MEF Dipartimento del Tesoro

Newsletter

Frauds: some facts

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

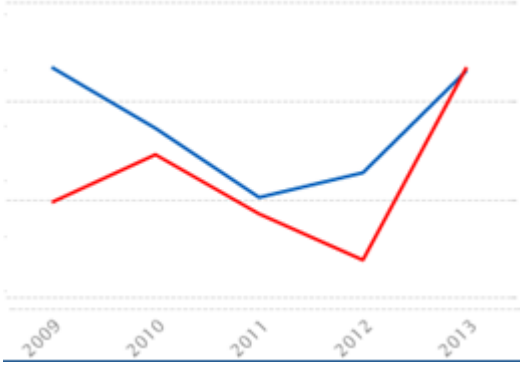
UCAMP:
Ufficio Centrale Antifrode Mezzi di Pagamento

Newsletter n° 7 - Luglio 2014

In questo numero:

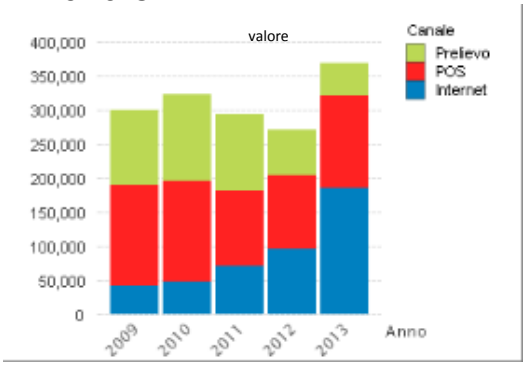
Le transazioni non riconosciute:

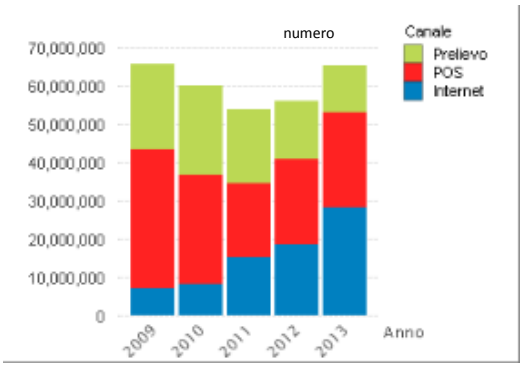
Dinamica per categoria merceologica - approfondimento di General Retails.

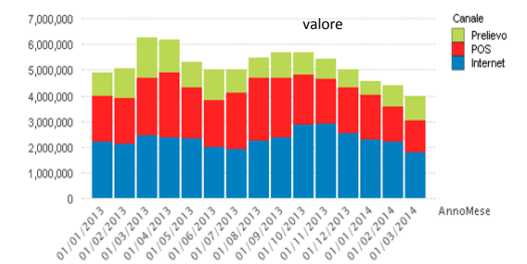


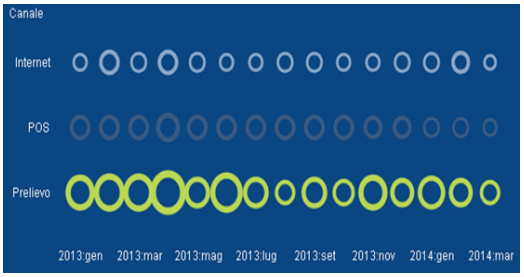
L'esame dei dati[1] annuali relativi alle frodi con Carte di pagamento mostra un aumento, per l'anno 2013, sostenuto in termini di numero di transazioni e uno molto inferiore, in termini di valore, come già anticipato nello scorso numero. Le transazioni non riconosciute sono aumentate sensibilmente di numero riducendosi, però come valore medio. Il grafico, sulla sinistra, mostra valori (linea blu) e numerosità (linea rossa) delle transazioni. Risulta evidente la forte crescita della linea rossa, che supera abbondantemente il livello, già elevato, del 2009.

L'analisi per canale di pagamento mostra la sostanziale riduzione dei prelievi rispetto agli altri canali, sia in termini di valore che di numero.
L'analisi dello stesso dato a livello mensile fa emergere come all'aumento rilevato nei primi mesi del 2013 sia seguita una lenta ma costante diminuzione a partire dal mese di ottobre, che porta il valore complessivo delle frodi su livelli inferiori a inizio 2013.





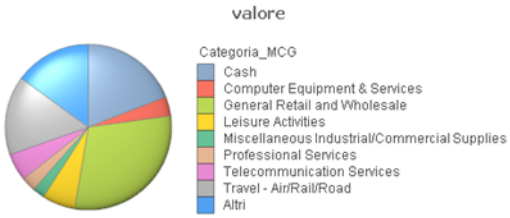




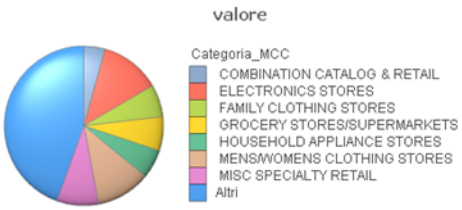
Categorie merceologiche

Il valore medio delle transazioni per canale mostra come la riduzione già citata del valore medio sia concentrata nei canali Internet e POS.

L'analisi dei canali POS e Internet, per gruppi di categorie merceologiche, conferma la netta preponderanza, come già visto nel numero precedente, del gruppo (MCG) *General Retail and Wholesale* (grafico di sinistra).

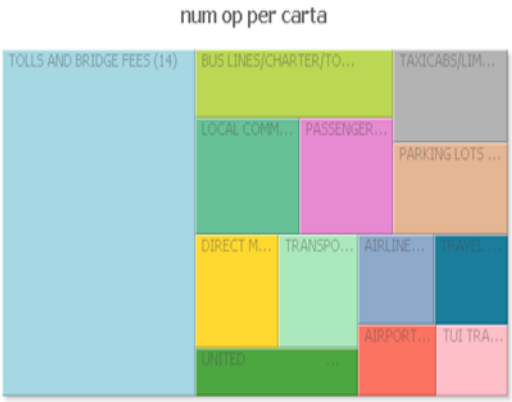


Da notare che questo specifico gruppo di Categorie Merceologiche(grafico di destra) si ripartisce sostanzialmente equamente tra i canali POS e Internet.



Analizzando direttamente l'insegna dell'esercizio commerciale o il sito Internet di riferimento, spicca in maniera netta la presenza di un venditore leader nella vendita di contenuti multimediali on-line che da solo copre sostanzialmente l'intera categoria merceologica *Record stores.*

L'analisi del numero di transazioni per carta, evidenzia, come tale numero sia sostanzialmente costante e estremamente basso per tutte le categorie, con alcune interessanti eccezioni. In particolare, come mostra la mappa accanto, nella categoria *Tolls and bridge fees* il numero di transazioni è estremamente più elevato. Si tratta soprattutto di transazioni di bassissimo valore, concentrate nei pedaggi autostradali.



[1]*Fonte SIPAF, Sistema Informatizzato Prevenzione Amministrativa Frodi Carte di Pagamento, Ministero dell'Economia e delle Finanze/Dipartimento del Tesoro. Analisi in collaborazione con Sogei.*

Euro - UN ANNO DI SIRFE.

Con l'emanazione del DM del 1 febbraio 2013, pubblicato sulla G.U. della Repubblica nr.37 del 13 febbraio 2013, comunemente noto come ""Decreto SIRFE"", è stato aggiunto un altro importante tassello alla complessiva normativa volta a garantire la tutela e la protezione dell'euro.
Quest'ultima novità dal punto di vista normativo ha apportato un innovativo cambiamento tecnologico nell'ambito della trasmissione ad UCAMP dei verbali di ritiro delle banconote e delle monete sospette di falsità. Sostanzialmente è stato formalizzato il passaggio alla modalità telematica per la trasmissione dei dati e delle informazioni relative ai ritiri di valuta - cartacea o metallica - denominata in euro sospetta di falsità. Si parla cioè di:

a) dati identificativi del gestore del contante;
b) dati identificativi delle banconote/monete ritirate;
c) dati identificativi del soggetto segnalante.

Nulla è cambiato relativamente all'obbligo di ritiro dalla circolazione e di trasmissione delle banconote e delle monete in euro sospette di falsità. Le banche e gli altri soggetti che gestiscono o distribuiscono a titolo professionale banconote e monete metalliche in euro hanno l'obbligo di ritirare dalla circolazione le banconote e le monete metalliche in euro sospette di falsità e di trasmetterle senza indugio, rispettivamente, ai centri deputati per le perizie, ovvero al CNA della Banca d'Italia e al CNAC dell'Istituto Poligrafico e Zecca dello Stato.

Condizione necessaria per l'invio riguarda l'abilitazione al sistema, ovvero l'accreditamento, senza la quale il gestore del contante non può alimentare il sistema. L'accreditamento ha rappresentato uno snodo fondamentale per poter inserire i relativi verbali e, quindi, per ottemperare all'obbligo dell'utilizzo del mezzo telematico. L'obiettivo che l'UCAMP si era prefisso, e che è stato raggiunto, era rendere il servizio efficiente e in grado di ricevere tutte le informazioni attinenti la contraffazione dell'euro.
I primi auspicati positivi effetti di tale innovazione si sono palesati già dalla sua entrata in esercizio (14 maggio 2013, quando si è avuto il passaggio definitivo al nuovo sistema), con i primi risultati espressi nel Bollettino semestrale 2013 edito dall'UCAMP.

Si è subito notato un incremento del numero di verbali ricevuti dovuto principalmente a:

1. maggior consapevolezza, da parte dei gestori del contante, dell'obbligo dell'invio ad UCAMP dei dati e delle informazioni raccolte relativi ai casi di sospetta falsità;
2. efficacia e certezza nella raccolta dei dati.

Il primo Bollettino, dalle caratteristiche squisitamente statistiche, ha aperto la strada a ciò che sarà una analisi più puntuale e efficiente delle future pubblicazioni UCAMP, già previste per l'inizio del prossimo anno.
Il successo del nuovo applicativo, che ha riscosso il plauso da parte di tutti gli attori interessati, offre indubbiamente notevoli vantaggi consentendo in primo luogo l'inserimento diretto e preciso dei dati direttamente da parte degli enti segnalanti.

Si avrà così:

- una rappresentazione in tempo reale della situazione della sospetta contraffazione euro nel paese;
- una comunicazione efficiente, puntuale e immediata con l'UCAMP;
- un'agevole gestione e analisi delle numerose informazioni ivi contenute;
- puntualità;
- velocità di trasmissione;
- accuratezza;
- risparmio risorse sia umane che economiche;
- valido ausilio per potenziali attività informative e investigative.

I dati, così ricevuti, consentono di avere un numero di informazioni sempre aggiornato e preciso, tali da consentire l'elaborazione di analisi anche di tipo socio-economico oltre a quelle ovviamente marcatamente statistiche.
Questo circuito alimenta ""il circolo della conoscenza"" permettendo all'Ufficio di poter immediatamente:

- condividere le informazioni;
- aggiornare la statistica;
- individuare la problematica (ad es. geolocalizzazione);
- valorizzare i dati raccolti al fine di preservare la moneta unica, *LA NOSTRA MONETA,* da un uso fraudolento e improprio che non fa altro che impoverire e danneggiare l'economia.

Solo conoscendo il fenomeno, si possono adottare le giuste contromisure necessarie a contrastare le azioni criminose.
La nuova modalità per via telematica ben si adatta alla modernità e ai cambiamenti della società e consente quindi di raggiungere quei risultati voluti e auspicati. In merito alla gestione del sistema, l'UCAMP fornisce assistenza tecnica e formativa ai gestori del contante.

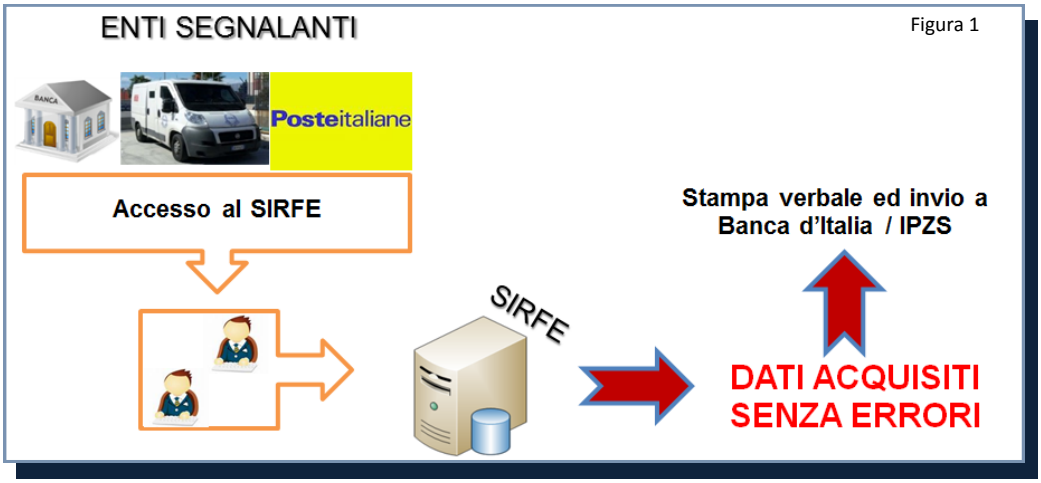
L'UCAMP assicura l'assistenza nei confronti dei soggetti obbligati:

- per ciò che attiene le modalità di accreditamento;
- per la gestione delle criticità che possono verificarsi;
- nell'aggiornare il manuale utente, utile strumento, facilmente consultabile per trovare una rapida soluzione ad ogni problematica applicativa.

Lo stesso Decreto promuove appositi incontri formativi e di aggiornamento rivolti ai gestori del contante oppure, anche a richiesta, direttamente presso gli enti organizzatori.

*Nella **figura 1** è rappresentato lo schema di funzionamento del sistema, con il quale i gestori del contante, ottenute le credenziali di accesso, possono inserire direttamente e quindi con maggiore accuratezza e precisione i dati e le informazioni relative ai casi di sospetta falsità dell'euro.*

Figura 1



Va ricordato, infine, che dal 1 gennaio 2014 i Paesi aderenti all'Eurozona sono ora 18, grazie all'ingresso della Lettonia.

I cambiamenti non finiscono qui. Le stesse banconote stanno cambiando con la progressiva introduzione della nuova serie "Europa", che presenta caratteristiche di sicurezza sempre più sofisticate. Il 2 maggio 2013 è stata introdotta la nuova banconota da 5 euro, che rappresenta la prima delle nuove emissioni. Entro l'estate 2014 sarà introdotta la seconda serie della banconota da 10 euro e ogni anno a seguire saranno modificati tutti i tagli allo stato in circolazione.

In virtù di questi cambiamenti, l'Ufficio ha deciso, inoltre, di aderire al programma della Banca Centrale Europea "La Nostra Moneta", al fine di poter fornire sempre più un ausilio nel contrasto alla diffusione del fenomeno per la formazione di cittadini e operatori, che quotidianamente sono sottoposti al rischio di ricevere un danno economico dalla circolazione di banconote false.

Non si tratta di una variazione stilistica, ma si avverte sempre più la necessità di proteggere "LA NOSTRA MONETA", introducendo innovative tecniche di contrasto alla contraffazione dell'euro. Anche in tale contesto il SIRFE, rispondendo a criteri di praticità, consente immediatamente di allinearsi alle nuove esigenze. L'euro, fin dal suo debutto, ha rappresentato e rappresenta uno dei pilastri della nuova Unione europea. Esso rappresenta uno strumento transnazionale, volto ad unire diversi popoli sotto l'insegna di un'unica valuta, forte, stabile e sicura: un linguaggio univoco tra i cittadini europei per incentivare la circolazione delle persone, facilitare gli scambi commerciali, favorire le transazioni economiche, eliminare le barriere tra gli Stati. L'euro va considerato un bene comune, un bene da tutelare e difendere sia dalle manovre inflazionistiche che dai tentativi di contraffazione.

Policy e misure di sicurezza informatica

acquistiamo on-line con le carte di pagamento riducendo il rischio di frodi

Di Stefano Russo - Docente di Informatica giuridica - Luiss Guido Carli

L'acquisto di beni e servizi da siti *web* di *e-commerce* è ormai pratica molto diffusa. Le transazioni *on-line* rappresentano sicuramente uno degli aspetti più innovativi offerti da Internet.

Le ragioni di questo successo sono dovute principalmente al fatto che i prezzi dei beni e/o servizi acquistati *on-line* sono competitivi e che gli acquisti possono essere effettuati con totale abbattimento delle barriere spazio-temporali.

Dal punto di vista giuridico questa pratica costituisce una forma di commercio a distanza in cui la transazione viene effettuata attraverso il *web* con valore di contratto legale.

L'impegno di pagamento però è anteriore al momento di godimento del bene o del servizio acquistato e solitamente avviene *on-line* utilizzando una carta di pagamento.

La consegna del bene potrà avvenire in maniera elettronica, via Internet (ad esempio *software*, filmati, musica, biglietteria varia, scommesse, *e-book*, servizi informativi, assicurazioni, ecc.) oppure potrà essere recapitata al domicilio dell'acquirente (ad esempio libri, computer, abbigliamento ecc.).

Gli attuali *software* di sicurezza adottati dai siti *web* di *e-commerce* più aggiornati e affidabili riducono notevolmente sia i rischi di intercettazione del numero della carta di pagamento nel momento in cui l'acquirente la fornisce sia quelli di violazione del database aziendale del venditore in cui sono contenuti i dati dei clienti.

Gli utenti/acquirenti però si espongono ai rischi derivanti dal vasto mondo del *web* poiché sono spesso disattenti e superficiali.

Ci sono comportamenti e misure di sicurezza informatica che se fossero sempre seguiti consentirebbero di effettuare acquisti *on-line* con le carte di pagamento in modo più sicuro e conseguente riduzione del rischio di frodi.

Purtroppo gli utenti/acquirenti spesso effettuano transazioni *on-line* utilizzando computer non sicuri.

Infatti queste macchine possono non avere: a) un *firewall* attivo che vigili sullo scambio di dati tra il computer e il mondo esterno e sugli eventuali tentativi d'intrusione; b) un *software* di tipo antivirus aggiornato regolarmente e frequentemente che impedisca di "infettare" il computer con virus che possano raccogliere dati condivisi e trasmetterli a estranei; c) *patch* recenti del sistema operativo e dei *software* applicativi (ad esempio i *browser* per la navigazione sul *web*); d) Java, JavaScript e Activex disabilitati.

Quelle che abbiamo elencato sono tutte misure di sicurezza fisica, ma esistono anche misure di sicurezza logica spesso ignorate da parte degli utenti/acquirenti.

Si tratta di *policy* che andrebbero scrupolosamente seguite per accertarsi che il sito *web* prescelto sia sicuro.

Innanzitutto sarebbe una buona pratica verificare che sul sito *web*: 1) sia correttamente indicato il nome o ragione sociale del venditore; 2) sia indicato oltre all'indirizzo *e-mail* del venditore un suo recapito fisso; 3) siano adottati dall'acquirente sistemi di protezione delle comunicazioni che utilizzino protocolli di sicurezza (ad esempio Secure Socket Layer – SSL) che impediscano l'accesso, casuale e non, ad altri utenti; 4) non vengano richieste informazioni personali relative al proprio conto corrente all'interno della pagina *web* dove si perfeziona la transazione (di norma sono richiesti solo il nome e cognome dell'intestatario della carta di credito, il numero della carta di credito, data di scadenza della carta e codice di sicurezza CVV2 o CVC2 o CID a secondo del circuito di pagamento).
Inoltre sarebbe opportuno effettuare controlli in tempo reale attraverso servizi di *home banking* sul proprio estratto conto per verificare che non ci siano addebiti di spese mai effettuate.
Infine sarebbe consigliabile utilizzare per i pagamenti *on-line* le carte prepagate ricaricabili. In quanto esse si sostanziano per lo più in carte virtuali "usa e getta" valide per un unico acquisto oppure in carte virtuali di durata, valide per più acquisti da effettuarsi in un arco temporale definito (di solito 12 mesi). Con tali tipi di carte si può indicare un importo massimo spendibile che limite fortemete i rischi delle altre carte.
Il costo del canone di questi strumenti di pagamento è irrisorio o del tutto gratuito. Pertanto gli utenti potranno difendersi dalle frodi *on-line* solto adottando le summenzionate misure di sicurezza informatica e *policy*. Riteniamo che investire in massive campagne educative a riguardo non potrà che ridurre il rischio di frodi e favorire la crescita digitale, in vista di una miglior globalizzazione dell'economia mondiale.

Formazione & Eventi

L'UCAMP ha preso parte nel mese di giugno 2014 alla 66^ riunione dell'Euro Counterfeiting Experts Group (ECEG).

L'Ufficio ha partecipato alle riunione del GAFI dal 23 al 27 giugno (FATF "-Financial Action task force) – Organismo intergovernativo che stabilisce standards legislativi a livello internazionale ai fini di antiriciclaggio e di lotta al finanziamento del terrorismo.

Attività GIPAF

Gruppo di Lavoro Interdisciplinare per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento

Il giorno 4 giugno si è tenuta l'undicesima riunione del GIPAF, nel corso della quale sono stati portati a conoscenza dell'assemblea plenaria i risultati del sottogruppo "Analisi Legislativa" e "Rapporti statistici ed altre pubblicazioni". Si è illustrata l'esigenza di rinnovare, senza stravolgere, il dettato della legge 166/2005 e del relativo DM di attuazione 112/2007, basandosi sull'esperienza acquisita in questi anni nel corso della gestione del sistema SIPAF, ritenendo opportuno allineare i due provvedimenti alle mutate esigenze dettate dalla continua evoluzione del mondo delle carte 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

ISSN .....