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° 12 - Marzo 2016

In questo numero:

Carte di Pagamento l'analisi statistica: *Merchant Category Group*

Nel corso del 2015 l'andamento generale del fenomeno disconoscimenti delle carte di pagamento è stato caratterizzato da una diminuzione del valore del frodato pari al -3% e da una diminuzione del numero di frodi pari -12%. Conseguente si è avuto un aumento dell'importo medio, che passa a 165 euro nel 2015 dai 151 del 2014 .

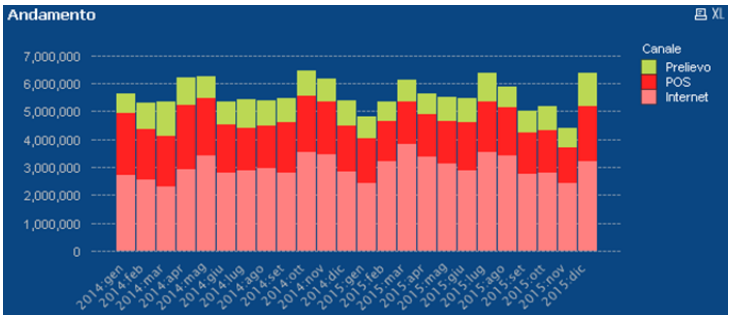

Figura 1 Valore delle transazioni non riconosciute

In generale il fenomeno si riduce in Italia mentre rimane stabile all'estero. Infatti, nel grafico di *figura 2* il fenomeno frodi relative al canale internet cresce all'estero del +5% in termini di valore.

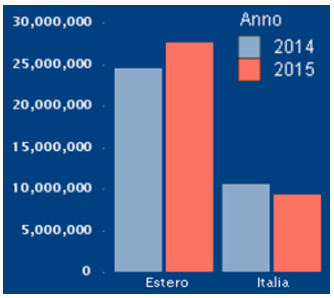

Figura 2 Canale internet

Analizzando la classifica dei paesi esteri con il più alto livello di valore frodato nel biennio 2014/2015 (*figura 3*), la Gran Bretagna ottiene il primo posto ed un incremento sostanziale in termini di valore frodato. Al secondo posto abbiamo gli Stati Uniti, seguono, sempre con una variazione positiva, Francia, Lussemburgo e Germania anche se con livelli relativamente minori rispetto ai Gran Bretagna e Stati Uniti.

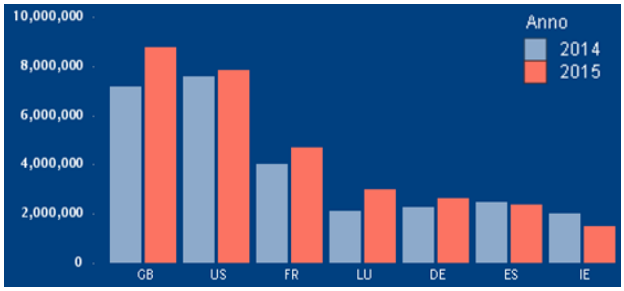

Figura 3 Valore primi 7 paesi stranieri

Un'analisi annuale per categorie merceologiche, mirata al solo canale internet, evidenzia che già negli anni passati il fenomeno si concentrava principalmente nella *Merchant Category Group - General Retail*, che appare in rosso nel grafico di figura 4. Questo gruppo di categorie merceologiche è anche quello con il più elevato tasso di crescita annuale.

Affinando l'analisi ed entrando nel dettaglio delle categorie merceologiche che compongono la MCG - General retail, rileviamo, in figura 5, che il sotto insieme maggiormente colpito risulta essere *Men's women's clothing store* (indicato dalla freccia), e corrispondente ad un esercizio commerciale di abbigliamento on-line.

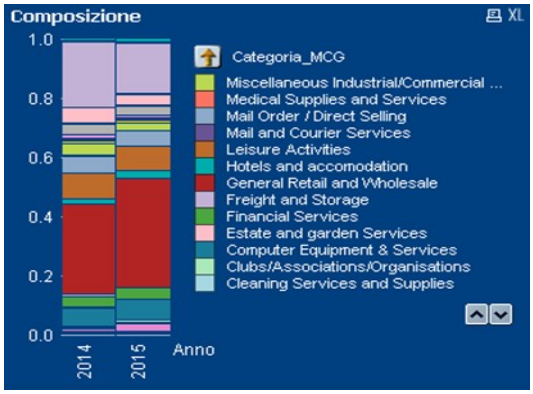

Figura 4 Merchant Category Group

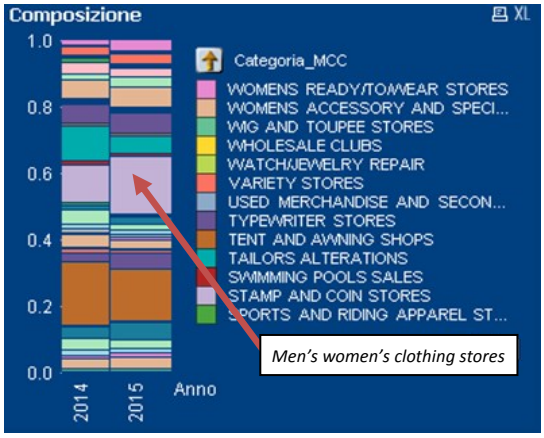

Figura 5 MCG - General retail

Approfondendo il dettaglio della sola categoria merceologica *Men's women's clothing stores* ed effettuando un'analisi granulare per insegne punto vendita, possiamo notare, in figura 6, la persistenza delle frodi su due singole insegne punto vendita, rispettivamente rappresentate all'interno dell'istogramma dal colore blu e verde acqua. Entrambe fanno capo alla stessa compagnia di vendite on-line, leader del settore.

Infine, effettuando un'analisi sul valore medio delle frodi prodotte da questa particolare categoria merceologica, rileviamo un aumento del valore medio delle frodi, negli anni 2014/2015, che passa da 293 a 332 euro. Possiamo concludere affermando che l'aumento prodotto da questa particolare categoria merceologica contribuisce a chiarire il complessivo aumento del valore medio delle transazioni avvenute durante il corso dell'anno 2015.

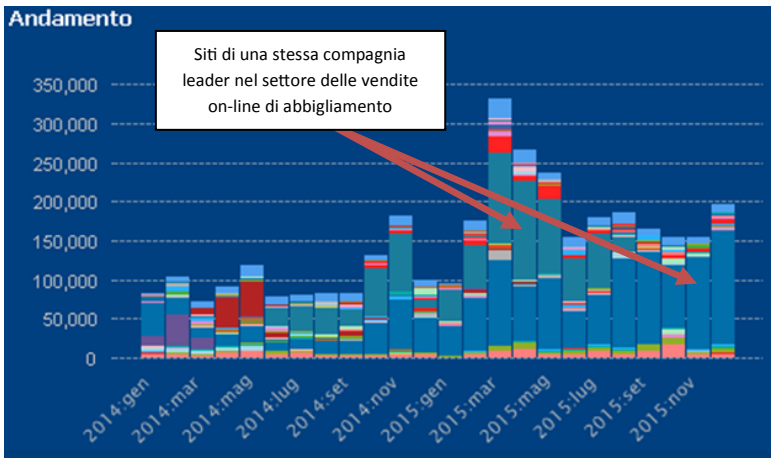

Figura 6 MCG - General retail

Black Market transnazionale: *la comunità russa, cinese, brasiliana, statunitense, giapponese e la crescente comunità tedesca*

Per comprendere l'evoluzione dei fenomeni criminali nel *deep web* e di come le principali organizzazioni orientano la propria offerta in relazione agli eventi che accadono nel cyberspazio, uno studio dei *Black Market* è essenziale. L'analisi dell'ecosistema criminale deve prendere in considerazione le differenti attitudini delle numerose comunità di criminali informatici operanti sul globo che utilizzano i *Black Market* come strumento di vendita di prodotti e servizi. Particolare attenzione verrà data alla comunità ***russa, cinese, brasiliana, statunitense, giapponese,*** nonchè alla crescente comunità ***tedesca***.

Gli esperti di sicurezza reputano l'underground **russo** come il più fertile, almeno per quanto riguarda le frodi relative alle carte di pagamento e l'*hacking*, mentre l'ecosistema criminale **cinese** risulta più popolare per quanto concerne le frodi in ambito mobile.

Spostandoci dall'altra parte del globo, la comunità dell'underground criminale **brasiliano** si specializza nella realizzazione di piattaforme volte alla realizzazione di frodi nell'online banking, mentre il mercato **statunitense** presenta molte similitudini con quello russo.

Altre comunità che meritano attenzione sono sicuramente quella **giapponese**, in rapida ascesa, e quella **tedesca,** che molti esperti considerano la succursale russa, per similitudine di prodotti e servizi.

Iniziamo dall'underground **russo**, senza dubbio il più prolifico per quanto concerne prodotti e servizi connessi a frodi con carte di pagamento. Tra i principali forum di questa comunità numerose sono le offerte di prodotti oltre ai consueti lotti di dati relativi a carte di pagamento rubate. Infatti, continuiamo ad assistere ad una crescente offerta di servizi per la verifica e la validità dei dati delle carte di pagamento. Numerosi venditori offrono contestualmente lotti di carte e servizi per il controllo della loro validità. Molto gettonati sono i servizi di *Money-laundering* i quali attraverso organizzazioni criminali operanti nell'ecosistema russo sono in grado di offrire ai propri utenti la possibilità di riciclare il denaro in vari modi (i.e. acquisto biglietti aerei, prenotazione di hotel, affitti di ville lussuose). Facciamo un esempio pratico, supponiamo che un criminale A acquisti un biglietto aereo con una carta di credito rubata per un secondo criminale B oppure per una persona che intende effettuare l'acquisto e ha espresso la sua intenzione in rete, all'interno di qualche forum. Il biglietto che normalmente costa 300 euro, è venduto dal criminale B ad un prezzo inferiore di circa il 50%-60% dell'importo effettivo. Questa forma di riciclaggio è rapida e remunerativa per coloro i quali rivendono i biglietti acquistati con dati relativi a carte rubate.

Per di più, come descritto in un uno degli ultimi rapporti pubblicati da Trend Micro, stiamo assistendo alla rapida diffusione di nuovi servizi disponibili nell'underground criminale russo, quali "Fake identity-approval-call-receiving services", *Drop-as-a-service* e "Logs for sale".

I servizi di "**Fake identity-approval-call-receiving services**" consentono ai criminali di operare in paesi di lingua differente dalla loro, in particolare tali servizi si specializzano nella risposta telefonica agli istituti di credito che potrebbero contattare l'utente che effettua la transazione (*proof-of-identity*), per verificarne l'identità e validarne l'operazione. Praticamente un criminale russo intento a frodare un titolare italiano di una carta di pagamento, potrebbe essere contattato dal personale della banca, a quel punto il personale "specializzato", che lavora nelle retrovie del *call-receiving services,* si fingerebbe il titolare italiano e risponderebbe senza destare sospetti relativi ad accenti linguistici.

Interessante anche la diffusione di servizi "**Drop-as-a-service**", utilizzati per incassare il denaro proveniente da carte di pagamento rubate. Alcuni di questi servizi solitamente gestiscono dalle 10 alle 1.000 persone che sono coinvolte in maniera consapevole o meno nelle attività di *cash out*.

Infine vi sono i servizi di "**Logs for sale**," ovvero rivendita dei file di log relativi ai dati esfiltrati da macchine infette. Tipicamente l'operazione è effettuata da specialisti operanti dietro grandi *botnet*. Il contenuto informativo riguarda tendenzialmente credenziali di accesso a molteplici servizi, dati sensibili e ovviamente dati relativi a carte di pagamento. I criminali, che acquistano file di log, devono necessariamente effettuare operazioni di scrematura (*parsing*) alla ricerca di contenuti interessanti.

Come anticipato, nell'underground russo vi sono numerosi forum specializzati nella vendita di prodotti e servizi riguardanti le frodi con carte di pagamento, *Rescator* è senza dubbio il più popolare, ma ve ne sono di nuovi ed estremamente efficienti e ristretti ad un numero limitato di operatori come ad esempio gocvv.cc. *(figura 1)*

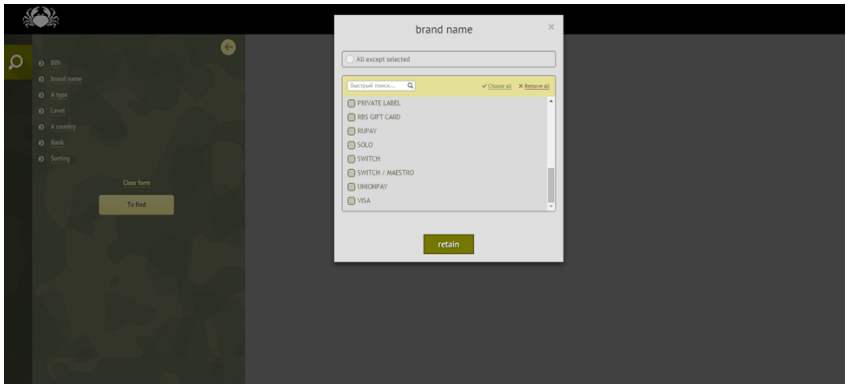

Figura 1 - gocvv.cc Website

Voliamo quindi in **Cina**, paese in cui la comunità underground si specializza soprattutto nelle frodi nei confronti di utenti possessori di dispositivi *mobile*. Questo mercato non presenta peculiarità per quanto concerne le frodi relative alle carte di pagamento: i principali venditori offrono dati relativi a carte di pagamento provenienti da altri mercati, tipicamente a Stati Uniti, Europa, Giappone ed ovviamente Cina. Interessante notare, invece, che molti venditori offrono ogni genere di *skimmer* a prezzi competitivi.

Tra i principali prodotti offerti vi sono *PoS Skimmer, Pocket skimmer, ATM Skimmer, Pin pad Skimmer* e persino tutorial per il loro utilizzo ottimale.

Il costo di un *PoS skimmer* (*figura 2*) oscilla tra poche centinaia di dollari a circa 1.200 dollari per dispositivi che includono moduli di notifica via SMS.

Figura 2 - PoS Skimmer

Il mercato underground **brasiliano**, data la forte propensione all'uso di piattaforme di online banking, si specializza per tutto ciò che concerne attacchi verso servizi *mobile*. Per quanto concerne le frodi relative alle carte di pagamento vi si trovano principalmente dati relativi a carte di pagamento statunitensi a prezzi che sono in linea con altri black market. Il mercato brasiliano è molto interessante per quanto concerne la vendita di tutorial specializzati sulle frodi con le carte di pagamento nonchè per l'offerta di *skimmer* carte.

Tra le curiosità annoveriamo la vendita di generatori di numeri di carte di credito (150 numeri di carte sono offerti a poco più di 76 dollari), ovviamente non affidabili al 100%, ma che comunque continuano ad essere oggetto di interesse per alcuni novizi criminali (*figura 3*).

Offering	Price
10 sets of credit card credentials	R$200 (US$51.16)
20 sets of credit card credentials	R$400 (US$102.32)
50 sets of credit card credentials	R$700 (US$179.06)

Table 1: Credit card credential offerings with their prices

Figura 3 - Underground Brasiliano (Trend Micro)

Nell'underground criminale **nord americano** è molto facile imbattersi in individui e organizzazioni che offrono prodotti e servizi per coloro i quali intendono operare frodi con carte di pagamento. La maggior parte delle informazioni offerte nei forum statunitensi è relativa a carte emesse negli Stati Uniti, Canada ed alcune nazioni europee come Il Regno Unito e la Francia.

Offering	Price
Classic US-issued credit card credentials	US$19–22 (100 sets)
Gold, Platinum, or Business US-issued credit card credentials	US$36–42 (50 sets)
Classic Canada-issued credit card credentials	US$47–50 (40 sets)
Gold, Platinum, or Business Canada-issued credit card credentials	US$50–65 (35 sets)
Fake US-issued credit card (physical)	US$210–874

Figura 4 - Offerta dati carte di credito mercato underground Nord America (Trend Micro)

Come riportato in *figura 4*, l'acquisto di dati relativi a carte di pagamento è estremamente economico, poche decine di dollari per acquistare lotti composti da diverse decine di record.

Tornando in Asia, in **Giappone**, l'elevata propensione tecnologica dei suoi cittadini sta diventando terreno fertile per la criminalità informatica, sebbene le forze dell'ordine esercitino una pressione significativa sulle organizzazioni locali dedite a questo tipo di crimini.

Anche in questo caso è possibile trovare numerosi siti che si specializzano nella fornitura di servizi e prodotti connessi alle frodi con carte di pagamento.

Uno dei più popolari è senza dubbio *Orda Project*, un *hidden service* ospitato nella rete *Tor* che presenta una ampia offerta ricomprendente dati relativi a carte di credito rubate. Ad esempio, sono sufficienti 60 dollari per comprare dati relativi a carte verificate da Visa attraverso il servizio VBV, mentre i record comprensivi di numero carta e data di scadenza sono offerti per poco meno di 10 dollari.

Country	Selling price	Number of accounts for sale
Credit cards		
Japan	US$14–78 (Average: ~US$60)	207
US	US$2–84 (Average: ~US$7)	126,707
Brazil	US$6–10 (Average: ~US$8)	17,385
UK	US$8–61 (Average: ~US$8)	28,336
Canada	US$3–60 (Average: ~US$16)	36,423

Figura 5- Selling Price - Rapporto Trend Micro

Per i più curiosi, si veda la tabella di *figura 5,* presa dal rapporto pubblicato da *Trend Micro* sull'underground giapponese, nella quale sono proposti i prezzi di vendita dei principali paesi esaminati.

Chiudiamo la nostra rapida panoramica con un il mercato **tedesco**. In questo specifico ecosistema criminale operano molti degli operatori dell'underground russo, per questo motivo è facile imbattersi nei medesimi siti specializzati nella vendita di prodotti e servizi di frodi carte.

Per coloro i quali volessero dare un'occhiata all'offerta dell'ecosistema criminale tedesco consiglio *German-plaza.cc* (*figura 6)*, un black market ospitato sul servizio *CloudFlare,* che presenta un'offerta articolata e sempre aggiornata. Per quanto riguarda i prezzi, seppur estremamente variabili, presentano una maggiorazione rispetto al mercato russo, sintomo che gli operatori cercano di incrementare i propri guadagni localizzando l'offerta o semplicemente facendo da tramite con le principali organizzazioni russe, ipotesi avvolorata dalla presenza di numerosi banner dei

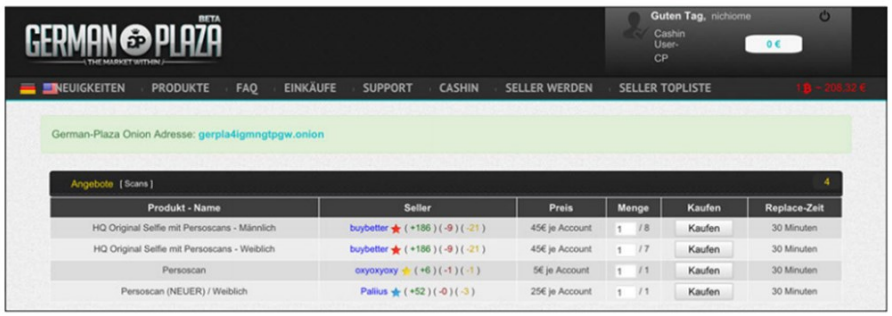

Figura 6 – German Plaza underground Market (Foto Rapporto Trend Micro)

principali black market russi.

Il mercato tedesco differisce dal mercato russo principalmente nell'utilizzo di *hidden service* nella rete Tor, spesso questi servizi sono un *mirror* dei servizi presenti in Internet ed accessibili con normali browser. Di seguito alcuni esempi :

Sito Web	Mirror su rete Tor
Bus1nezz.biz	Bizznza4vtgsdrgb.onion
Black2hack.cc	Gerpla4igmngtpgw.onion
German-plaza.cc	Gerpla4igmngtpgw.onion
Crimenetwork.biz	Crimenc5wxi63f4r.onion

Concludendo, possiamo affermare che l'analisi dell'attività criminale nei diversi *black market* è cruciale per comprendere le dinamiche di un ecosistema estremamente complesso. Le informazioni illustrate, credo, potranno essere estremamente utili alle forze dell'ordine, alle aziende di sicurezza nonché a tutte quelle società che operano nei comparti colpiti dall'attività criminale, come il Retail ed il settore bancario.

Ing. Pierluigi Paganini

Il nuovo rapporto statistico sulle frodi con le carte di pagamento

Il 17 dicembre 2015, in occasione della riunione del Gruppo Interdisciplinare di lavoro per la Prevenzione Amministrativa delle Frodi sulle carte di pagamento (GIPAF), è stato presentato il nuovo rapporto statistico sulle frodi con le carte di pagamento. Il rapporto ha cadenza annuale ed è elaborato sulla base dei dati estratti dal Sistema Informatizzato per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento (SIPAF). La pubblicazione si propone di fotografare la realtà italiana in materia di frodi legate alle carte di pagamento, per approfondire la conoscenza della portata del fenomeno e rendere più consapevole e informato il cittadino, anche attraverso una sezione dedicata al confronto internazionale con paesi che si sono dotati di simili strumenti di monitoraggio, quali: Regno Unito, Francia e Australia. Il rapporto contiene, in particolare, un'analisi statistica di quattro distinti fenomeni, che sono analizzati nella loro evoluzione temporale e nella loro distribuzione geografica:

- le frodi effettuate con le carte di pagamento;
- la rilevazione delle categorie merceologiche coinvolte;
- le revoche delle convenzioni con i punti di vendita per motivi di sicurezza;
- le manomissioni degli ATM.

Fino all'adozione della nuova versione il rapporto ha scontato un approccio poco divulgativo, non rendendo agevole ed immediata la lettura, utilizzando una veste grafica anche poco accattivante. Proprio il confronto con le pubblicazioni degli altri paesi, al di là dell'analisi dei contenuti, ha posto il problema di rinnovarne la linea editoriale. La versione 2015 si mostra in una nuova veste grafica ricca di contenuti, arricchiti anche dall'importante contributo fornito dagli stakeholders. Il target degli esperti di settore è sempre presente, ma sono disponibili delle aggregazioni di dati di semplice lettura, destinati ad una platea più vasta, per fini anche didattici. In realtà, l'idea di una revisione del rapporto è stata maturata già nel 2014 e annunciata in occasione della riunione GIPAF del 4 giugno da uno degli esperti, la Dott.ssa M. Mignone, che, partendo dall'analisi delle fonti disponibili a livello comunitario ed internazionale (rapporti e surveys), ne ha proposto una revisione della struttura, suggerendo alcuni cambiamenti stilistici proprio con l'obiettivo di rendere la pubblicazione più chiara ed efficace dal punto di vista divulgativo, di rispondere alle diverse esigenze informative di tutti gli stakeholders (istituzioni, forze dell'ordine, industria dei pagamenti, cittadini/utenti), e di porsi in una prospettiva di comparabilità delle statistiche con altri paesi. In particolare, sono stati individuati i principali obiettivi da perseguire:

- capacità di rappresentare il contesto italiano a livello europeo ed internazionale (comparabilità dei dati statistici);
- capacità di promuovere il SIPAF come buona pratica in ambito comunitario;
- capacità di fornire un'analisi di scenario (contesto e tendenze) per tutti gli stakeholders (in particolare, istituzioni, forze dell'ordine e industria dei pagamenti);
- capacità di promuovere una maggiore in-formazione dei cittadini ed una maggiore disponibilità all'uso dei mezzi di pagamento alternativi al contante (in particolare, le carte di pagamento);

- capacità di incrementare la visibilità del tema della sicurezza delle carte di pagamento e delle misure di auto-tutela nei media/ICT (comunicabilità dei dati sulle frodi).

In concreto è stata individuata una struttura più razionale, per semplificare e rendere più immediata e chiara la spiegazione dei dati, ad esempio sostituendo le tabelle con i grafici e ricorrendo a info-grafiche e schemi sull'esempio del rapporto del Regno Unito.

Le maggiori novità sono state un *executive summery* e la possibilità di approfondire uno specifico tema di interesse, quali *crime-mapping*, internet/siti e settori economici maggiormente vulnerabili, paesi di maggiore spendita delle carte clonate. La nuova struttura non avrebbe certo dovuto rinunciare all'adozione di una metodologia scientifica solida, alla trasparenza e alla completezza dei dati, ma avrebbe dovuto aggiungere un'analisi non solo statistica, ma anche criminologica del fenomeno e delle sue possibili evoluzioni, così come comprendere il tema più generale del sistema dei pagamenti e delle diverse iniziative pubblico-private per la messa in sicurezza degli acquisti mediante carte di pagamento sia offline sia online. Nella riunione GIPAF del 17 dicembre 2014 l'Ufficio stesso ha presentato agli esperti un'ipotesi di struttura del nuovo rapporto, così articolato:

- Executive summary;
- UCAMP – competenze ed attività;
- Analisi del fenomeno:
  - Trend e statistiche con analisi criminologica;
  - Comparazione internazionale;
  - Rischi futuri.
- Approfondimento monotematico;
- Misure di prevenzione e contrasto, iniziative e novità tecnologiche;
- Annex statistico:
  - Nota metodologica;
  - Tabelle.

Tale struttura è molto vicina a quella adottata in via definitiva, che ha visto aggiungere al capitolo "Analisi del fenomeno" una serie di paragrafi, tra cui "Manomissioni ATM", "Revoche convenzioni POS", "Nota criminologica". In conclusione, le novità hanno riguardato la previsione di un Executive summary, la notevole riduzione del capitolo sulle competenze dell'Ufficio (Ufficio Centrale Antifrode dei Mezzi di Pagamento - UCAMP), descritte in una solo pagina, l'approfondimento monotematico, dedicato quest'anno allo studio dei *black markets*, la collaborazione attiva del settore privato con il contributo fornito tramite il capitolo sulle misure di prevenzione e contrasto, nella consapevolezza del ruolo svolto dai segnalanti nel contrastare il fenomeno frodi, l'adozione di un'info-grafica capace di riassumere graficamente e in solo due pagine gli aspetti salienti del rapporto.

Non si vuole in questa sede riprendere i dati e i contenuti del rapporto 2015, che è, anche per un confronto tra la versione 2015 e le precedenti, facilmente scaricabile all'indirizzo:

http://www.dt.tesoro.it/it/attivita_istituzionali/antifrode_mezzi_pagamento/rapporti_statistici/carte_pagamento.html

Tuttavia, va sottolineato che nel 2014, con riferimento alle carte emesse in Italia, è diminuito il valore delle transazioni non riconosciute (frodi) rispetto al totale dei pagamenti genuini mediante carta (dallo 0,0195% allo 0,0189%), dimostrando, ancora una volta, come il timore di un uso fraudolento delle carte di pagamento è più percepito che reale.

SIRFE/SIPAF – NOVITA' & NUOVE FUNZIONALITA'

Con il DM del 1 febbraio 2013, pubblicato sulla G.U. della Repubblica nr. 37 del 13 febbraio 2013, è stata sancita la modalità telematica, attraverso il SIRFE (Sistema Informatizzato Rilevazioni Falsificazioni Euro), come unico metodo di trasmissione dei dati tecnici, statistici ed informativi relativi ai ritiri di valuta - cartacea o metallica - denominata in euro sospetta di falsità. Il nuovo sistema ha fatto riscontrare sin da subito i suoi effetti positivi, con un incremento considerevole del numero di segnalazioni pervenute all'UCAMP ed una più approfondita elaborazione ed analisi dei dati, anche a livello socio-economico oltre che più marcatamente statistico.

Nel corso degli anni si è cercato di rendere sempre più fruibili ed intuitive le procedure che gli Enti Segnalanti utilizzano per poter inserire i verbali di ritiro all'interno del SIRFE. In particolare, sono aumentati i controlli automatici sulla correttezza e la congruenza dei dati immessi dagli operatori all'atto della compilazione dell'apposito form telematico, sono stati forniti aiuti visivi con l'intento di limitare eventuali errori di compilazione, è stata, inoltre, resa disponibile la funzionalità di anteprima del verbale che consente all'operatore di verificare le informazioni inserite prima di procedere definitivamente all'invio delle stesse ad UCAMP.

L'UCAMP ha ritenuto opportuno accogliere una serie di esigenze segnalate dagli operatori del settore, tra cui la necessità di modificare/annullare in autonomia i verbali già inviati ad UCAMP, ma non ancora spediti alla Banca d'Italia o all'Istituto Poligrafico e Zecca dello Stato. Infatti, a partire dal 19 gennaio u.s., tale attività può essere effettuata autonomamente dall' operatore dell'ente segnalante direttamente dall'applicativo SIRFE, eliminando di fatto le attese connesse all'utilizzo della vecchia procedura.

Siamo lieti di segnalare il completamento e l'avvio della nuova procedura di riconciliazione automatica tra i verbali di ritiro delle monete sospette di falsità già presenti nel SIRFE e le perizie effettuate da IPZS - CNAC. Tale nuova funzionalità consente a tutti gli Enti Segnalanti di verificare in tempo reale l'esito delle perizie sulle monete che sono state oggetto di ritiro.

Spostandoci sull'applicativo SIPAF, ricordiamo che come anticipato durante il corso della plenaria GIPAF del 17/12/2015, a far data dal **01/04/2016**, l'accesso all'applicativo SIPAF avverrà esclusivamente dal Portale Dipartimentale (**PortaleDT**), raggiungibile al seguente indirizzo:

https://portaletesoro.mef.gov.it/

Affinché l'operazione possa avvenire correttamente, ricordiamo che sarà necessario assicurarsi che la propria utenza censita in SIPAF sia abbinata al proprio codice fiscale. Sarà, inoltre, necessario verificare che la propria utenza faccia riferimento ad un'email aziendale personale anziché un'email di gruppo. In caso contrario l'utenza non potrà essere migrata all'interno del nuovo portaleDT.

Infine ricordiamo che l'invio del formulario di accreditamento al SIPAF dovrà essere effettuato esclusivamente tramite invio al seguente indirizzo PEC: **dt5reatifinanziari@pec.mef.gov.it** e non più in forma cartacea.

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

Via XX Settembre, 97
00187 – Roma
Tel. 0647613535
Web: http://www.dt.tesoro.it
e-mail: ucamp.carte@tesoro.it