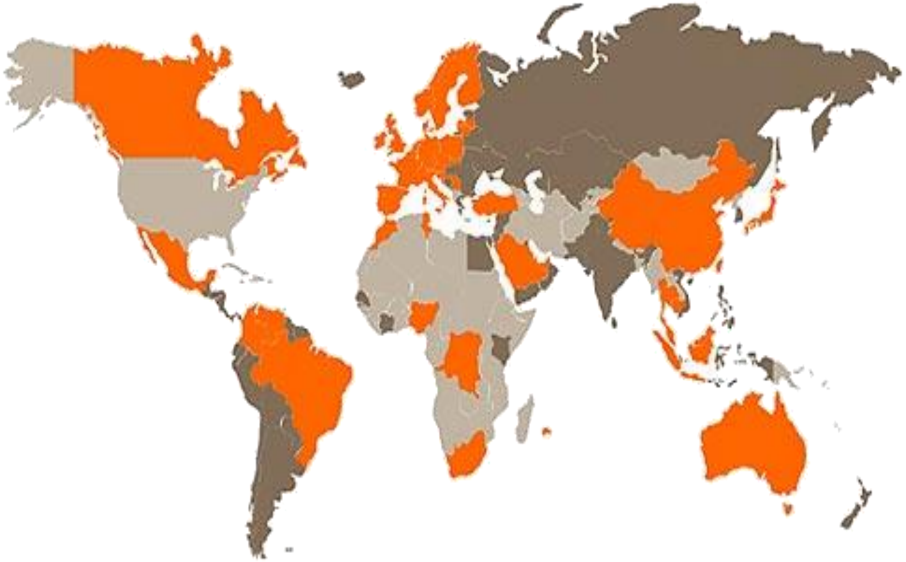
Risks of Offline Verify PIN on Contactless Cards

Martin Emms, Budi Arief, Nick Little, Aad van Moorsel

Newcastle University

Centre for Cybercrime & Computer Security

What are EMV Chip & PIN Cards



barclaycard
4929 4926 1094 5031
4929 MONTH/YEAR MONTH/YEAR
VALID FROM 06/10 EXPIRES END 08/13
H J EMMS
VISA

- 1.5 Billion EMV cards in circulation
- Visa & MasterCard to implement in USA 2015 (TBD)
- Wireless access to the "contact" protocol

Contactless Verify PIN

- Verify PIN directly on the card (offline mode)
- Wireless Access to Verify PIN
  - Accessed without the cardholders knowledge
- Redundant functionality
  - No PIN required in contactless transaction
- Viable attack scenario to find the PIN
- Amex and MasterCard have prohibited the functionality – MC “for security reasons”

Door Entry Attack Scenario

Always leave 1 PIN attempt remaining so the card is not locked

Day 1

PIN – 1983 X

PIN – 6383 X

Day 2

PIN – 0306 X

PIN – 0603 X

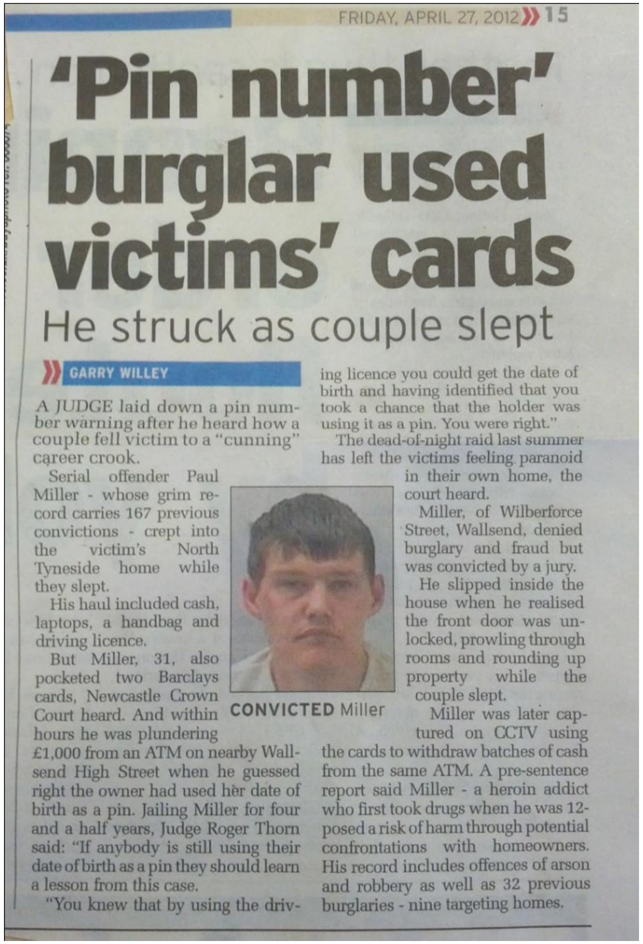
Day 3

PIN – 1234 X

PIN – 0683 ✓

Birthday Based PINs

- Bonneau et al. FC 2012
  - Birthday in every 11 wallets
  - Bad chioces in user chosen PIN
- Real Life Example
  - Birthday used as PIN
  - Same PIN on 2 cards
  - Birthday on driving licence
  - £1,000 within hours



FRIDAY, APRIL 27, 2012 15

'Pin number' burglar used victims' cards

He struck as couple slept

GARRY WILLEY

A JUDGE laid down a pin number warning after he heard how a couple fell victim to a "cunning" career crook.

Serial offender Paul Miller - whose grim record carries 167 previous convictions - crept into the victim's North Tyneside home while they slept.

His haul included cash, laptops, a handbag and driving licence.

But Miller, 31, also pocketed two Barclays cards, Newcastle Crown Court heard. And within hours he was plundering £1,000 from an ATM on nearby Wallsend High Street when he guessed right the owner had used her date of birth as a pin. Jailing Miller for four and a half years, Judge Roger Thorn said: "If anybody is still using their date of birth as a pin they should learn a lesson from this case.

"You knew that by using the driving licence you could get the date of birth and having identified that you took a chance that the holder was using it as a pin. You were right."

The dead-of-night raid last summer has left the victims feeling paranoid in their own home, the court heard.

Miller, of Wilberforce Street, Wallsend, denied burglary and fraud but was convicted by a jury.

He slipped inside the house when he realised the front door was unlocked, prowling through rooms and rounding up property while the couple slept.

Miller was later captured on CCTV using the cards to withdraw batches of cash from the same ATM. A pre-sentence report said Miller - a heroin addict who first took drugs when he was 12 - posed a risk of harm through potential confrontations with homeowners. His record includes offences of arson and robbery as well as 32 previous burglaries - nine targeting homes.

CONVICTED Miller

Why is this Important?

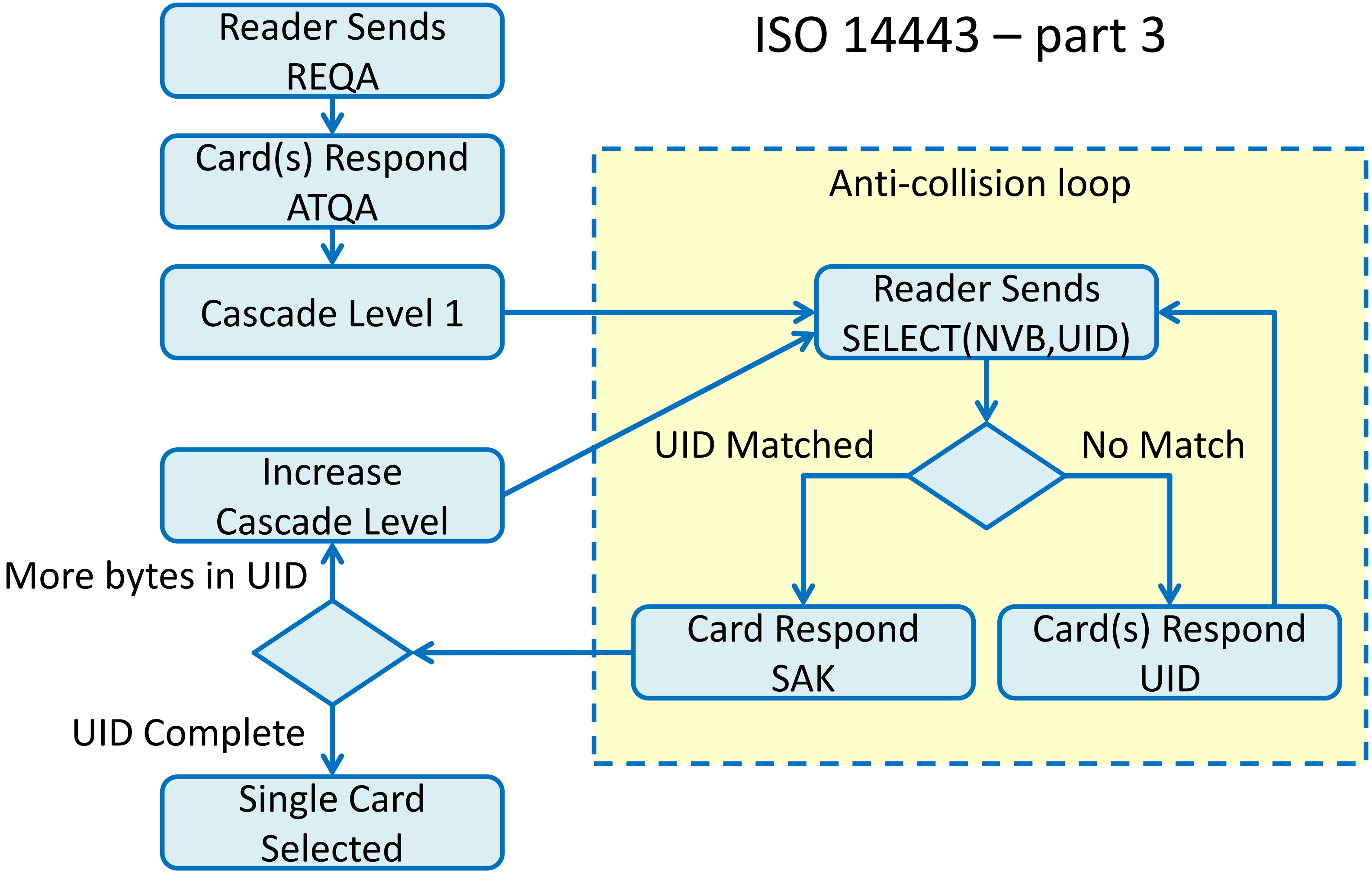
What are my rights if I'm a victim of fraud and my bank doesn't give me my money back?

If your bank or card company has evidence to show that you have acted fraudulently or without reasonable care then they may not refund your losses.

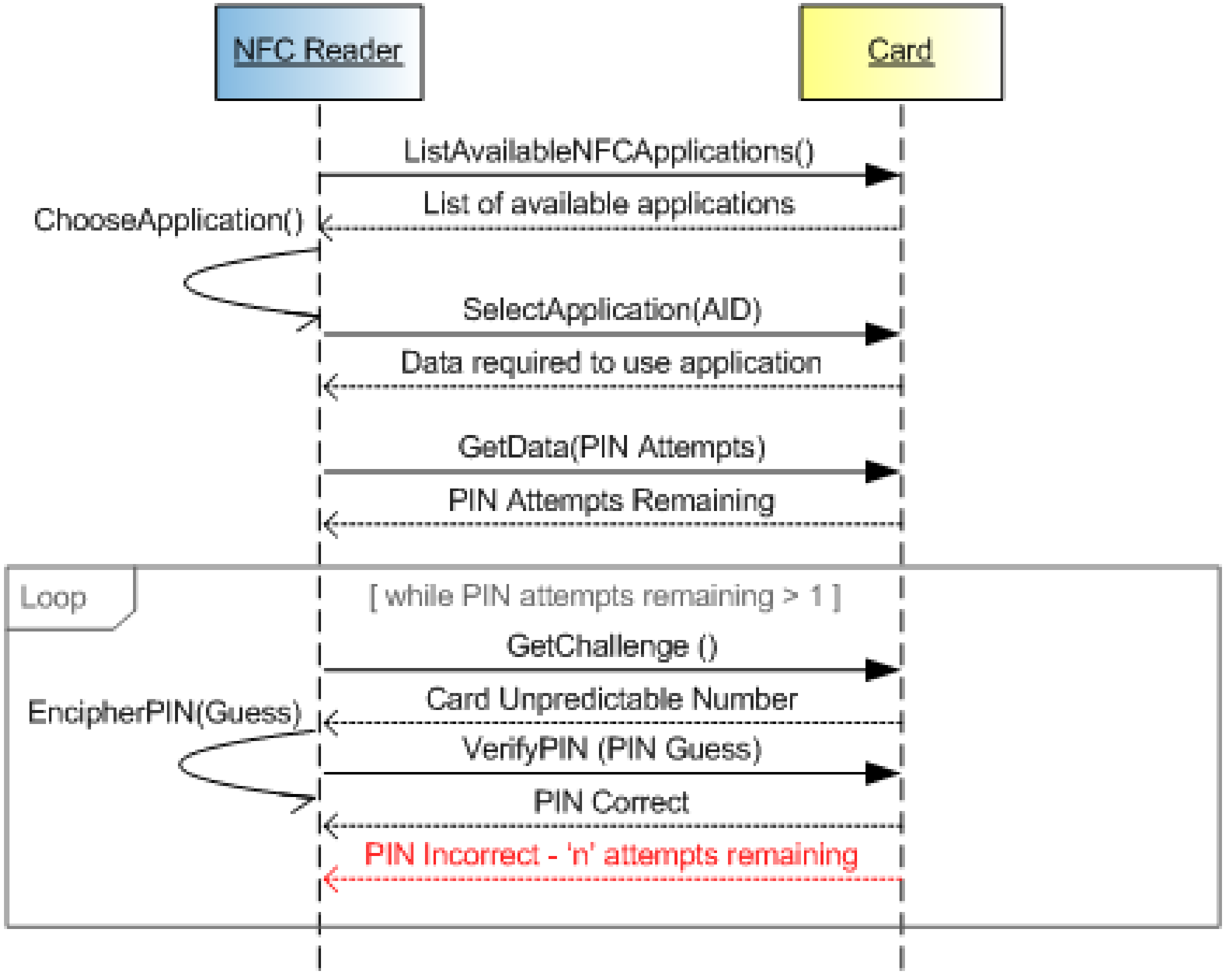
(Source – The UK Cards Association 2010)

How does it work? - Multi-card

ISO 14443 – part 3



How does it work? - PIN Verify


NFC Reader
Card
ListAvailableNFCApplications()
List of available applications
ChooseApplication()
SelectApplication(AID)
Data required to use application
GetData(PIN Attempts)
PIN Attempts Remaining
Loop
[while PIN attempts remaining > 1]
GetChallenge ()
Card Unpredictable Number
EncipherPIN(Guess)
VerifyPIN (PIN Guess)
PIN Correct
PIN Incorrect - 'n' attempts remaining

Results

Total attack time for a wallet containing a door entry card and a credit card

Activity	(ms)
Identify door entry card	214.4
Identify credit card and select it	214.4
List credit card applications	18.4
Select application (Visa, MasterCard, Amex etc.)	19.2
Get the number of available PIN attempts	29.8
Ask the card to generate an unpredictable number	24.6
VerifyPIN (PIN)	175.8
Ask the card to generate an unpredictable number	12.2
VerifyPIN (PIN)	177.2
Total	**886.0**

Conclusions

- Redundant functionality can be removed
- Attack gives many chances to find PIN
- Total Attack Time 866.0ms (2 cards)
- Birthday PIN higher probability of success
- Undermines the security of Chip & PIN

Any Questions?

Thank You