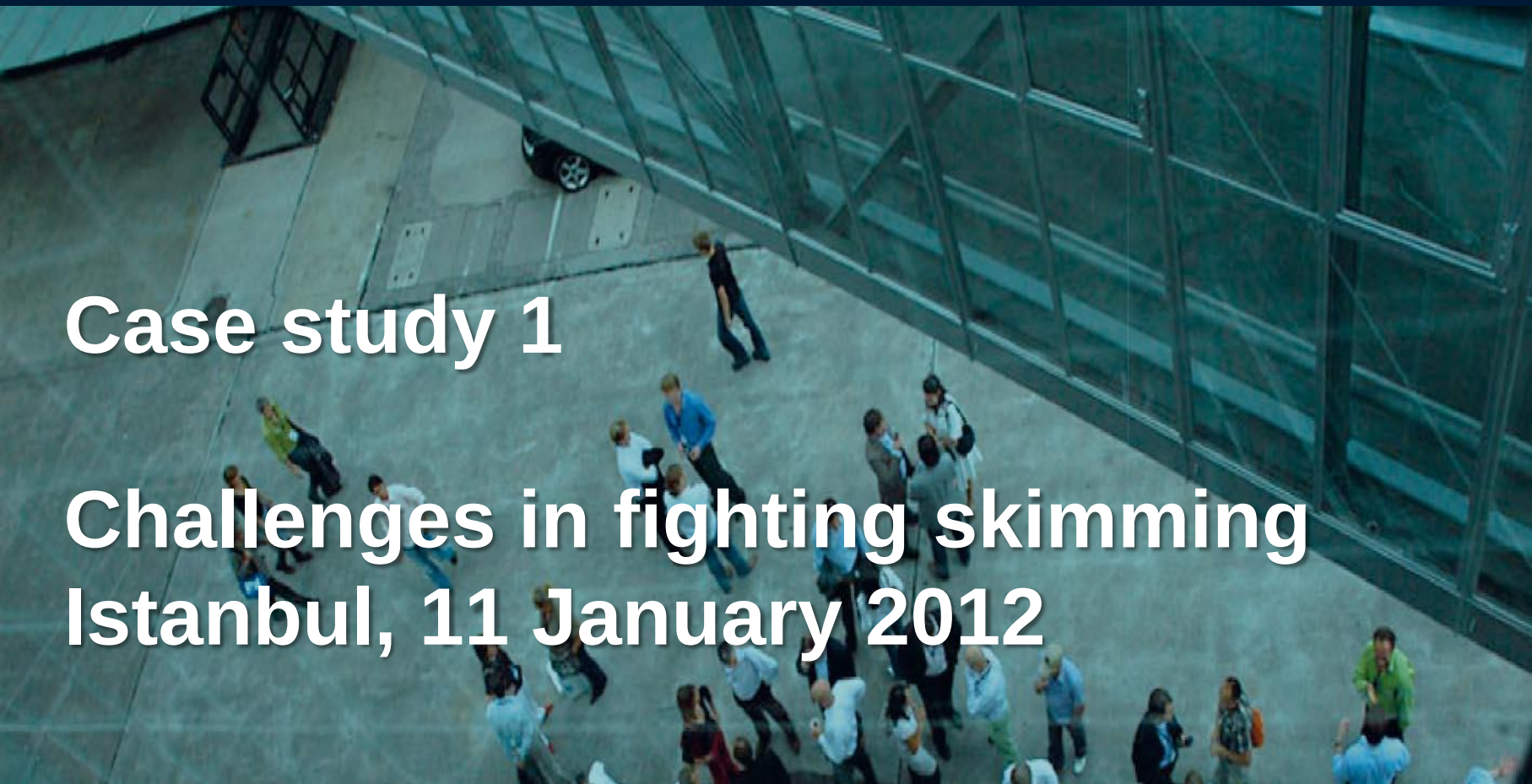
Georges van den Eshof

Cybercrime prosecutor / Ciber suç savcısı

Maastricht Prosecution Service / Maastricht Savcılık Idaresi

The Netherlands / Hollanda

OPENBAAR MINISTERIE



Case study 1

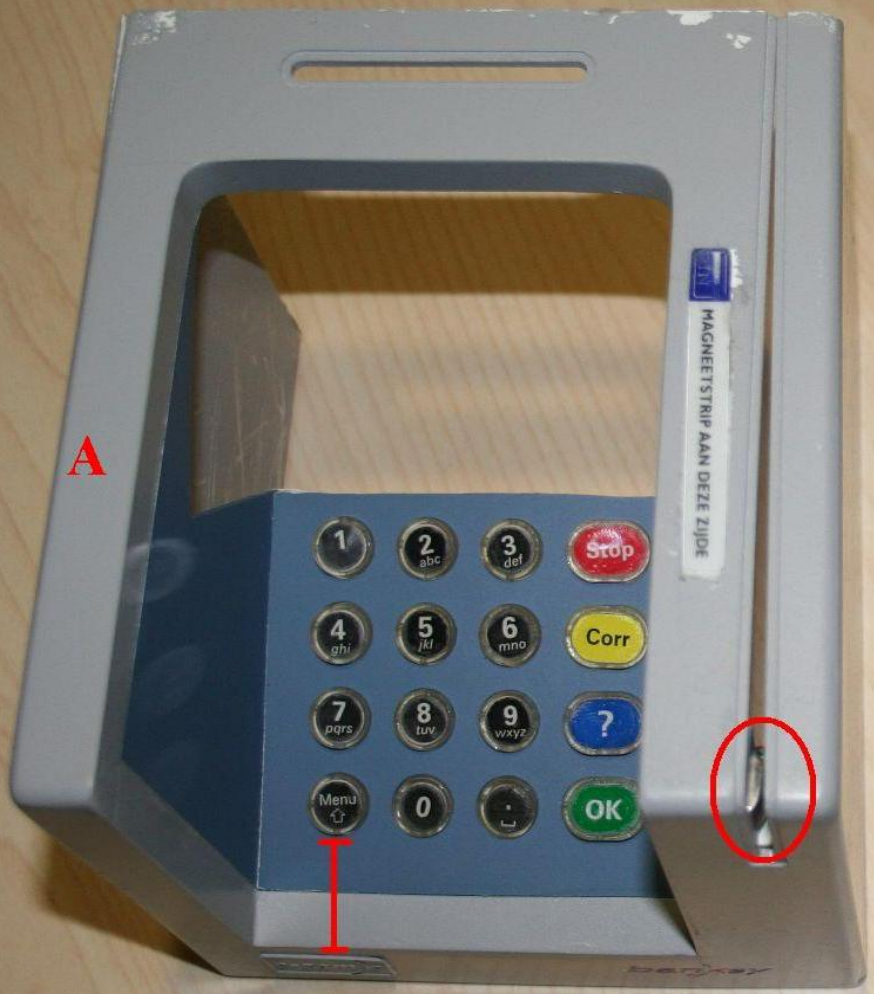
Challenges in fighting skimming
Istanbul, 11 January 2012

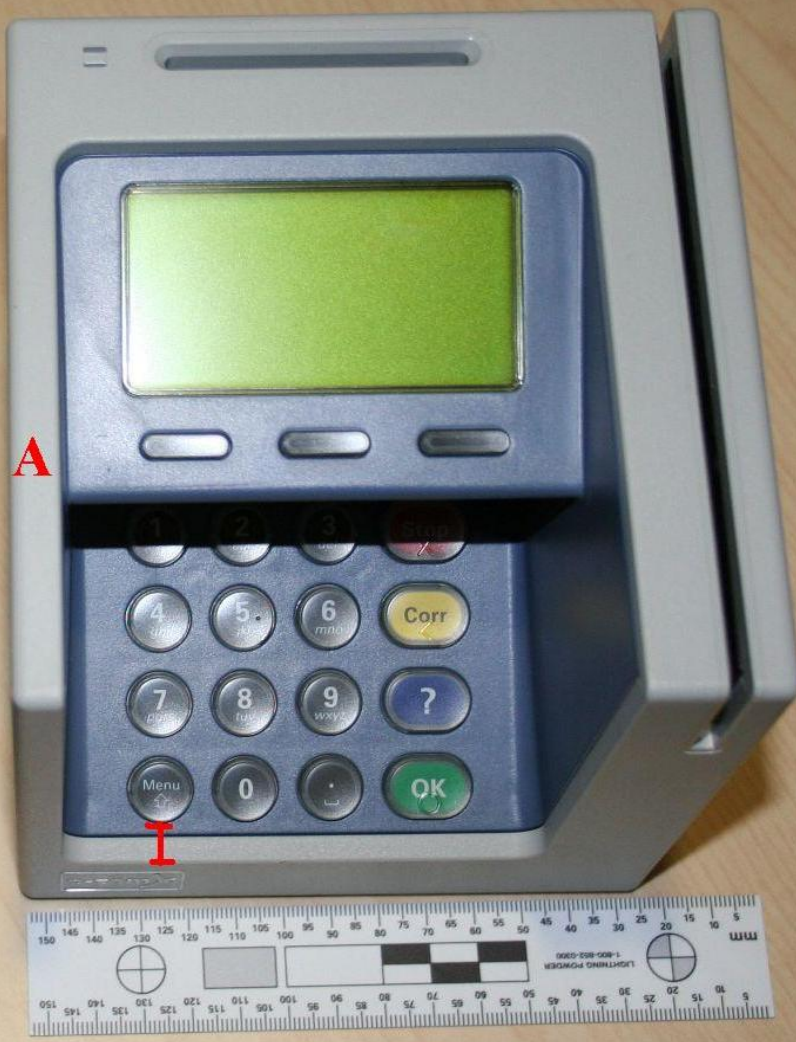
A bit of terminology…

- Skimming
- Trapping
- Tampering with internet banking authentication devices
- Carding
- Shouldering or shoulder surfing
- Reversal fraud
- Handskimmers

The Dutch case

- Mostly a Romanian trade (70%)
- Highly organised gangs with tasks for engineers, operatives,..
- Netherlands: interesting target for skimmers


A
MAGNEETSTRIP AAN DEZE ZIJDE
1
2 abc
3 def
Stop
4 ghi
5 jkl
6 mno
Corr
7 pqrs
8 tuv
9 wxyz
?
Menu
0
OK


A
Corr
Menu
0
OK

Articles in Dutch Criminal Code (DCC)

- Art 232 DCC: copying or using a carrier of information or value
  - Not only banking or credit cards! Also medical cards, transportation tokens, …
- Art 234 DCC: having or transferring goods or data that can be used to commit a crime under 232 DCC
  - Skim devices, blank plastic cards, cardwriters, …
- Art 140 DCC: criminal organisation
- Art 310 and 311 DCC: theft and aggravated theft (with false key, breaking, trespassing, …)
- Art 326 DCC: fraud
- Art 420bis DCC: money laundering and profiteering

Problem : Coordination

- Police had no central point
  - Mostly suspects caught red-handed
  - Almost no long-term investigations...
- Only Equens (private sector)
  - Monthly skimming bulletin with trends and figures
  - Use photo-analyst for assisting police

National Skimming Point LSK

- Started on 1 December, 2011.
- Cooperation between police (fraud unit), prosecution service and the private sector banks.
- Example of public-private cooperation
- ONLY for skimming cases
- Collection and analysis of skimming information, coordination of national and international investigations

Electronic Crimes Task Force

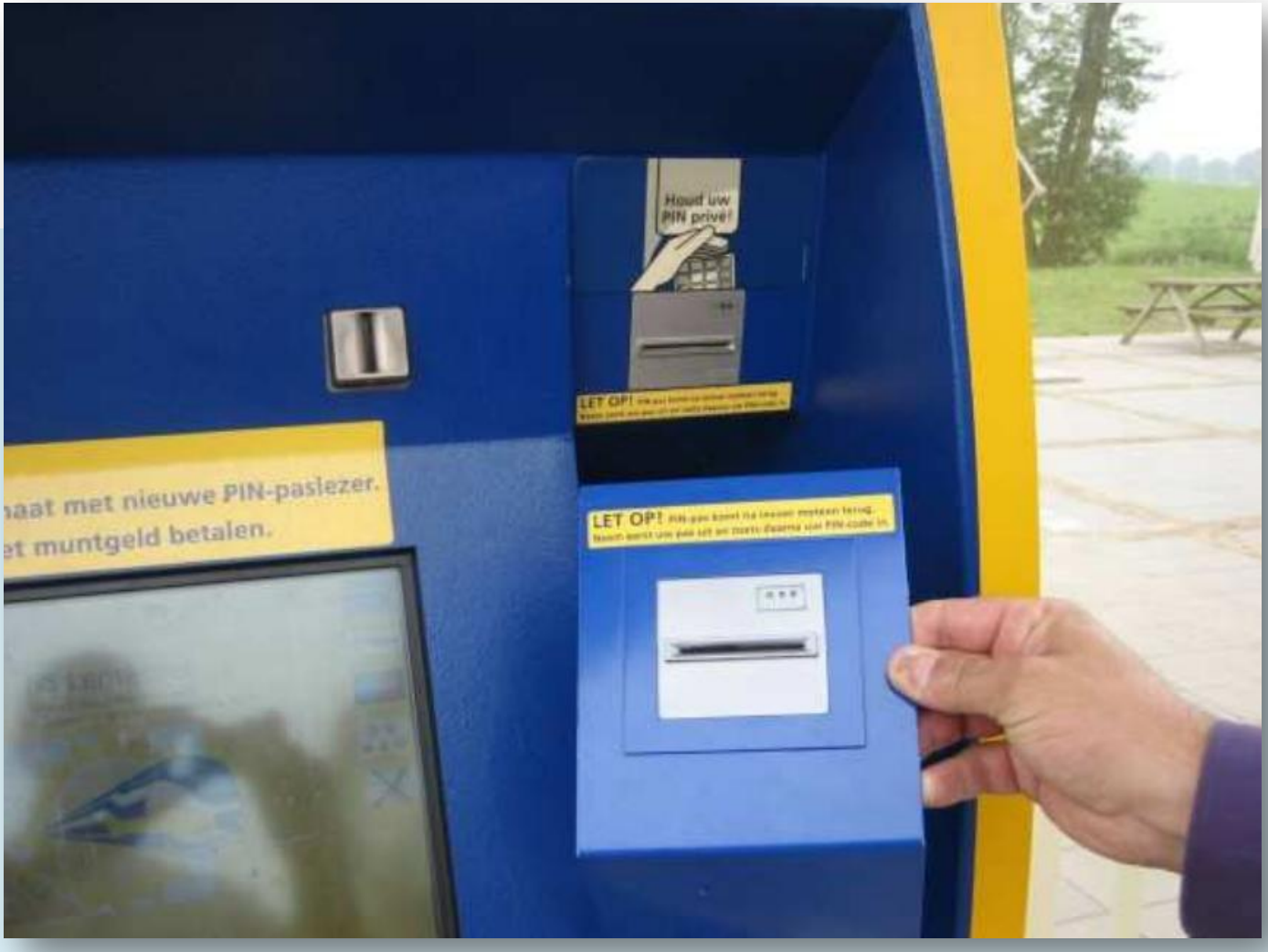
- Part of national police agency KLPD
- In coordination with banks
- Geared towards various high-tech attacks on internet banking (not specifically skimming)
- Example: Aries case (manipulation of internet banking authentication devices)

Problem : legal (and technical) knowledge

- Police level
- Prosecution level
  - Cybercrime-savvy prosecutors
  - What to charge the skimmers with?
- Courts and judges
  - Interpretation of technical issues
  - Differences in sentences?
  - Understanding the cost and dangers

Cat and mouse games

- Introduction of EMV chip vs magnetic strip
- Enhanced approach against skimming results in migration effect
  - More shoulder surfing, especially with older victims
  - More incidents of internet banking fraud


Houd uw
PIN privé!
LET OP!
LET OP!


Inleggen
Inschuiven
Houd uw PIN privé!

Relevant questions in fighting skimming (and cybercrime)

- Eradicating skimming is impossible, but not administering justice is not an option
- How is the awareness at all levels of police and judiciary?
- Do you have the necessary technical and legal knowledge on call to succesfully prosecute?
- Is the cooperation with the private sector optimal (and possible?)
- (Dutch case) Do you have coordination?

Thank you for your attention

Any questions?