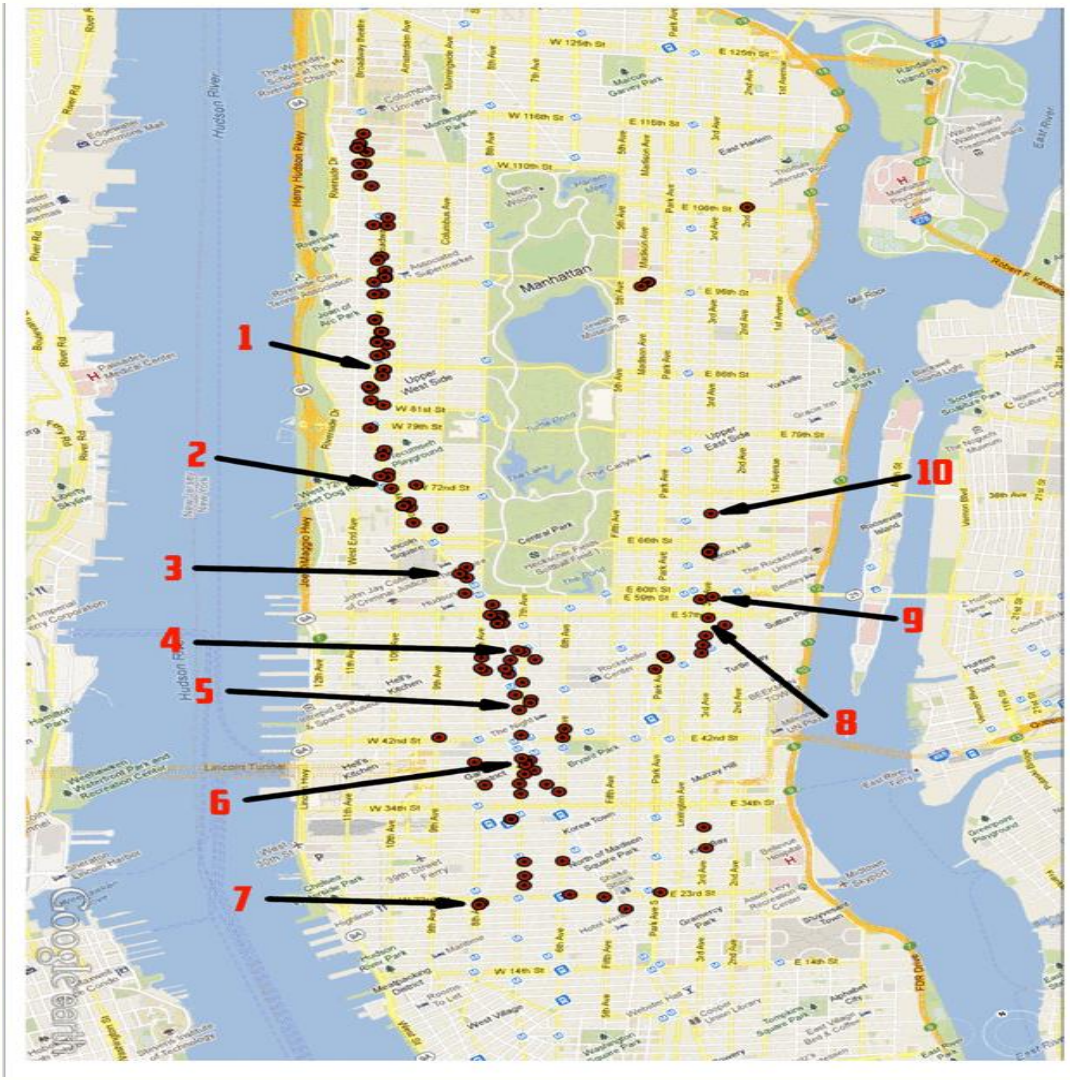
Flawless MONEY Ltd

Situational Awareness in detecting Fraud or Financial Crime

Dr Andrew Lenaghan,
Information security officer / consultant

An example…

$30,000 in A.T.M. withdrawals in 6h (Manhattan NY)

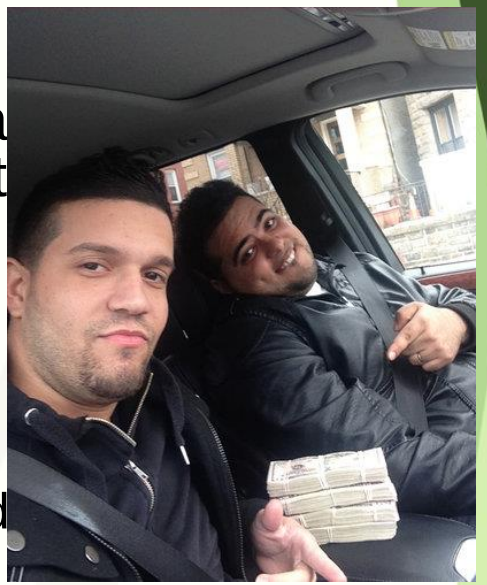


Credit: United States Attorney's Office for the Eastern District of New York

Prepaid card ATM heist 2013 [1][2]

Scale - $45m (£29m) across 26 countries.

- Inc. law enforcement agencies in US, Japa Canada, the UK, Romania +12 other count
- Seven charged in New York



March - Elvis Rafael Rodriguez, left, and Emir Yasser Yeje, charged with ML in Brooklyn (with $40,000)

How

- Hackers (Not caught)
  - compromise computer systems of card processors to steal data on prepaid debit card
  - Manipulated withdrawal limits on cards
  - distributed card information to accomplices aka "cashers" around the world
- Cashers (1 US Gang caught)
  - loaded stolen info onto magnetic stripe cards
  - used cloned card to make cash withdrawals at ATMs

Two attacks

Attacks

1: December 2012

Issuer: Rakbank (United Arab Emirates)

- Network intrusion into Indian credit card processor
- Increase limits on 5 prepaid cards issued by Rakbank
- Overall
  - casher cells execute 4,500 ATM transactions
  - in about 20 countries
  - Obtained $5m

2: Feb 2013 – x8 more costly

Issuer: Bank of Muscat (Oman)

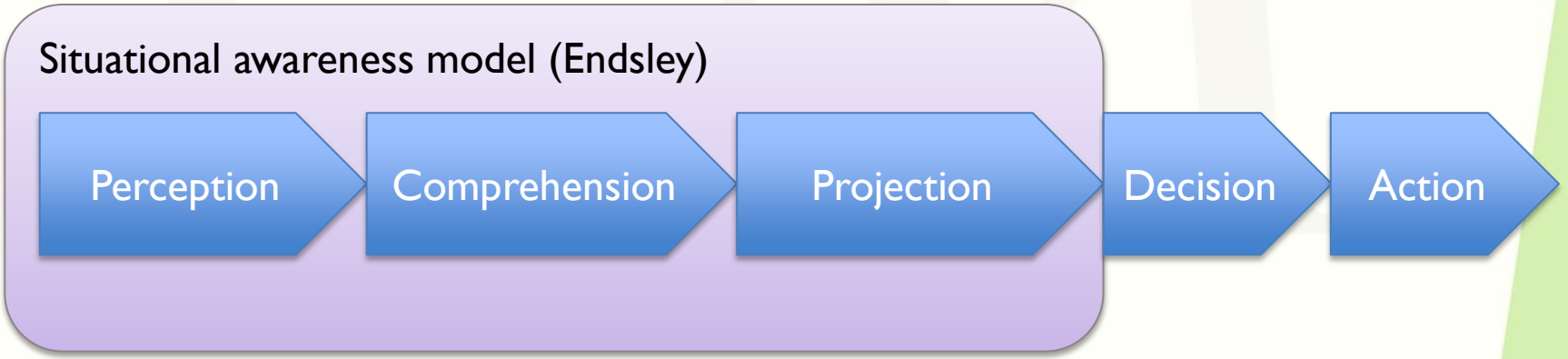
- Network intrusion into US credit card processor
- Obtained details and increased limits on 12 prepaid accounts
- Overall
  - casher cells executed 36,000 ATM transactions
  - in 24 countries
  - worth $40m (<24h hours)

What is know about the NY cashing crew?

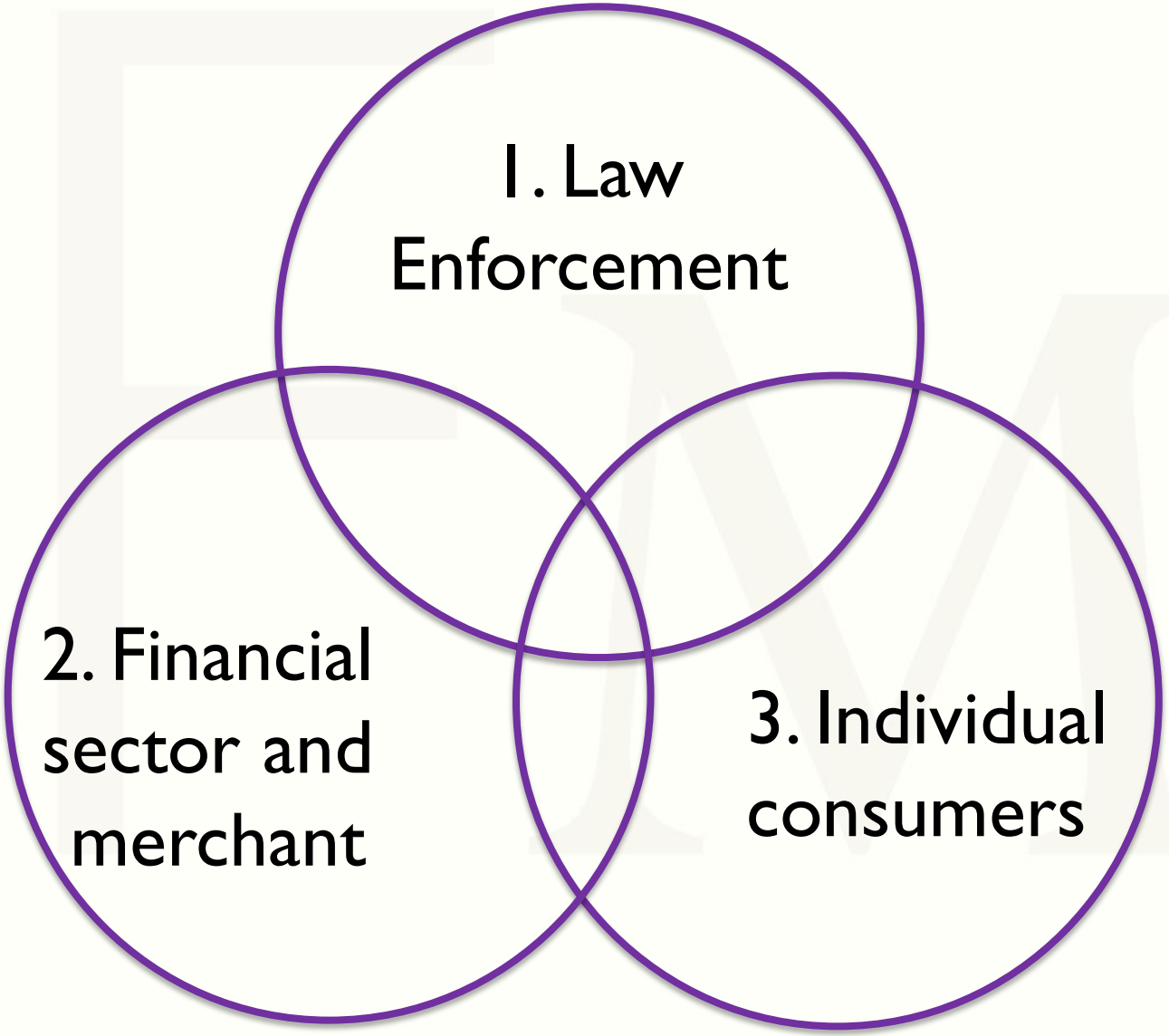
- Structured : Leader + 7 named associates
- Equipment & technical ability : modest
  - able to receive card details via internet
  - clone details on to mag. stripe to create fake cards
- Planning / execution - good
  - Short duration of attacks, coordinate internationally
  - Hundreds / thousand transactions conducted with hours
- What did they do with the proceeds ($2.7m)?
  - Cash recovered – $60K
  - Money banked – $100k in 2 accounts
  - Buy Rolex oyster perpetual watches

Financial Crime

- Adversarial environment
  - victim / attacker - both have awareness
- Crime types - financial
  - Fraud – obtaining good and service by deception
  - Money laundering– handling the proceeds of crime
- Well defined underground marketplace and roles for financial information



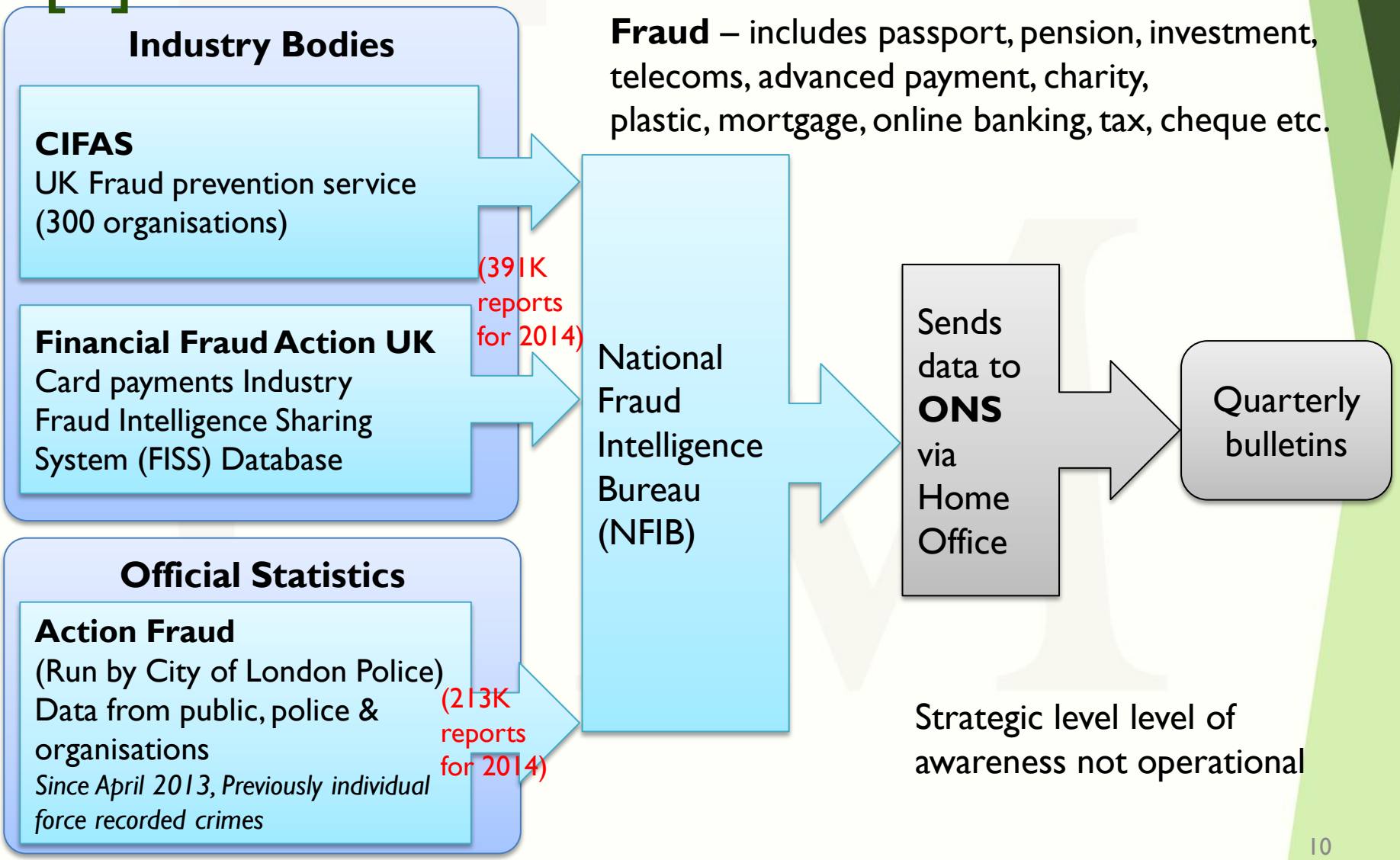
Who might be aware of financial crime?



1. Law enforcement

- Local police forces
  - Tend not to have high tech capablities.
  - Capablities do exist– eg UK's National Cyber Crime Unit part of the National Crime Agency (NCA) - limited
  - (Consumer more likely to contact payment service provider or merchant to resolve crime).
- Money laundering reporting in the financial sector
  - Compulsory Role: money laundering reporting officer
  - File **Suspicious activity reports** (SARs)

UK Fraud reporting : data sources [3]



2. Financial sector / merchants

- **Perception**
  - more information / more quickly at hand
- **Comprehension**
  - Dedicated fraud teams / investigators
  - Fraud detection systems :
    - Threshold
    - Rules / pattern matching to identify anomalous transaction
    - IP geo-location / device fingerprinting / stolen card lists
  - Industry typologies of know threats (indicators, actors)
- **Projection**
  - ‘Risk based’ approach
  - Risky transaction – blocked or subject to more stringent checks

3. Individuals (consumers)

- Low awareness of threat / attack

- **Perception** : May not spot warning signs
  - Phishing attacks often cunning
- **Comprehension**
  - Often unaware they have been targeted until merchants / payment service providers contact them.
- **Projection**
  - Unsure what to do / lacking technical capability to deal with threat.

Future trends…

Two Challenges…

- Alternative currencies
  - Eg Bitcoin
  - Bring cash like anonymity to payment
- Network Anonymisation technologies
  - Eg Tor networking
  - Hide src/dst

Both make it harder to trace money or identify end points.

Two Opportunities…

- Strong (2F) Authentication for payment
- Mandate better communication / education from payment service providers about the threats consumer face

(Coming from EBA European banking authority – guidelines on security of internet payments)

References

[1] Santora M 9/5/2013, NY Times, *In Hours, Thieves Took $45 Million in A.T.M. Scheme*
http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html
[2] BBC News,10/5/2013 *Cybercriminals 'drained ATMs' in $45m world bank heist*
http://www.bbc.co.uk/news/world-us-canada-22470299
[3] Office for National Statistics, **User Guide to Crime Statistics for England and Wales**, January 2015, p.53