



# Sommario

## Sommario

Sommario .....	2
Executive summary.....	1
UCAMP Competenze e attività .....	5
Analisi del fenomeno .....	6
Trend e statistiche .....	6
Incidenze.....	6
Andamento generale .....	8
Frodi per canale di pagamento.....	9
Categorie merceologiche.....	10
Distribuzione Geografica .....	12
Tipologia di disconoscimento .....	14
Prelievi su ATM Italia .....	15
Prelievi su ATM all’Estero .....	16
Confronti internazionali.....	19
Manomissioni ATM.....	21
Revoche convenzioni POS .....	23
Approfondimento monotematico .....	26
Frodi relative alle carte di pagamento ed evoluzione dell’ecosistema criminale .....	26
Infografiche.....	30
Nota metodologica.....	32
Le Transazioni non riconosciute .....	32
Manomissioni ATM.....	34
Revoche convenzioni POS .....	35
Confronti Internazionali .....	36
Gruppo di lavoro.....	37



© Ministero dell'Economia e delle Finanze, 2009 - 2016

Dipartimento del tesoro  
Direzione V, Ufficio VI (UCAMP)  
Ufficio Centrale Antifrode dei Mezzi di Pagamento  
Area Carte di Pagamento

Indirizzo

Via XX Settembre, 97  
00187 Roma

Telefono

+39 06.47613391

E-mail

[ucamp.carte@tesoro.it](mailto:ucamp.carte@tesoro.it)

[augusto.santori@tesoro.it](mailto:augusto.santori@tesoro.it)

Sito internet

<http://www.mef.gov.it>

<http://www.dt.tesoro.it>

Tutti i diritti riservati. È consentita la riproduzione  
a fini didattici e non commerciali,  
a condizione che venga citata la fonte.

ISSN 2239-0189

*Aggiornato con i dati relativi ai casi di frode relativi all'annualità 2015*



## Executive summary

Il Rapporto annuale analizza sotto diversi aspetti i fenomeni delle frodi su carte di pagamento, le manomissioni agli ATM e le revocche delle convenzioni dei POS. In particolare rispetto alle frodi su carte di pagamento (transazioni non riconosciute) si fa riferimento alle frodi perpetrate da carte emesse in Italia e spese ovunque.

### Transazioni non riconosciute

Nel 2015, con riferimento alle carte emesse in Italia, sono diminuiti sia i valori delle transazioni non riconosciute (frodi) rispetto al totale dei pagamenti genuini mediante carta (dallo 0,0189% allo 0,0173%), che, in maniera ancor più rilevante, il numero (da 0,0131% a 0,0112%). Nel 2015 il totale dei pagamenti genuini, sia in valore sia in numero, è aumentato rispettivamente del 8% e del 10%<sup>1</sup>.

Il valore delle frodi è diminuito dell'1%, mentre il numero del 6%, con un aumento del valore medio delle singole transazioni (da 151€ a 159€). Questa inversione di tendenza, rispetto alla diminuzione degli ultimi due anni, si potrebbe spiegare come il parziale *riassorbimento* del fenomeno della parcellizzazione delle transazioni fraudolente.

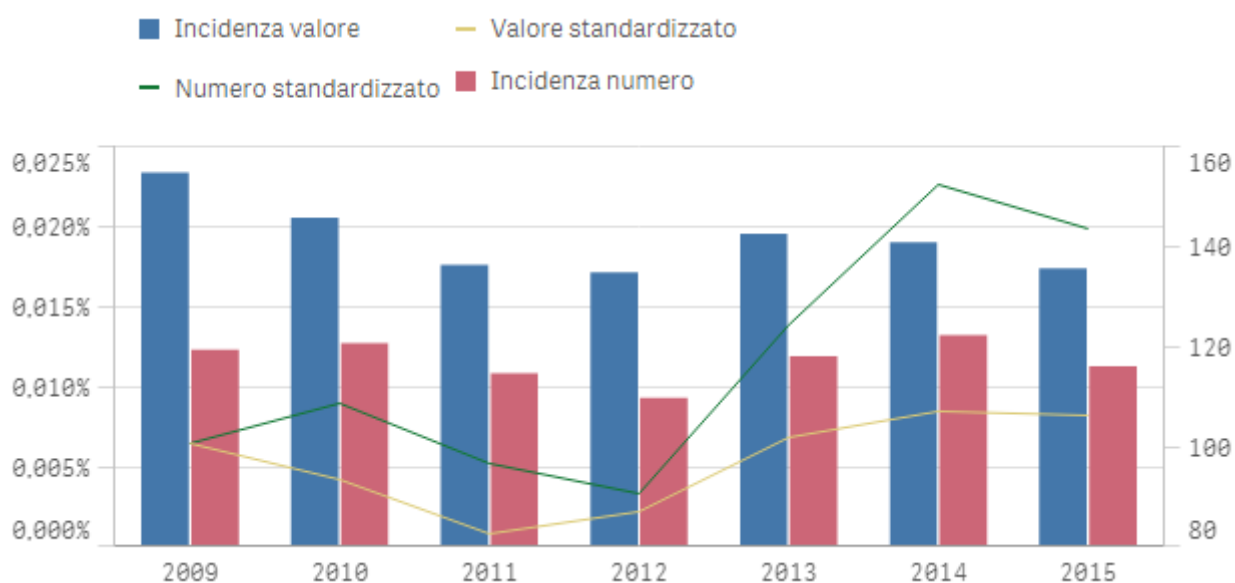


Figura 1: Incidenza e frodato in termini di valore e numero, serie storica

**Incidenza valore:** Valore in euro delle transazioni non riconosciute su carte emesse in Italia diviso per il valore di tutte le transazioni genuine effettuate con carte italiane.

**Incidenza numero:** Numero delle transazioni non riconosciute su carte emesse in Italia diviso per il numero di tutte le transazioni genuine effettuate con carte italiane.

**Valore standardizzato:** Valore delle transazioni non riconosciute su carte emesse in Italia dell'anno di riferimento diviso per il valore del 2009. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

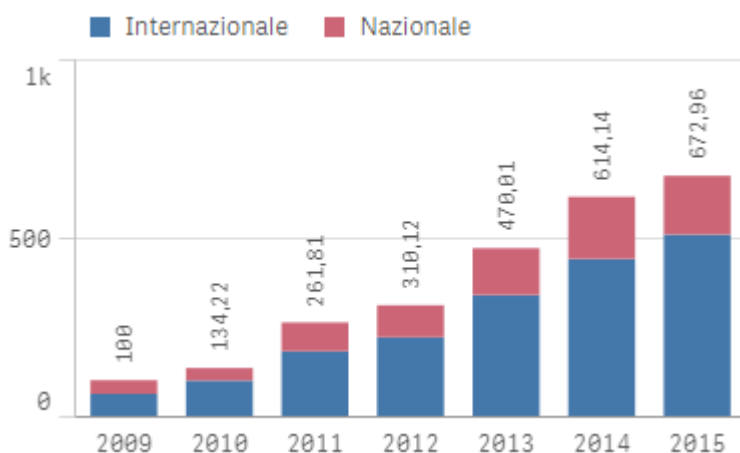
<sup>1</sup> Dal 2009 al 2015 il totale dei pagamenti genuini, sia in valore sia in numero, è costantemente aumentato, a riprova di un maggior utilizzo degli strumenti di pagamento alternativi al contante. L'aumento nel periodo è stato pari al 56% in numero e al 42% in valore.

**Numero standardizzato:** Numero delle transazioni non riconosciute su carte emesse in Italia dell'anno di riferimento diviso per il numero del 2009. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

L'analisi della serie storica 2009-2015 descrive un fenomeno sostanzialmente sotto controllo sia in termini di valore che di numero transazioni. In particolare l'incidenza in termini di valore si conferma in diminuzione per il secondo anno consecutivo, a differenza di quanto accade nei principali paesi europei.

In termini incidenza delle frodi per **canali di pagamento** mentre Internet si caratterizza per una tendenza alla crescita, i POS e i prelievi su ATM registrano una flessione. La crescita di Internet è comunque inferiore a quella verificatasi negli ultimi due anni.

### Canale internet



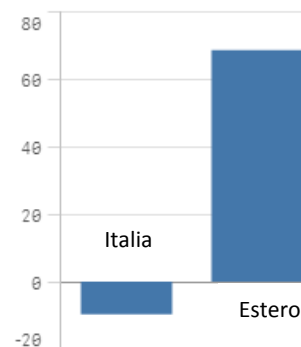
Sul canale **Internet** si è verificato un aumento delle frodi (+5,1% in termini di incidenza valore e +9,6% come valore del frodato). Viceversa l'incidenza in termini di numero è scesa del 4,3%.

Il fenomeno si verifica soprattutto all'Estero<sup>2</sup>.

Per la prima volta dal 2009, cioè dall'inizio della rilevazione, il valore del frodato su Internet in Italia diminuisce, in buona parte grazie alla riduzione verificatasi nella categoria merceologica *Betting / Casinò Gambling*, fenomeno del quale ci eravamo occupati con un approfondimento specifico nello scorso Rapporto.

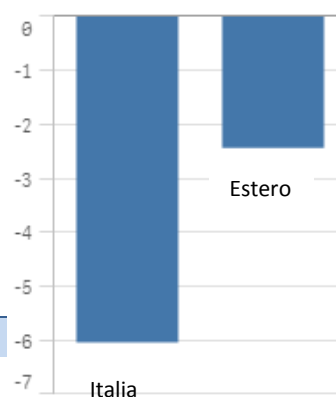
All'estero l'aumento è molto rilevante, riguarda principalmente la *MCG General Retail*, con particolare riferimento agli acquisti di abbigliamento.

I tre paesi in cui l'aumento è maggiore sono europei (Regno Unito, Francia e Lussemburgo), il quarto è la Cina che per il secondo anno consecutivo si conferma tra le prime nazioni dove le frodi vengono perpetrate.



### Canale POS

Nel canale **POS** si assiste ad un calo generalizzato del fenomeno a tutti i livelli: incidenza e frodato sia in termini di valore che di numero.



<sup>2</sup> Estero: insieme di tutte le nazioni del mondo esclusa l'Italia.

Di particolare interesse, di nuovo, la scomposizione tra Italia ed Estero: il fenomeno presenta un forte calo in Italia ed un calo molto più contenuto all'estero. Questa differenza si riduce se esaminiamo i dati in termini di numero (-15% vs -17%). Infatti l'importo medio all'estero cresce mentre in Italia cala e questo amplifica le differenze sul controvalore.

Italia. In termini di categoria merceologica il calo di gran lunga più rilevante si determina nella MCG *General Retail*, in particolare supermercati e abbigliamento.

La Lombardia e la Campania sono le regioni dove il fenomeno cala maggiormente.

Estero. La diminuzione si concentra sulle MCG legate ai viaggi, in particolare in Francia ed Irlanda.

Merita un cenno la situazione degli Stati Uniti, nazione dove il fenomeno delle frodi su POS è più rilevante e si concentra solitamente nella MCG *General Retail*. Nel corso del 2015 le frodi su POS negli Stati Uniti aumentano e sempre nella MCG *General Retail*.

#### Canale prelievi su ATM

Anche per il 2015, come già in tutti gli anni precedenti, si conferma una tendenza alla riduzione del fenomeno delle frodi su **Prelievi su ATM**. La riduzione è meno marcata sul valore (-9% in termini di incidenza e -8% in termini di frodato) rispetto al numero (-25% in termini di incidenza e -22% in termini di frodi).

All'estero, dove il fenomeno si concentra negli Stati Uniti, si assiste ad un calo molto pronunciato dei prelievi fraudolenti, pari a -32%.

#### **Manomissioni ATM**

Le **manomissioni di ATM**, che avevano raggiunto il loro minimo storico nel 2014, sono cresciute del 15% sia in termini di incidenza che di numero. Questa dinamica va però letta alla luce di una variazione nel sistema di rilevazione: da quest'anno vengono infatti rilevate anche le manomissioni su sportelli di Poste Italiane, senza le quali il fenomeno avrebbe manifestato una sensibile diminuzione.

L'aumento più vistoso si verifica nelle regioni del centro Italia, in particolare in Toscana. Le uniche aree in cui l'aumento è molto ridotto (+1,3%) è l'area del Nord Ovest. Importante la crescita del fenomeno anche nelle Marche, che porta questa regione al secondo posto dopo il Piemonte per incidenza.

**Incidenza valore:** Valore in euro delle transazioni non riconosciute su carte emesse in Italia diviso per il valore di tutte le transazioni genuine effettuate con carte italiane.

**Incidenza numero:** Numero delle transazioni non riconosciute su carte emesse in Italia diviso per il numero di tutte le transazioni genuine effettuate con carte italiane.

La tipologia di manomissione più diffusa è l'apposizione di skimmer che, come tipologia, è più che triplicata nel corso dell'anno.

### Revoche convenzioni POS

Le **revoche convenzioni** POS in Italia diminuiscono in maniera sostanziale: -26% in termini di incidenza<sup>3</sup> e -31% in numero. Tutte le regioni in cui il fenomeno è rilevante mostrano una netta diminuzione del numero: Lazio -42%, Campania -22% ed Emilia-Romagna -9%.

Le uniche regioni in cui il fenomeno aumenta, ad esempio Umbria e Marche, sono regioni in cui il fenomeno nel 2014 era sostanzialmente irrilevante.

---

<sup>3</sup> Numero di revoche di convenzioni di apparecchiature POS rispetto al totale delle convenzioni attive nell'anno.

## UCAMP Competenze e attività

### Le attività dell'UCAMP

Il Dipartimento del tesoro, nell'ambito delle proprie attribuzioni, è suddiviso in settori omogenei di attività e, tra questi, rilevanza assume l'area della prevenzione dei reati finanziari (Direzione V).

L'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP) costituisce la struttura operativa, nell'ambito della suddetta area, preposta ai seguenti compiti:

- il monitoraggio delle falsificazioni dell'Euro;
- la prevenzione delle frodi sulle carte di pagamento;
- l'attività di formazione di carattere specialistico, nei settori di competenza, sia a livello nazionale sia internazionale.

L'UCAMP trae origine dal Regolamento (CE) 1338/2001, istitutivo del sistema europeo di protezione dell'Euro, e funge da Ufficio centrale italiano per la raccolta e lo scambio dei dati statistici su banconote e monete sospette false al fine di effettuare un'analisi strategica del fenomeno delle falsificazioni e valutarne l'impatto sul sistema economico e finanziario. Per lo svolgimento di tali funzioni l'UCAMP si è dotato di un Sistema Informatizzato Frodi Euro (SIRFE), che consente la trasmissione telematica dei verbali di sequestro delle banconote sospette di falsità.

Con la legge n.166/2005, istitutiva del Sistema di prevenzione delle frodi sulle carte di pagamento, e con il relativo Regolamento di attuazione (D.M. n.112/2007) sono state attribuite all'UCAMP le attuali competenze in materia di prevenzione, sul piano amministrativo, delle frodi sulle carte di pagamento.

In attuazione della richiamata normativa l'UCAMP ha curato la realizzazione del Sistema Informatizzato per la Prevenzione delle Frodi sulle carte di pagamento (SIPAF), che permette la consultazione e la condivisione, in tempo reale, di dati e informazioni riguardanti esercizi commerciali sospetti e operazioni con transazioni non andate a buon fine. In tale ambito è stato costituito un gruppo di lavoro con funzioni consultive (GIPAF), al quale partecipano esperti nel settore delle frodi designati dalle Amministrazioni statali, dalla Banca d'Italia, dall'ABI, dalle Forze di Polizia, dalle società segnalanti, nonché esperti provenienti dal mondo accademico e scientifico.

La strategia operativa dell'UCAMP nella realizzazione e nella gestione del sistema di prevenzione mira alla tutela del sistema bancario e delle società emittenti, ma, in ultima analisi, è finalizzata alla tutela del cittadino, che ripone la propria fiducia negli strumenti di pagamento sostitutivi del contante.

L'UCAMP promuove e coordina attività formative in ambito nazionale e internazionale, in particolare, relativamente alla falsificazione dell'Euro, ha organizzato numerosi seminari e workshop indirizzati a tutte le categorie coinvolte nel fenomeno della contraffazione monetaria, in attuazione del programma comunitario di formazione denominato Pericles.

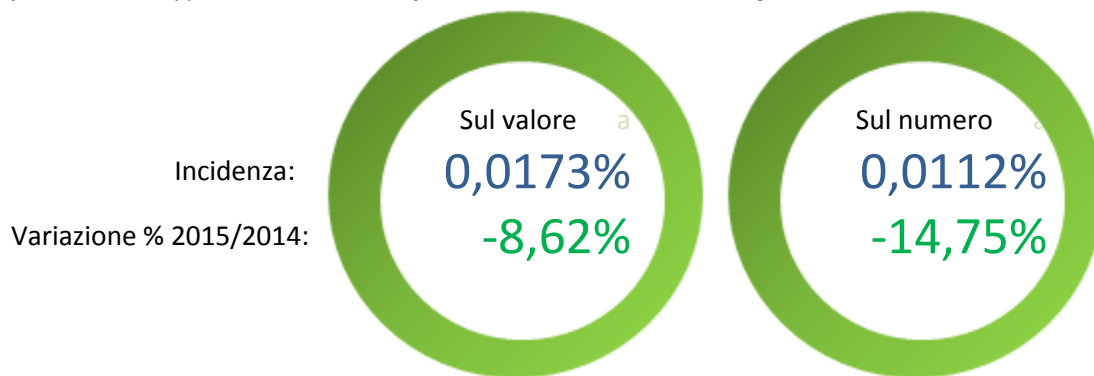


# Analisi del fenomeno

## Trend e statistiche

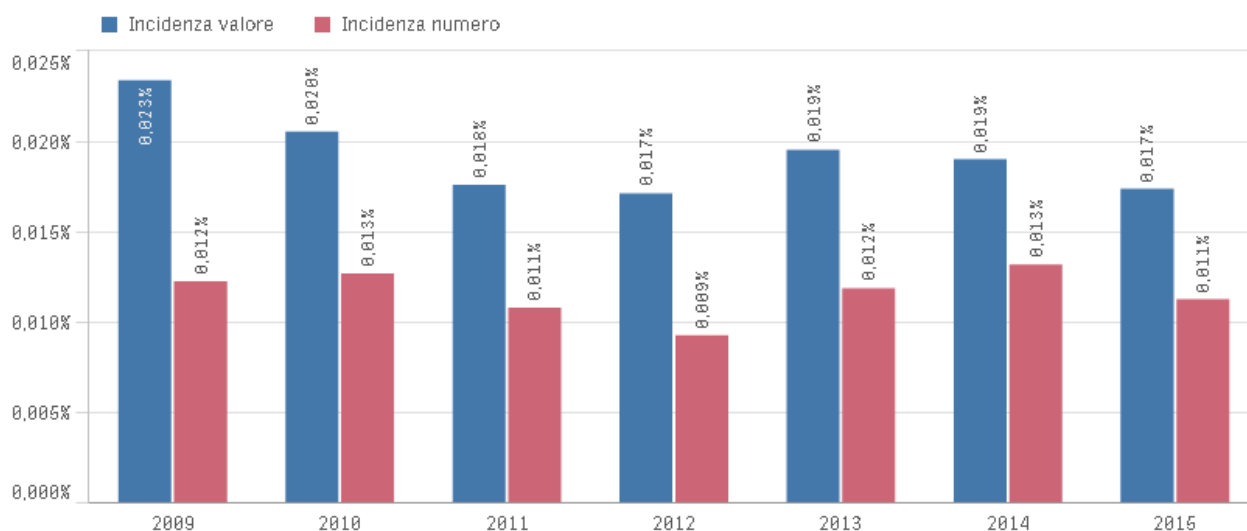
### Incidenze

L'incidenza si definisce come il rapporto tra le transazioni frodate e il totale delle transazioni genuine avvenute nell'anno.



Nel corso dell'anno 2015 l'incidenza in valore ed in numero si sono entrambe ridotte (-8,62% e -14,75%). Dunque il valore medio delle singole transazioni è leggermente aumentato.

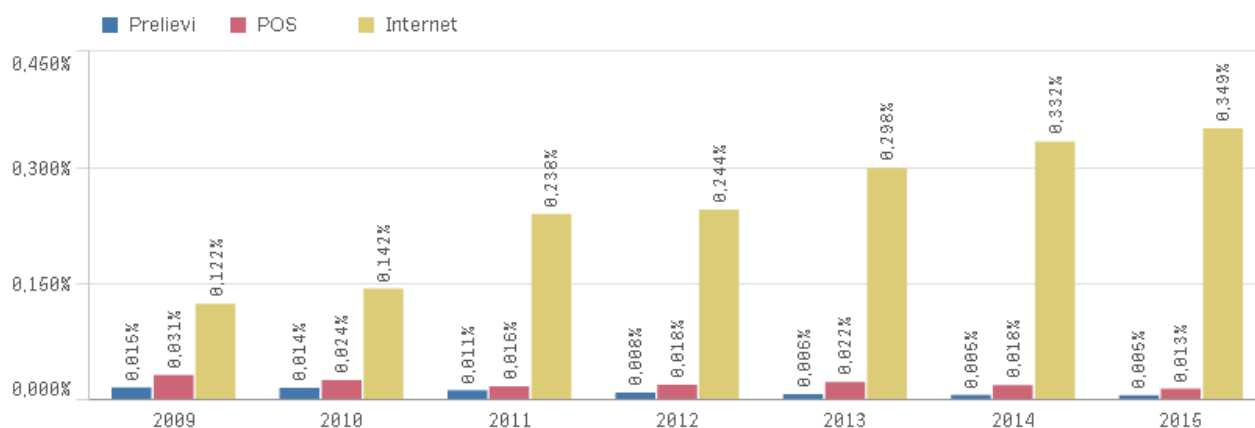
### Incidenza su valore e numero transazioni



Incidenza delle frodi sul totale transazioni

Figura 3: Incidenza delle frodi sul totale transazioni in numero e valore

**Incidenza per canale**



*Incidenza delle frodi sul totale transazioni*

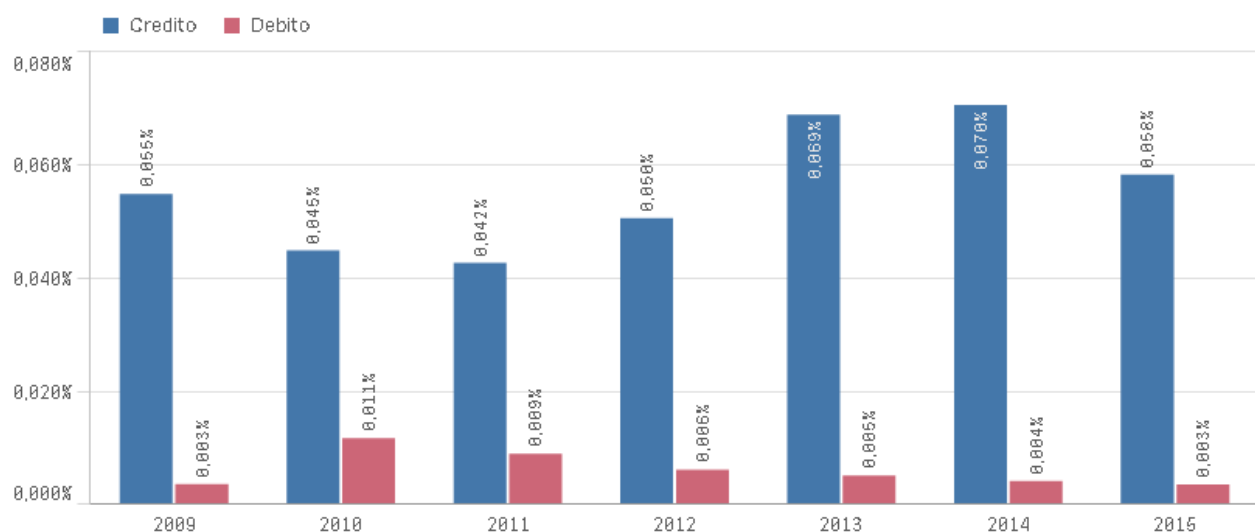
Figura 4: Incidenza per canale di pagamento

Variatione percentuale 2015/2014 del valore delle incidenze per canale

Internet: **+5,08%**      POS: **-26,54%**      Prelievi su ATM: **-9,06%**

Continua la crescita dell'incidenza delle frodi su Internet mentre si conferma la diminuzione su POS e Prelievi su ATM. Le incidenze delle frodi in valore per Debito/Credito mostrano una sensibile riduzione per quanto riguarda il Credito.

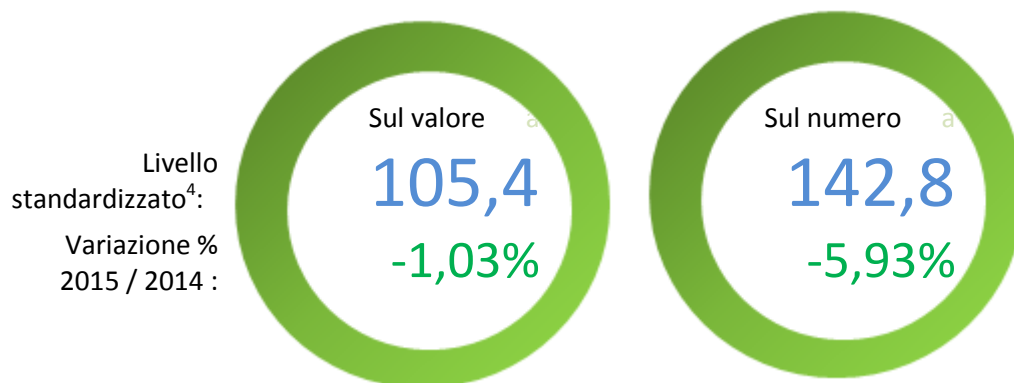
**Incidenza per debito e credito**



*Incidenza delle frodi sul totale transazioni*

Figura 5: Incidenza per debito e credito

## Andamento generale



In valore le frodi sono molto simili (105,4) al livello del 2009 mentre in numero sono aumentate di oltre il 40% (142,8). Il valore medio è leggermente aumentato durante il 2015.

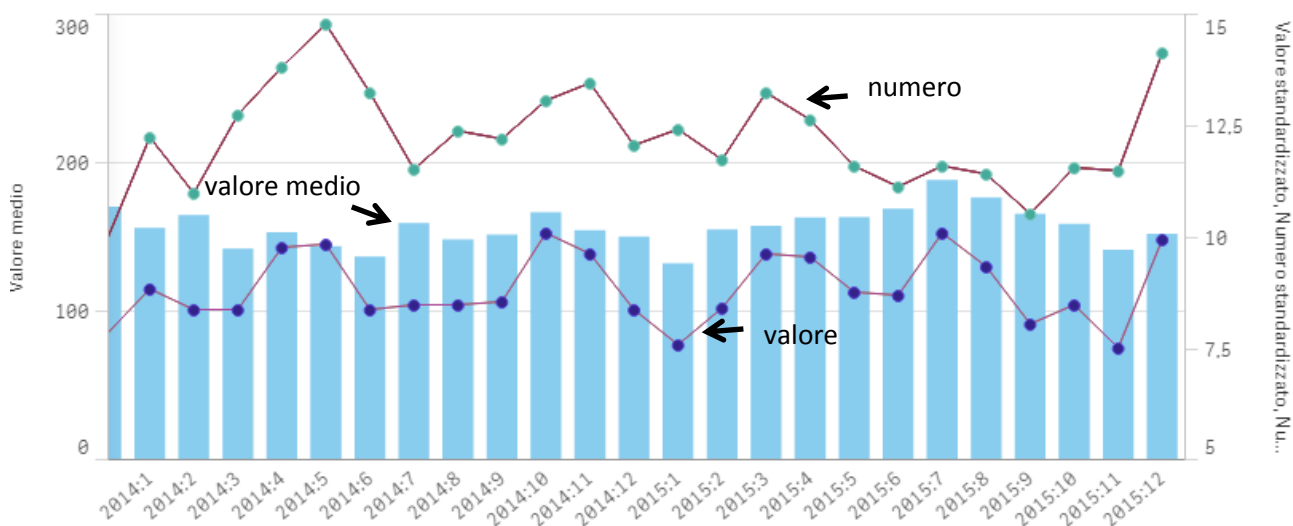


Figura 6: Andamento mensile di numero e valore standardizzati, valore medio

<sup>4</sup> Valore standardizzato: Valore delle transazioni non riconosciute nell'anno di riferimento diviso per il valore del 2009, su carte emesse in Italia. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

Numero standardizzato: Numero delle transazioni non riconosciute nell'anno di riferimento diviso per il numero del 2009, su carte emesse in Italia. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

## Frodi per canale di pagamento



Figura 7: Composizione del frodato in valore in base al luogo in cui le carte sono spese (Italia/Estero), distinto per canale

### Variazione percentuale 2015/2014

Internet: **+9,6%** POS: **-12,7%** Prelievi su ATM: **-7,6%**

In termini di frodato, senza tenere conto delle transazioni totali genuine, si conferma quanto già visto nelle incidenze: Internet è in crescita mentre scendono gli altri canali.

La maggior parte delle frodi su Internet risulta avvenuta all'estero.

### Valori standardizzati

2009=100

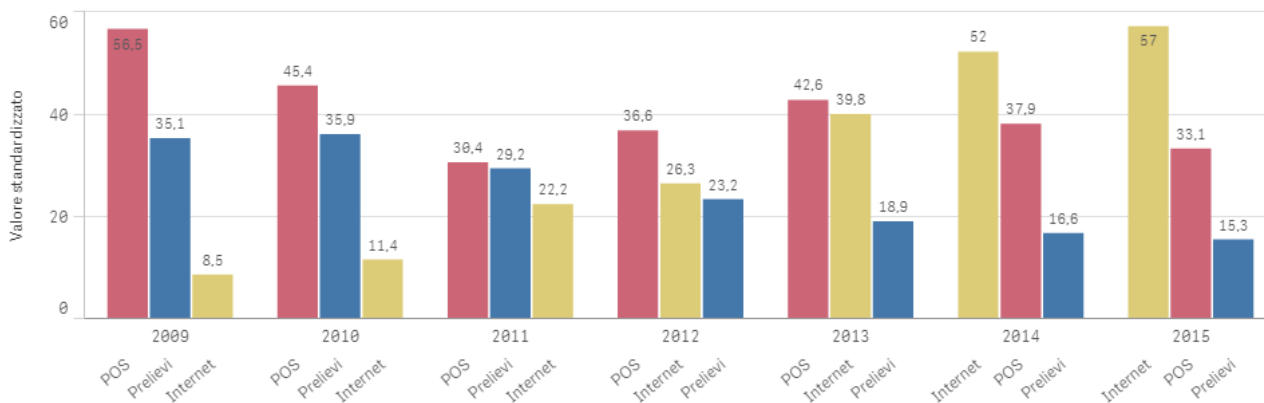
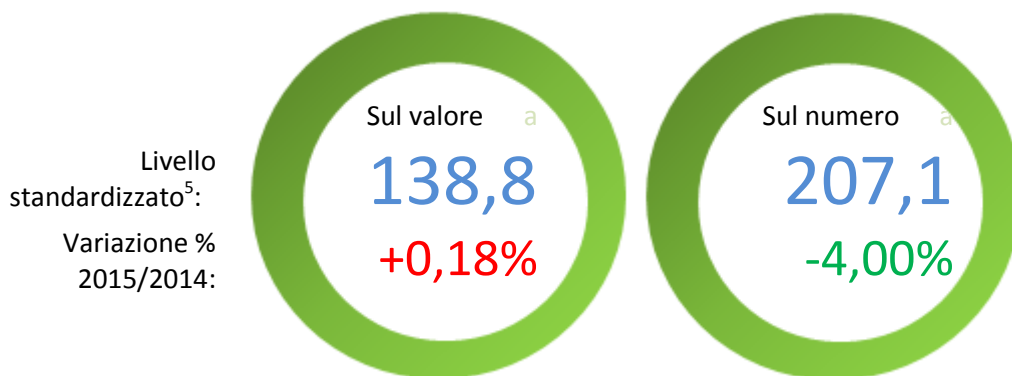


Figura 8: andamento frodi per canale

## Categorie merceologiche

Canali di pagamento POS e Internet.



### Valori standardizzati

2009=100

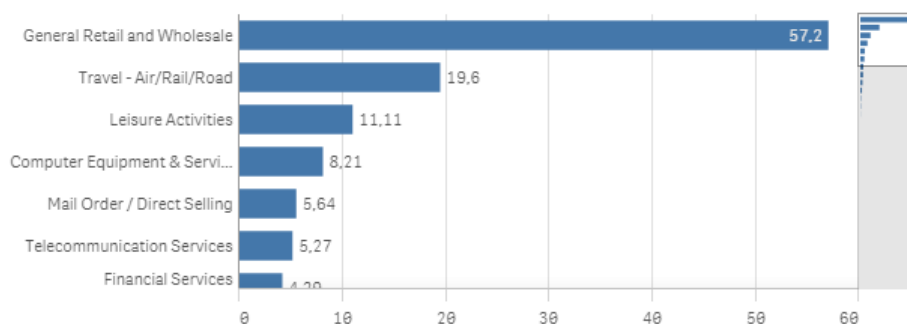


Figura 9: Le 6 Merchant Category Group più importanti in termini di frodato

### Variazione 2015 su 2014

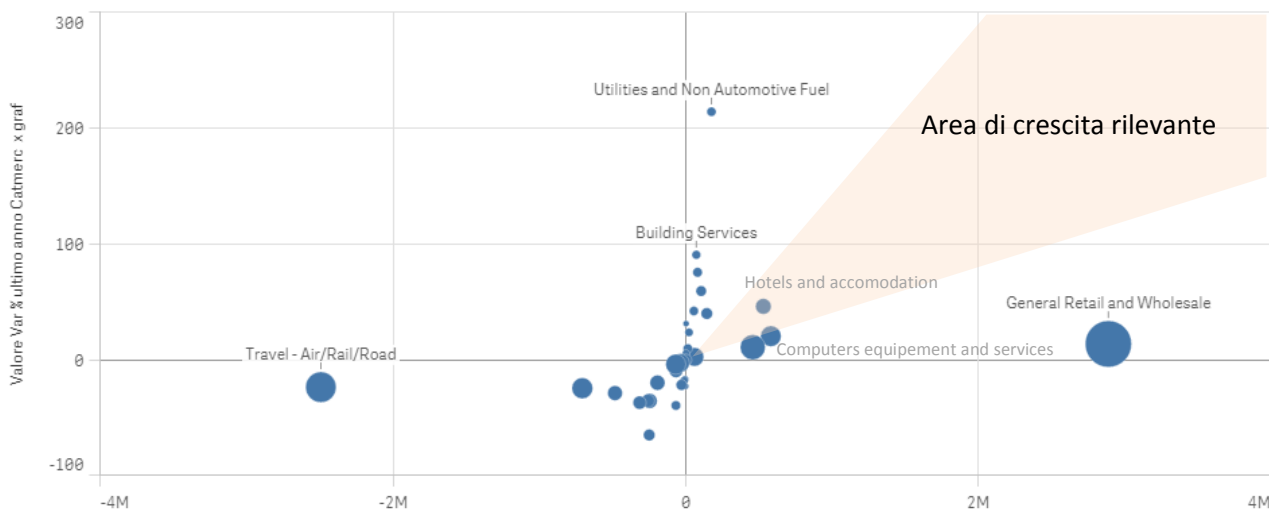
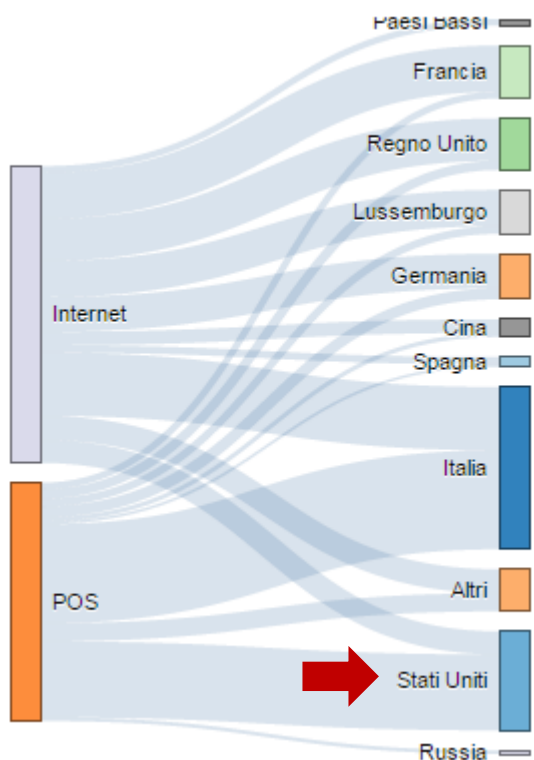


Figura 10: Le Merchant Category Group in valore (dimensione bolla), in variazione assoluta (asse x) e variazione percentuale (asse y)

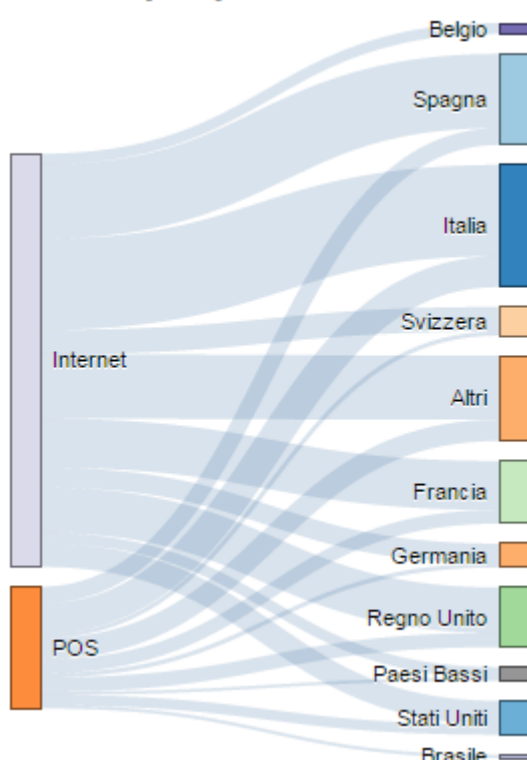
<sup>5</sup> Vedi nota 6.



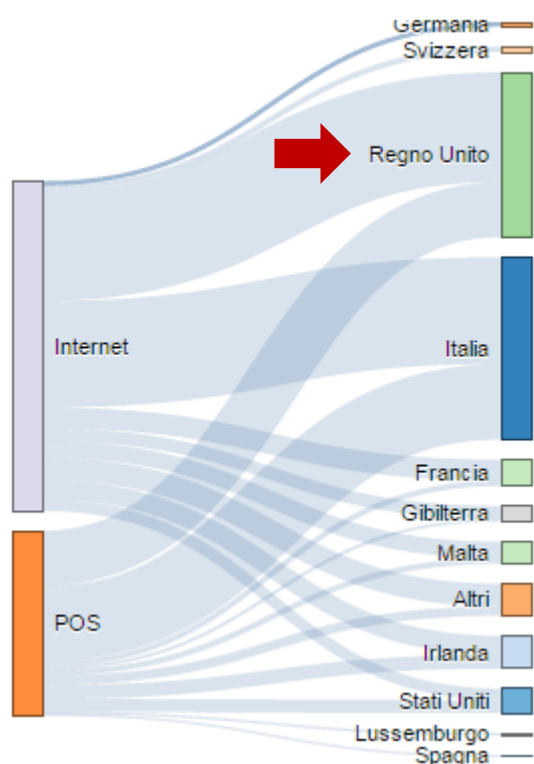
### General Retail and Wholesale



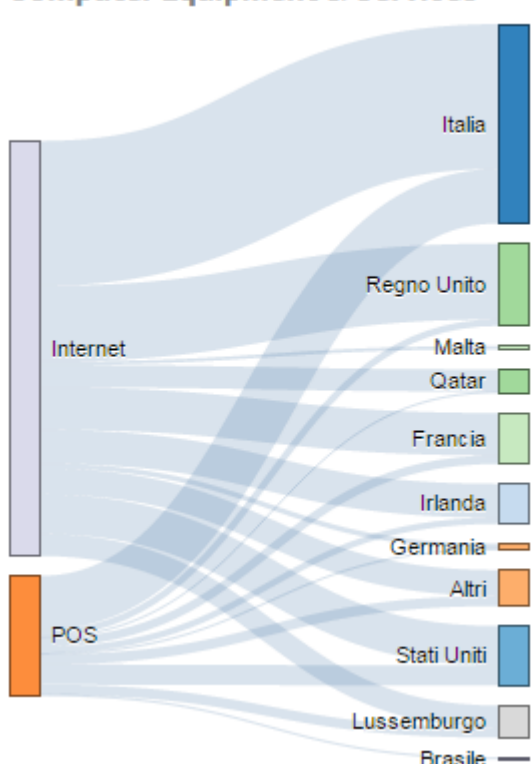
### Travel Air/Rail/Road



### Leisure activities



### Computer Equipment & Services



L'analisi delle quattro maggiori categorie merceologiche mostra come ogni nazione sia *specializzata* su specifiche categorie e canali. Es. Stati Uniti POS – *General Retail* mentre Regno Unito – *Leisure activities* (vedi frecce).

## Distribuzione Geografica

Canali di pagamento POS e Internet.

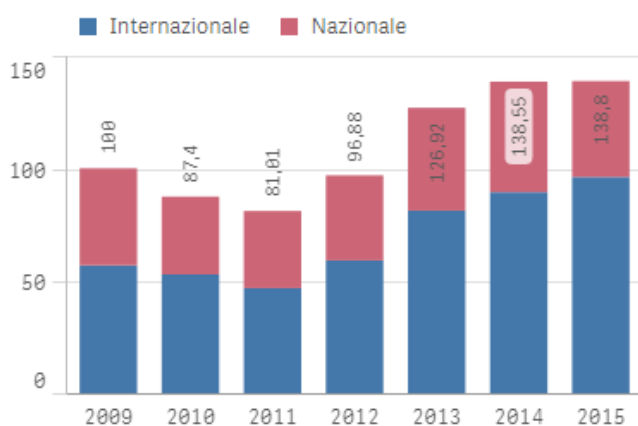


Figura 11: Valore standardizzato canali POS e Internet in base al luogo in cui le carte sono spese (Internazionale/Nazionale)

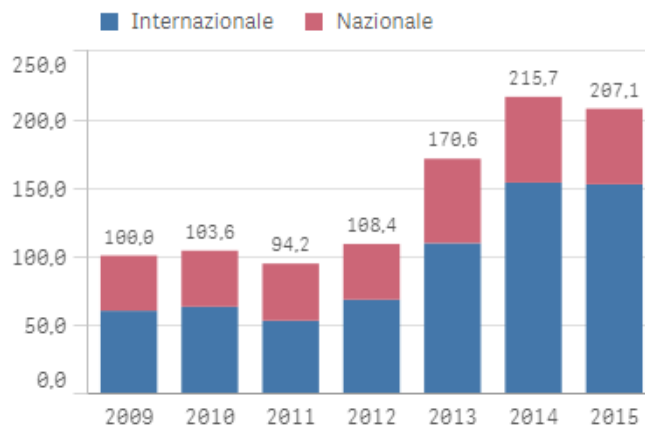


Figura 12: Numero standardizzato canali POS e Internet in base al luogo in cui le carte sono spese (Internazionale/Nazionale)

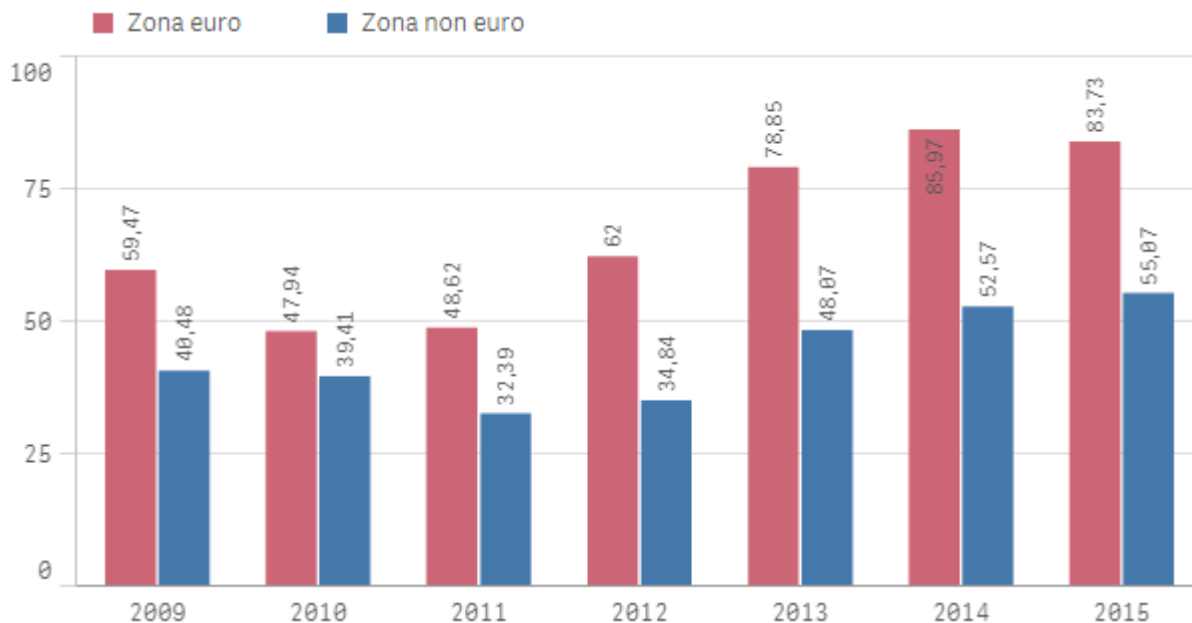


Figura 13: Valore standardizzato canali POS e Internet, carte emesse in Italia e spese in zona euro/non euro

Variazione percentuale 2015/2014

**Valore**

Zona euro: **-2,61%** Zona non euro: **+4,74%**

**Numero**

Zona euro: **-7,18%** Zona non euro: **+0,48%**

Canali di pagamento POS e Internet - Estero

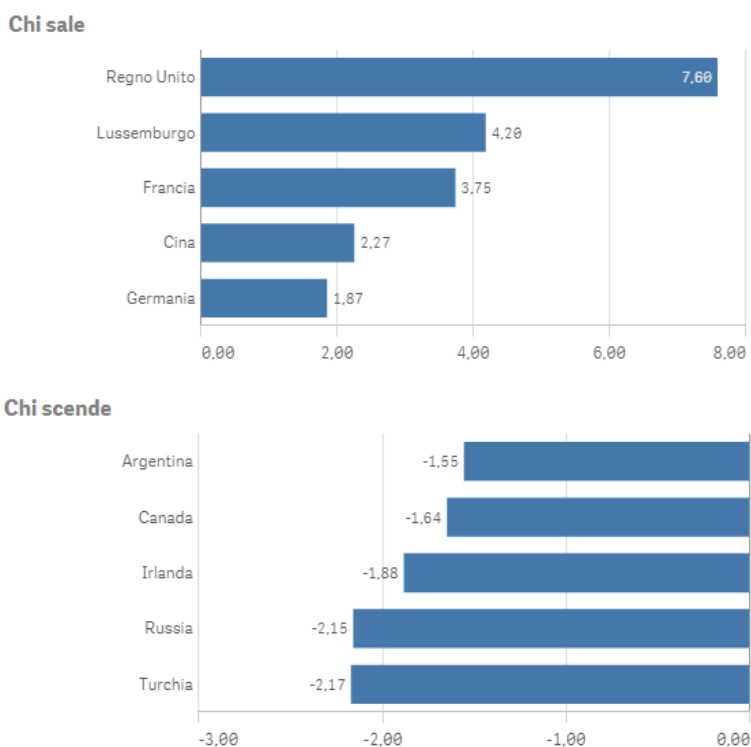


Figura 14: Variazioni 2015 - 2014 del valore standardizzato, primi 5 paesi

Estero: Variazione percentuale 2015/2014

Valore: **+7,6%** Numero: **-0,81%**

I grafici in alto mostrano i cinque paesi esteri con la maggiore crescita (o diminuzione) di frodi sui canali POS e Internet. In basso invece la mappa riporta la distribuzione delle frodi nel 2015.

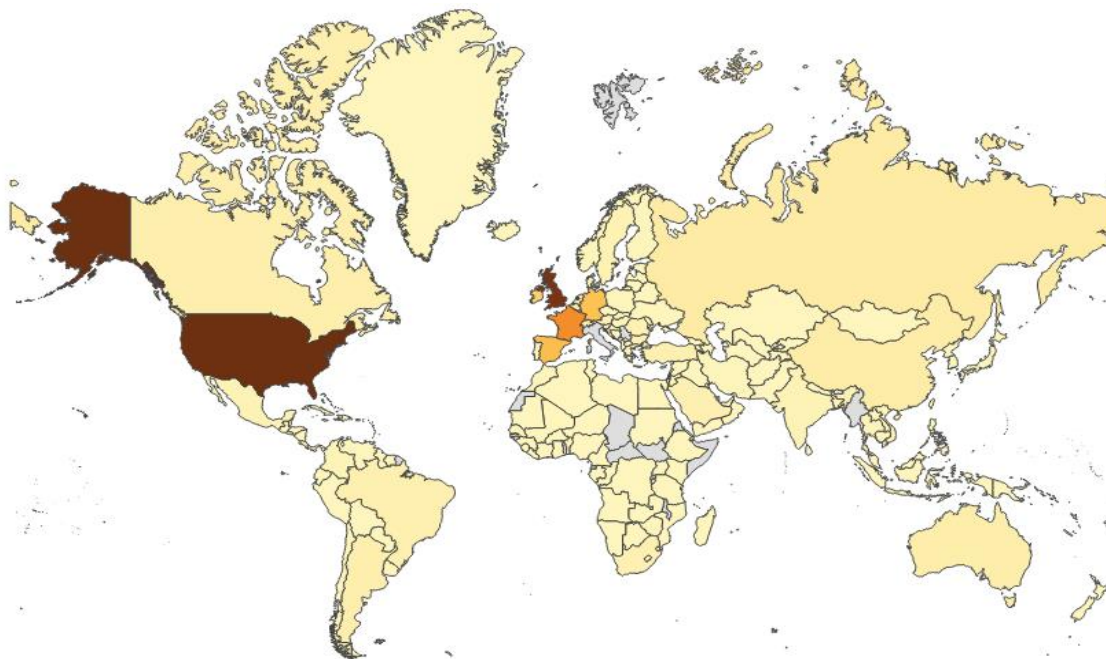


Figura 15: la mappa per valore delle frodi 2015 all'estero (il colore esprime l'intensità del fenomeno)



## Tipologia di disconoscimento

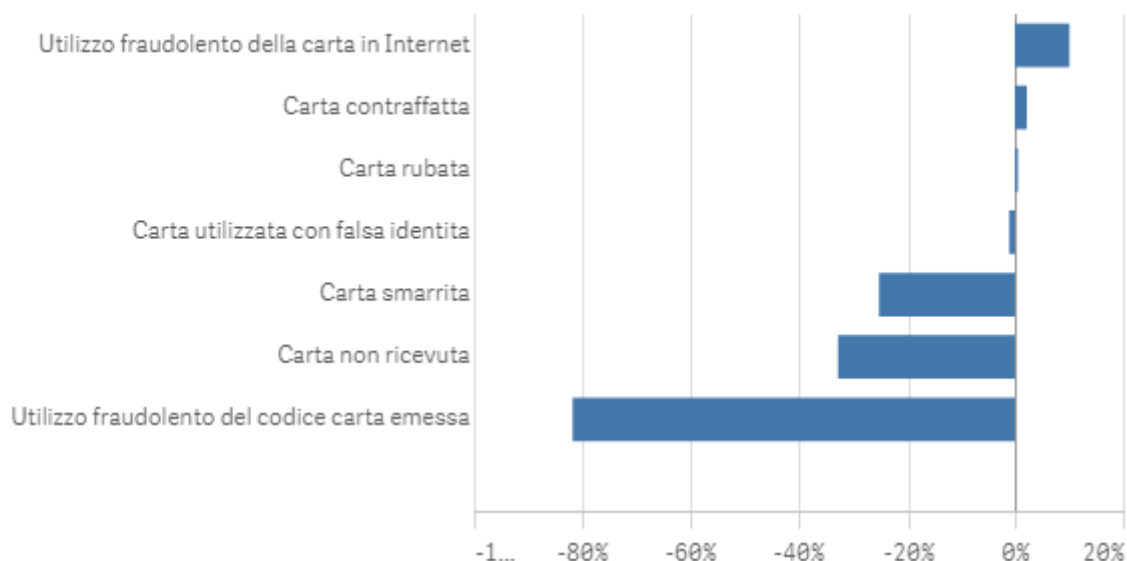


Figura 16: Variazione percentuale valore del frodato per tipologia di disconoscimento

Anche quest'anno si conferma l'aumento della tipologia su *Internet* mentre rimane sostanzialmente costante *Carta Contraffatta*.

### Valori standardizzati

2009=100

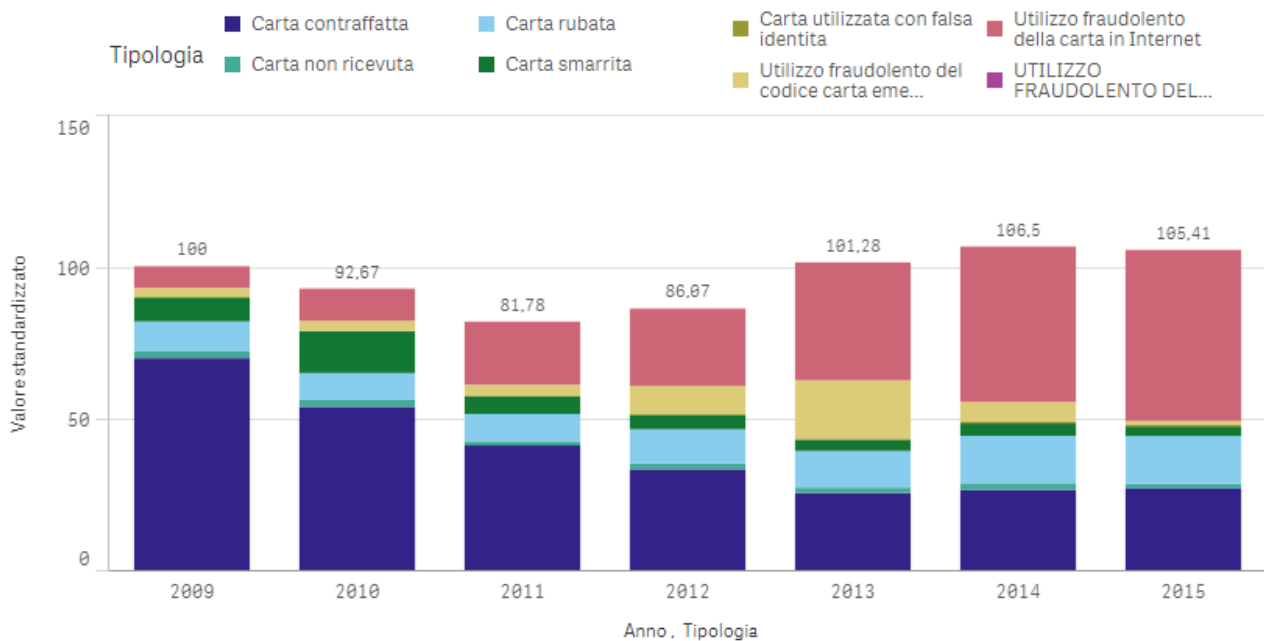


Figura 17: Andamento annuale del valore standardizzato per tipologia di disconoscimento

## Prelievi su ATM Italia

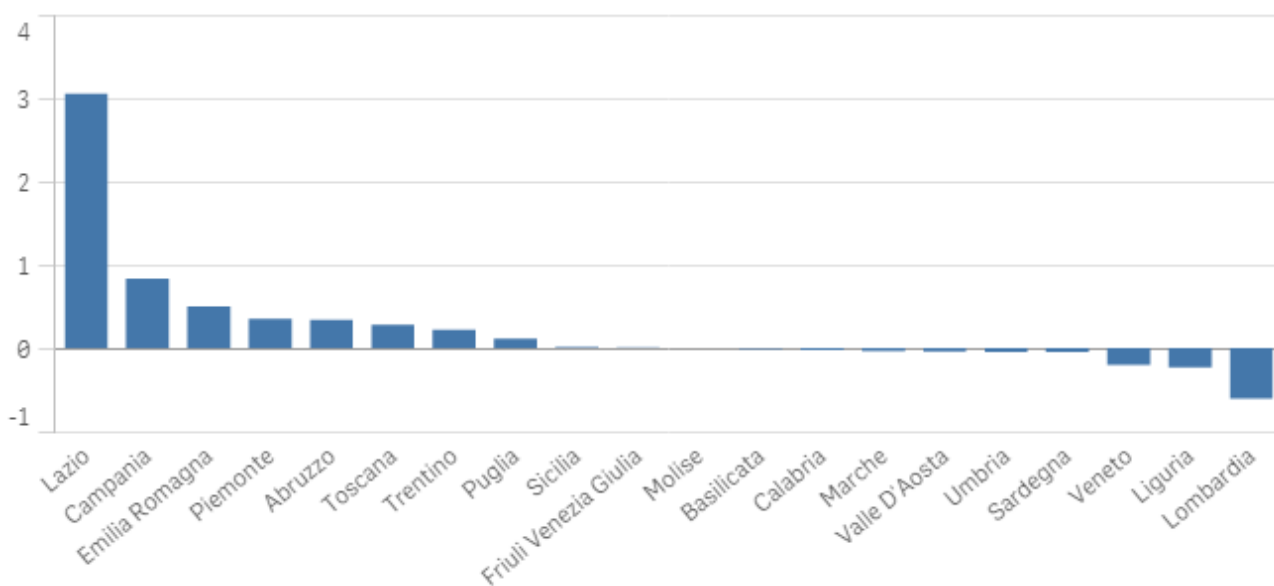


Figura 18: variazione del valore standardizzato dei prelievi in Italia

Variazione percentuale 2015/2014

**+10,56%**

Nel corso del 2015 i Prelievi sono cresciuti del 10%, aumento in larga parte imputabile alla dinamica del *Lazio*.

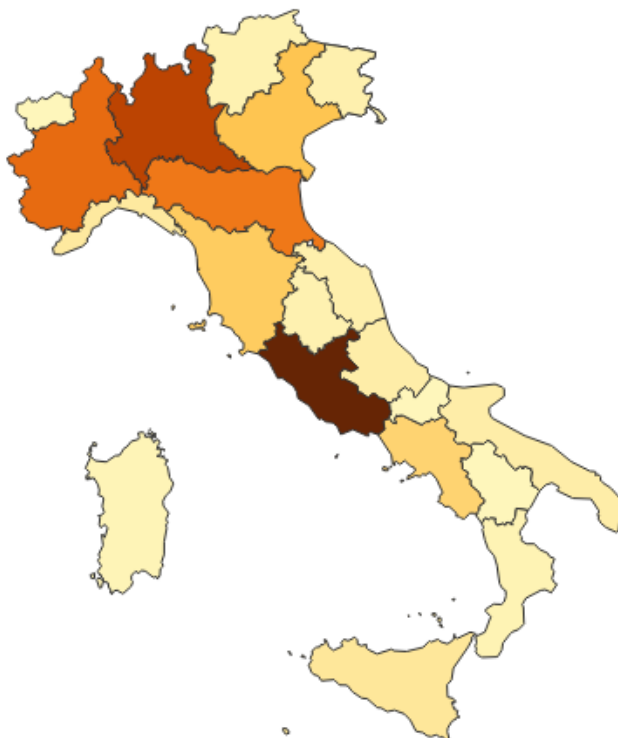


Figura 19: Mappa delle frodi su prelievi in Italia (il colore esprime l'intensità del fenomeno)

## Prelievi su ATM all'Estero

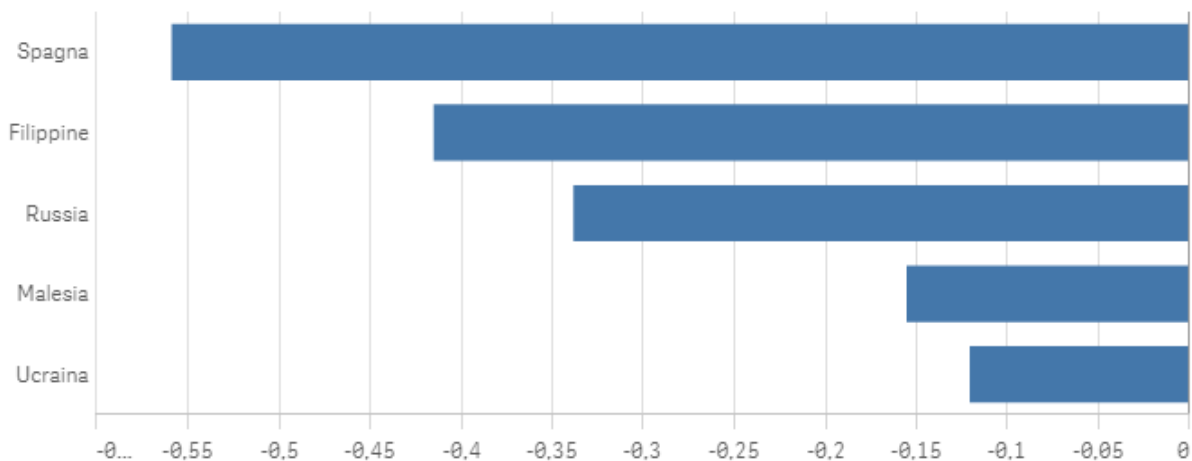


Figura 20: i 15 paesi con la maggiore decrescita delle frodi su Prelievi

Variazione percentuale 2015/2014

Valore: **-31,96%**

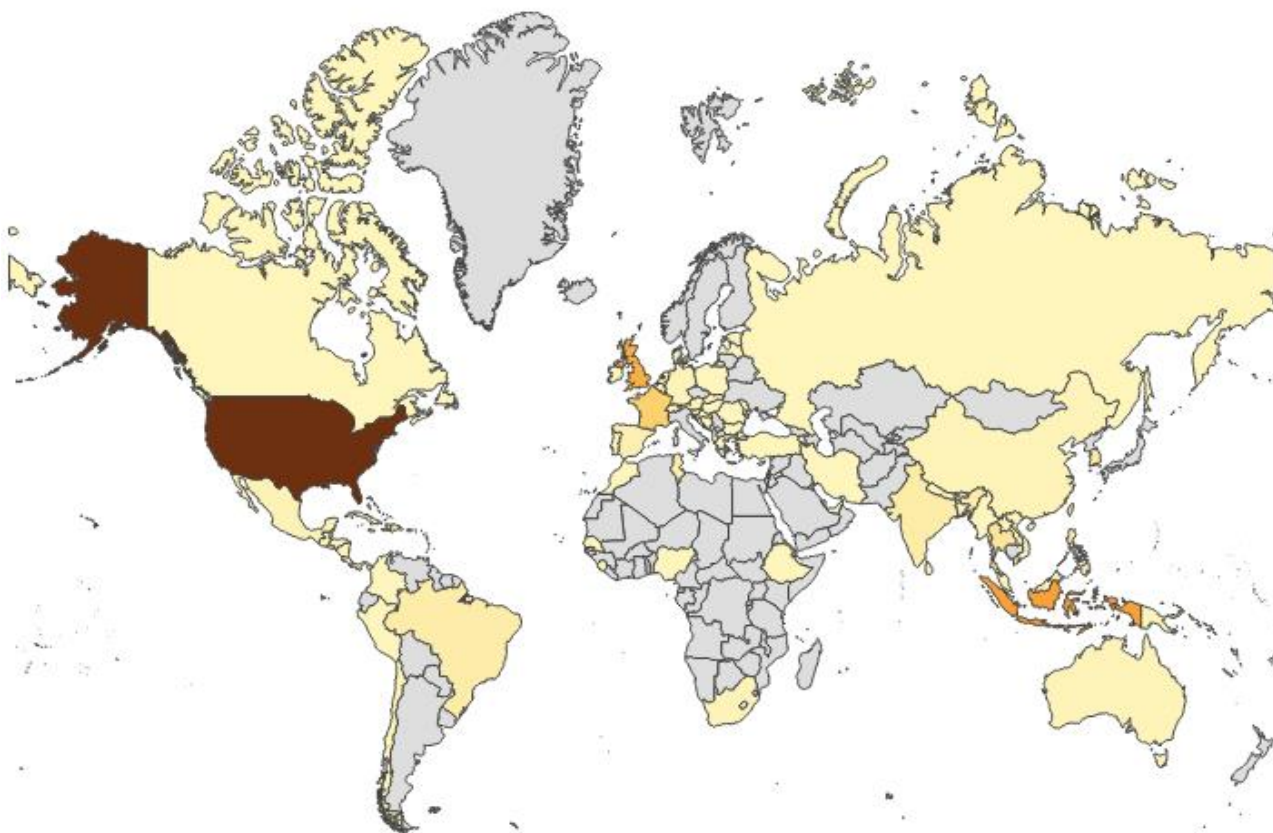


Figura 21: Mappa delle frodi su Prelievi nel resto del mondo (il colore esprime l'intensità del fenomeno)

Valori medi

**Valore medio:** rapporto tra il valore delle frodi e la loro numerosità

Valori medi

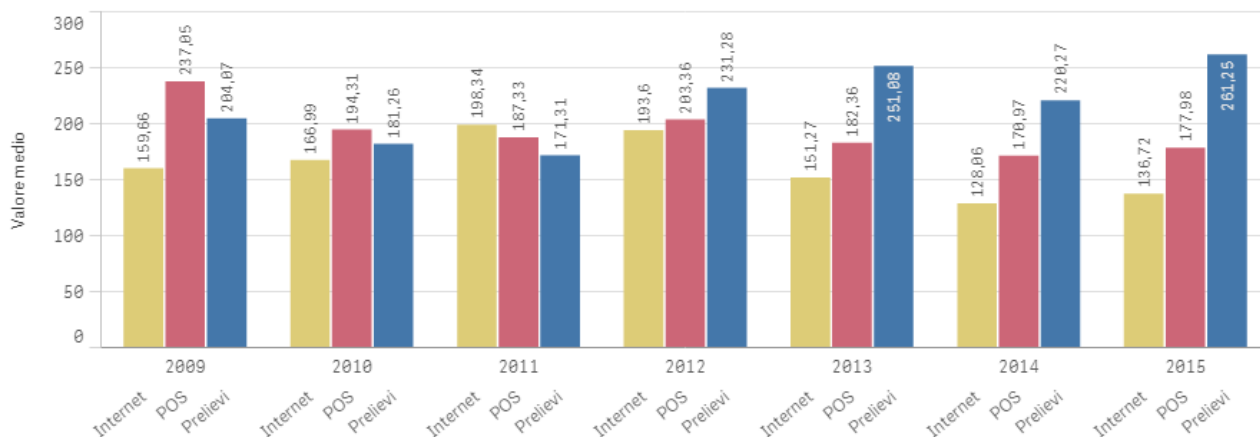


Figura 22: valori medi delle transazioni per canale

Variatione del valore medio delle transazioni 2015 – 2014 in euro

Internet: **+6,76%** POS: **+4,1%** Prelevi: **+18,6%**

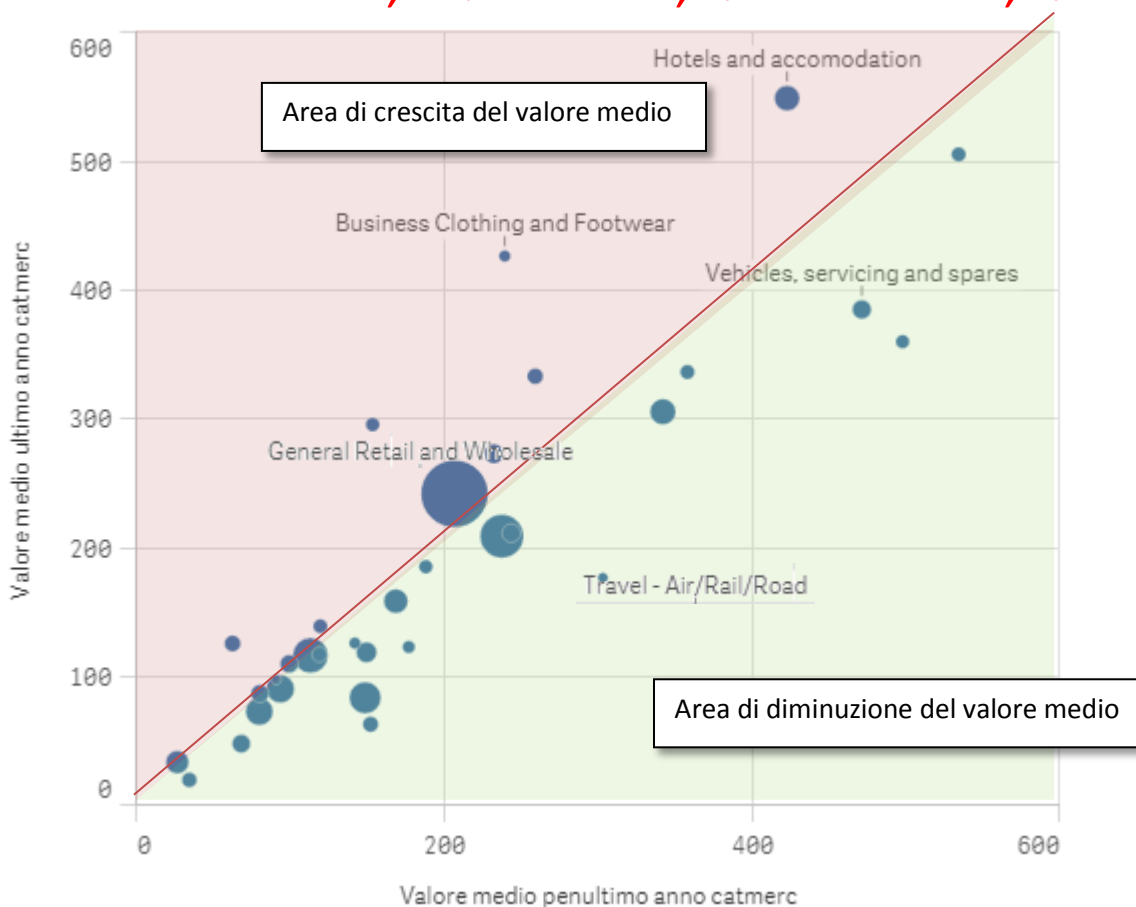


Figura 23: Valori medi per categoria merceologica



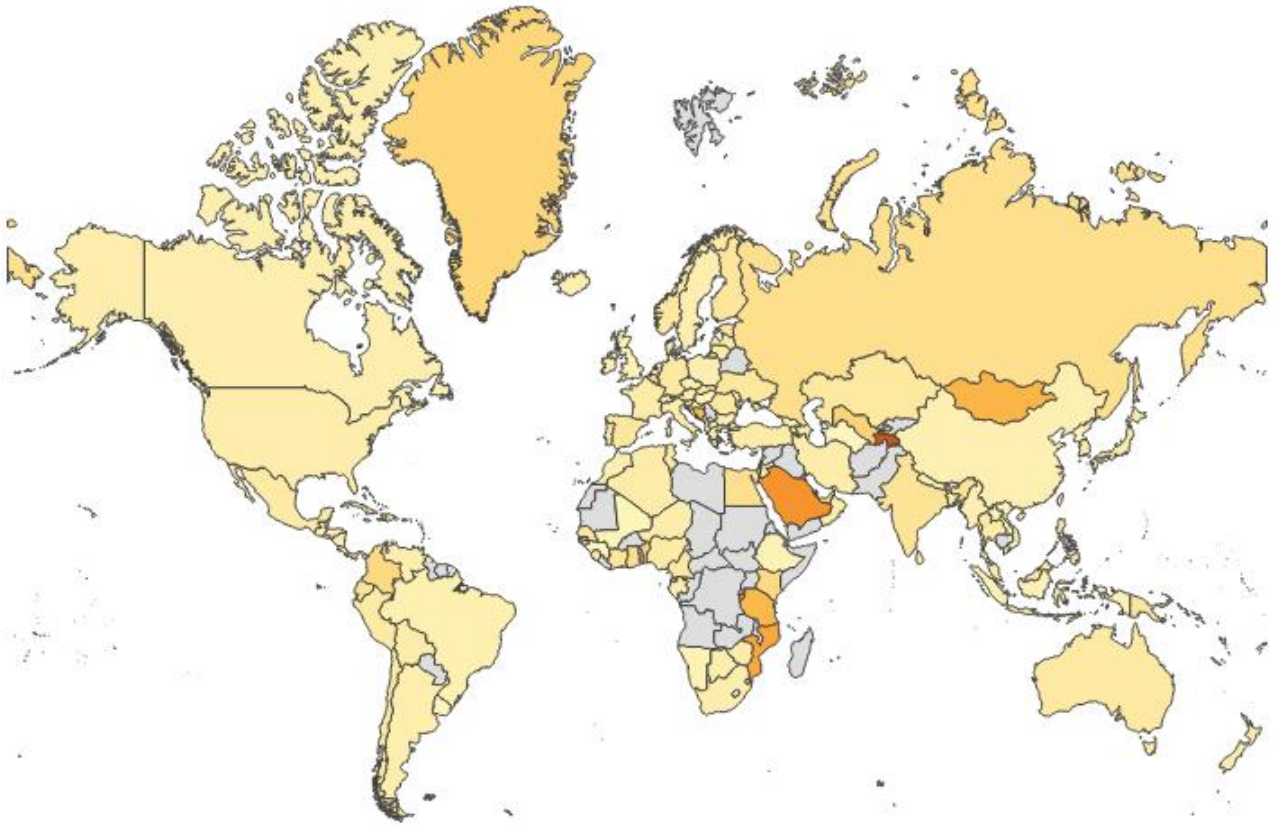


Figura 24: Valori medi per nazione (il colore esprime l'intensità del fenomeno)

I paesi con valori medi di transazioni frodate più elevati appartengono tutti ad Asia e Africa.

## Confronti internazionali

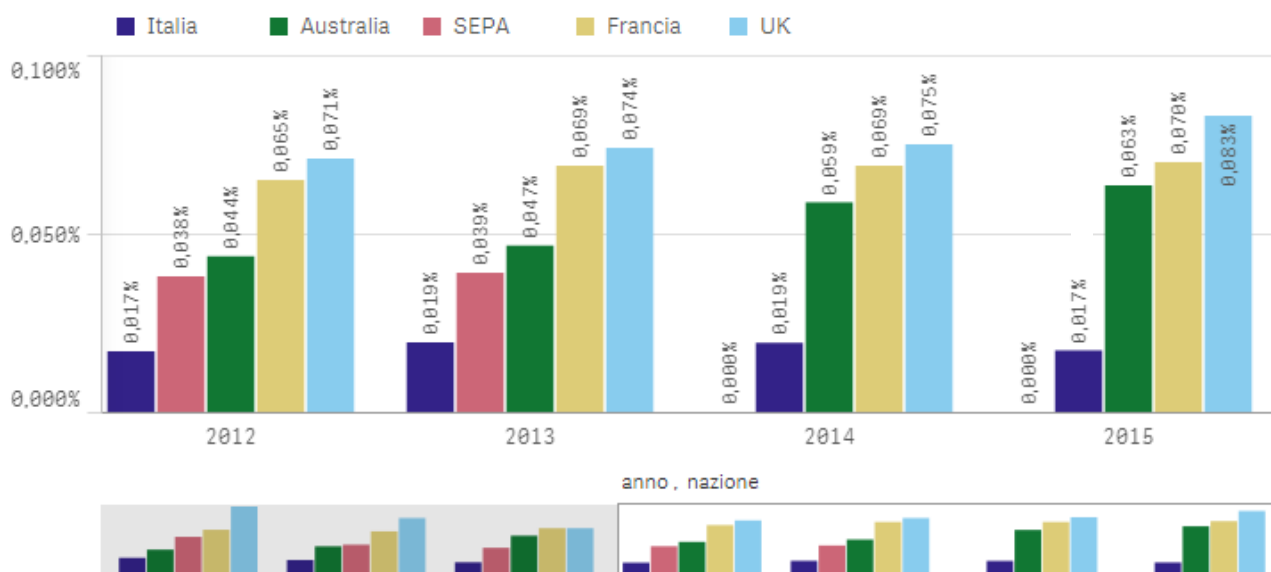


Figura 25: Confronto dell'incidenza in valore per i principali paesi

Nel 2015 si assiste ad un considerevole aumento dell'incidenza in UK e Australia, la Francia rimane stabile e l'Italia mostra una lieve diminuzione.

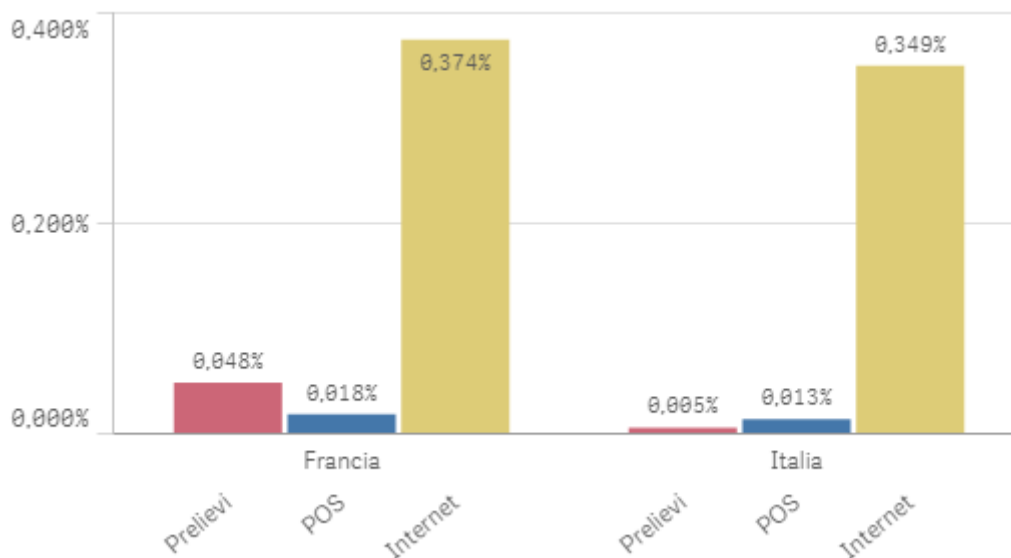


Figura 26: Confronto dell'incidenza in valore per canale Italia - Francia<sup>6</sup>

<sup>6</sup> I dati pubblicati dai vari paesi consentono il confronto dell'incidenza in valore per canale con la sola Francia.

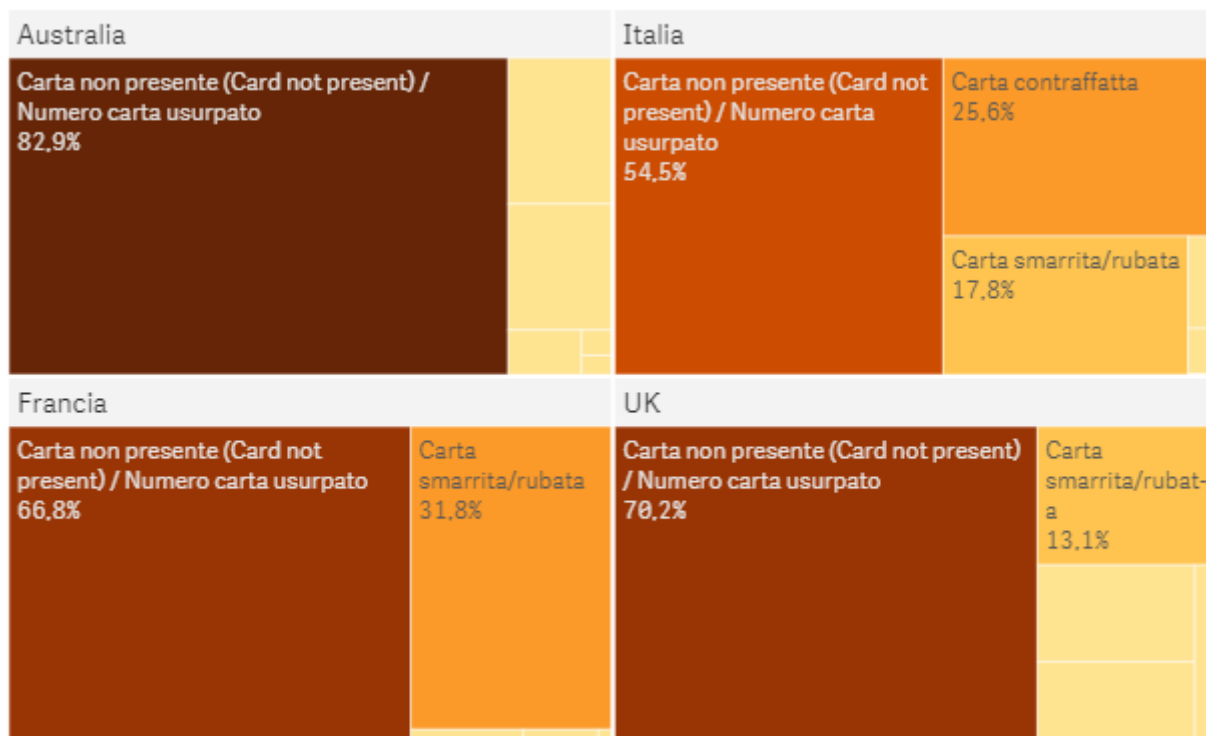


Figura 27: Tipologia di disconoscimento per nazione, anno 2015 composizione percentuale

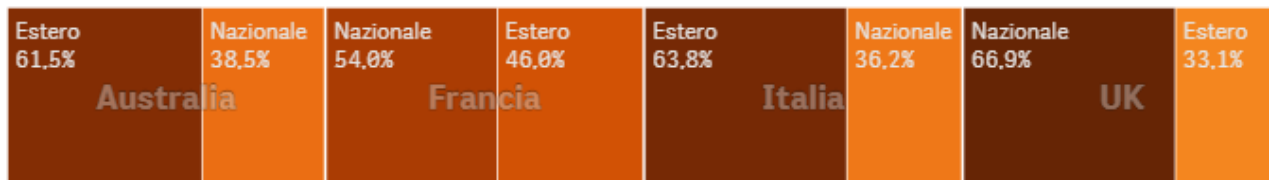


Figura 28: Nelle diverse nazioni composizione del frodato in valore in base al luogo in cui le carte (emesse nel paese di provenienza) vengono spese

## Manomissioni ATM

*Incidenza: rapporto fra il numero di manomissioni ATM ed il numero di ATM attivi.*

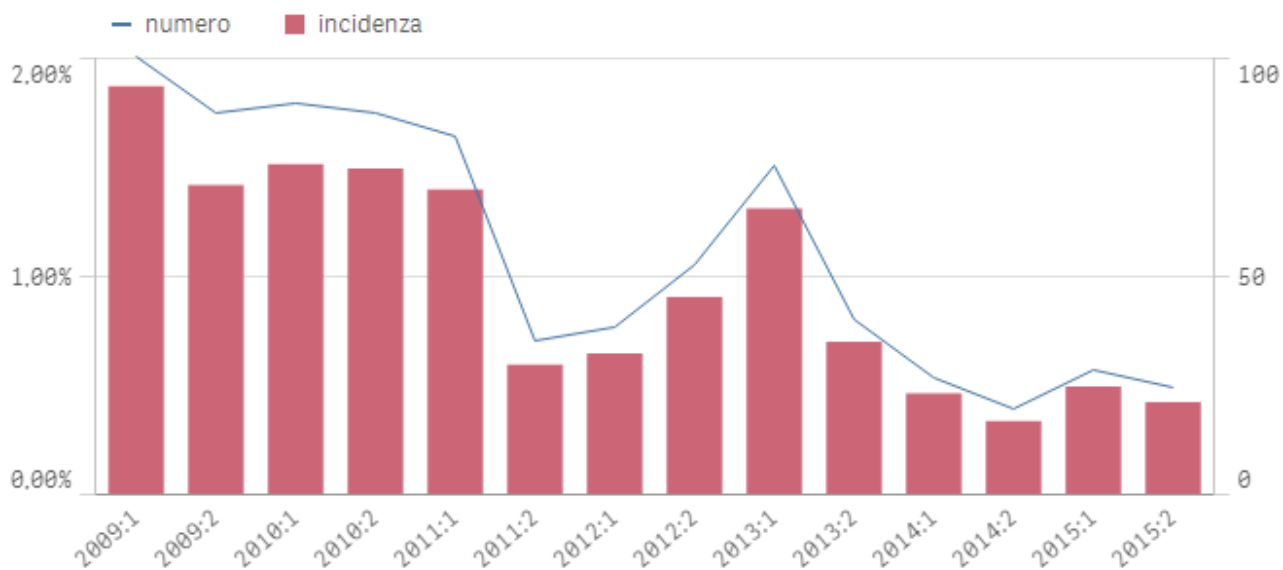


Figura 29: Numero di attacchi (linea) e incidenza (istogramma)

Incidenza 2015: **0,46%** variazione percentuale 2015/2014 **+15%**

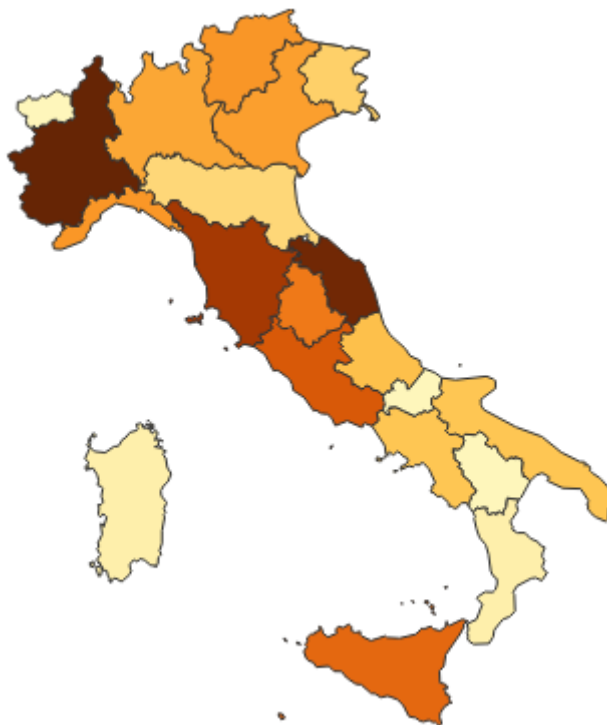


Figura 30: mappa dell'incidenza degli attacchi ad ATM regionale 2015 (il colore esprime l'intensità del fenomeno)



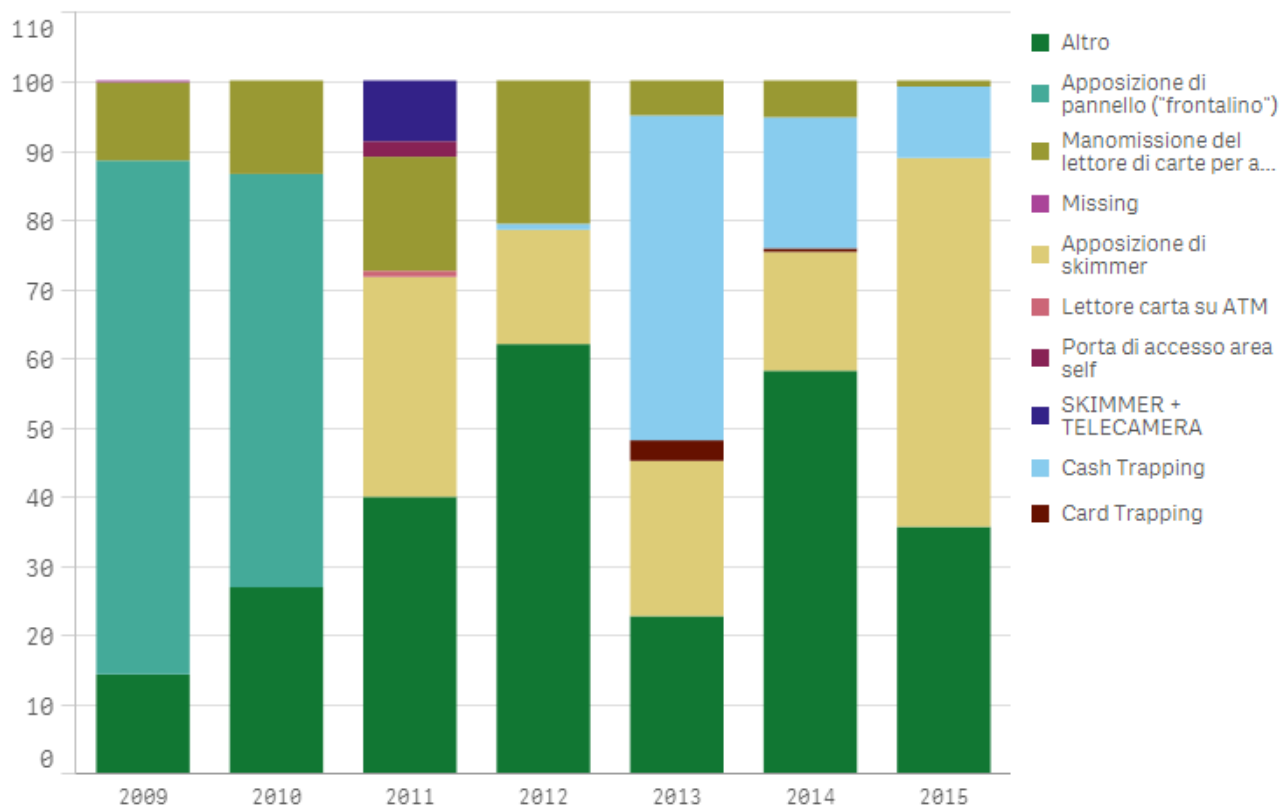


Figura 31: Tipologie di manomissione, composizione percentuale

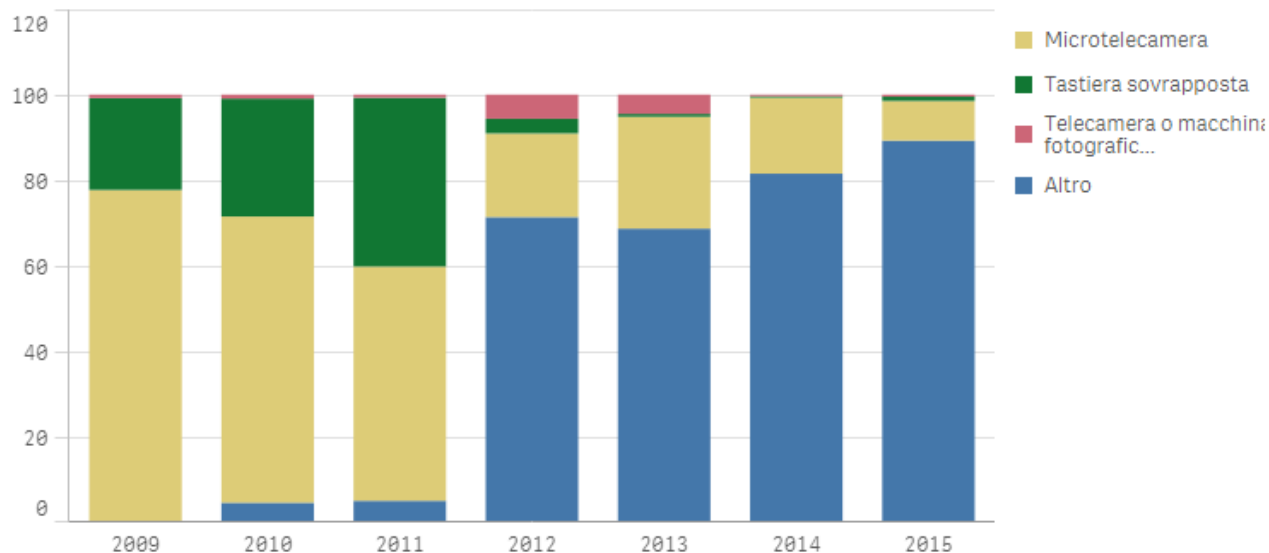


Figura 32: Tipologia di cattura del PIN

## Revoche convenzioni POS

*Incidenza: rapporto fra il numero revoche convenzioni su totale convenzioni attive*

*Numero standardizzato: Numero delle transazioni non riconosciute su carte emesse in Italia dell'anno di riferimento diviso per il numero del 2009. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.*

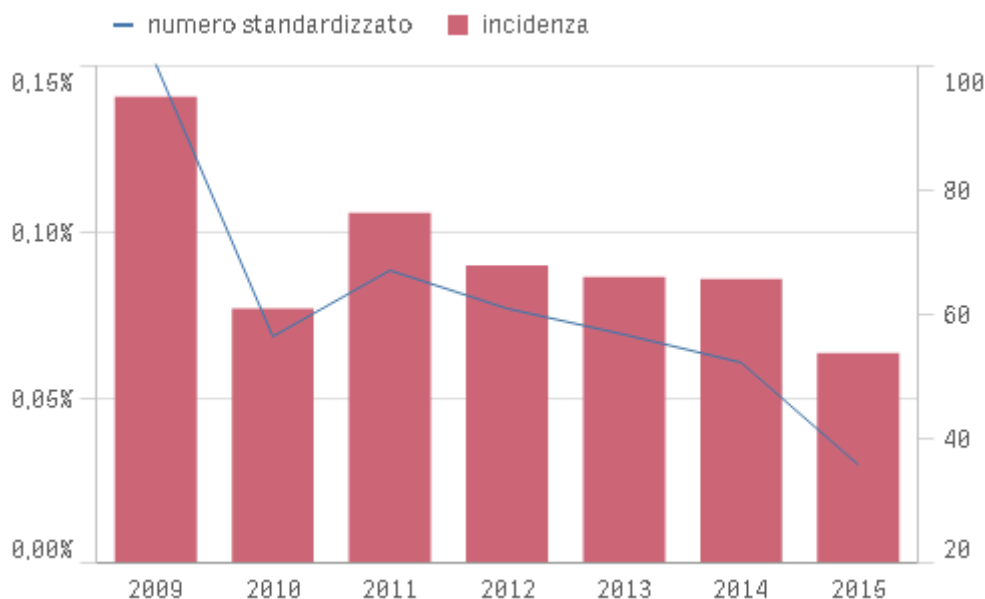


Figura 33: Numero revoche convenzioni e incidenza delle revoche su totale convenzioni attive

Incidenza 2015: **0,06** variazione percentuale 2015/2014 **-26%**



Figura 34: distribuzione regionale revocche convenzioni (il colore esprime l'intensità del fenomeno)

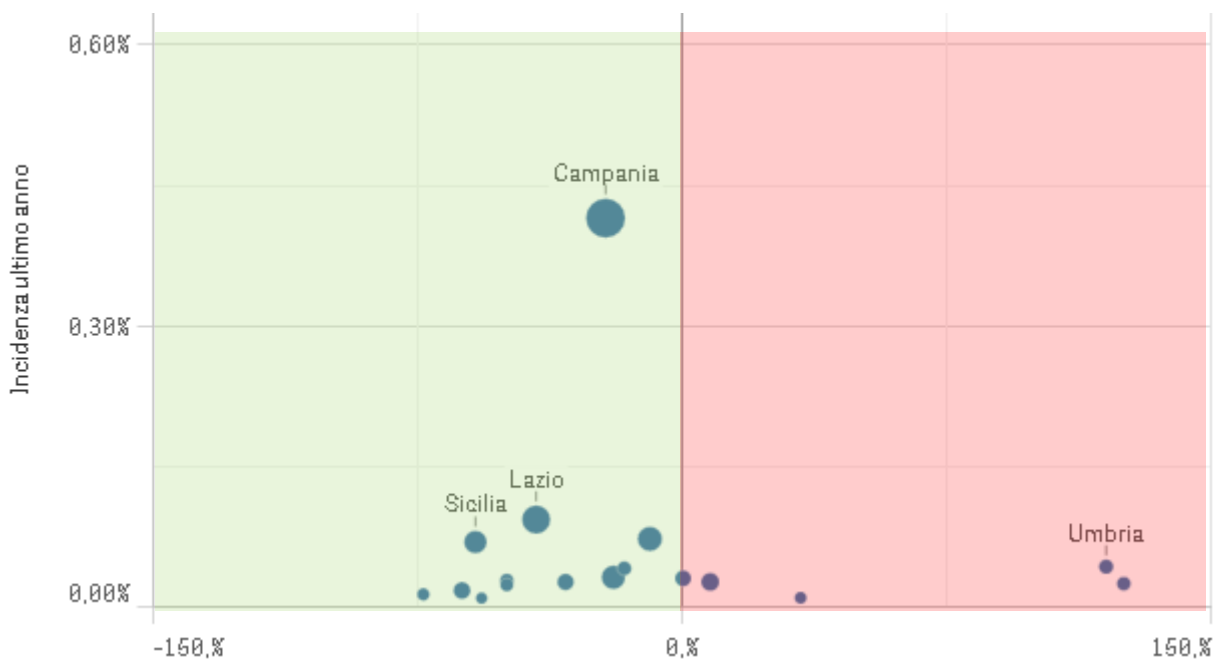


Figura 35: Variazione percentuale 2015/2014 (asse x), incidenza (asse y) e dimensione del fenomeno (dimensione bolla)

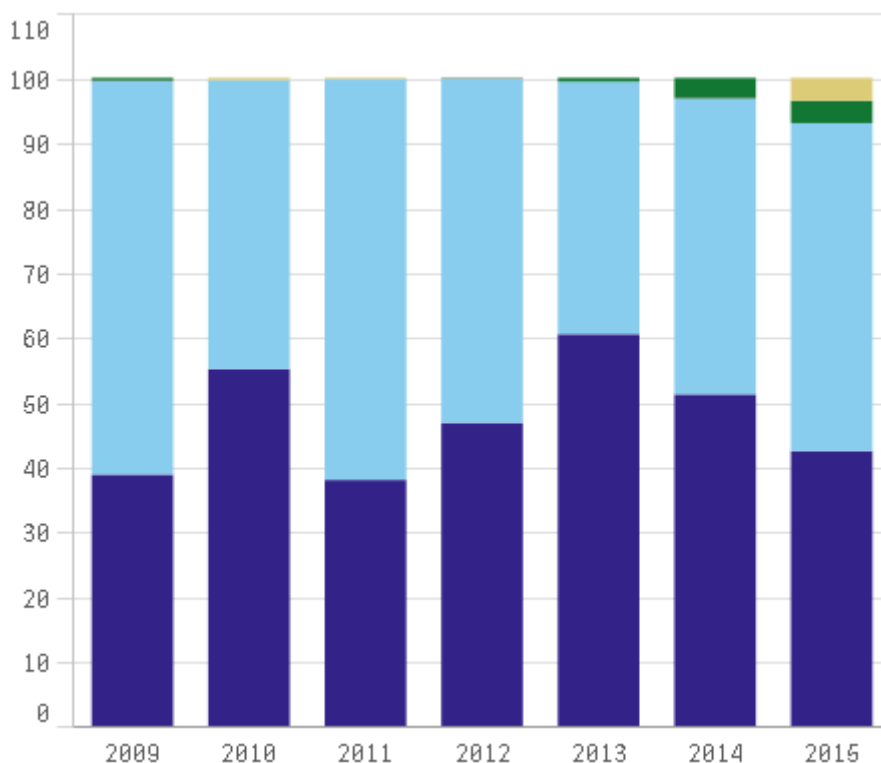


Figura 36: composizione percentuale delle causali di disconoscimento

- *Coinvolgimento dell'esercente in attività che la società segnalante ha ritenuto essere sospette, in base a verifiche o controlli o riscontri da essa stessa effettuati*
- *Motivi di sicurezza generici*
- *Ricezione di comunicazione, proveniente da altre società che emettono o gestiscono carte di pagamento, concernente l'inosservanza colposa o dolosa dell'esercente alle norme che regolano l'accettazione in pagamento delle carte*
- *Qualificazione del punto vendita come "sospetto punto di compromissione", in base a verifiche o controlli o riscontri effettuati dalla società segnalante*
- *Ricezione di comunicazione, proveniente dalle società che gestiscono i circuiti di pagamento, concernente l'inosservanza colposa o dolosa dell'esercente alle norme che regolano l'accettazione in pagamento delle carte*

## Approfondimento monotematico

### Frodi relative alle carte di pagamento ed evoluzione dell'ecosistema criminale

Come già illustrato lo scorso anno, molti forum in Internet 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<sup>7</sup> è impresa ardua per le forze dell'ordine e richiede uno sforzo tecnologico ed operativo significativo.

Nel precedente Rapporto sono stati analizzati 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.

Secondo uno studio pubblicato da McAfee, intitolato "The Hidden Data Economy", i dati finanziari continuano ad essere merce preziosa nell'ecosistema criminale. Grazie alle numerose violazioni di dati che si sono verificate lo scorso anno, molti venditori nei principali black market sono riusciti ad offrire merce utilizzabile e con elevato riciclo dei prodotti proposti.

All'offerta classica dei dati presenti sulla carta si abbina sempre più spesso la disponibilità di "Fullinfo"<sup>8</sup>, ovvero di pacchetti comprensivi di informazioni addizionali 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). A prima vista è possibile notare come i prezzi dei dati relativi alle carte di pagamento negli USA siano decisamente inferiori rispetto a quelli di altri paesi, proprio per la grande disponibilità di questa tipologia di informazioni. Per completezza riportiamo la definizione del termine "Random", che è usato nel rapporto per indicare un numero di carta casualmente scelto da uno degli archivi compromessi reperibile nel black market.

<sup>7</sup> Sono luoghi in rete (e.g. Forum, piattaforme di e-commerce) gestiti da gruppi criminali per la commercializzazione di prodotti e servizi illegali, quali armi, droga e servizi di hacking.

<sup>8</sup> Il termine "Fullz" è utilizzato nell'ecosistema criminale per indicare l'insieme completo delle informazioni relative ad un particolare individuo che comprende i suoi dati personali, dati relativi alle carte di pagamento, il numero di previdenza sociale e una collezione di informazioni accessorie, tra cui eventuali bollette delle principali utenze dell'intestatario della carta.



Dump Track With High Balance	Price
Track 1&2: PinATM United States	\$110
Track 1&2: PinATM United Kingdom	\$160
Track 1&2: PinATM Canada	\$180
Track 1&2: PinATM Australia	\$170
Track 1&2: PinATM European Union	\$190

Figura 37 - The Hidden Data Economy Report (McAfee)

Dump track prices per card.

Source: McAfee Labs.

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.

Figura 38 - The Hidden Data Economy Report (McAfee)

Come sempre gli acquirenti hanno molteplici opzioni in fase di acquisto, sempre più spesso è consentito di scegliere l'origine geografica della carta e talvolta l'importo ad esso associato. Questi due fattori sono essenziali per l'attività criminale ed ovviamente hanno un impatto significativo sul prezzo del bene offerto nel black market.

Tra i prodotti più contrattati continuano ad esserci i cosiddetti 'Dump'<sup>9</sup>, ovvero informazioni copiate elettronicamente dalla banda magnetica della carta mediante dispositivi skimmer. Le informazioni sono contenute in due tracce ed includono almeno nome e numero di conto del cliente, data di scadenza, il codice CVV<sup>10</sup>. Questi dati sono utilizzati per la clonazione di carte e pertanto molto richiesti dalle organizzazioni criminali in diversi paesi. Ancora una volta è possibile notare il prezzo nettamente inferiore di dati rubati da carte negli Stati Uniti.

Dando un'occhiata ai principali fenomeni accaduti lo scorso anno non possiamo non menzionare l'uscita di scena di alcuni importanti player nell'ecosistema criminale.

<sup>9</sup> Il termine Dump è utilizzato per indicare i dati grezzi immagazzinati nella banda magnetica di una carta di credito, informazioni di solito catturate mediante attività di "skimming" oppure attraverso l'uso di malware che infettano i sistemi di pagamento PoS.

<sup>10</sup> Il termine CVV è utilizzato dagli operatori dell'underground criminale specializzati nella commercializzazione delle carte di pagamento per indicare i record relativi alla carta e che possono includere il nome dell'intestatario, l'indirizzo dell'intestatario, la data di scadenza.

Ricorderete che uno dei mercati più interessanti ospitato nella rete TOR<sup>11</sup> era Agorà, una piattaforma conosciuta principalmente per la vendita di sostanze stupefacenti che tuttavia ospitava alcuni venditori di prodotti relativi alle carte di pagamento.

In Settembre, i proprietari di Agorà hanno deciso di chiudere la piattaforma temendo di essere rintracciati dalle autorità. In luglio, infatti, un gruppo di ricercatori del Massachusetts Institute of Technology (MIT) annunciò di aver elaborato una tecnica che consentiva loro di localizzare i server nascosti nella rete TOR.

Gli esperti sfruttarono la presenza di falle nell'architettura della rete TOR per mettere a punto la tecnica, bastò la notizia per convincere gli amministratori di Agorà a chiudere la piattaforma. Chiaramente la totalità degli operatori di Agorà si è riversata nei mesi successivi in altri black market.

Con l'uscita di scena di Agorà, altri black market hanno investito per ottimizzare la loro offerta e migliorare i propri servizi: questo è il caso di AlphaBay, un 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.

CC Autoshop

Welcome to the CC autoshop! This section allows you to search for credit cards or fulls in the most convenient way possible. Be careful when using checkers, as they can have side effects on the cards. When you purchase a card, you have 1 hour to check it if required.

Buy Cards My Purchased Cards

DOB: (Any) SSN: (Any) Birth Year: 0000 to 9999 Price: 0.01 to 999.99 Seller: (Any) Bank: (Any) Type: (Any) Credit: (Any) Level: (Any) Search Clear All

BIN	Exp.	Seller	Name	City	State	Zip	Country	DOB	SSN	Price
<input type="checkbox"/>	551257	2 / 17	RedSon	Tisha ...	Brooks,	21	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	442714	8 / 17	RedSon	David ...	Youngstown	15	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	418846	10 / 17	RedSon	Kathry...	Port Clinton	52	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	473702	9 / 15	RedSon	Raven ...	Milford	50	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	473304	2 / 18	RedSon	Edgard...	Westfield	85	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	434256	4 / 17	RedSon	Dianna...	Livermore	51	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	442742	5 / 17	RedSon	Gwangs...	Torrance	04	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	460580	10 / 15	RedSon	Jessic...	Toledo	06	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	411770	3 / 19	RedSon	Lori M...	New Bedford	40	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	540168	8 / 17	RedSon	Mary N...	Soquel	73	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	475427	7 / 15	RedSon	Vipul ...	east brunswick	16	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	481582	2 / 19	RedSon	Reem K...	North Hollywood	02	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	481583	3 / 18	RedSon	prisci...	compton	20	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	481582	6 / 18	RedSon	yumna ...	santa clara	51	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	414334	9 / 17	RedSon	Nancy ...	Easton	42	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	426684	5 / 15	RedSon	xin ma...	montvale	45	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	519955	12 / 17	RedSon	Lyudmi...	Wayne	70	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	426684	6 / 15	RedSon	Keith ...	Lafayette	49	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	544846	10 / 17	RedSon	Daniel...	Swansea	77	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	475824	8 / 16	RedSon	Angela...	Salt Lake City	16	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	425627	10 / 17	RedSon	Cheryl...	Easton	45	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	434256	2 / 18	RedSon	mashar...	ceres	07	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	433218	1 / 17	RedSon	neil a...	highwood	40	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	438857	9 / 16	RedSon	Michae...	Oakley	51	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	545238	12 / 15	RedSon	Tuan T...	Lake Orion	50	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	448027	8 / 15	RedSon	patric...	fond du lac	37	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	434256	11 / 17	RedSon	Peter ...	santa cruz	52	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	477840	7 / 15	RedSon	umakan...	fremont	36	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	414709	2 / 17	RedSon	Anup S...	Attleboro	03	United States	N/A	N/A	\$8.50
<input type="checkbox"/>	467621	10 / 16	RedSon	Ming X...	Newark	50	United States	N/A	N/A	\$8.50

Figura 39 - Servizio AlphaBay per la vendita di dati relativi alle carte di pagamento

Forum e black market specializzati nella vendita di dati relativi alle carte di pagamento sono anche presenti nel surface web, e quindi accessibili a tutti. Proprio lo scorso anno è apparso in rete una interessante piattaforma web chiamata Central Shop specializzata nella vendita di dati rubati relativi a carte di credito.

Il sito web è davvero ben fatto, l'interfaccia web è molto curata così come le funzionalità di ricerca dei prodotti all'interno del suo portafoglio.

La prima cosa che si nota quando si accede al sito è una mappa interattiva che permette ai visitatori di scegliere i paesi da cui provengono i dati rubati.

<sup>11</sup> (acronimo di The Onion Router) – Tor è un sistema di comunicazione anonima per Internet basato sulla seconda generazione del protocollo instradamento, noto come “onion routing”.

La possibilità di scegliere l'origine dei dati delle carte di pagamento è molto importante per i criminali informatici che possono utilizzare tali informazioni per ottimizzare le operazioni di cash out, ovvero di conversioni dei dati in contanti e di aggirare alcuni dei controlli attuati dagli istituti di credito per identificare attività fraudolente.

Chiudiamo con una doverosa menzione agli sforzi compiuti dalle forze dell'ordine nel contrasto di questa pratica illegale.

Nel Marzo del 2015 Thomas Jiřikovský, sospettato di essere il proprietario del black market Sheep Marketplace, è stato arrestato mentre cercava di acquistare una casa di lusso con i proventi delle sue attività.

Nel Luglio dello stesso anno un'operazione condotta da forze dell'ordine di più paesi ha consentito l'arresto di decine di persone attive sul popolare forum criminale Darkode.



Figura 40 – Operazione Shrouded Horizon

L'operazione ha consentito di individuare molti criminali che a vario titolo erano coinvolti anche in attività fraudolente relative alle carte di pagamento, come personalizzazione e sviluppo di malware per il furto di dati da ATM e sistemi di pagamento utilizzati nel settore Retail.

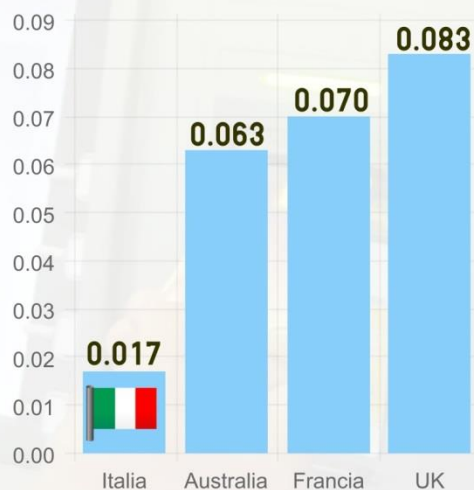


## Infografiche

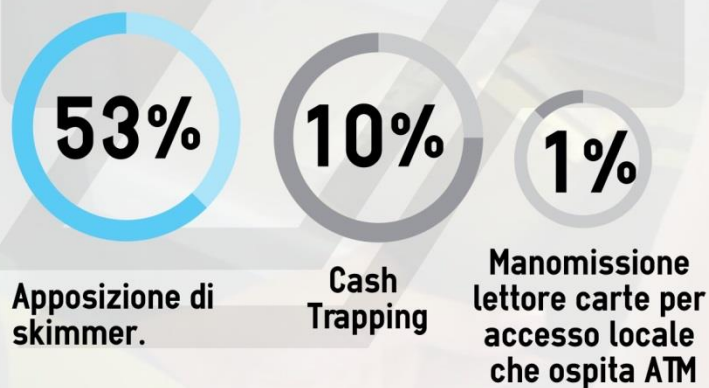
### Valore medio transazioni non riconosciute (€) per Area Geografica



### Tasso di Frode 2015



### Manomissioni ATM per Tipologia (2015)



### Tecniche di cattura PIN



**Nel 55% dei casi la tecnica di cattura del PIN utente è sconosciuta**

### Tor Black markets e Frodi Carte

- Alpha Bay Market
- Dream Market
- Italian Darknet Community
- Heaven
- Abraxas

**\$150-\$800** noleggio settimanale di un Exploit Kit per diffondere un Trojan bancario

**\$ 500-\$2500** costo base di un Trojan bancario

**\$150-\$1250** noleggio semestrale di un Malware bancario come SpyEye

### Listino prezzi - Frodi Carte

**\$3-\$25** CVVs (Dati carte pagamento rubati online)

**\$20-\$60** Dump Carta di Credito (Cattura completa contenuto carta di credito)

**\$25-\$125** Fullz (Dati Carta Credito + Documenti Titolare)

**I Black Market e l'impresa criminale**  
 Chiunque abbia un computer può entrare in un black market e reperire prodotti e servizi per le frodi relative alle carte di pagamento.



## Nota metodologica

### Le Transazioni non riconosciute

Le statistiche sul fenomeno delle transazioni non riconosciute sono essenzialmente di due tipi: per numero e per valore in euro. Le statistiche non vengono fornite in termini assoluti ma in termini relativi. Possono essere espresse in rapporto a quelle genuine e in tal caso si parlerà di incidenze percentuali e si offrirà una misura del rischio di disconoscimento di una generica transazione, oppure, in rapporto a un loro valore osservato nel passato, si offrirà una misura della dinamica temporale del livello dei mancati riconoscimenti.

Le statistiche (relative o meno) sul numero e/o sul valore delle transazioni non riconosciute si riferiscono sempre ad un insieme specifico i cui lineamenti sono individuati e mantenuti invariati nel tempo al fine di omogeneizzare i confronti delle serie storiche.

Le transazioni di riferimento sono esclusivamente quelle effettuate con carte di pagamento emesse da banche e/o da altri intermediari finanziari, autorizzati e vigilati dalla Banca di Italia<sup>12</sup>, attraverso la sottoscrizione di un contratto con clienti titolari di qualsiasi nazionalità e avvenute in ogni Paese tramite l'uso di uno dei seguenti canali: POS, ATM e Internet.

Rientrano nell'insieme di osservazione le carte di credito, di debito e le prepagate.

Nell'insieme delle transazioni di riferimento rientrano anche quelle effettuate senza utilizzo diretto della carta di pagamento (*card-not-present*), sia su carte emesse da banche che da altri intermediari finanziari. Inoltre, qualificate come operazioni di prelievo, rientrano anche gli anticipi di contante con carte di credito.

All'interno di tali transazioni di riferimento sono considerate come non riconosciute solo quelle ritenute non riconosciute in modo definitivo, escludendo dunque i disconoscimenti annullati in un momento successivo a quello iniziale.

Il valore economico di ogni transazione è espresso in euro; per quelle effettuate in altra valuta si opera una conversione sulla base dei tassi di cambio validi per il giorno in cui avviene la transazione e diffusi dalla Banca d'Italia (ex Ufficio Italiano Cambi).

La data in cui avviene la transazione è anche il riferimento temporale della transazione non riconosciuta e non si considera, quindi, come riferimento temporale la data di disconoscimento o di altro evento diverso. Le transazioni non riconosciute sono attribuite ad un determinato intervallo temporale (mese, semestre o anno) in base alla data giornaliera di riferimento, ovvero di transazione.

Oltre alla data ed al valore, alle transazioni non riconosciute vengono attribuite altre caratteristiche: causale di disconoscimento, tipo e luogo di transazione.

La causale di disconoscimento viene attribuita dall'ente segnalante (banca o intermediario finanziario emittente la carte e aderente al SIPAF) e può essere di sette tipi: *Carta contraffatta*, *Carta non ricevuta*, *Carta rubata*, *Carta smarrita*, *Carta rubata con falsa identità*, *Utilizzo fraudolento del codice carta emessa* e

<sup>12</sup> A questi si aggiungono alcuni Enti Segnalanti, che pur non avendone più l'obbligo, continuano ad alimentare l'applicativo SIPAF.

*Utilizzo fraudolento della carta in internet.* Le modalità di attribuzione seguono il manuale operativo predisposto per l'alimentazione del SIPAF. Alle transazioni prive di causale non ne viene riattribuita alcuna e in fase di elaborazione statistica tali casi costituiscono *missing value*.

Il tipo di transazione, o canale, viene attribuito dall' UCAMP sulla base delle informazioni fornite dall'ente segnalante e può essere di tre tipi: *POS*, *Internet* e *Prelievi*<sup>13</sup>. La classificazione avviene attraverso un processo di selezione sequenziale. Le transazioni di tipo *Internet* sono quelle che l'ente segnalante ritiene avvenute su POS e che presentano come attributo località un indirizzo internet e/o come causale di disconoscimento *Utilizzo fraudolento della carta su Internet*. Seguono le transazioni su POS ritenute, da parte dell'ente segnalante, effettuate su POS ma non attribuite alle categorie merceologiche *Cash* o *Automated Cash Disburse*. Queste operazioni POS di tipo *Cash* vengono assegnate al tipo *Prelievi*, insieme a quelle transazioni ritenute, da parte dell'ente segnalante, effettuate su ATM<sup>14</sup>. Le transazioni ritenute effettuate su *POS* che non presentano valori per la località, per la causale di disconoscimento e per la categoria merceologica mantengono l'attributo di transazione su POS. In definitiva, ad ogni transazione non riconosciuta è comunque assegnato un canale.

Le transazioni sono articolate anche in relazione alla funzionalità debito/credito della carta utilizzata. Appartengono alla funzionalità credito le operazioni effettuate sui circuiti American Express, VISA, Mastercard, JCB e Diners; mentre le operazioni effettuate sui circuiti VPAY, VISA Electron, Postamat, Maestro e Bancomat/Pagobancomat sono classificate come funzionalità debito.

La descrizione del luogo di transazione è fornita da due variabili: una in cui si distingue solamente Italia da Estero e l'altra in cui si descrive la nazione per le transazioni estere o la località per quelle italiane. L'articolazione fra Italia ed Estero viene effettuata per ogni tipo di transazione in base a quanto attribuito dall'ente segnalante in termini di codici ISO delle varie nazioni. Le mancate valorizzazioni dello Stato in cui si è effettuata la transazione generano dei *missing value* che non sono riattribuiti, salvo rimanere in capo alla modalità Estero.

Per le transazioni italiane si attribuisce la località, in particolare il comune, solamente per la tipologia prelievi. L'attribuzione è effettuata dall'UCAMP mediante l'uso dei codici ABI e CAB relativi all'ATM su cui è avvenuto il prelievo e sulle modalità di raccordo, fornite dalla Banca di Italia, fra tali codici ed i comuni italiani, validi per l'anno in cui è avvenuta la transazione. Dai comuni si risale, poi, alle classificazioni per Provincia e/o Regione secondo i criteri indicati dall'ISTAT validi, anch'essi, per l'anno in cui è avvenuta la transazione. Per le transazioni avvenute su POS ma classificate, come detto, nei prelievi l'assenza dei codici ABI e CAB non consente l'applicazione del metodo esposto. In tali casi si elabora l'informazione relativa alla località in cui è avvenuta la transazione mediante un avanzato processo di *data quality*.

Ultima caratteristica di rilievo delle transazioni non riconosciute è la categoria merceologica. Per essa si fa riferimento alla classificazione MCC (Merchant Category Code) che si basa su un codice di 4 cifre elaborato e utilizzato da MasterCard/VISA per classificare le differenti tipologie di business. Accanto a tale classificazione che prevede circa 600 differenti tipologie, vi è anche una sua aggregazione che indica circa 30 tipologie di business.

<sup>13</sup> Attualmente non è possibile enucleare anche il canale *card non present*.

<sup>14</sup> Eventuali transazioni su POS che presentano località *Internet* e categoria merceologica *Cash* e affini vengono attribuite al tipo *Internet*.

## Manomissioni ATM

Il fenomeno degli ATM manomessi è osservato in termini di numero degli eventi in un determinato intervallo di tempo e di area geografica e, nel rapporto statistico, non è fornito in valore assoluto ma relativo. Esso è espresso in rapporto al numero degli ATM presenti nella stessa area geografica ed intervallo temporale. In tal caso si parlerà di tasso di manomissione specificando la natura dell'intervallo temporale di riferimento (mensile, semestrale, annuale). Il confronto fra tassi osservati in differenti aree geografiche e/o momenti temporali va effettuato sempre con lo stesso tipo di tasso (mensile, semestrale, annuale). Il tasso di manomissione semestrale, ad esempio, indica il numero di possibili attacchi che un singolo ATM può ricevere nell'arco di un semestre. Quando è pari all'1% significa che un singolo ATM riceve un attacco mediamente ogni 100 semestri; oppure significa che ogni 100 ATM, 1 riceve un attacco nell'arco di un semestre.

Il numero delle manomissioni può essere rapportato anche a quello osservato in un altro momento temporale (numero indice), in tal caso offre una misura della dinamica temporale del livello assoluto degli attacchi.

Le statistiche, relative o meno, al numero delle manomissioni si riferiscono sempre ad un insieme specifico i cui lineamenti sono individuati e mantenuti invariati nel tempo al fine di omogeneizzare i confronti delle serie storiche.

Le manomissioni di riferimento sono tutte quelle dichiarate come tali dall'ente segnalante (banca o intermediario finanziario aderente al SIPAF) e si riferiscono ad ATM collocati nel territorio italiano ed associati a banche e/o da altri intermediari finanziari autorizzati e vigilati dalla Banca di Italia.

La data di riferimento per la manomissione è la data di inizio dello stato di manomissione dell'ATM interessato ed è dichiarata dall'ente segnalante. Essa coincide o precede la data di scoperta della manomissione ed è una stima della data effettiva di manomissione (solitamente ignota).

Il luogo di riferimento per la manomissione è, naturalmente, quello in cui è collocato l'ATM ed è dichiarato dall'ente segnalante.

Oltre alla data ed al luogo, alle manomissioni sono attribuite altre caratteristiche quali: tipologia manomissione e modalità cattura PIN. Entrambe sono attribuite dall'ente segnalante in base ai criteri illustrati nel manuale operativo predisposto per l'alimentazione del SIPAF.

La tipologia manomissione può essere di cinque tipi: *Apposizione di skimmer*, *Manomissione del lettore di carte per accesso al locale interno ove è dislocato lo sportello stesso*, *Cash trapping*, *Card trapping*, *Altro*. La modalità cattura PIN può essere di quattro tipi: *Microtelecamera*, *Tastiera sovrapposta*, *Telecamera o macchina fotografica a distanza*, *Altro*. Alle manomissioni prive del tipo modalità cattura PIN non è riattribuito alcun tipo di modalità e, in fase di elaborazione statistica, tali casi costituiscono *missing value*. Spesso in tali modalità rientrano casi in cui è avvenuta una manomissione ma non una cattura del PIN, come nel caso del *Cash trapping*.

## Revoche convenzioni POS

Il fenomeno delle convenzioni revocate è osservato essenzialmente in termini di numero degli eventi in un determinato intervallo di tempo e di area geografica e, nel rapporto statistico, non è fornito in valore assoluto ma relativo. Esso può essere espresso in rapporto al numero complessivo delle convenzioni presenti nella stessa area geografica ed intervallo temporale. In tal caso si parlerà d'incidenza percentuale (%), specificando la natura dell'intervallo temporale di riferimento (mensile, semestrale, annuale). Il confronto fra incidenze osservate in differenti aree geografiche e/o momenti temporali deve essere effettuato sempre con lo stesso tipo di incidenza % (mensile, semestrale, annuale).

Il numero delle revoche può essere rapportato anche a quello osservato in un altro momento temporale (numero indice). In tal caso si offre una misura della dinamica temporale del livello assoluto delle revoche.

Le statistiche, relative o meno, al numero delle revoche si riferiscono sempre a un insieme specifico i cui lineamenti sono individuati e mantenuti invariati nel tempo al fine di omogeneizzare i confronti delle serie storiche.

Le revoche di riferimento sono tutte quelle dichiarate come tali dall'ente segnalante (banca o intermediario finanziario aderente al SIPAF) e si riferiscono a convenzioni stipulate fra l'*acquirer*, istituzione finanziaria autorizzata e vigilata da Banca Italia, e l'esercente, dove il titolare di una carta di pagamento effettua la spesa. Gli esercenti di riferimento sono tutti quelli che operano nel commercio iscritti nel registro delle imprese delle Camere di Commercio. Ad un esercente convenzionato solitamente corrisponde un solo punto vendita e un solo terminale POS, ma possono anche corrispondere più punti vendita sul territorio e/o più terminali POS.

Ad un esercente cui è stata revocata una convenzione può esserne assegnata, successivamente, una nuova. Quindi, ad un esercente possono corrispondere, nel tempo, più revoche di convenzioni.

La data di riferimento per la revoca e la località sono quelle dichiarate dall'ente segnalante. La località è quella indicata per l'esercente convenzionato.

Ad una revoca è attribuita, dall'ente segnalante, una causale che può essere di due tipi: *Coinvolgimento dell'esercente in attività sospetta* e *Motivi generici di sicurezza*.

Alle revoche prive di causali non è riattribuito alcun tipo di causale e in fase di elaborazione statistica tali casi costituiscono *missing value*.

## Confronti Internazionali

I dati relativi ai confronti internazionali sono disponibili presso i seguenti siti:

<http://www.apca.com.au>

<http://www.banque-france.fr>

<http://www.cardwatch.org.uk>

<http://www.ecb.int>

<http://www.observatoire-cartes.fr>

<http://sdw.ecb.europa.eu>

<http://www.theukcardsassociation.org.uk>

Il dato sul controvalore delle transazioni non riconosciute relativo a UK comprende anche le transazioni avvenute per telefono e per posta, che vengono aggregate nel canale Internet.

Il dato sul controvalore delle transazioni non riconosciute, disaggregato per tipologia di disconoscimento, fa riferimento, per la Francia, alle sole transazioni avvenute in Francia.

Per quanto riguarda l'Australia, i dati sul controvalore delle transazioni non riconosciute sono pienamente coerenti con le classificazioni adottate per l'Italia.

# Gruppo di lavoro

## **COORDINATORE DEL RAPPORTO**

*Antonio Adinolfi*

## **GRUPPO OPERATIVO**

### **Sogei S.p.A.:**

*Francesca di Brisco*

*Stefano Grossi*

*Alessandra de Castro*

*Massimo Palombi*

### **Ufficio VI:**

*Augusto Santori*

### **G. di. F. - UCAMP**

## **GRUPPO CONSULTIVO**

### **Banca d'Italia**

*Servizio Supervisione sui Mercati e sul Sistema dei Pagamenti, Divisione Strumenti e Servizi di Pagamento al Dettaglio*

### **ABI – ASSOCIAZIONE BANCARIA ITALIANA**

*Ufficio Sistemi e Servizi di Pagamento*

### **Enti aderenti al SIPAF**

## **Contributi esterni**

### **G. di. F. - Nucleo Speciale Polizia Valutaria**

*Gruppo Antifalsificazione Monetaria ed Altri Mezzi di Pagamento*

### **Direttore Master Cyber Security Link Campus University**

*Ing. Pierluigi Paganini*

### **RISSC - Centro Ricerche e Studi su Sicurezza e Criminalità**

*Dott.ssa Mara Mignone*