

Frauds: some facts

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

UCAMP:
Ufficio Centrale Antifrode Mezzi di Pagamento

Newsletter n 14 - Dicembre 2016

In questo numero:

Carte di Pagamento, in calo numero e valore delle transazioni non riconosciute

p. 1

Approfondimento monotematico:
Frodi relative alle carte di pagamento e evoluzione dell'ecosistema

p. 3

Contro la falsificazione dell'euro vincono scambio di best practices e innovazione...

p. 5

Carte di Pagamento, in calo numero e valore delle transazioni non riconosciute

Buone notizie dal 2015 sul fronte della lotta alle frodi perpetuate tramite carte di pagamento. Il numero di carte oggetto di disconoscimento si è attestato infatti intorno alle 100 mila unità, con un calo di circa il 6% rispetto al 2014. In calo anche il numero ed il valore delle transazioni non riconosciute, così come rappresentato nella figura 1. A ridursi è anche l'ammontare dei giorni di esposizione (giorni intercorsi fra la prima e l'ultima transazione disconosciuta sulla singola carta). Il calo del controvalore è, tuttavia, marginale se paragonato a quello del numero delle carte: ciò implica un aumento del controvalore frodato per carta (pro capite).

Anno(**)	Carte	Transazioni		Giorni(*) esposizione (MGL)
		Numero	Valore (MGL euro)	
2013	106.696	373.611	67.057	540
2014	108.300	448.789	68.534	1.162
2015	101.353	430.178	68.192	1.054
2015/14	-6,4%	-4,1%	-0,5%	-9,3%

(*) Ammontare dei giorni intercorsi fra il primo e ultimo disconoscimento sul complesso delle carte oggetto di disconoscimento

(**) Anno in cui è stata bloccata la carta

Figura 1

Sulla singola carta la struttura delle frodi può assumere infatti forme differenti. Osservando i grafici in basso, possiamo vedere che almeno il 75% delle carte frodate vengono intercettate lo stesso giorno in cui avviene il primo disconoscimento. Nel 90% dei casi questo avviene comunque nei primi 4-12 giorni. Nonostante il 90% delle carte sia comunque intercettato entro i primi 12 giorni dal primo disconoscimento, il tempo medio di intercettazione non supera gli 11 giorni. Ciò è dovuto all'influenza sul valore medio di una quota ridotta di carte (5%) che presenta tempi di intercettazione estremamente lunghi (oltre 40 giorni).

Una simile analisi può essere eseguita in termini di numero frodi effettuate sulla stessa carta. In quasi la metà dei casi si tratta di una sola frode, nel 90% della quota rimanente dei casi non si va oltre le 6-7 frodi.

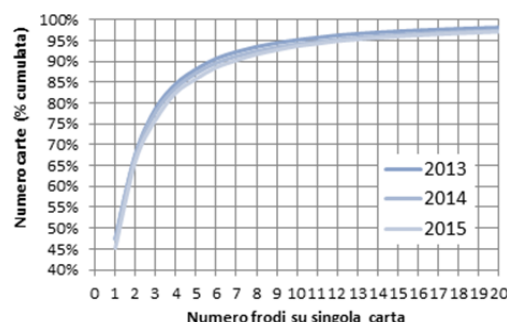
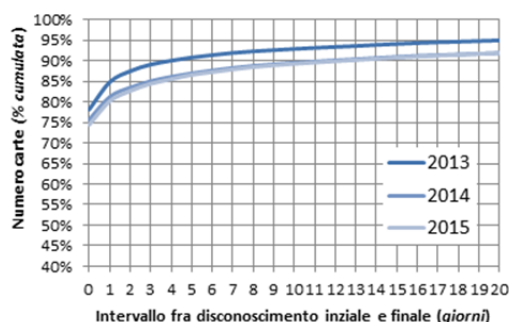


Figura 2

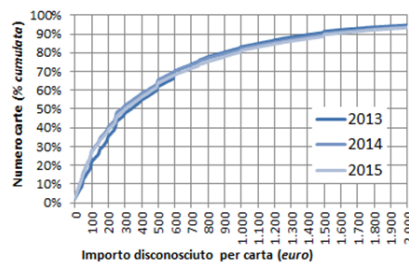


Figura 3

In merito ai profili di utilizzo della carta sui singoli canali si evidenziano aspetti differenti. La carta frodata utilizzata sul canale Internet determina, rispetto alle altre, importi pro capite per transazione più bassi e frequenze medie giornaliere di transazioni disconosciute più alte, come si può notare nei grafici in basso.

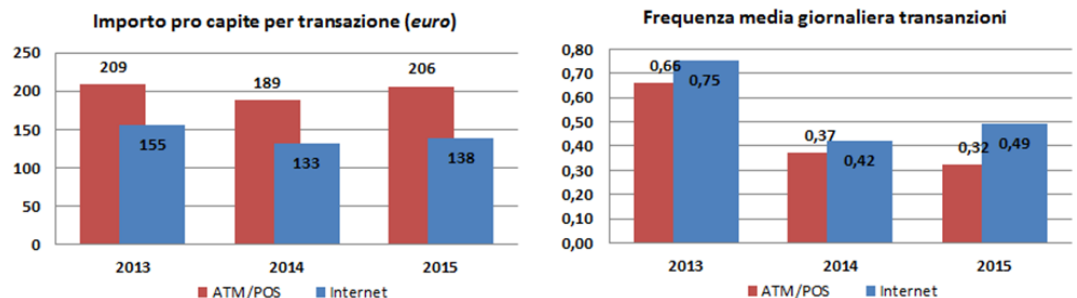


Figura 4

Il canale Internet mostra nell'anno passato un andamento sostanzialmente in linea con quello degli anni precedenti sia come dinamica - aumenta del 12% - sia come modalità di esecuzione della frode. L'incremento annuale del frodato è dunque spiegato, quasi completamente, dall'aumentato numero di carte utilizzate per le frodi.

La modalità di esecuzione della frode non sembra variare: l'importo pro-capite per transazione rimane quasi stabile (+4%), così come l'importo pro capite per carta (-2%). Le forti variazioni riguardano i giorni di esposizione delle carte (-20%) e il numero di transazioni giornaliere (+16%), ma queste due dinamiche vanno ad annullarsi vicendevolmente.

Molto diversa la situazione sui canali ATM/POS. A fronte di una riduzione del frodato di circa il 10% assistiamo ad una diminuzione del numero di carte utilizzate molto più marcata: -28%.

La spiegazione di questa asimmetria va ricercata in un cambio di comportamento nell'esecuzione della frode. Rispetto all'anno 2014, infatti, l'importo pro capite per carta aumenta del 25%, così come la durata di esposizione in giorni di una singola carta (+31%). In altri termini si riduce fortemente il numero di carte ma tale riduzione non si traduce totalmente in una diminuzione del frodato, poiché ogni singola carta viene "sfruttata" molto più di prima, sia in termini di importo medio per transazione (+9%) sia, soprattutto, in termini di giorni di esposizione della carta stessa.



Approfondimento monotematico

Frodi relative alle carte di pagamento e evoluzione dell'ecosistema criminale

Sempre più numerosi sono i forum in Internet che offrono prodotti relativi ad attività illegali connesse alle carte di pagamento. Molto spesso i gestori di questi servizi optano per le reti di anonimizzazione, come la **rete Tor**, con l'intento di garantire il proprio anonimato e quello dei propri clienti.

Identificare gli operatori dietro i **principali black market** è impresa ardua per le forze dell'ordine e richiede uno sforzo tecnologico e operativo significativo. Nello scorso numero abbiamo analizzato tutti i principali black market in cui venivano offerti prodotti e servizi connessi alle attività illegali relative alle carte di pagamento.

I dati rubati relativi alle carte di pagamento continuano ad essere tra le merci con il maggior numero di transazioni nei principali mercati underground, così come anche confermato da *"The Hidden Data Economy"*, uno studio pubblicato da McAfee.

All'offerta classica dei dati presenti sulla carta si abbina sempre più spesso la disponibilità di *"Fullzinfo"*, ovvero di pacchetti comprensivi di informazioni aggiuntive, quali documenti del possessore della carta, del numero di previdenza sociale e di altri dati che possono essere utilizzati per dimostrare l'identità della vittima in caso di frodi telematiche, note come *"Card No Present fraud"* - CNP (i.e. *Nome della madre, Paese di nascita di un genitore, animale preferito, etc.*).

Nella tabella seguente sono riportati i prezzi per i dati di carte di pagamento rubate negli USA (Visa, MasterCard, American Express, Discover), caso emblematico perché è possibile notare come i prezzi dei dati relativi alle carte di pagamento siano decisamente inferiori rispetto a quelli di altri paesi, proprio per la grande disponibilità di questa tipologia di informazioni.

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Random	\$5-\$8	\$20-\$25	\$20-\$25	\$21-\$25	\$25-\$30
With Bank ID Number	\$15	\$25	\$25	\$25	\$30
With Date of Birth	\$15	\$30	\$30	\$30	\$35
With Fullzinfo	\$30	\$35	\$40	\$40	\$45

Estimated per card prices, in US\$, for stolen payment card data (Visa, MasterCard, Amex, Discover).

Source: McAfee Labs.

Tabella 1

Tra i prodotti più contrattati continuano ad esserci i cosiddetti *'Dump'* ovvero informazioni copiate elettronicamente dalla banda magnetica della carta mediante dispositivi **skimmer**. Le informazioni sono contenute in due tracce e includono almeno nome e numero di conto del cliente, data di scadenza, il codice CVV1. Questi dati sono utilizzati per la clonazione di carte e pertanto molto richiesti dalle organizzazioni criminali in diversi paesi.

Uno dei mercati più interessanti, ospitato nella rete TOR, era **Agorà**, piattaforma oggi non più operativa e conosciuta principalmente per la

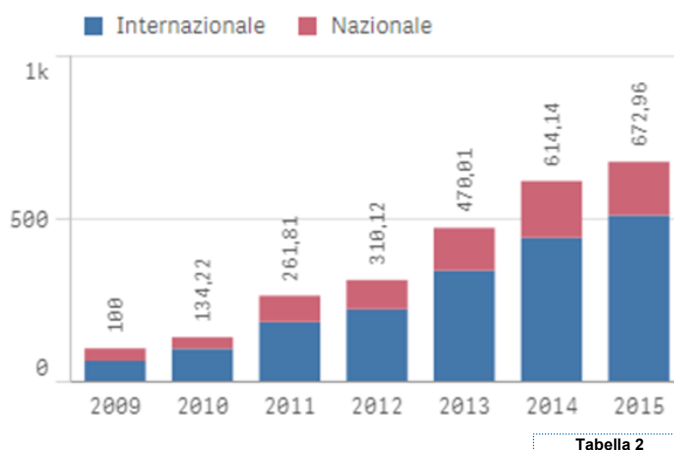


vendita di sostanze stupefacenti.

Chiaramente la totalità degli operatori di Agorà si è riversata nei mesi successivi in altri black market che, nel frattempo, hanno investito per ottimizzare la loro offerta e migliorare i propri servizi. E' il caso di **AlphaBay**, un altro black market nella rete TOR, che ha lanciato lo scorso anno un servizio completamente automatizzato per la vendita di dati rubati relativi a carte di credito.

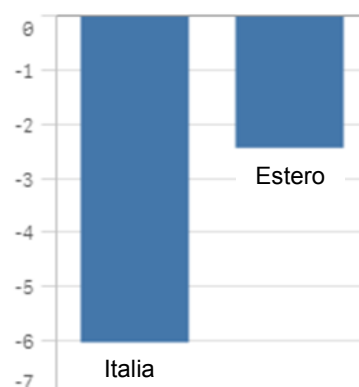
A complemento di quanto accennato vale la pena analizzare le frodi per **canali di pagamento**, dove Internet si caratterizza per una tendenza alla crescita e i POS e i prelievi su ATM registrano, invece, una flessione.

Sul canale **Internet** si è verificato infatti un aumento delle frodi soprattutto all'estero, così come si può evidenziare nella tabella 2.



Nel canale **POS** si assiste ad un calo generalizzato del fenomeno.

Di particolare interesse, di nuovo, la scomposizione tra Italia ed Estero: il fenomeno presenta un forte calo in Italia, molto più contenuto all'estero (vedi Tabella 3).



Per il 2015, come già in tutti gli anni precedenti, si conferma una tendenza alla riduzione del fenomeno delle frodi su **Prelievi su ATM**. Anche su questo canale la situazione è diversificata per Italia/Estero. In Italia il fenomeno è però in crescita nel Lazio. All'estero, dove il fenomeno si concentra negli Stati Uniti, si assiste ad un calo molto pronunciato dei prelievi fraudolenti, pari a -32%.

Contributo a cura dell'Ing. Pierluigi Paganini



Contro la falsificazione dell'euro vincono scambio di best practices e innovazione

Si è svolta a Tirana l'edizione 2016 del Pericles

Dal 5 al 7 Ottobre si è svolta a Tirana in Albania l'edizione 2016 del Pericles, che si è articolato in tre giornate tra seminari, work-shop e training per una comune strategia di protezione dell'euro nel Mediterraneo. L'evento ha visto la partecipazione di più di 60 delegati provenienti da Albania, Algeria, Croazia, Egitto, Francia, Italia, Malta, Montenegro, Olanda, Senegal, Stati Uniti d'America e Tunisia e rappresentanti delle istituzioni europee, dei ministeri dell'economia e della giustizia, degli interni, delle forze di polizia e delle banche centrali, fianco a fianco con rappresentanti delle banche commerciali, associazioni bancarie e altre realtà private.



Foto 1

Il programma europeo Pericles, creato nel 2001, è un progetto quasi interamente finanziato a livello comunitario, si occupa di formazione, confronto e scambio delle best practices, tra i diversi paesi partner, nella lotta alla contraffazione dell'euro. Fin dagli inizi l'Italia ha sostenuto pienamente il programma, contribuendone allo sviluppo e al successo attraverso la pianificazione e l'implementazione di specifici progetti di training, tra cui i più recenti in Turchia, Croazia e Marocco.

Filo conduttore dei lavori svoltisi a Tirana sono stati una maggiore attenzione agli stakeholders, alle innovazioni tecnologiche, alle novità normative. Sugli

stakeholders interessante il dibattito, moderato dal chair Antonio Adinolfi, in qualità di Direttore dell'Ucamp, relativamente alla ricerca tecnologica e alla proposta innovativa nel settore, con particolare riferimento all'esperienza delle banconote in plastica, da poco in sperimentazione nel contesto britannico, nonché alle app di identificazione del "presunto falso" sviluppate in Olanda.



Foto 2

Nel secondo workshop, coordinato dal chair Capitano Pollari del Nucleo Speciale Polizia Valutaria della Guardia di Finanza, l'attenzione è stata invece rivolta alle recenti modifiche normative comunitarie introdotte dalla direttiva comunitaria 2014/62/UE sulla protezione mediante il diritto penale dell'euro e di altre monete contro la



falsificazione.

Poi è stata la volta dei due training pratici, tenuti rispettivamente dalla BCE e Banca d'Italia e dall'Istituto Poligrafico Zecca dello Stato (IPZS), attraverso la simulazione del prezioso lavoro svolto dalle zecche e dalle banche centrali nell'individuazione delle monete e delle banconote contraffatte.

Ultima giornata, presso lo splendido contesto della Bank of Albania, ha visto l'intervento introduttivo dello US Secret Service e il confronto tra le diverse banche centrali dell'area balcanica.



Foto 3

“Nell'ambito della lotta alla contraffazione dell'euro, occorre dar vita a uno stakeholder approach, che veda il general public quale prima barriera contro la contraffazione. E' necessario quindi coinvolgere le associazioni di categoria, dai retailers alle associazioni bancarie, per rafforzare quella che noi definiamo la seconda barriera di lotta al falso. Infine, il nostro impegno è quello di potenziare il lavoro di intelligence, di scambio delle buone pratiche e di implementazione dei sistemi informativi attualmente operativi, al fine di aumentare l'efficacia del lavoro di analisi ed elaborazione dei dati e la collaborazione attiva con le forze di polizia” è stata la conclusione del Direttore dell'UCAMP.

“L'identificazione di una comune strategia per la protezione dell'euro nel bacino mediterraneo, in collaborazione con ECFIN, è un dovere per tutti noi, e l'Italia da anni non ha voluto mancare al suo ruolo proattivo di promozione e sostegno politico e logistico nei confronti di questo genere di iniziative. Lavoreremo in prospettiva affinché progetti come il Pericles possano continuare a rappresentare un faro per la formazione e il confronto nella lotta alla contraffazione monetaria”, sono state le parole del Capo della Direzione V, Giuseppe Maresca, all'apertura dei lavori.

©Ministero dell' Economia e delle Finanze, 2016
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. 0647613535
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.

