vista del dibattito, sia dal punto di vista normativo (che a volte precorre anche la norma europea – es. conto di base). Anche il quadro normativo nazionale ha così registrato negli ultimi anni delle novità gravide di impatti per il mercato dei pagamenti. Si pensi, ad esempio, all'art. 12 del cosiddetto decreto «Salva Italia» che ha posto forti limiti all'utilizzo del contante e ha introdotto specifici criteri nell'offerta di un conto di base al fine di dare una spinta all'inclusione finanziaria, nonché dato il là a un processo, non ancora concluso, che riguarda le regole per consentire la riduzione delle commissioni agli esercenti nei pagamenti mediante carta. Queste regole fanno *pendant* con le norme contenute nel D.L. "Crescita bis" atte a favorire ulteriormente l'utilizzo dei strumenti di pagamento elettronici, con benefici particolari per il consumatore ed il professionista. Il Decreto «Crescita bis» e la sua legge di conversione – ossia il Decreto Legge 18 ottobre 2012 convertito dalla legge 17 dicembre 2012, n. 221 – hanno inoltre modificato ed integrato in maniera sostanziale e per l'ennesima volta, anche l'art. 5 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005 n. 82) che definisce un quadro di regole volte ad assicurare il processo di digitalizzazione della Pubblica Amministrazione.

MyBank

In questo quadro di sempre maggiore ricerca di strumenti di pagamento in grado di supportare e incoraggiare il raggiungimento di obiettivi quali la "lotta al contante", la digitalizzazione dell'economia, l'inclusione finanziaria di soggetti attualmente ai margini del sistema, il mondo dell'e-payments sta affinando i servizi ormai in uso da anni e, contemporaneamente, sta arricchendo la gamma di prodotti con strumenti che meglio rispondano alle nuove esigenze dei consumatori in un mondo in cui lo sviluppo di canali "nuovi" (e-commerce, mobile payments, ecc) è sempre più rapido. Proprio per rispondere a tali esigenze, dallo scorso mese di giugno è disponibile in Italia, primo paese europeo a sperimentarla, una nuova piattaforma dedicata ai pagamenti online, il **MyBank**, una soluzione per l'autorizzazione elettronica dei pagamenti online, messa a punto da EBA Clearing, orientata a facilitare la crescita dell'e-commerce in Europa e a rendere più rapide e sicure le transazioni via web. MyBank consente agli acquirenti online di pagare per i loro acquisti su web in tutta Europa mediante la propria interfaccia di internet banking, a loro familiare. In questa fase, la soluzione può essere utilizzata per autorizzare l'esecuzione di SEPA Credit Transfer e supporterà la creazione dei mandati elettronici SEPA Direct Debit entro l'inizio del prossimo anno. MyBank, che certamente contribuirà a sviluppare l'e-commerce sul mercato nazionale ed europeo, rappresenta una soluzione innovativa per facilitare l'uso online degli strumenti di pagamento previsti dalla SEPA (l'Area unica dei pagamenti in euro).



L'importanza della prevenzione nelle TLC Fabrizio Testoni - Fraud Manager H3G Italia



Il mercato delle telecomunicazioni rappresenta senza dubbio uno dei contesti più sfidanti per chi si occupa di prevenzione del rischio di frode. Le TLC sono in costante evoluzione (per tecnologia, offerta, servizi) e di pari passo gli scenari di frode sono sempre in rapida trasformazione.

Se nei primi anni novanta la frode sulla neonata rete mobile analogica si identificava nella clonazione, l'introduzione della tecnologia digitale ha mutato i rischi in numerosissime tipologie e relative varianti. Inibita quindi alla radice la possibilità di clonare un'utenza si poteva prevedere che la frode da sottoscrizione e successivamente i furti di identità divenissero le principali casistiche di frode sui contratti postpagati. Più difficile era pensare che per diversi anni i principali pericoli sarebbero arrivati dai prodotti prepagati, o che le utenze mobili potessero essere utilizzate per svuotare conti correnti bancari ovvero per trasferire illecitamente denaro da un capo all'altro del mondo. Oggi poi, con l'avvento degli smartphone, tutto sta cambiando nuovamente.

Il "vecchio" telefonino si è trasformato in smartphone, strumento "all in one" per tutte le fasce di consumatori. Voce, internet, mail, social, mp3, games e tanto altro sono a disposizione praticamente ovunque in un unico oggetto che a breve probabilmente costituirà anche la principale forma di pagamento, almeno per le piccole spese. Una grandissima innovazione e un'opportunità unica di business ma anche un terreno vergine per i malintenzionati, sicuramente già pronti per sfruttare ogni passo falso o debolezza di

gioventù del sistema. Dal lato "oscuro del business" infatti questo scenario si traduce praticamente nella somma di tutti potenziali pericoli della telefonia, del finanziamento, di internet, dei sistemi di pagamento. Numerazioni premium, traffico internazionale, phishing, spamming, virus, skimming "all in one".



Insomma alla complessità tecnica dettata dal monitoraggio in real time del "tradizionale" traffico si assommano rischi altrettanto significativi legati alla tecnologia, alla vendita del bene e alla commercializzazione di servizi innovativi. Se fino a qualche anno al fraud manager "era necessario" possedere alcune competenze tecniche di rete per implementare un sistema di regole di monitoraggio, oggi è sempre più imprescindibile conoscere a fondo anche le nuove tecnologie, le condizioni di mercato, i sistemi di pagamento e come tutti questi elementi interagiscono insieme sul rischio specifico di prodotto. Ma le condizioni necessarie sono anche sufficienti per un'azione di successo?

I ridotti margini di una sempre più fitta concorrenza e la crisi che sta mordendo l'economia reale del paese aumentano i rischi e le conseguenze dei comportamenti fraudolenti che, se non ben gestiti, possono arrivare a incidere pesantemente sui budget aziendali arrivando a mettere a rischio intere classi di prodotto.



Ad esempio l'abbinamento di uno smartphone alla scheda telefonica rappresenta ormai uno dei principali prodotti per tutti gli operatori TLC. Creato allo scopo di diffondere rapidamente un buon numero di apparati di ultima generazione e quindi meglio veicolare le offerte di connettività di nuova generazione, ha avuto un grandissimo successo con incrementi e numeri da capogiro negli ultimi 2/3 anni. Tutti gli operatori italiani, seppur con alcune differenze, offrono formule di rateizzazione e/o finanziamento di questi device (smartphone, tablet, PC, ecc.) con costi più accessibili rispetto al mercato high tech, così da permettere a una vasta fetta di consumatori di accedere ai nuovi servizi. L'elevato valore e la relativa facilità nella rivendita di questi oggetti hanno immediatamente messo in moto un nuovo e consistente capitolo di frode e ogni anno migliaia di questi oggetti vengono rubati attraverso contratti fraudolenti e rivenduti su mercati paralleli. E la possibilità a breve di usare lo smartphone come una carta di credito implicherà nuovi schemi di frode. In definitiva, oltre al già ben consistente rischio da traffico (una sola utenza può arrivare a generare migliaia di euro per singolo giorno), le TLC si espongono così ai rischi del finanziamento e dei pagamenti con la complessità di un processo di attivazione gestito praticamente in real-time. La prevenzione è sempre più un must imprescindibile per contenere rischi e costi e il fattore "umano", cioè la capacità di cogliere ogni segnale di probabile rischio e anticipare così i possibili problemi, è l'elemento essenziale per definire la corretta strategia di contrasto.



3 Italia si è dotata di procedure e sistemi che vengono costantemente aggiornati in base al rischio dei nuovi servizi e prodotti e all'andamento dei KPI di monitoraggio. Le misure preventive sono diverse e lavorano in sinergia tra loro, in estrema sintesi la strategia si basa sui tre cardini:

1. filtri preventivi al fine di "evitare di far entrare il ladro in casa" (con l'immediata perdita dei device) attraverso l'implementazione di regole complesse, definite anche con motori di data mining capaci di evidenziare relazioni non scontate tra i soggetti richiedenti e lo storico dei comportamenti fraudolenti;
2. metodi di pagamento sicuri e automatici, privilegiando la carta di credito nelle fasce di prodotto più a rischio;
3. costante controllo dei venditori sulla compliance alle procedure di attivazione attraverso audit e visite on site.

Questo approccio ha permesso di identificare la maggioranza dei tentativi di frode nella fase di pre-attivazione, associando un rischio specifico a ogni nuovo Cliente in modo da imporgli il monitoraggio più adeguato, di mantenere una rete di vendita efficace e sinergica agli obiettivi di business con una riduzione delle perdite per frode di oltre il 50% negli ultimi 3 anni. Inoltre 3 Italia sta studiando un nuovo sistema di de-materializzazione in grado di assicurare un buon controllo sulla qualità dei documenti di identità forniti in attivazione, progetto che, in sinergia al sistema pubblico di prevenzione del MEF, contiamo che porterà a una drastica diminuzione dei casi di furto di identità.



Formazione & Eventi

63° Euro Counterfeiting Experts Group (ECEG/Olaf) Bruxelles (Belgio) 12 giugno 2013

Il 12 giugno l'UCAMP ha partecipato al 63° meeting dell'Euro Counterfeiting Experts Group presieduto dall'Unità di protezione dell'Euro dell'OLAF. Nel corso del meeting sono stati trattati i diversi punti all'OdG e in particolare un aggiornamento sulle questioni legislative inerenti la Direttiva volta a rafforzare la tutela dell'euro attraverso la normativa penale, la presentazione dei nuovi progetti 2013 co-finanziati dall'UE nell'ambito del programma "Pericles" tra i quali quello dell'UCAMP in Marocco, i risultati delle azioni formative dello scorso anno, la presentazione dei dati del Rapporto annuale del Centro Europeo di Analisi Tecnico Scientifica (ETSC) e un confronto tra gli intervenuti sui dati statistici confidenziali sulla contraffazione, presentati dalla Commissione Europea/OLAF e dalla Banca Centrale Europea.

©Ministero dell' Economia e delle Finanze, 2013
Dipartimento del Tesoro
Direzione V – Ufficio Centrale Antifrode Mezzi di Pagamento

Responsabile: Dott. Antonio Adinolfi
Dirigente Ufficio VI (UCAMP)

Via XX Settembre, 97
00187 – Roma
Tel. 0647610538
Web: <http://www.dt.tesoro.it>
e-mail: ucamp.carte@tesoro.it

Tutti i diritti riservati. E' consentita la riproduzione ai fini didattici
E non commerciali, a condizione che venga citata la fonte.

ISSN

