Banca Popolare di Sondrio

Servizio Organizzazione - Monetica e Sistemi di Pagamento

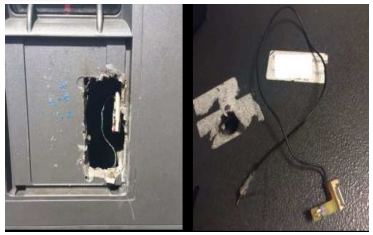
Payment Systems Revolution :

an opportunity for (too) many…

Evoluzione delle frodi in ambito monetica

1980	Voucher cartacei	→	Introduzione transazioni elettroniche POS
1990	Contraffazione carte	→	Introduzione CVC
	Skimming	→	Introduzione Chip EMV
	Manipolazione POS	→	POS meno vulnerabili
2000	Attacchi ATM	→	Antiskimming
	Compromissione Dati	→	Standard PCI-DSS e Autenticazione forte E-commerce

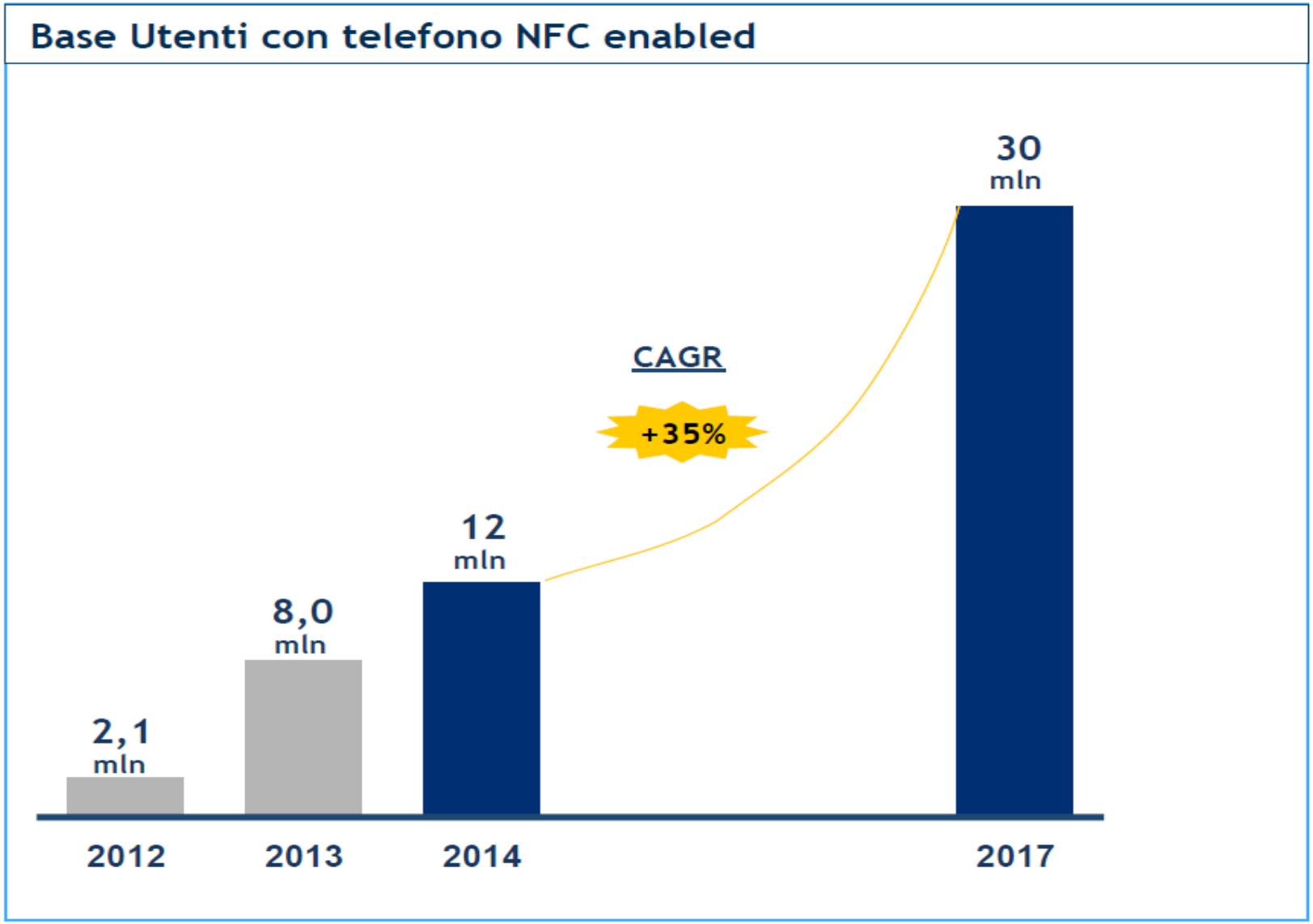
Evoluzione delle frodi in ambito monetica



- Shimming
- By-pass skimming
- Eavesdropping
- Fake terminal
- Ghost terminal
- Jackpotting

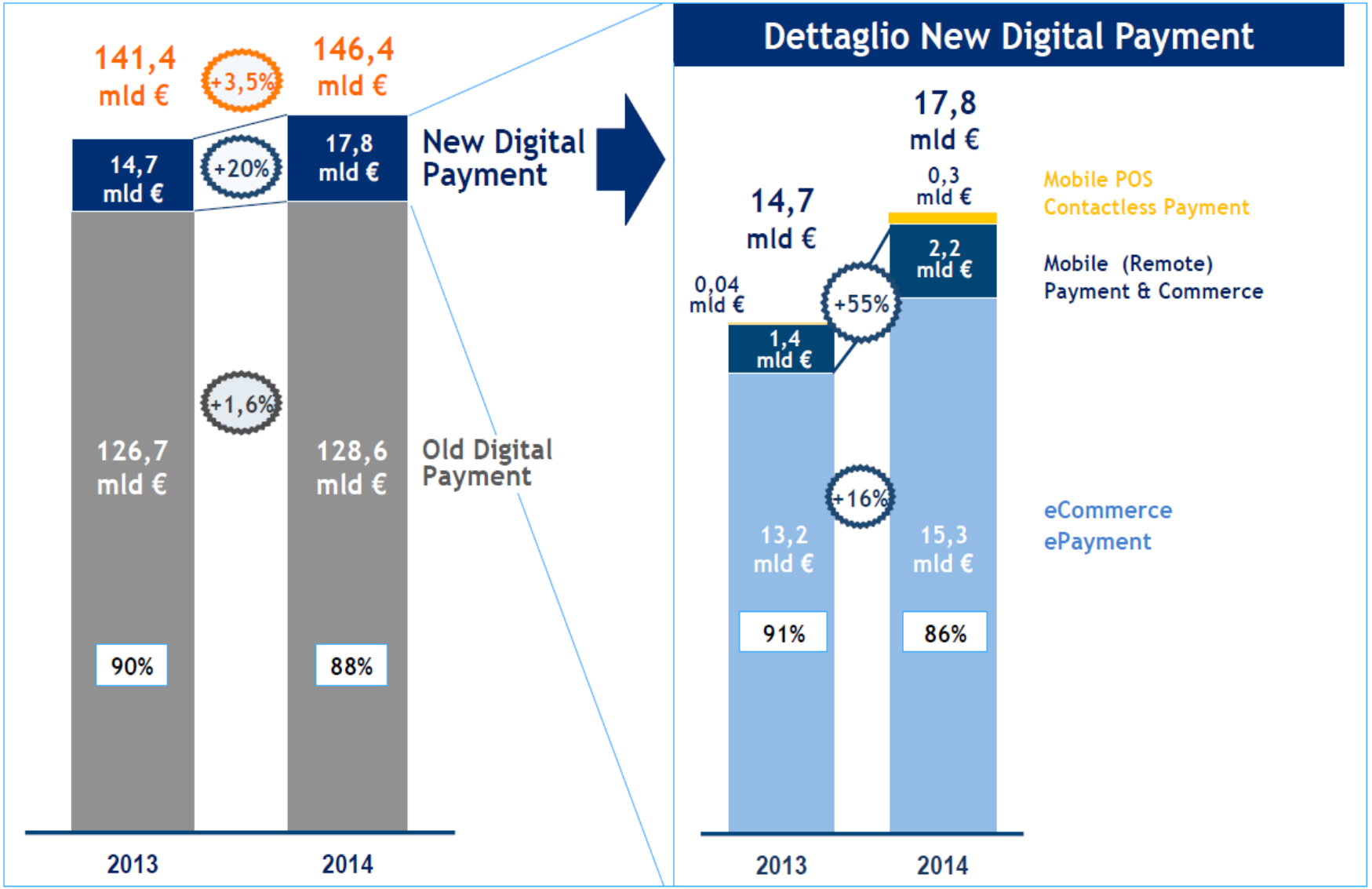
Payment systems revolution

Diffusione device



Fonte: Osservatorio Mobile Payment & Commerce Politecnico Milano

Trend Digital Payments...



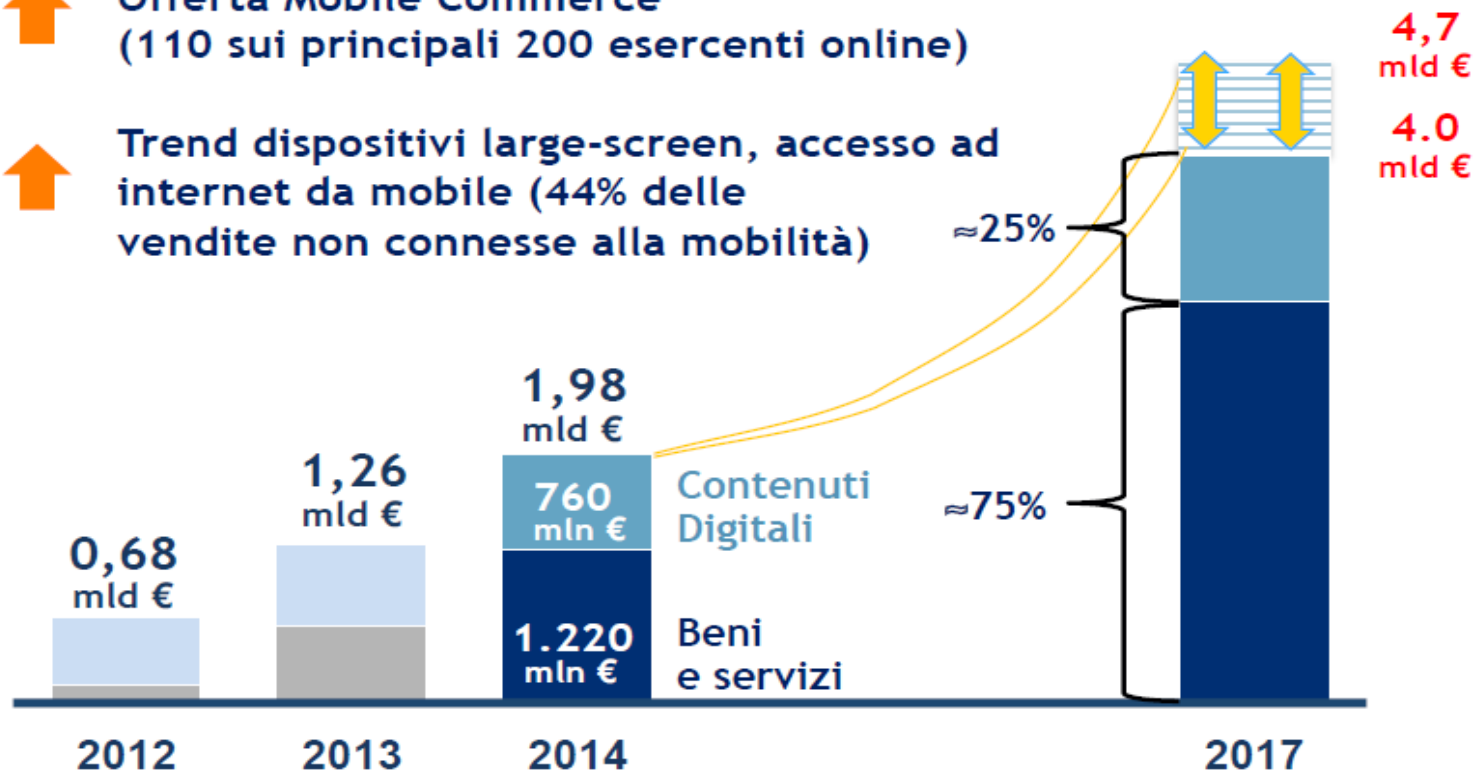
Fonte: Osservatorio Mobile Payment & Commerce Politecnico Milano

Il mondo va in questa direzione...

Valore transato Mobile Remote Commerce (2012-2017)

DRIVER:

- Offerta Mobile Commerce (110 sui principali 200 esercenti online)
- Trend dispositivi large-screen, accesso ad internet da mobile (44% delle vendite non connesse alla mobilità)



Fonte: Osservatorio Mobile Payment & Commerce Politecnico Milano


Volumi
Frodi

KYF – KNOW YOUR FRAUDSTER

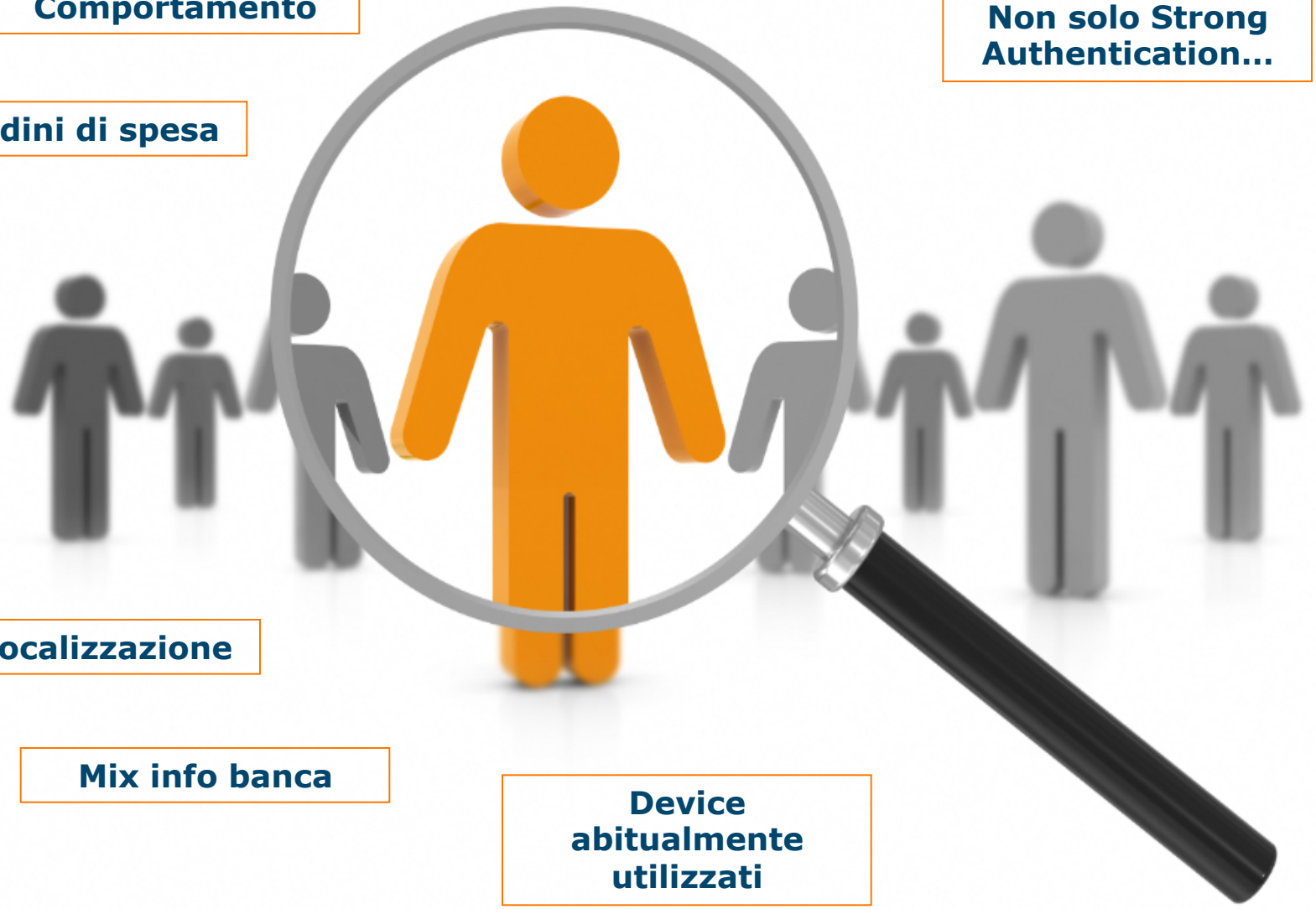
Chi sono?
Organizzazioni criminali internazionali

Target?
Banche – Processor - DB

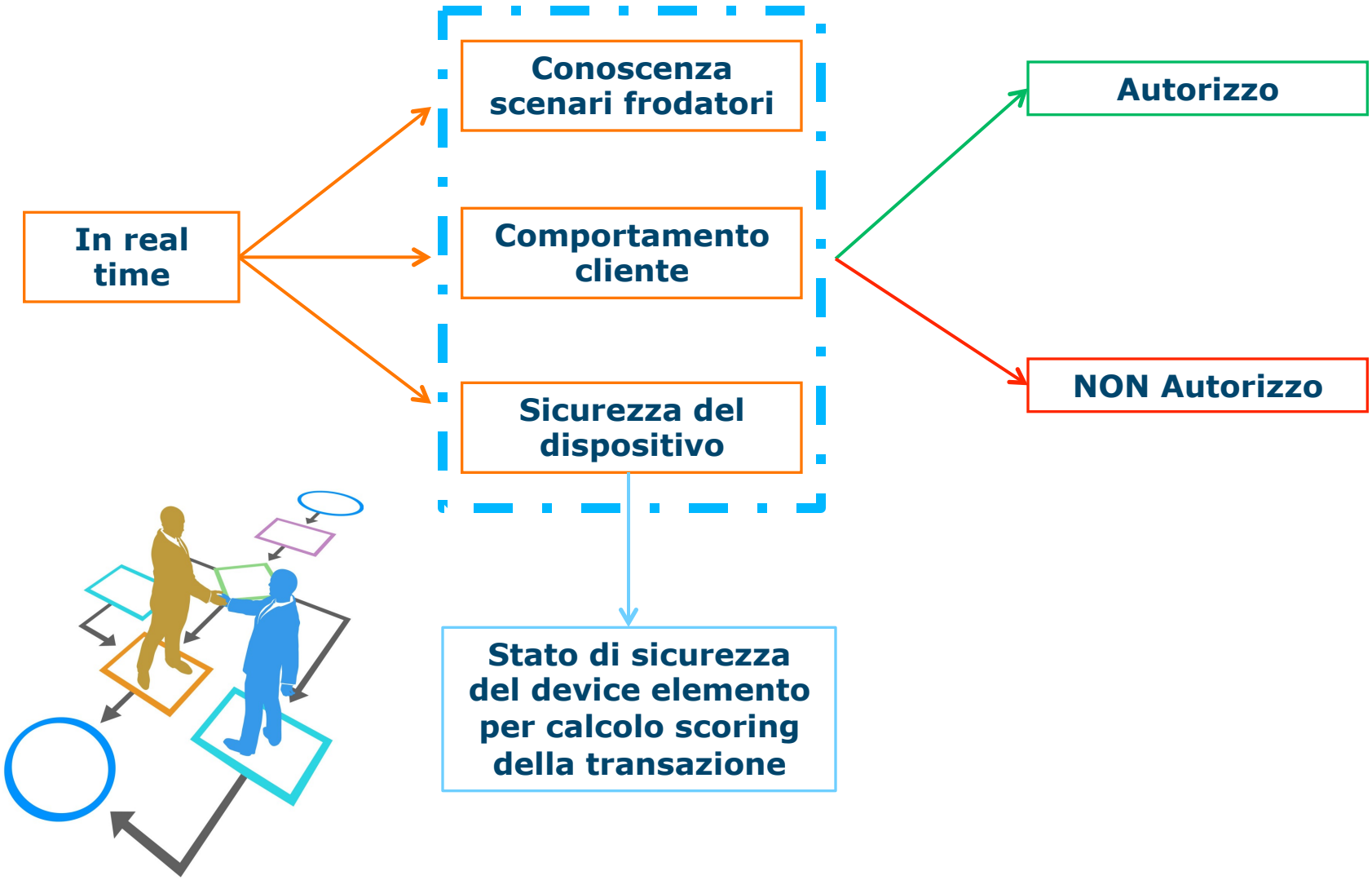
Tipi di attacco?
CP - CNP

Quali carte?
Debito – Credito - Prepagato

(R)KYC – (REALLY) KNOW YOUR CUSTOMER



CENTRALITA' E CRITICITA' DEL PROCESSO DECISIONALE



CARTE REGISTRATE SU APP DI PAGAMENTO/ DIGITAL WALLET DI TERZI

Le carte possono essere registrate ovunque…

Wallet e App gestite da operatori non tradizionali

I gestori dei wallet/App potrebbero appartenere a nazioni con regole meno restrittive

Dal messaggio autorizzativo non recepisco lo stato del device

Eventuale evoluzione dei sistemi di scoring dei circuiti

Messaggi autorizzativi ISO difficilmente modificabili per recepire nuove info

EVOLUZIONE DEGLI ATTACCHI

Phishing + **Carta Prepagata stessa banca** = **Ricarica con prelievo immediato**

- **Il prelievo è genuino**
- **L'identità del titolare carta corrisponde al vero**

Finto blocco spedizione merce a Natale

SMS per attivazione Social Card

Danni causati dalle frodi

Costi

Danno d'immagine

CARTE CONTO

Emissione nuove carte conto

- **Mancanza rischio creditizio**
- **KYC spesso light**

Vendite e-commerce fake senza spedizione della merche con pagamento a mezzo bonifico

Utilizzo del prodotto carta conto per accrescere la reputazione sul sistema interbancario, apertura nuovi rapporti di conto corrente nati come acquisizione clientela già bancarizzata

FRAUD EVOLUTION – DEBOLEZZE SISTEMI AUTORIZZATIVI

Generazione e instradamento di un elevato numero di transazioni EMV effettuate su BIN reali, ma con dati costruiti dai frodatori

↓

Sistema autorizzativo non gestisce / verifica correttamente tutti i valori della richiesta autorizzativa

↓

A causa dell'elevato numero di transazioni negate il sistema autorizzativo effettua lo switch sui sistemi di Stand-in

↓

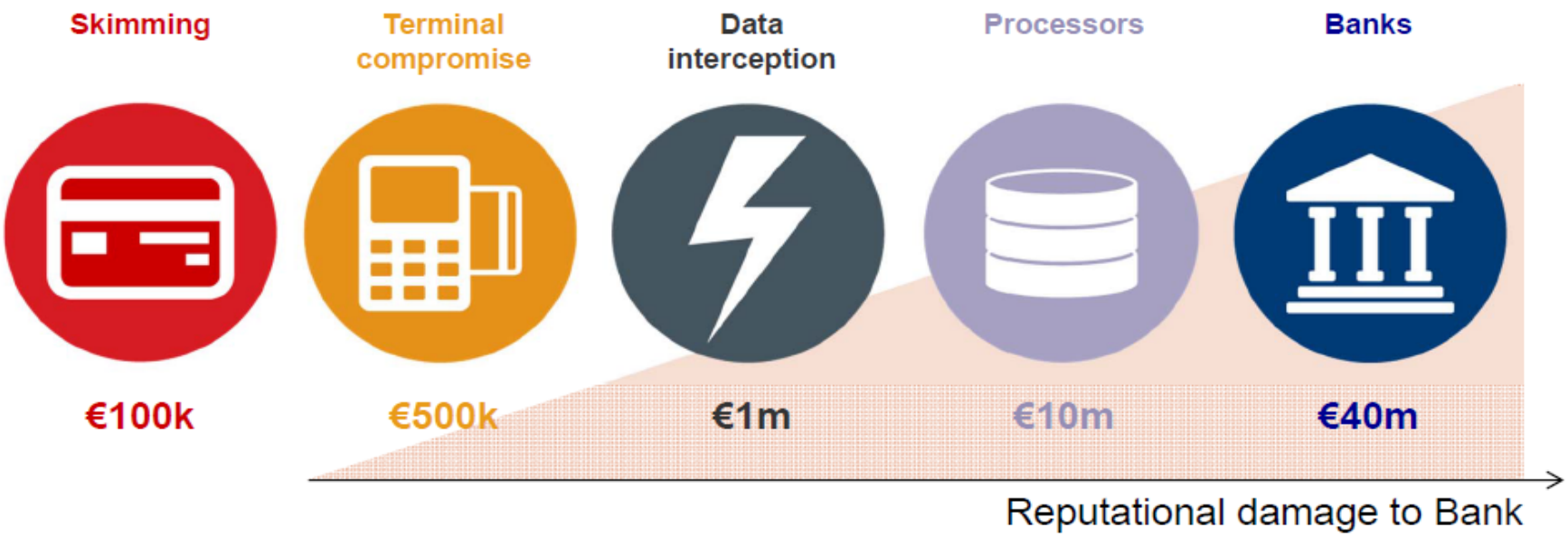
I sistemi di Stand-in effettuano uno screening più superficiale della transazione (vedi (R)KYC) e quindi le transazioni fake sono state autorizzate

Verifica puntuale di tutti i TAG previsti dallo standard EMV

Irrobustimento dei sistemi di backup

FRODI CATASTROFICHE

I frodatori stanno diventando sempre più sofisticati…

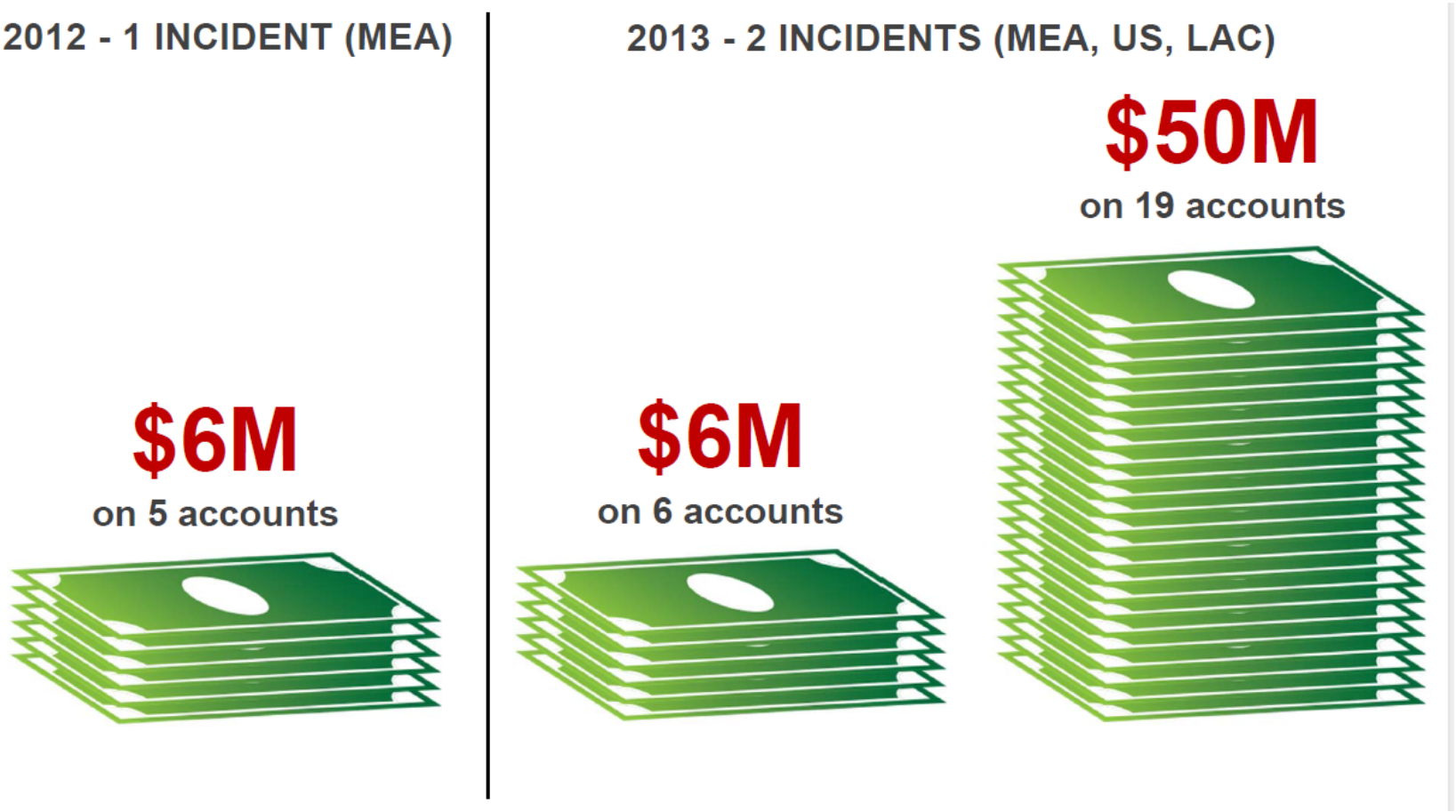


L'anello più debole viene sempre attaccato per primo

Sempre più utenti risultano compromessi

Il rischio reputazionale deve essere una priorità per tutti

FRODI CATASTROFICHE - DATI



Con le frodi catastrofiche vengono messi in discussione sia la reputazione che il business della banca / Processor.

Le perdite nette derivanti da tali attacchi possono raggiungere cifre spaventose.

FRODI CATASTROFICHE – AZIONI DI MITIGAZIONE

Risk Assessment
Quanto sono veramente esposto a questo tipo di attacchi?

Creazione di una seconda linea di difesa indipendente che possa agire nel momento in cui il sistema presenti picchi anomali

Il layer di difesa deve avere funzioni dispositive che consentano il blocco delle transazioni, non solo la semplice generazione di Alert

NORMATIVA DISOMOGENEA

L'IF Regulation prevede che negli accordi di licenza o nelle regole dei circuiti delle carte di pagamento per l'emissione di carte di pagamento o il convenzionamento delle operazioni di pagamento basate su carta sono vietate le restrizioni territoriali nell'Unione e le regole aventi effetto equivalente.

Le regole di accesso al mercato non sono ancora state armonizzate e pertanto i frodatori potrebbero sfruttare le eventuali debolezze di sistemi giuridici o degli organi di controllo per costruire complessi scenari di attacco anche al sistema italiano.

PRINCIPI CARDINE PER IL CONTRASTO A QUESTI ATTACCHI

Sicurezza accesso ai sistemi informatici / Base dati

Educazione della clientela

Conoscenza approfondita del cliente

Rendere disponibile la possibilità di configurare la propria carta

MA SOPRATTUTTO…

PRENDENDO ISPIRAZIONE DAL WEB 2.0 …

CONDIVISIONE

INTERAZIONE

PARTECIPAZIONE