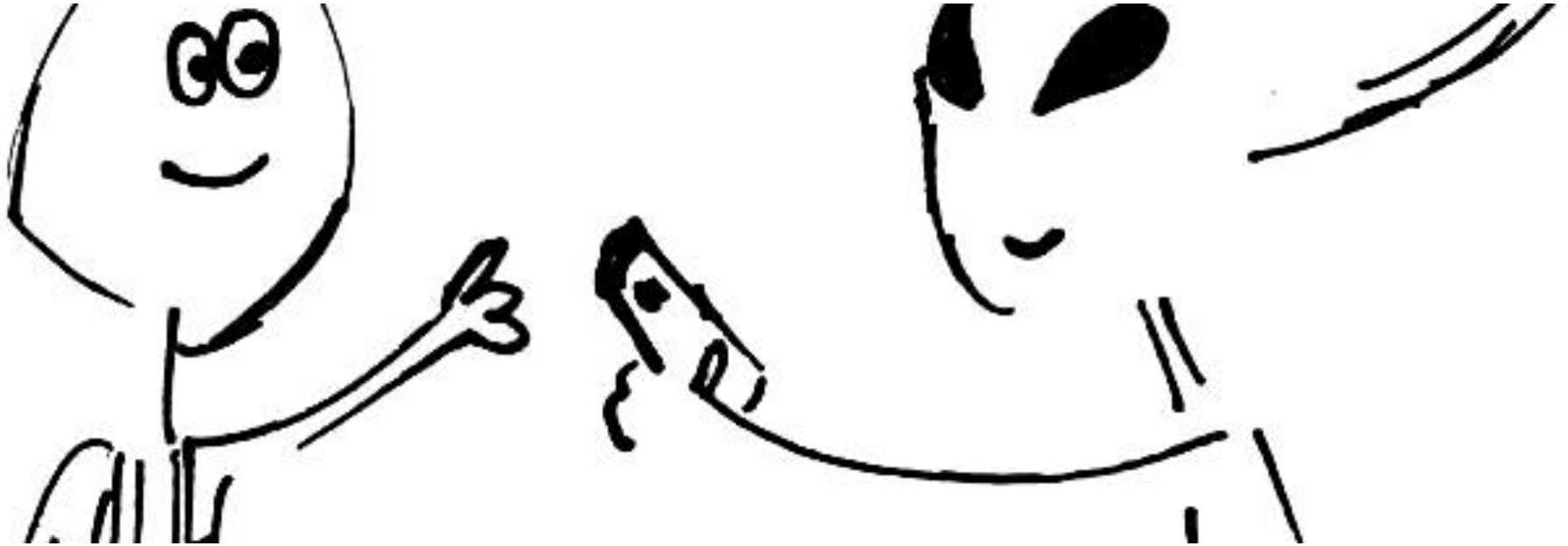
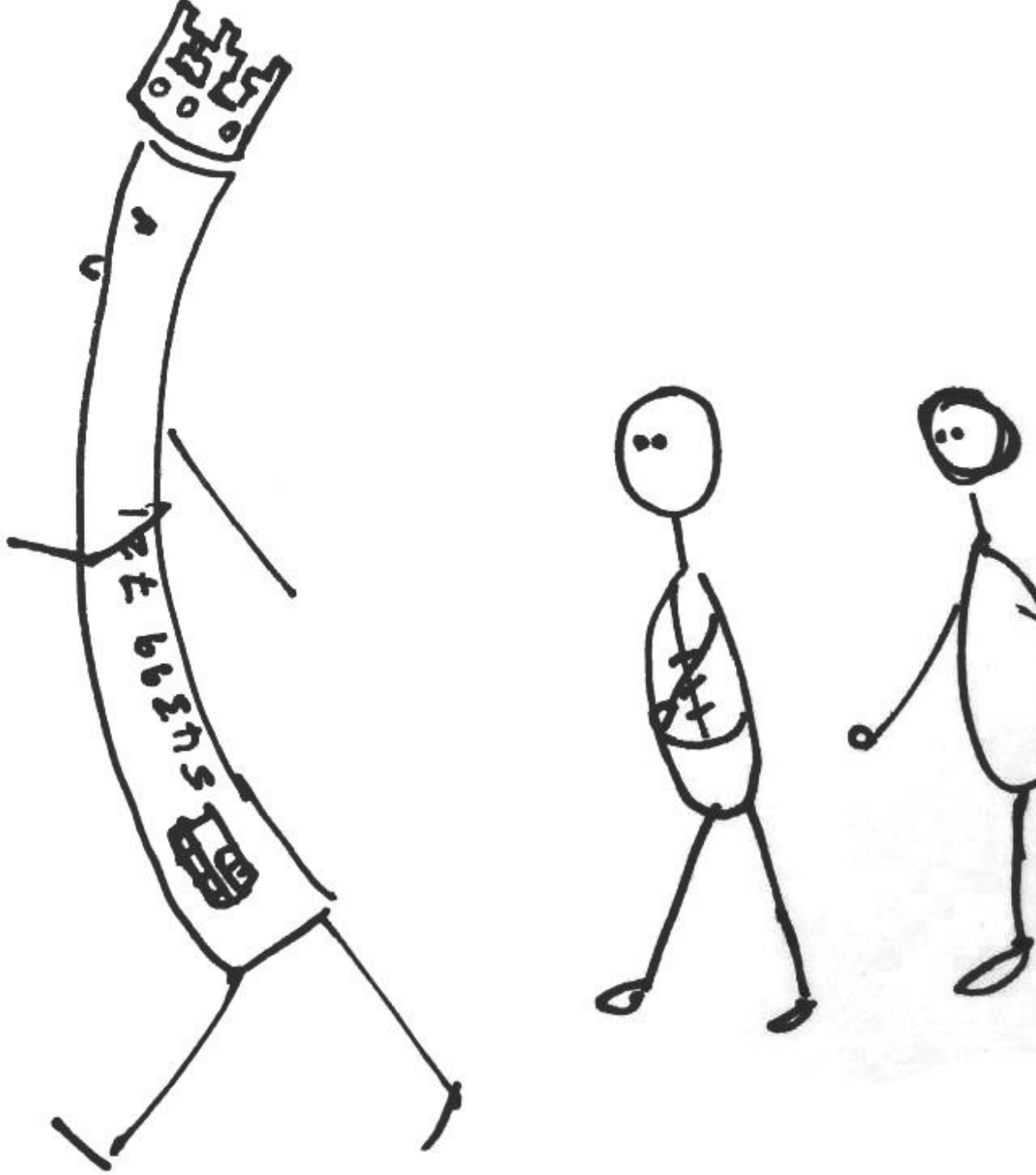
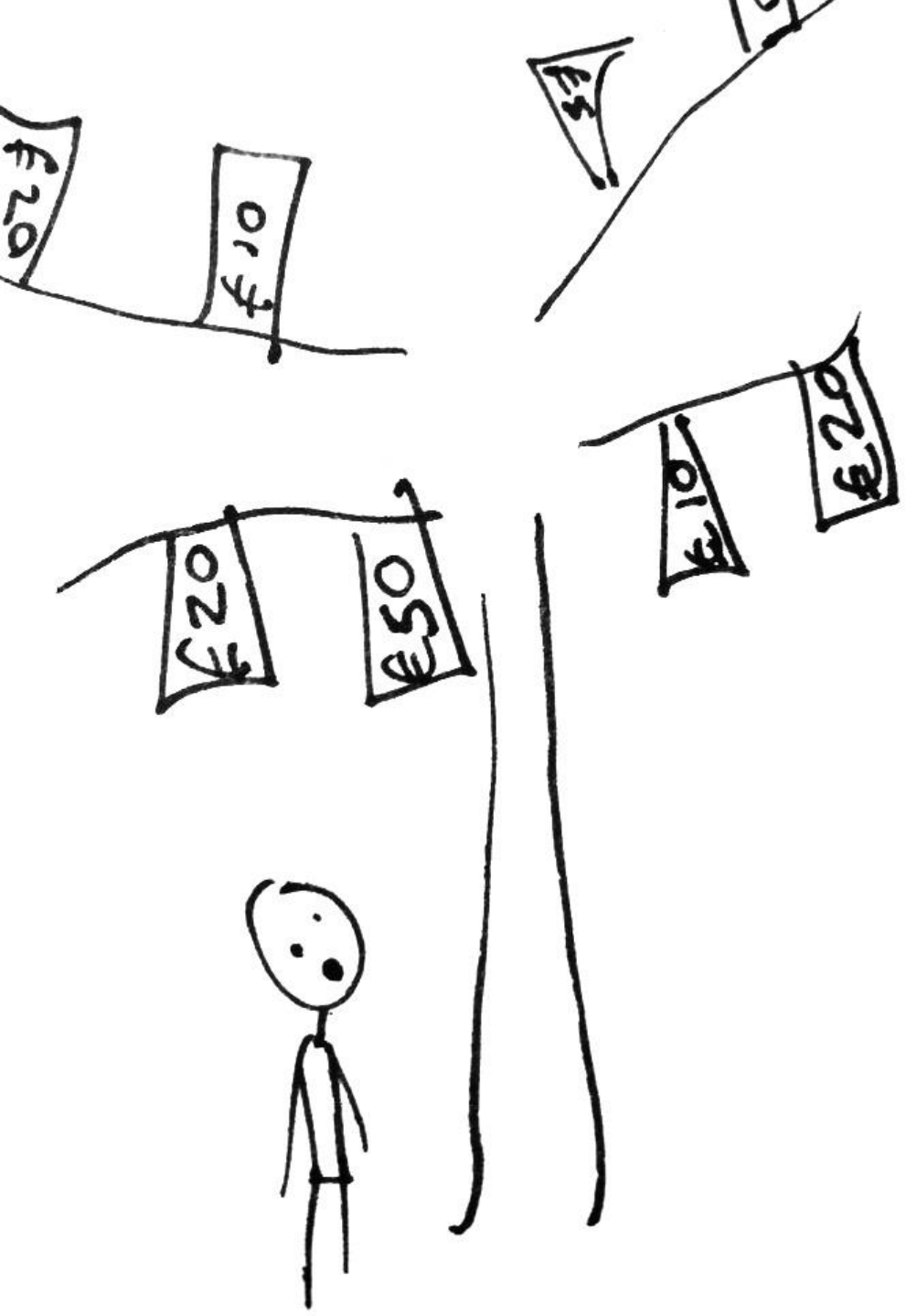


FIRST CONTACT:
New vulnerabilities in contactless payments

TO GOOD

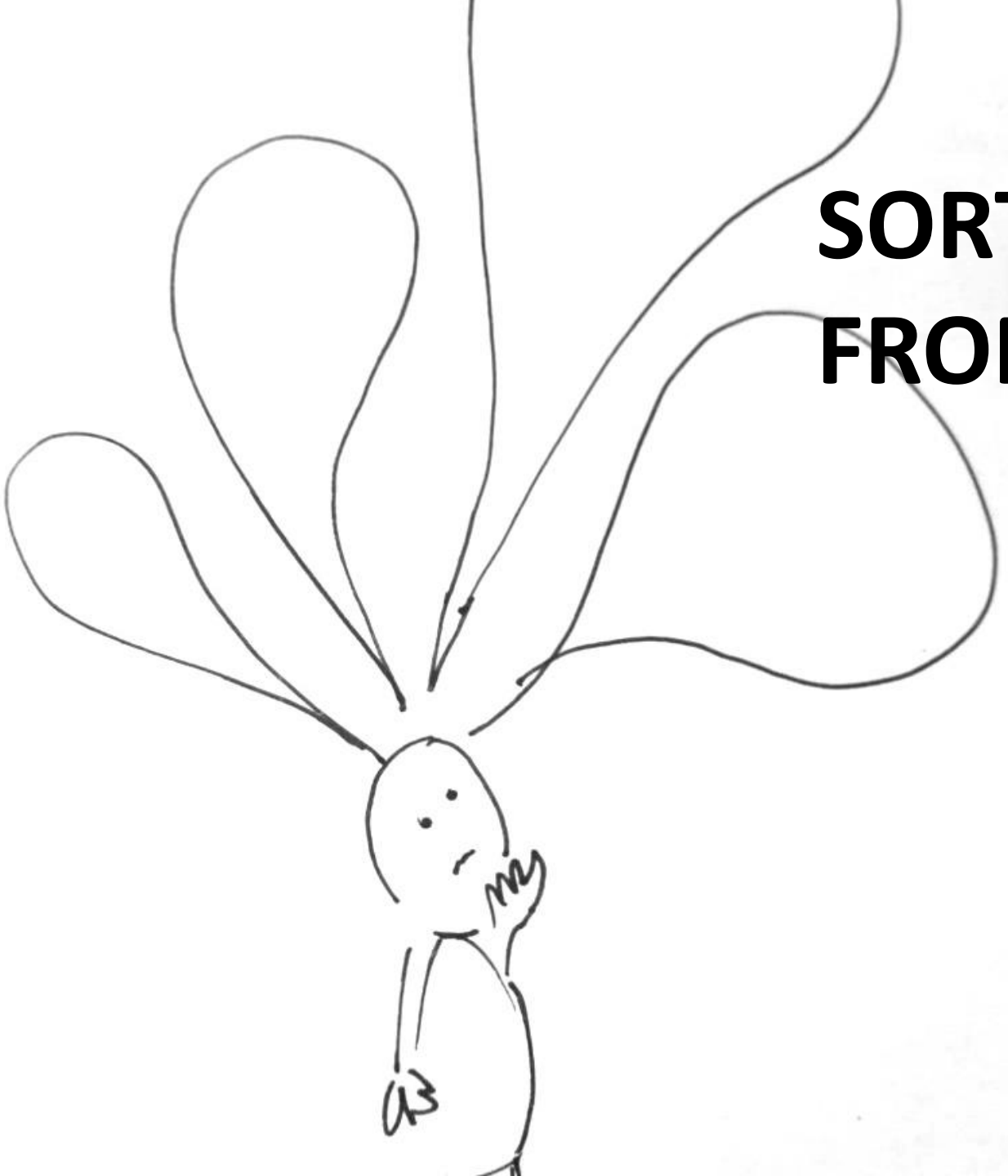
To be true?





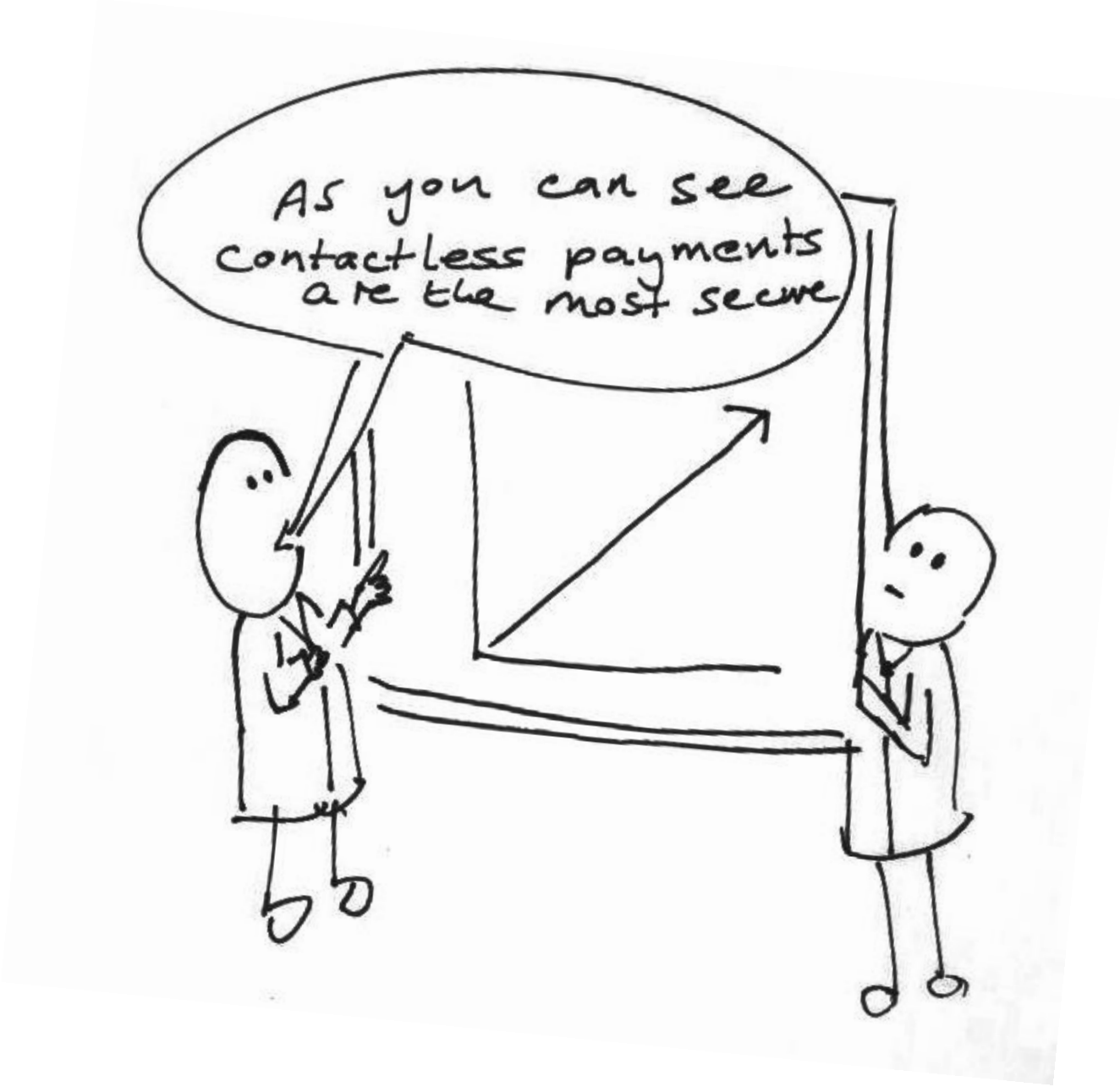
NEO BANKS

The big banking boom



SORT FACTS FROM FICTION

“I could accidently pay for someone else’s shopping”



WE TAKE SECURITY

~~At face value~~

HAS FRAUD REDUCED?

“Contactless payments have resulted in a fraud reduction”

Low fraud rates

While the use of contactless cards has increased rapidly, Visa's contactless fraud rate in Europe has declined by 40% between 2017 and 2018.[2] Specifically in the UK, a report by UK Finance found that fraud on

---

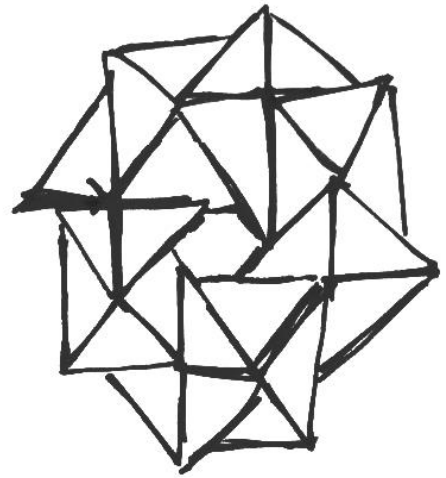
[1] Visa's Zero Liability Policy does not apply to Visa corporate or Visa purchasing card or account transactions. For specific restrictions, limitations and other details, please consult your card issuer.

[2] Visa in Europe data

[3] UK Finance, "2018 half year fraud update," Sept. 2018, Page 12, https://www.ukfinance.org.uk/wp-content/uploads/2018/09/2018-half-year-fraud-update-FINAL.pdf

Contactless fraud covers fraud on payments made by both contactless cards and mobile devices. Fraud on contactless cards and devices remains low with £8.4 million of losses during the first half of 2018, compared to spending of £31.9 billion over the same period.

Contactless fraud covers fraud on payments made by both contactless cards and mobile devices. Fraud on contactless cards and devices remains low with £8.4 million of losses during the first half of 2018, compared to spending of £31.9 billion over the same period.



UK
FINANCE

Data quietly released this week shows the instances of thefts relating to contactless cards doubled in just 10 months last year, according to Action Fraud, the national reporting centre for fraud and cybercrime.

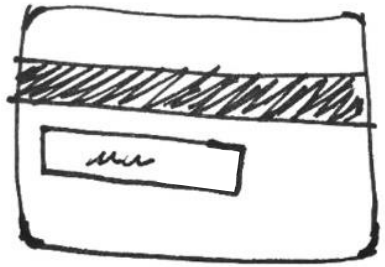
Up from 1,440 cases worth £711,000 over the same period in 2017 to around 2,740 cases worth almost £1.8m in 2018, the average amount stolen last year was more than £650. One case investigated by police reported a £400,000 loss after a card was used multiple times.

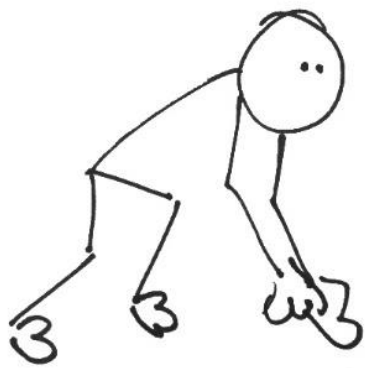
The 2018 cases, recorded between April 2017 and January 2018, represent more than half of all the reports of contactless-related fraud investigated by the City of London Police alone, which runs Action Fraud, since 2013.

Sharks and Tigers

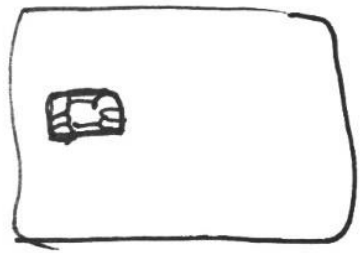
CONTACTLESS, A MODERN FORM OF PAYMENT?

1979

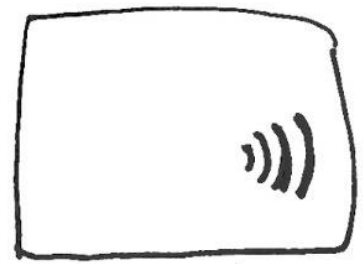


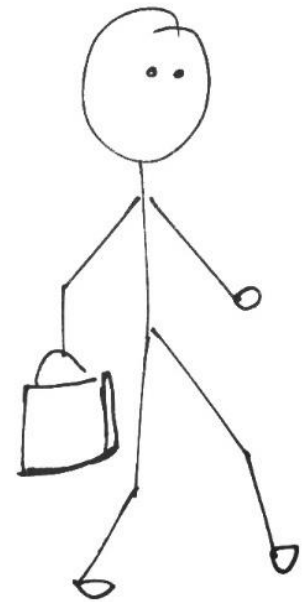


1996



2005

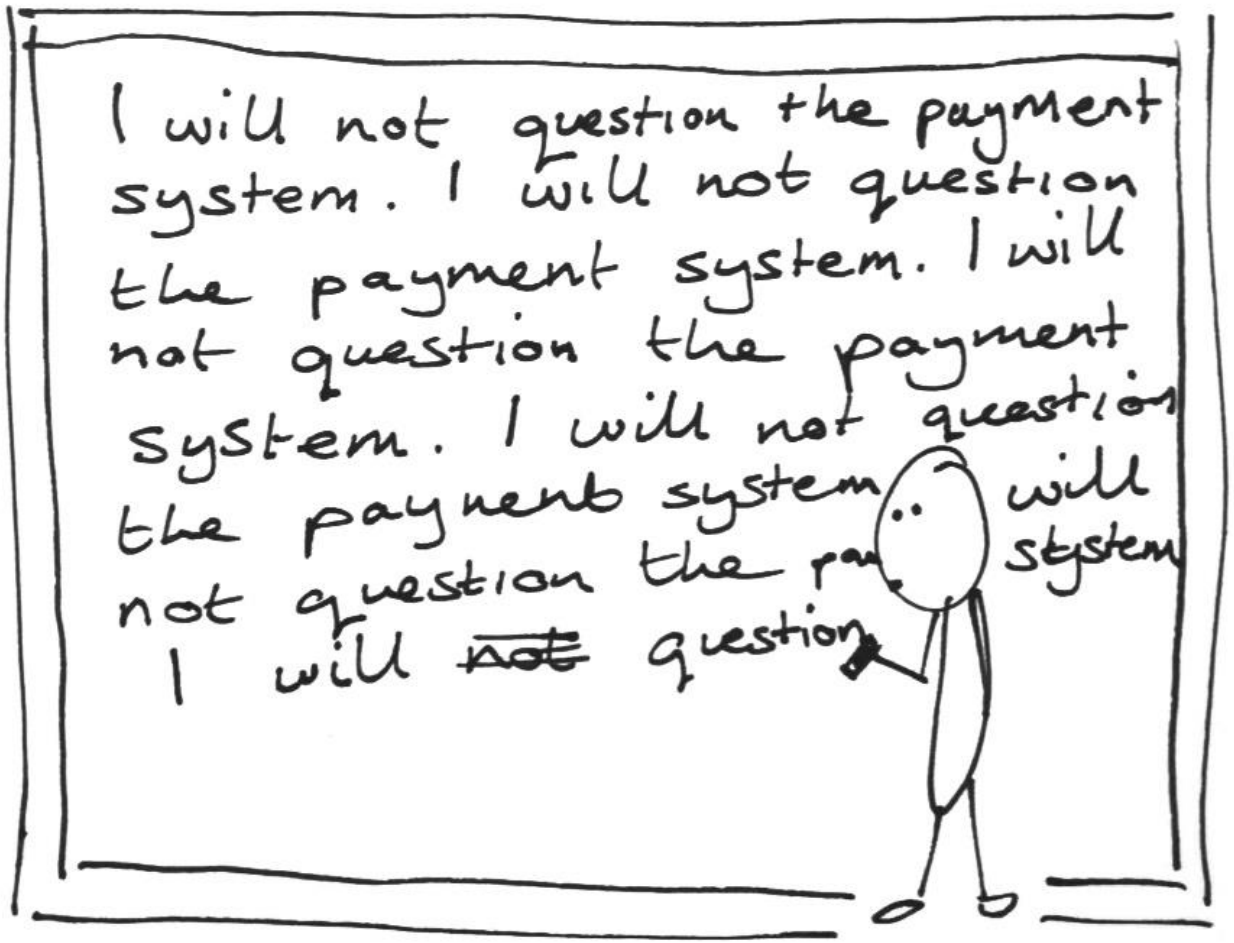




NFC is(n’t) different

- NFC includes legacy modes (magstripe) that CHIP didn’t.
- NFC uses the same key and same areas of memory on the CHIP as CHIP inserted.

ARE PAYMENTS STANDARDISED?




where can I find information on payments?


Ha Ha just go to the envco website there's over 700 pages of documents

EMV KERNELS

VISA

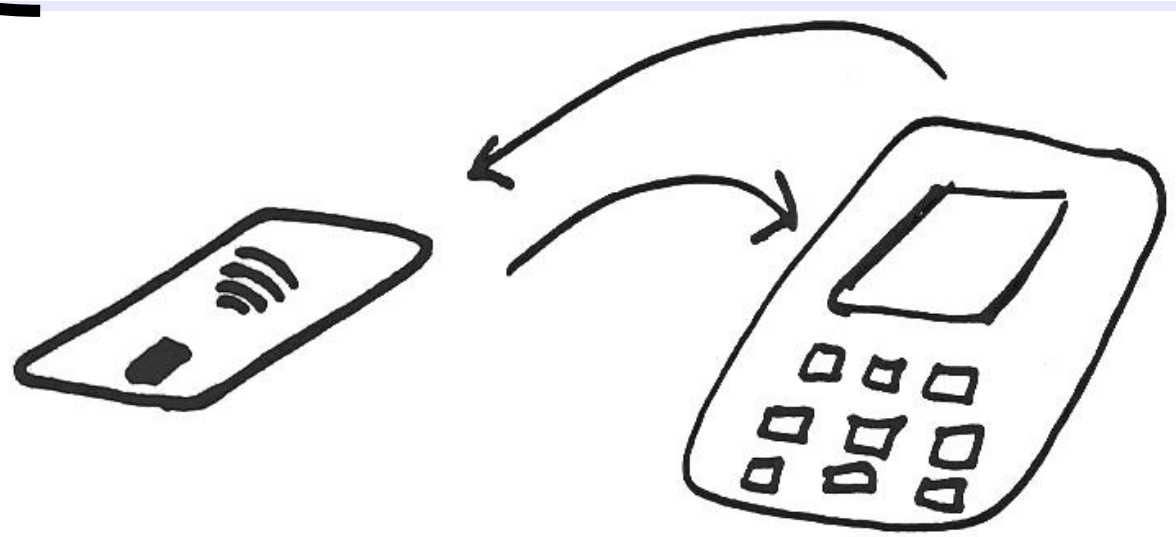
mastercard

VISA

FORMAT OF COMMUNICATION

APDU

```
6f 47 84 0e 32 50 41 59  2e 53 59 53 2e 44 44 46
30 31 a5 35 bf 0c 32 61  30 4f 07 a0 00 00 00 03
10 10 50 10 56 69 73 61  20 20 20 20 20 20 20 20
20 20 20 20 87 01 03 9f  0a 08 00 01 05 01 00 00
00 00 bf 63 04 df 20 01  80 90 00
```



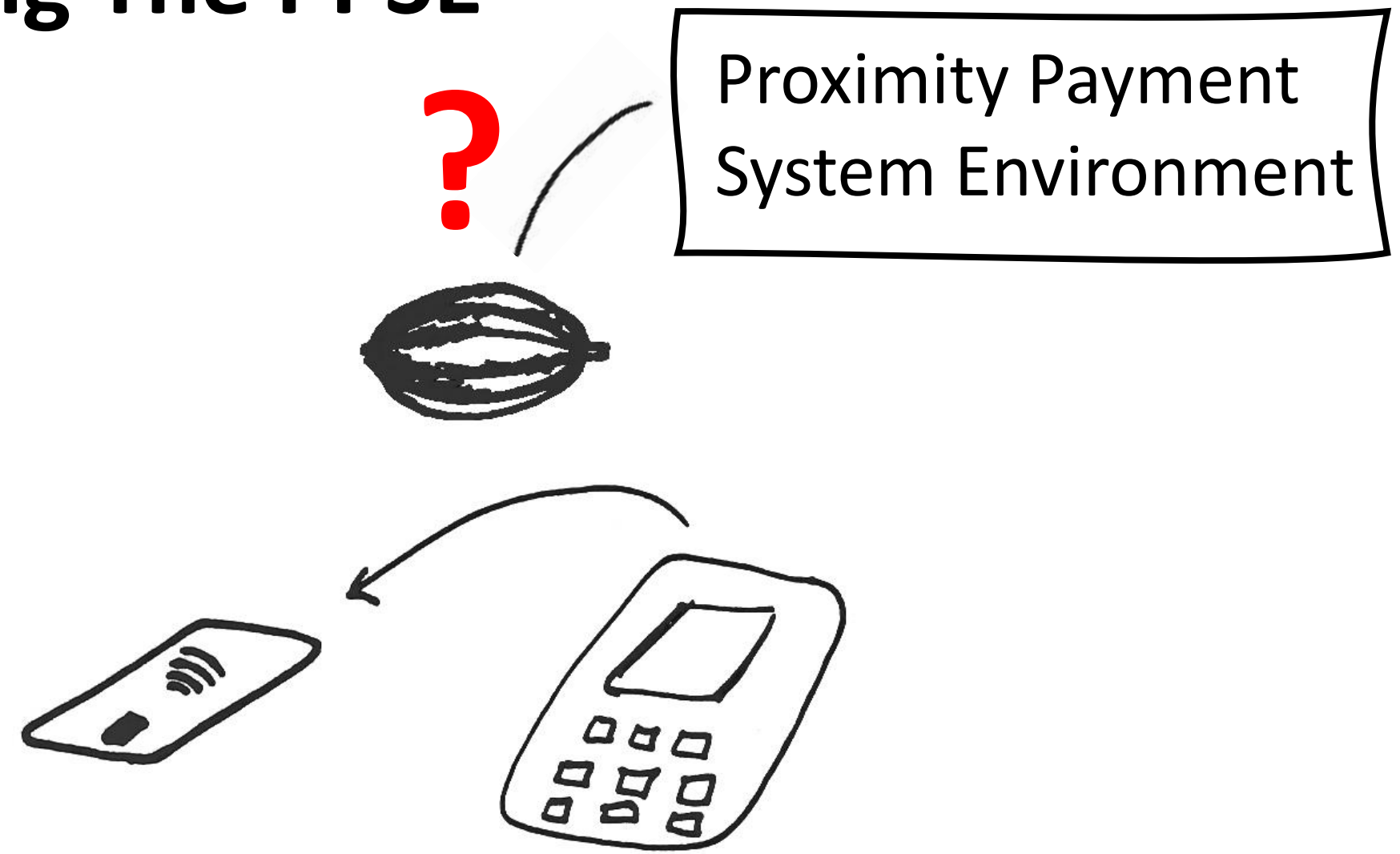
Value

2PAY.SYS.DDF

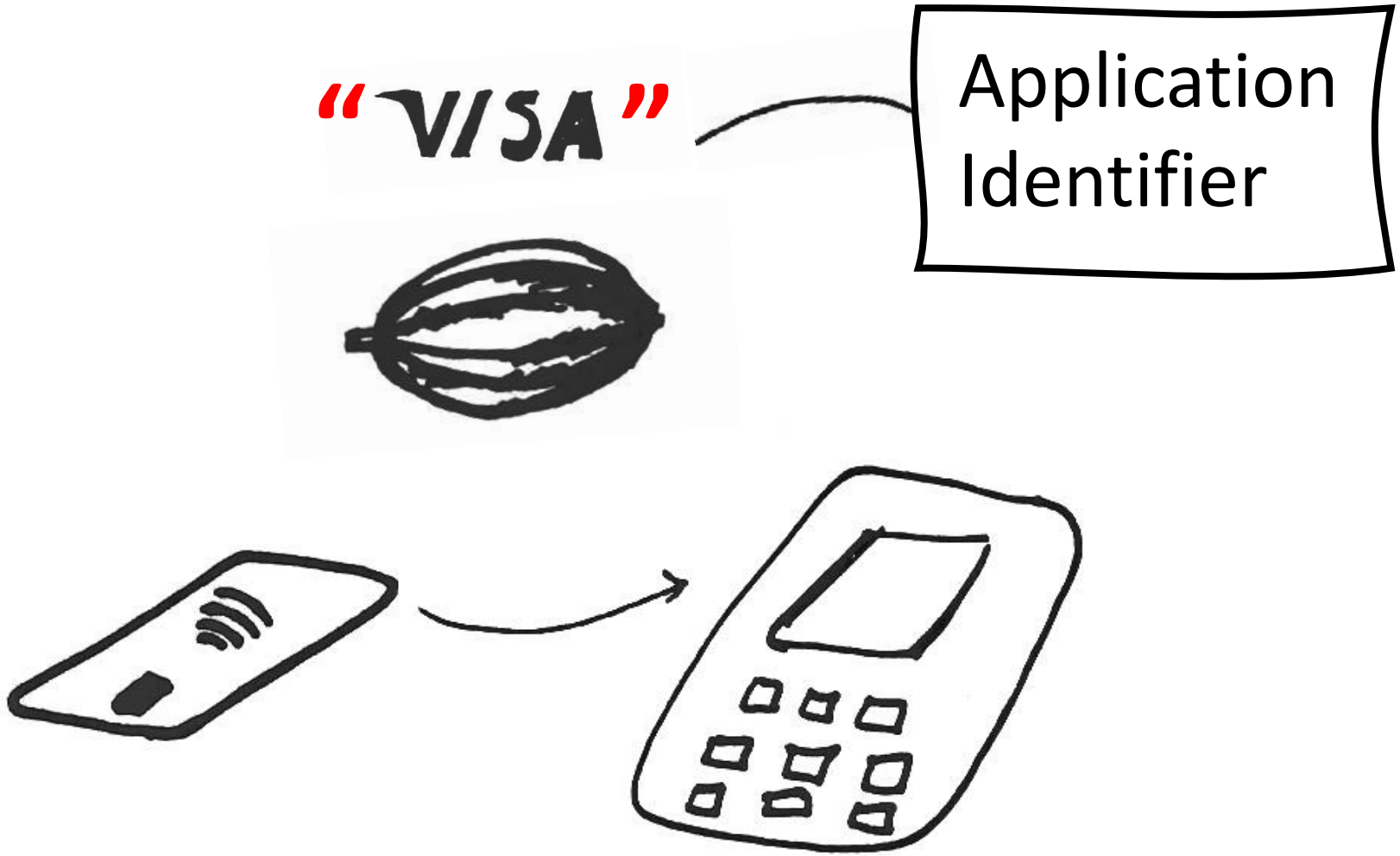
01

TLV = Tag Length Value

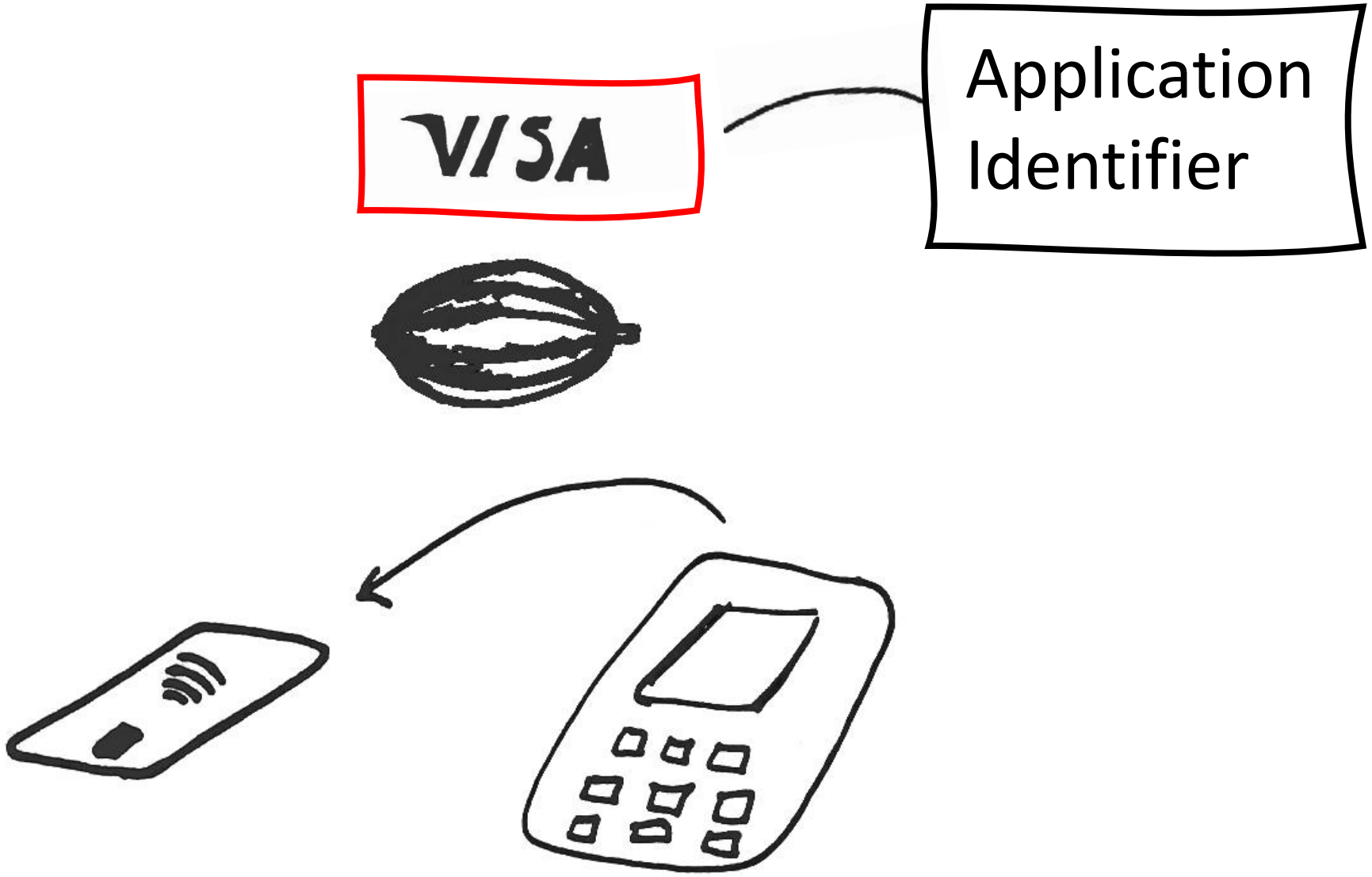
1. Reading The PPSE



2. Card responds with AID

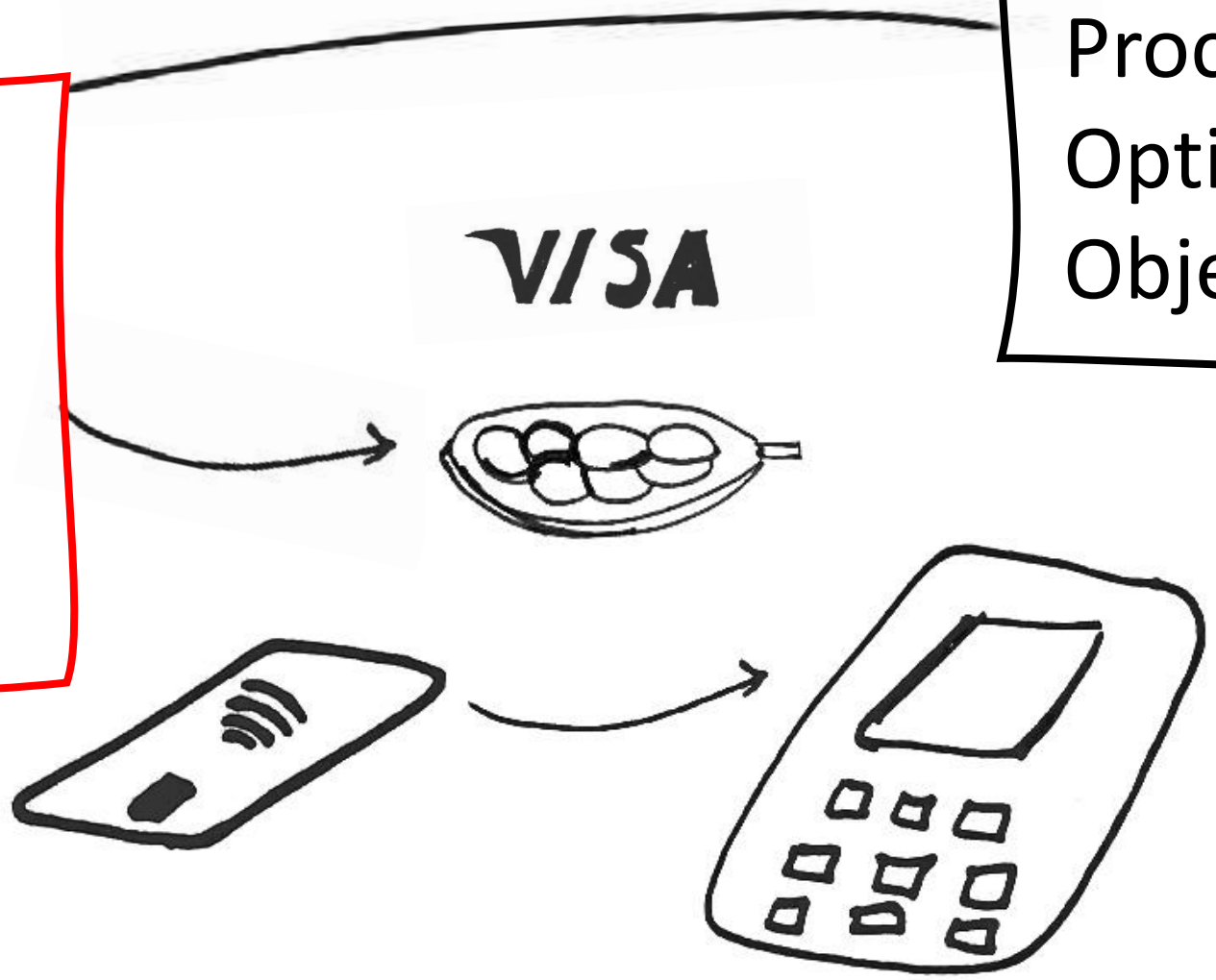


3. Terminal selects AID



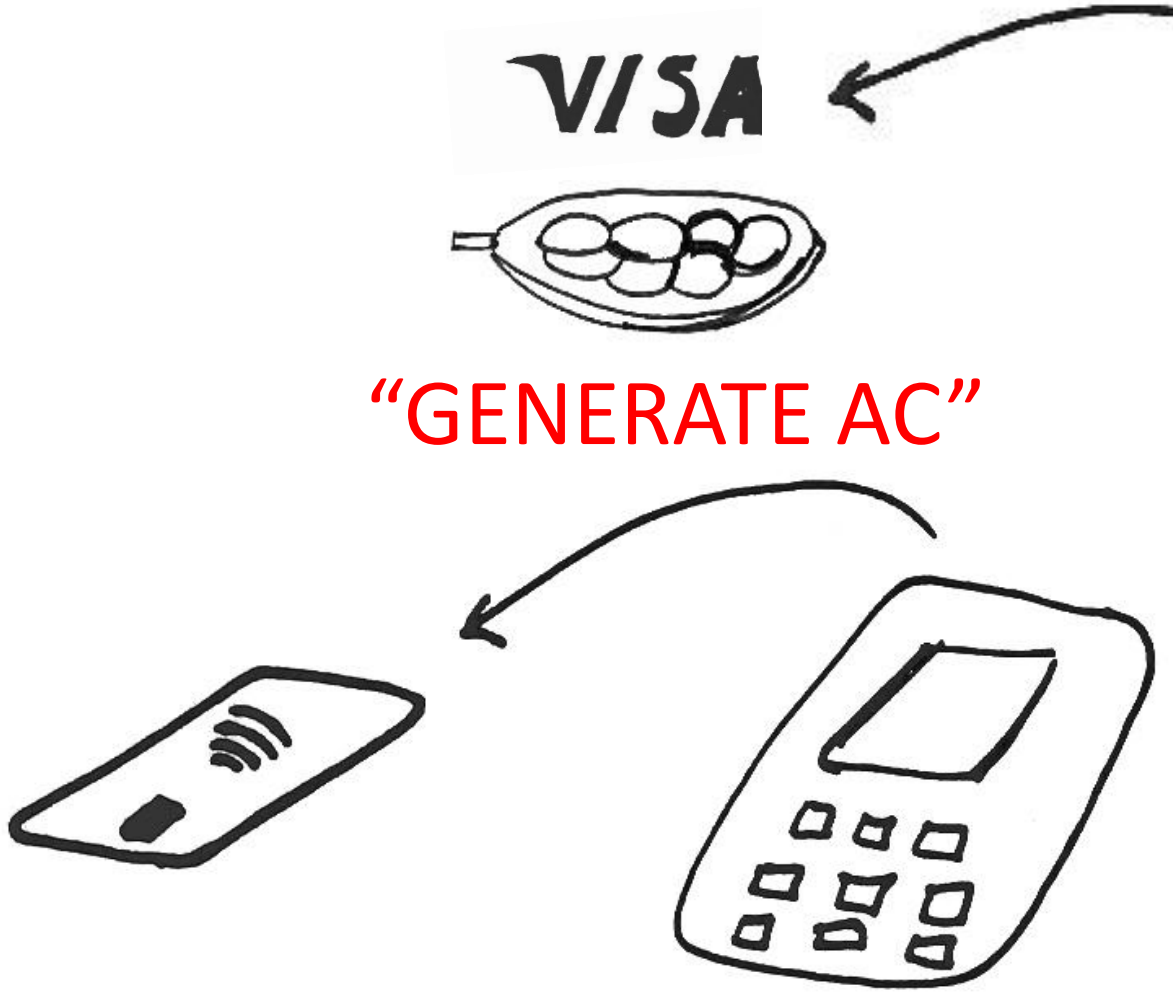
4. Card provides PDOL

Currency
Amount
UN
TTQ



Processing
Options Data
Object List

5. Terminal sends requested data



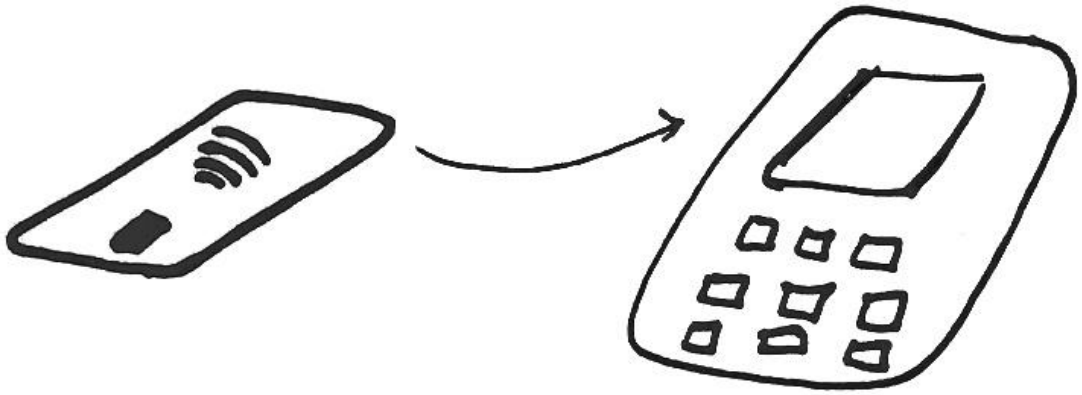
Currency
Amount
UN
TTQ

MSD?
EMV chip?
qVSDC?
CDCVM?

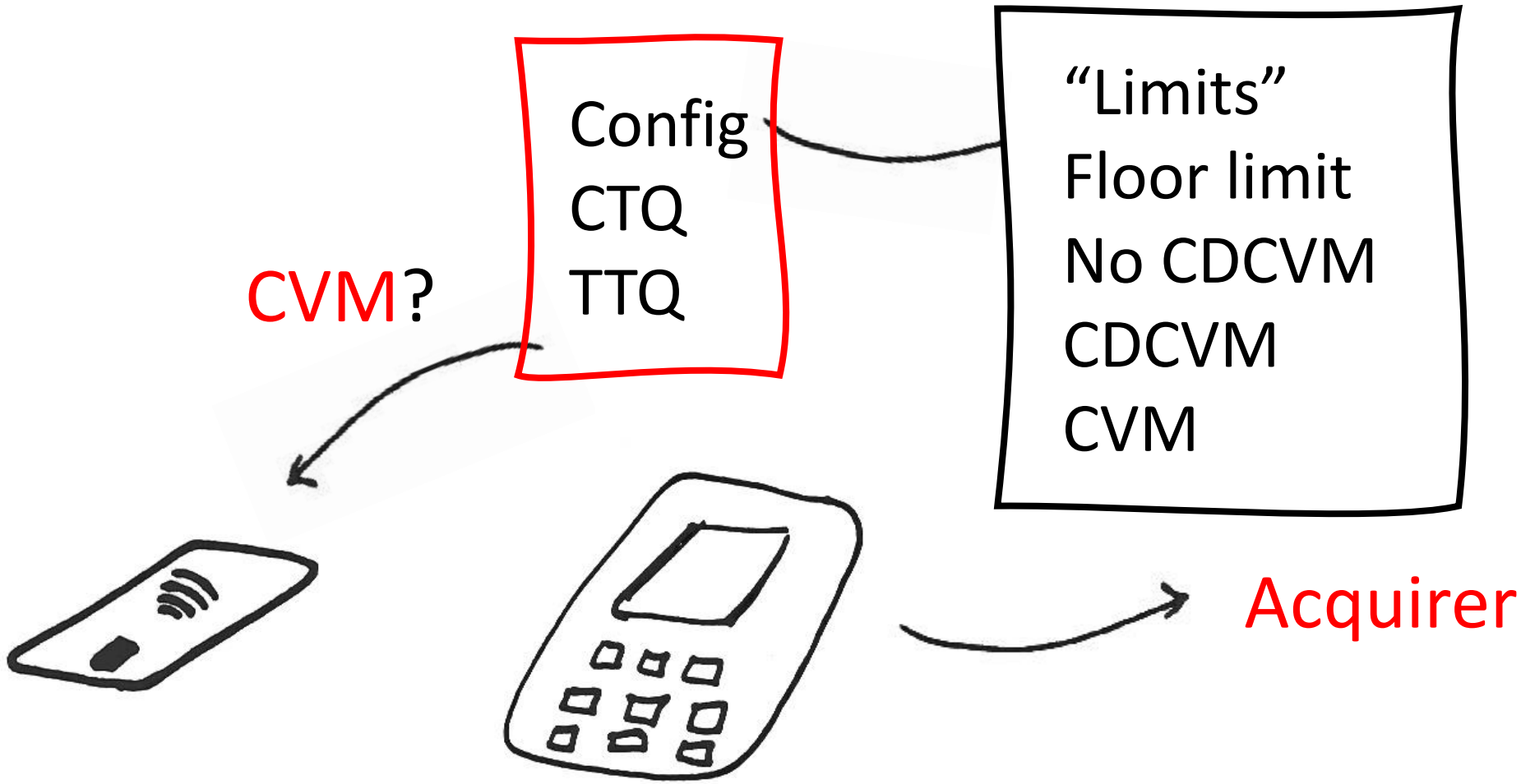
6. Card provides Application Cryptogram

ATC
Track2 Equiv
CTQ

Online Pin?
Signature?
CDCVM?



7. Terminal conducts risk analysis



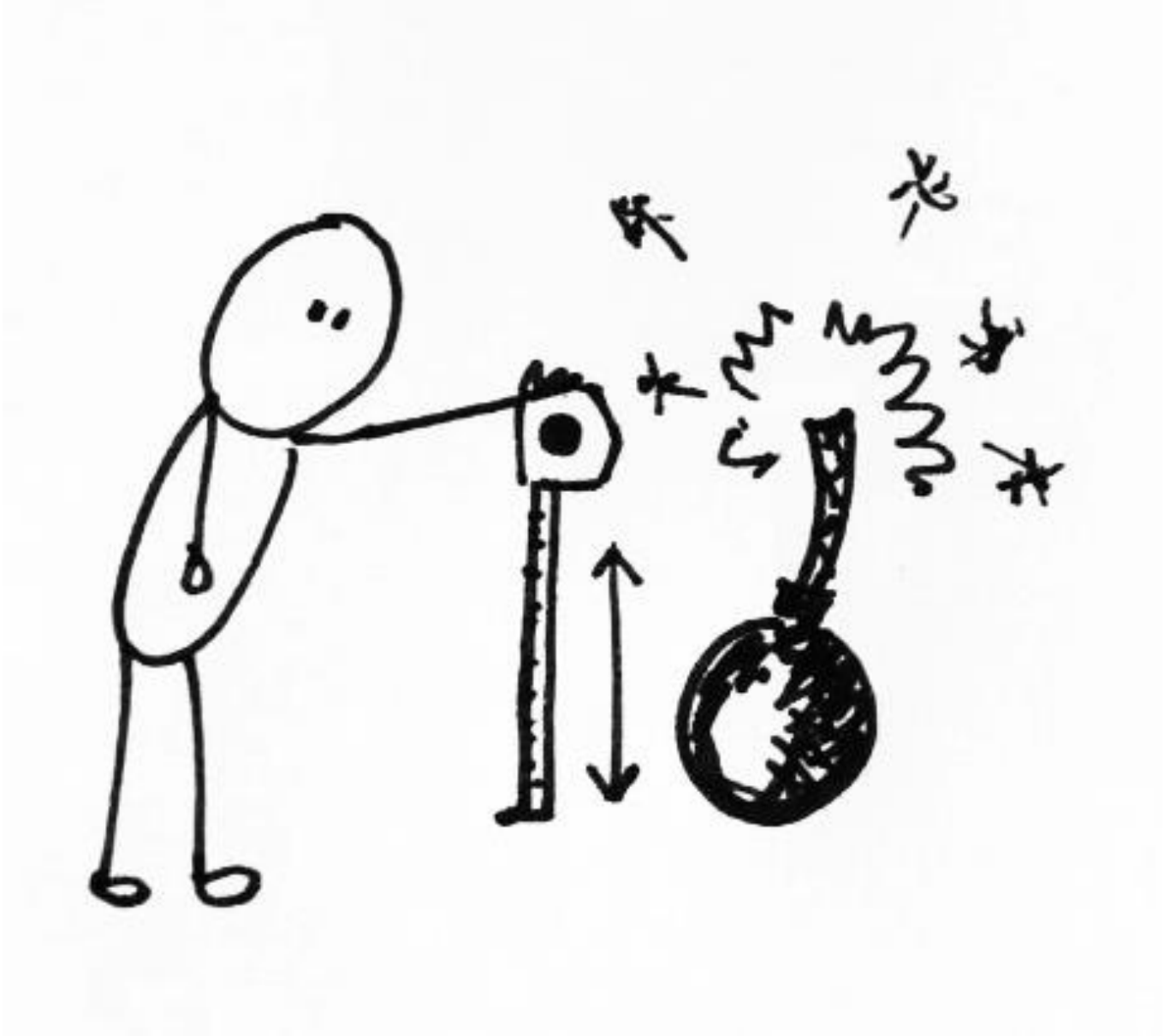
WHAT SECURITY MEASURES ARE IMPLEMENTED IN A TRANSACTION?

RISK ANALYSIS

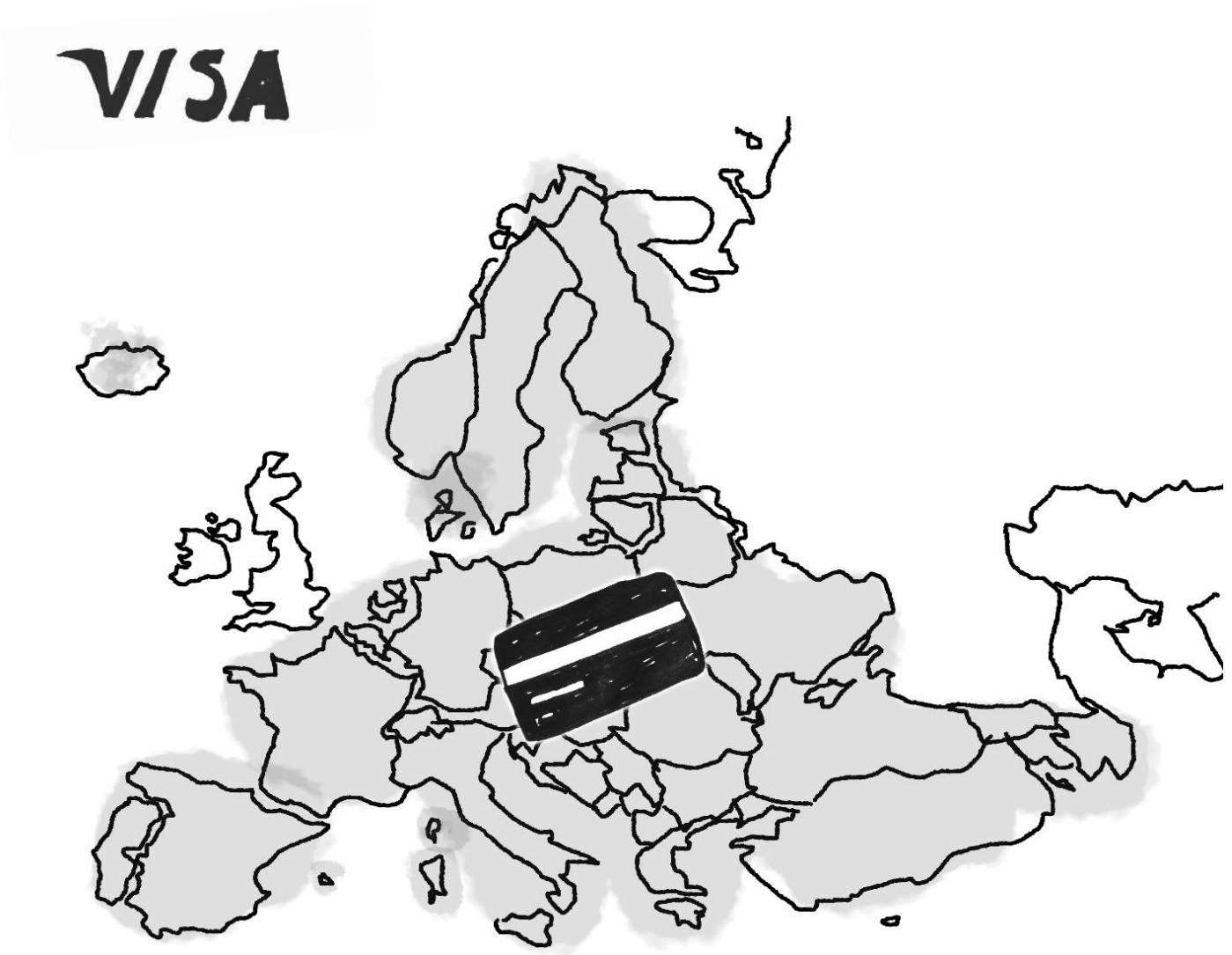
- Card authentication
- Transaction authorisation (cryptogram)
- Cardholder verification (CVM)

  Tap & Go limits

  - regulated by country
  - set up on the terminal
  - are not mandatory

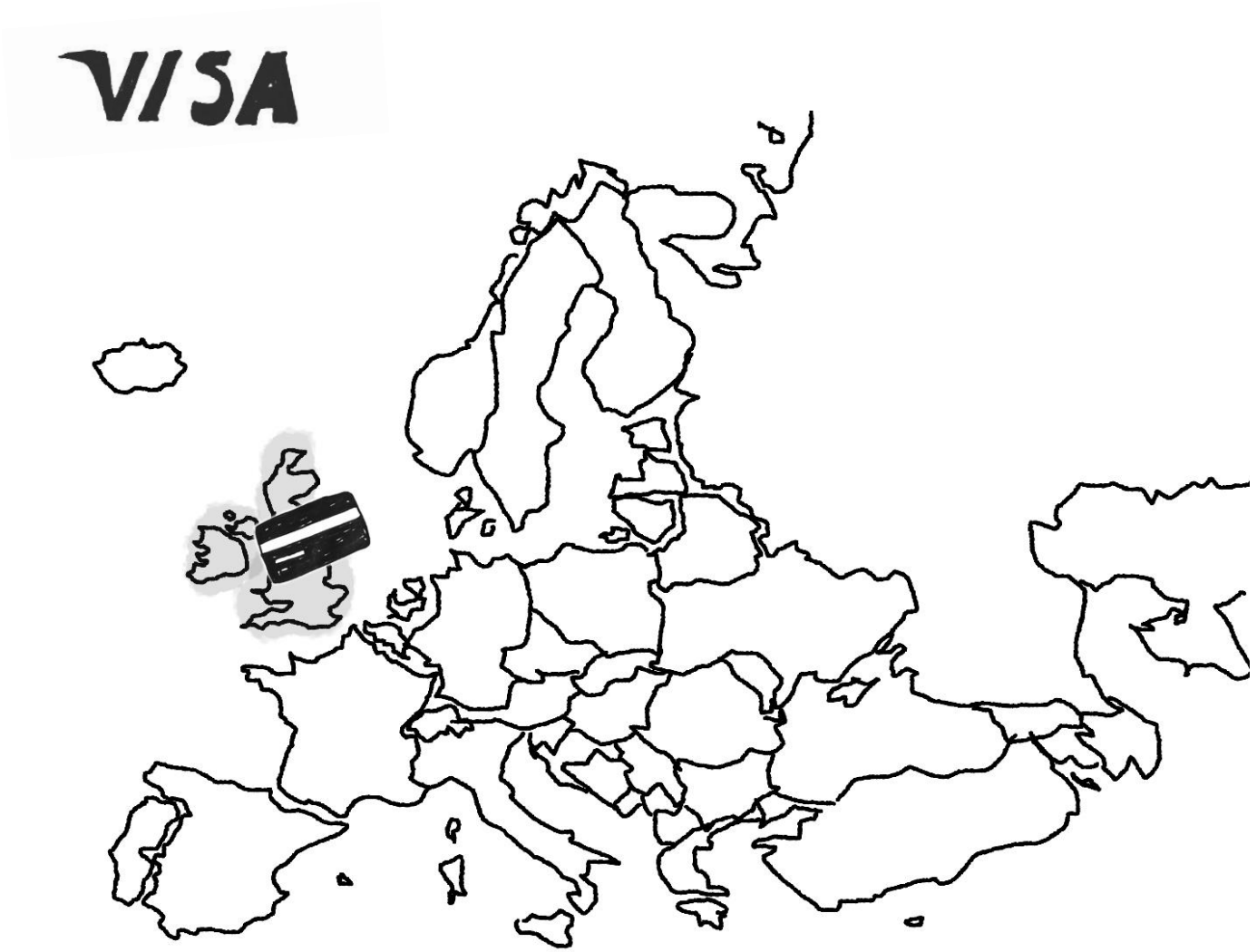


HOW “SOFT LIMITS” ARE IMPLEMENTED



HOW “HARD LIMITS” ARE IMPLEMENTED

UK VISA cards will ask to insert the chip if CVM is required



HOW “SOFT LIMITS” ARE IMPLEMENTED

3 different types of limits

on the terminal

HOW “HARD LIMITS” ARE IMPLEMENTED

VISA HAS A VULNERABILITY

C.2 Cryptogram Version Number 17('11')

Table C-1: Data Elements included in Cryptogram Version Number 17

Tag	Data Element
'9F02'	Amount, Authorized
'9F37'	Unpredictable Number
'9F36'	Application Transaction Counter (ATC)
'9F10'	Issuer Application Data (IAD) Byte 5

WHERE IS THE VULNERABILITY?

No currency/date

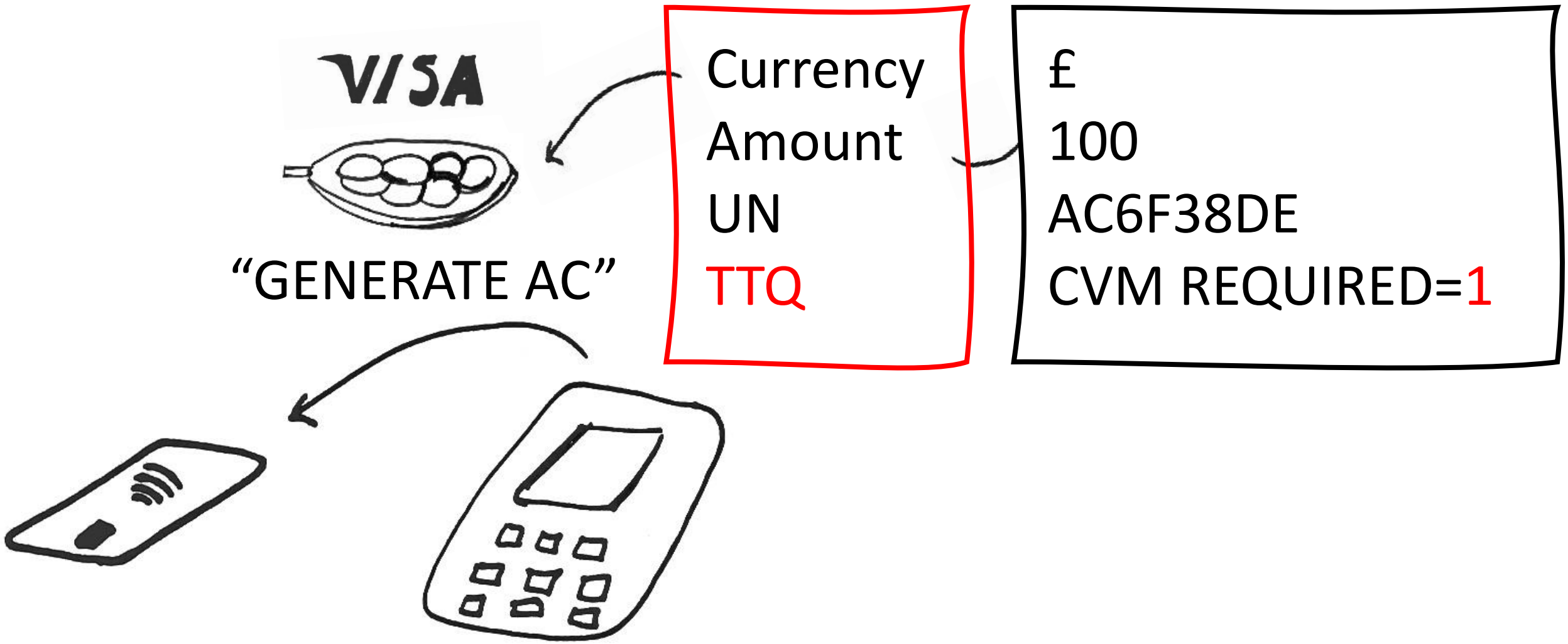
! No CTQ/TTQ

C.2 Cryptogram Version Number 17('11')

Table C-1: Data Elements included in Cryptogram Version Number 17

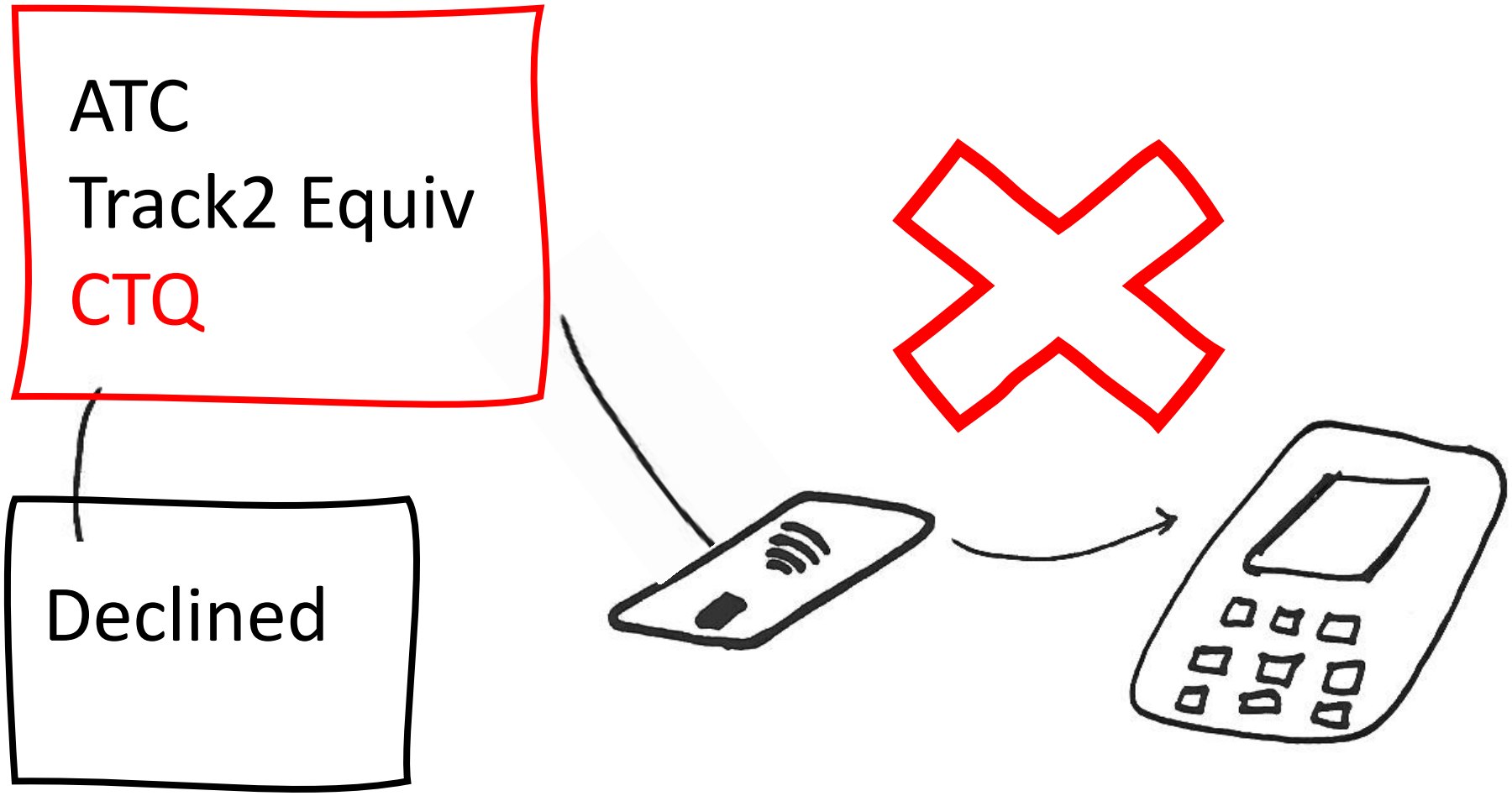
Tag	Data Element
'9F02'	Amount, Authorized
'9F37'	Unpredictable Number
'9F36'	Application Transaction Counter (ATC)
'9F10'	Issuer Application Data (IAD) Byte 5

5. Terminal sends requested data



Declines Transaction

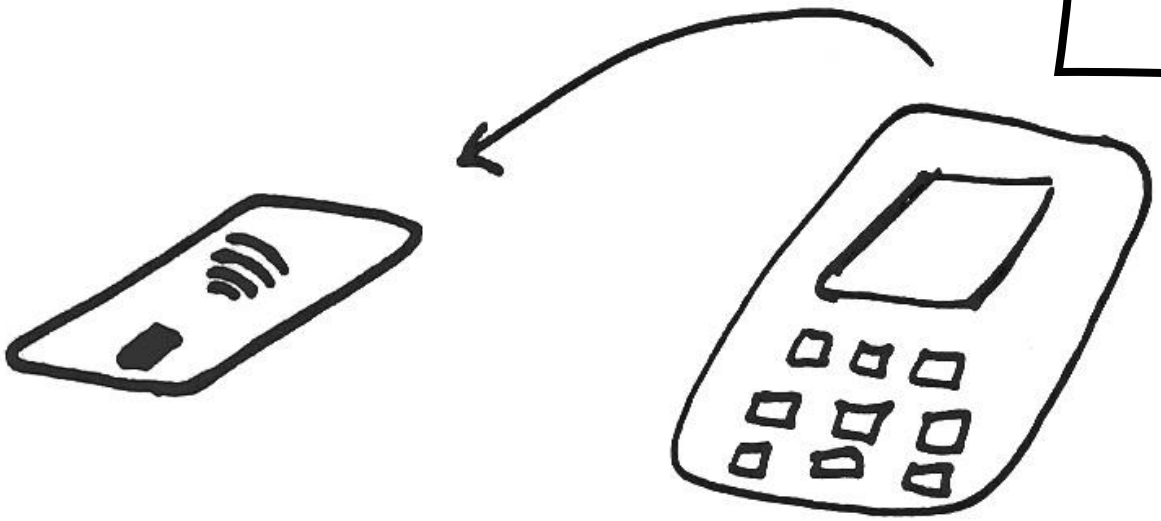
6. Card ~~provides Application Cryptogram~~



5. Terminal sends requested data

"GENERATE AC"

Currency	£
Amount	100
UN	1203946
TTQ	CVM REQUIRED=1

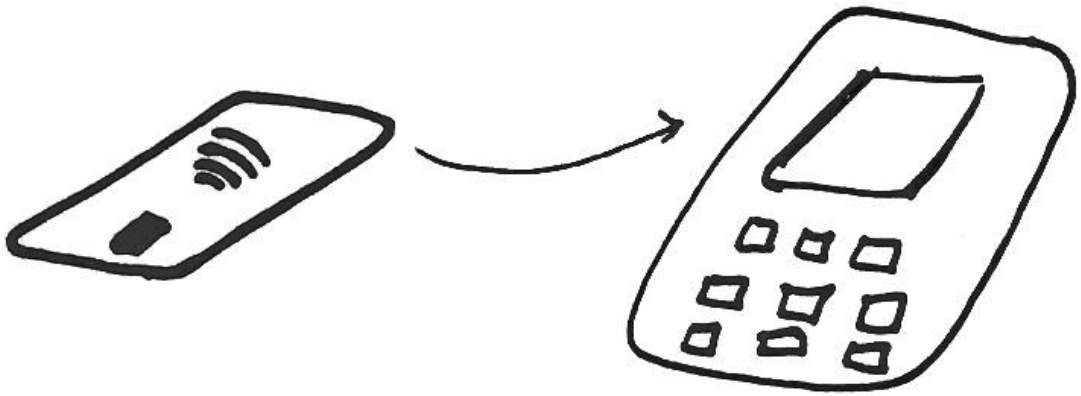


Change 1 to 0

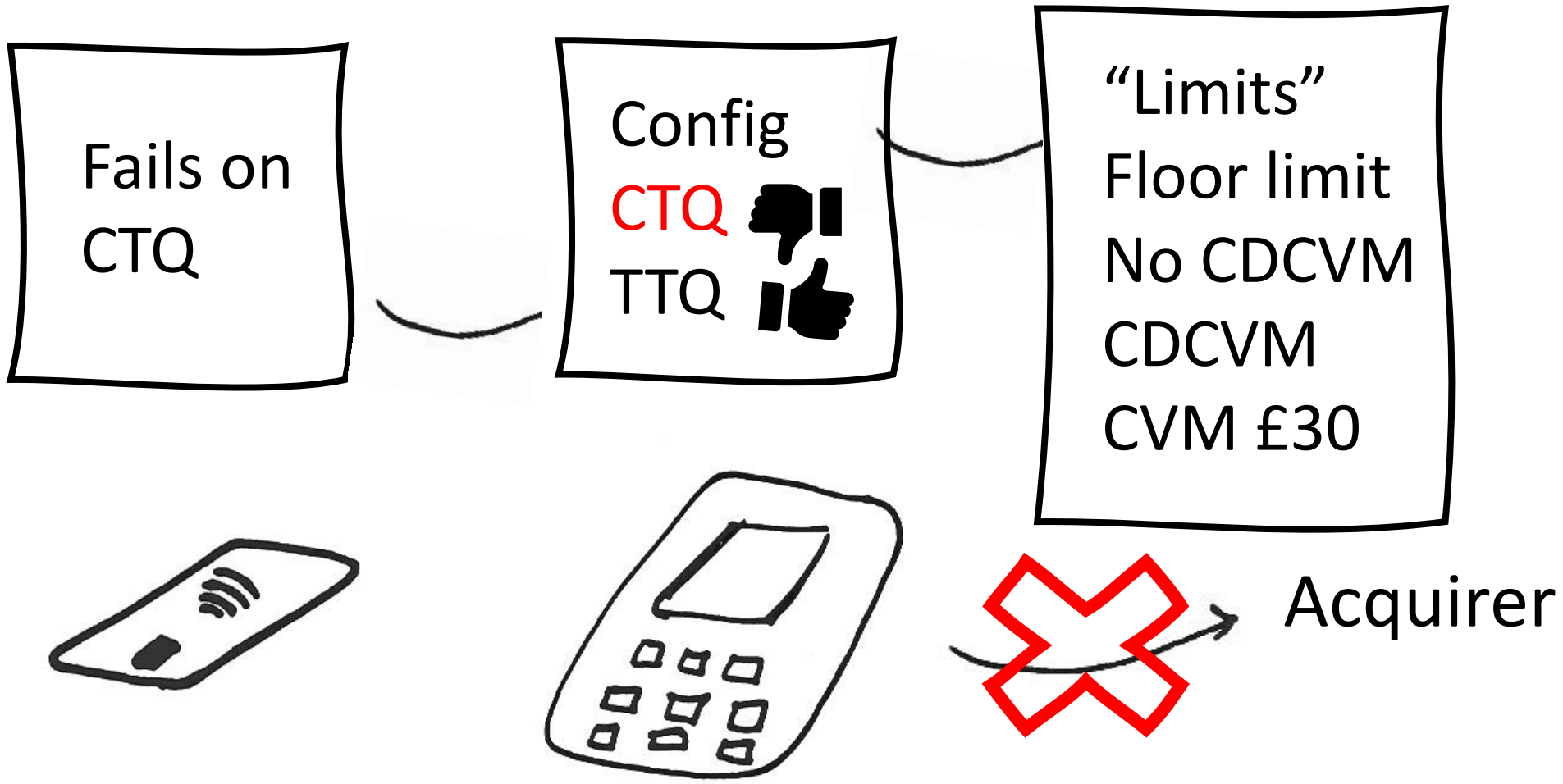
6. Card provides Application Cryptogram

ATC
Track2 Equiv
CTQ

Cryptogram is sent to terminal!



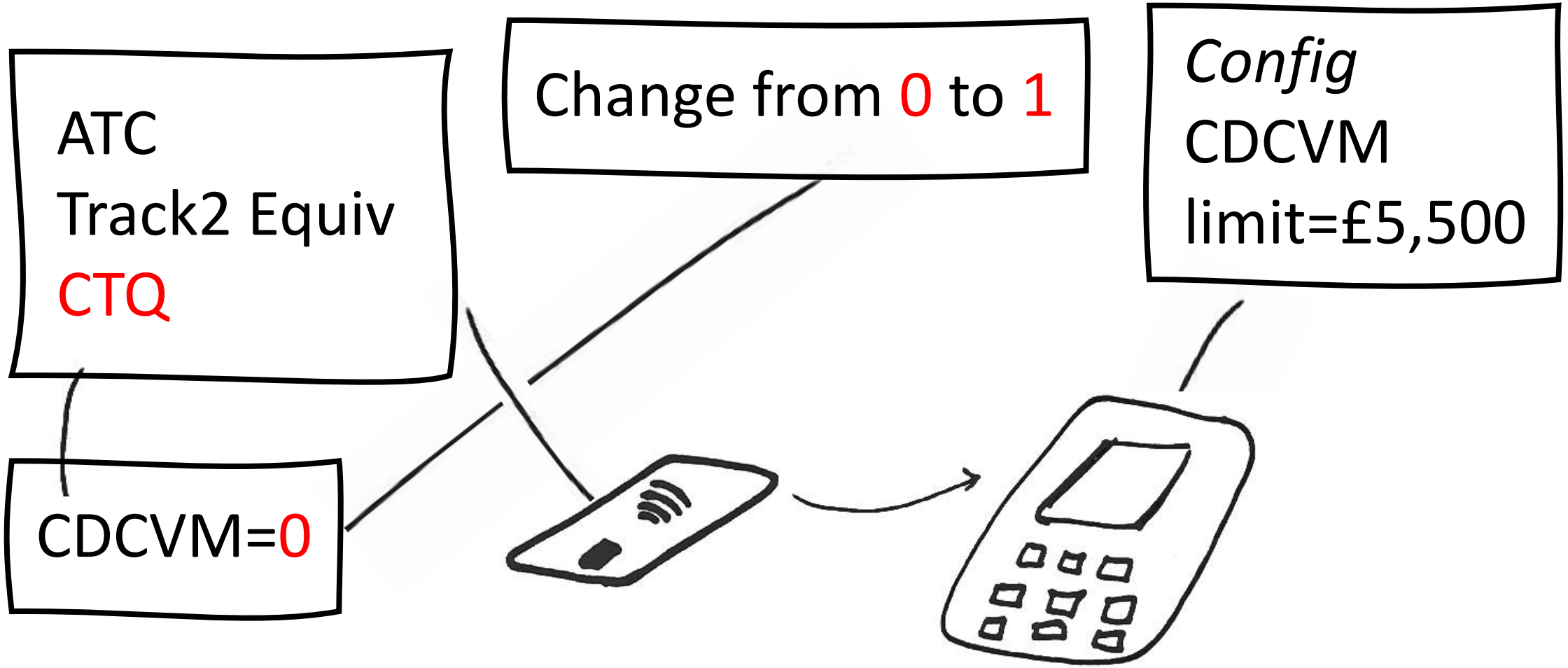
7. Terminal conducts risk analysis



CDCVM – CONSUMER DEVICE CVM

- Introduced with Apple Pay
- Represents the idea of CVM
- Fingerprint or PIN
- Much higher than Tap & Go limits (£5,500)

6. Card provides Application Cryptogram



1. Change TTQ “CVM Required” value from 1 to 0

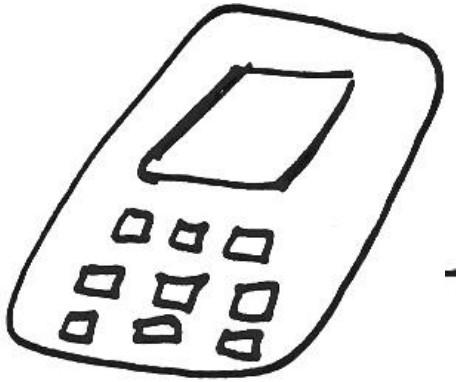
Currency
Amount
UN
TTQ

CVM REQUIRED=0

2. Change CTQ “CDCVM Performed” value from 0 to 1

ATC
Track2 Equiv
CTQ

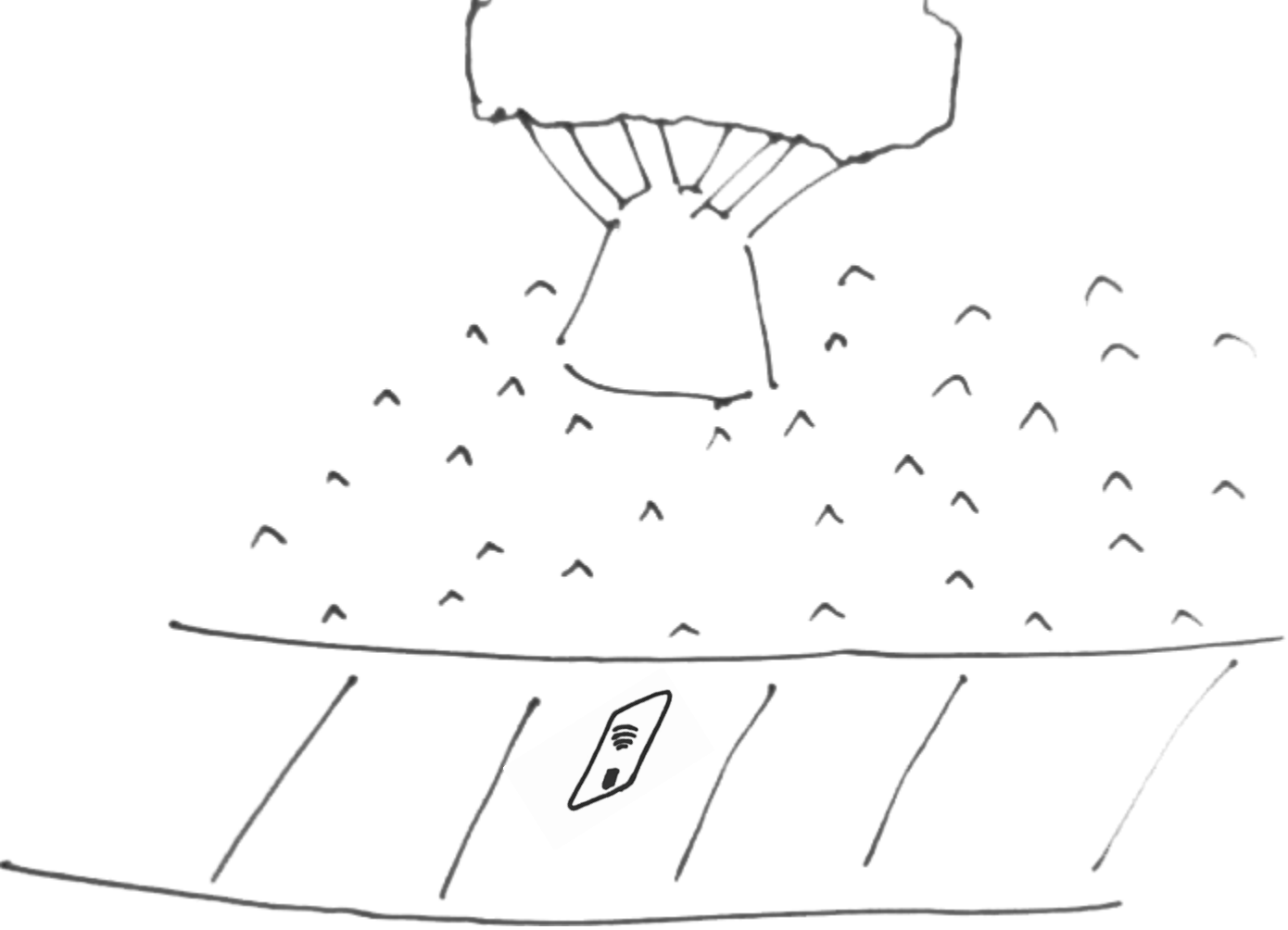
CDCVM=1



Acquirer


logitech
Insert card
NFC
logitech


logitech
Insert card



UK
FINANCE

VALUE - £95,000,000

VOLUME - 434,991

HOW MANY ARE AFFECTED?

All VISA cards
all cryptograms
are affected

12 VISA cards
UK, EU, US, Asia

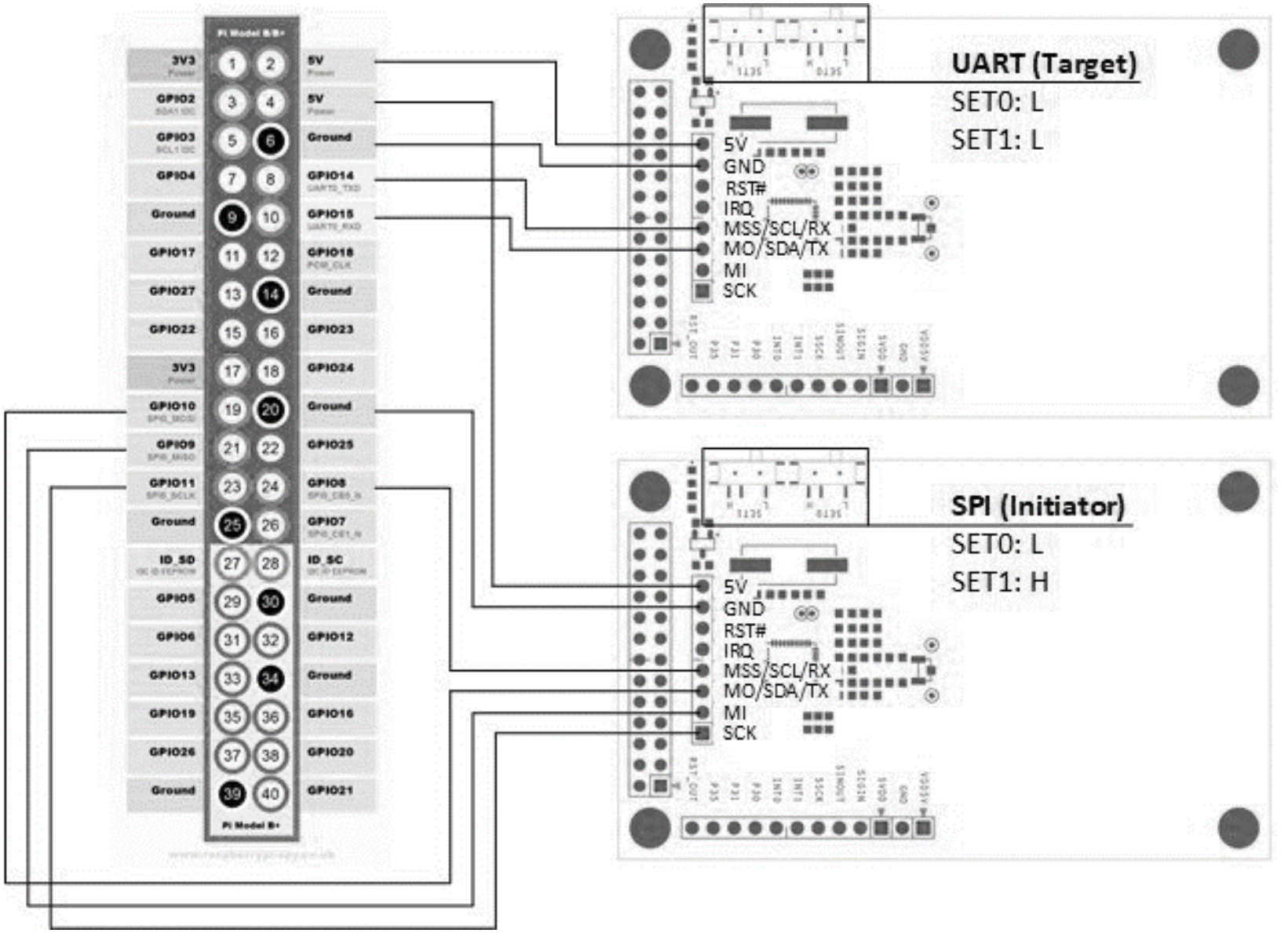
Only 2 banks
blocked £31
transactions*

* can be bypassed

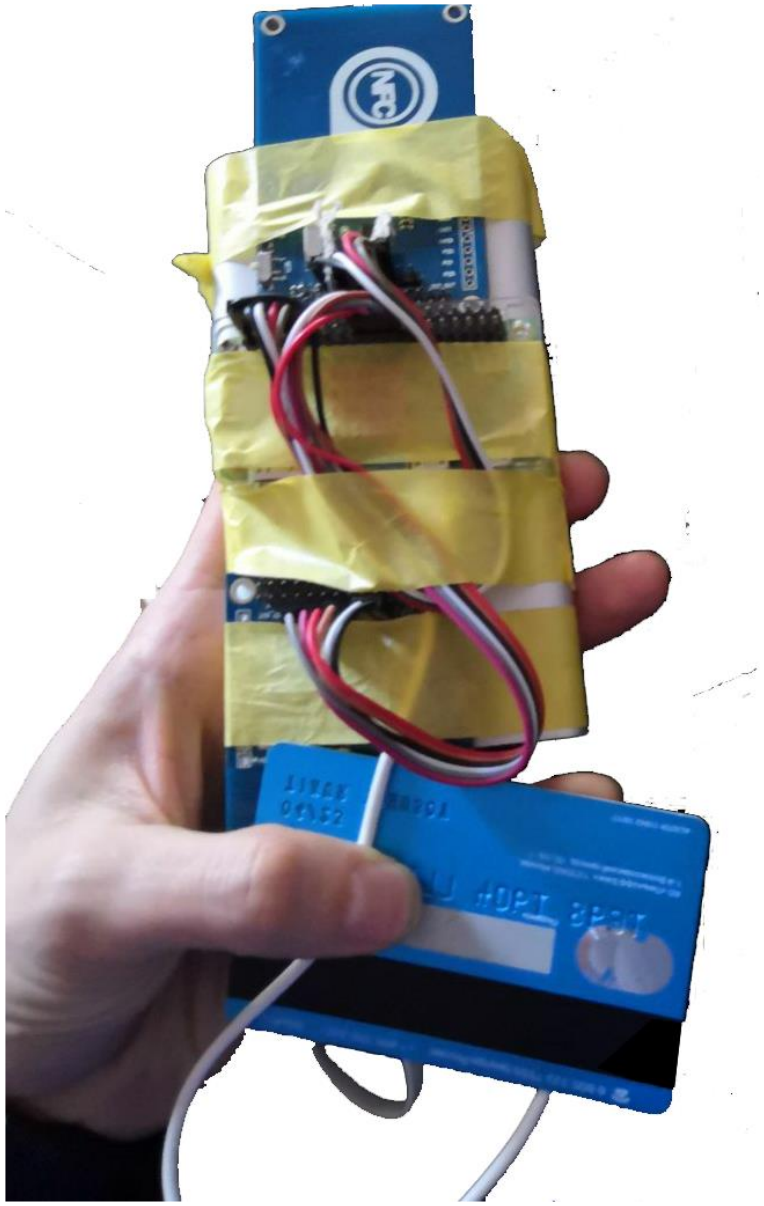
Min - £31
Max - £100

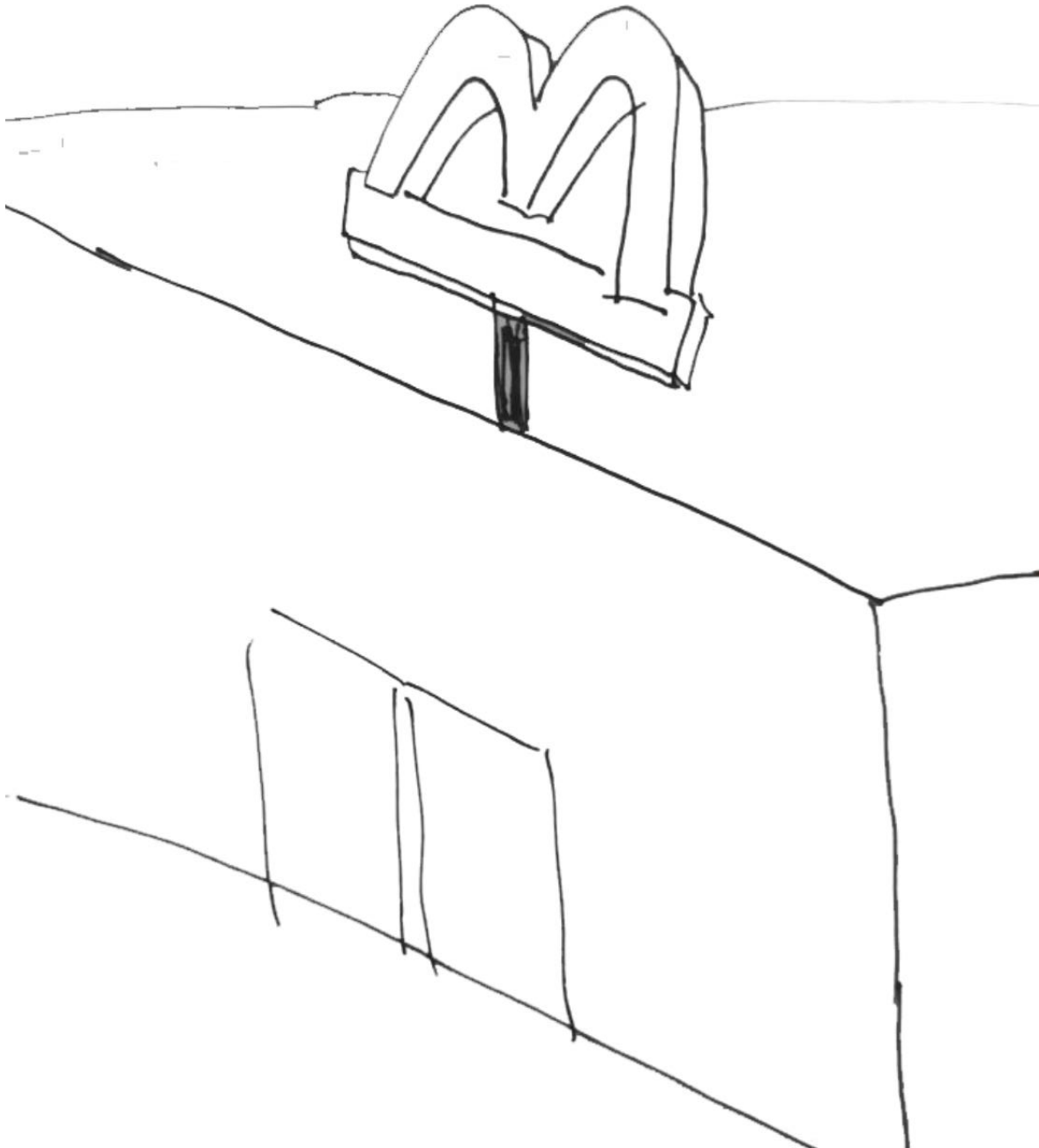
Tested in multiple places

Raspberry PI

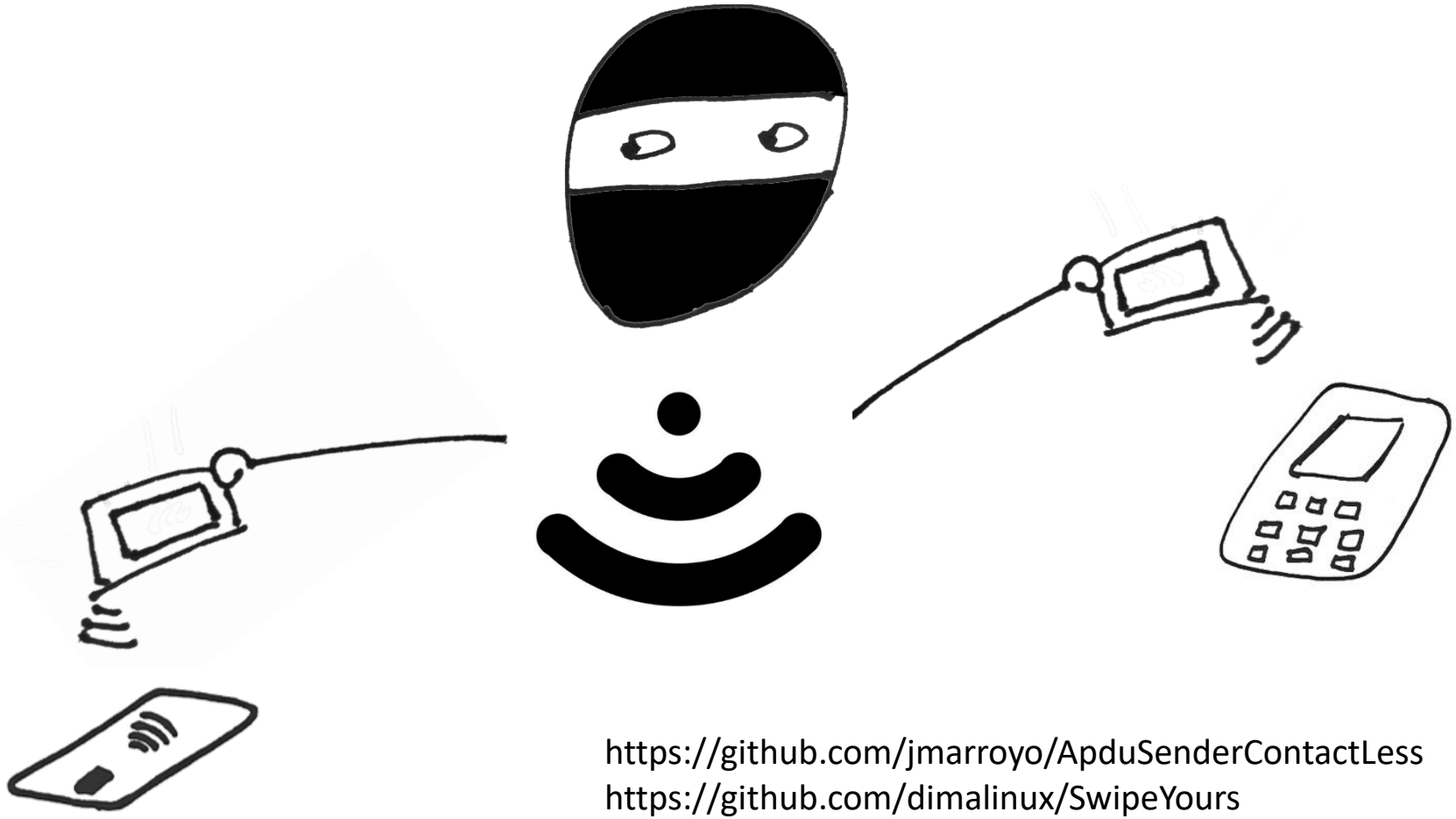


PN532





MITM PROXY FOR STEALTH

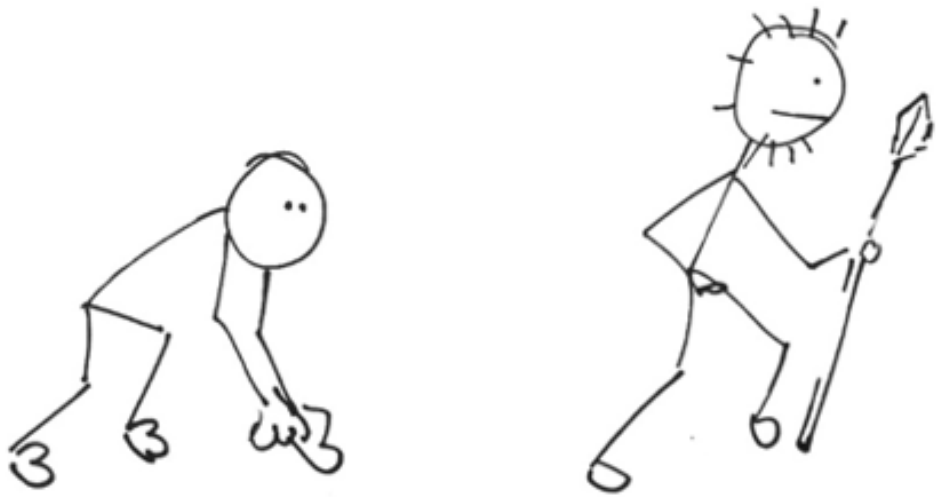


https://github.com/jmarroyo/ApduSenderContactLess
https://github.com/dimalinux/SwipeYours

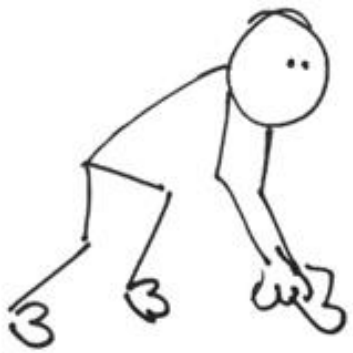
WHY IS ONLY VISA AFFECTED?

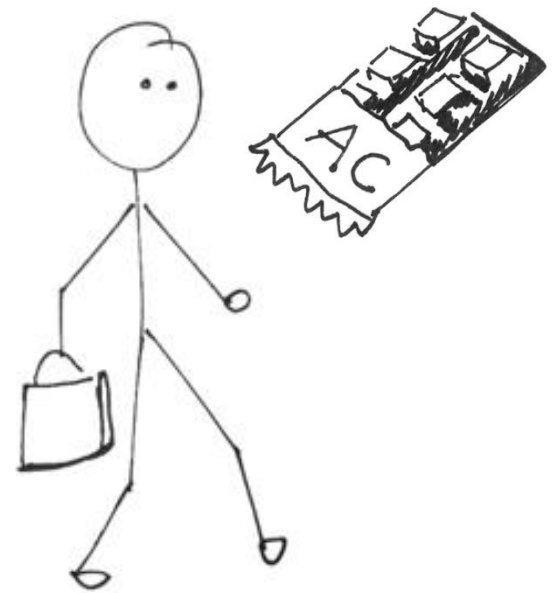
9f02 amount
5f2a currency
9f37 UN
82 AIP
9f36 ATC
CVR (part of 9f10)

9f03 amount, other
95 TVR
9f1a terminal country
9a date
9c type
9f27 CID

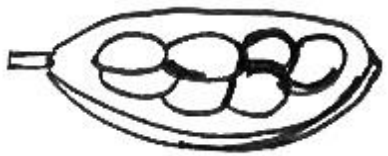



£1.00



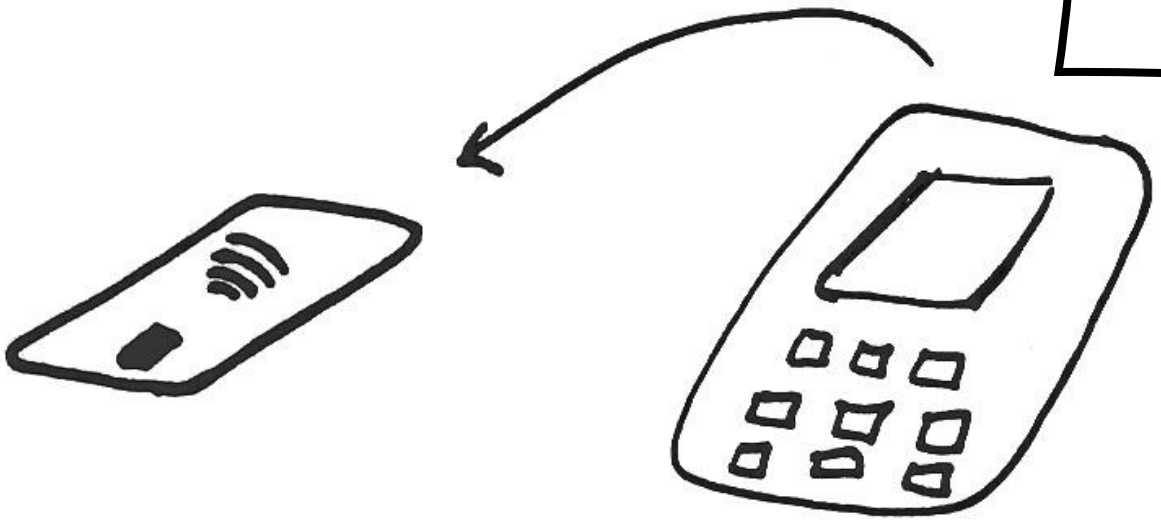

AC

ALL BRANDS HAVE A VULNERABILITY



"GENERATE AC"

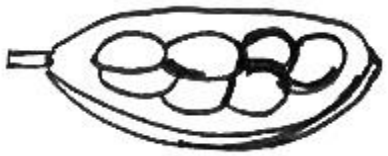
Currency	£
Amount	100
UN	AC6F38DE
TTQ	CVM REQUIRED



What if this is weak?

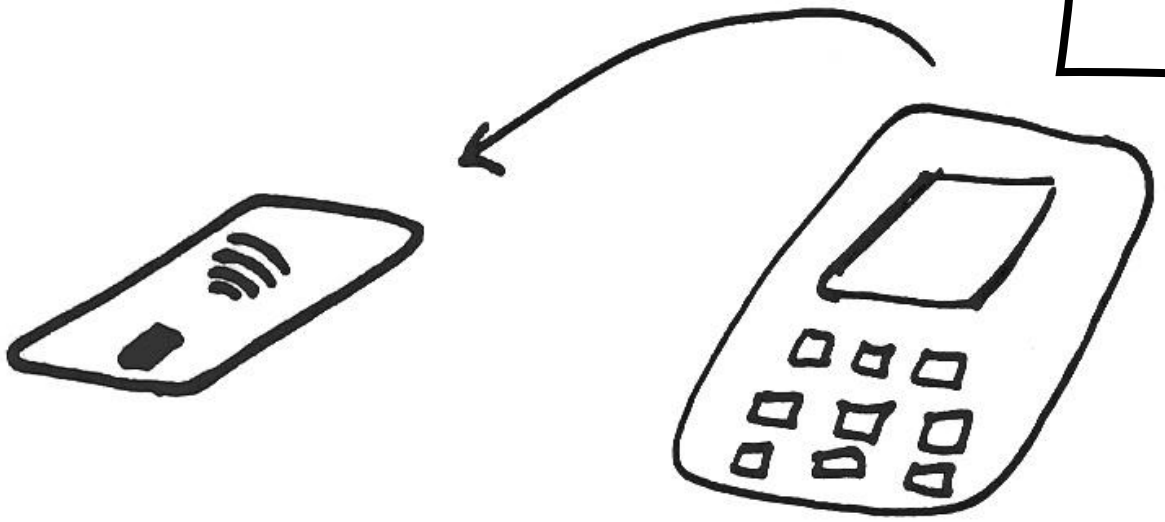
VISA

mastercard



"GENERATE AC"

Currency	£
Amount	100
UN	AAAAAAAA
TTQ	CVM REQUIRED



What if this is predictable?

VISA

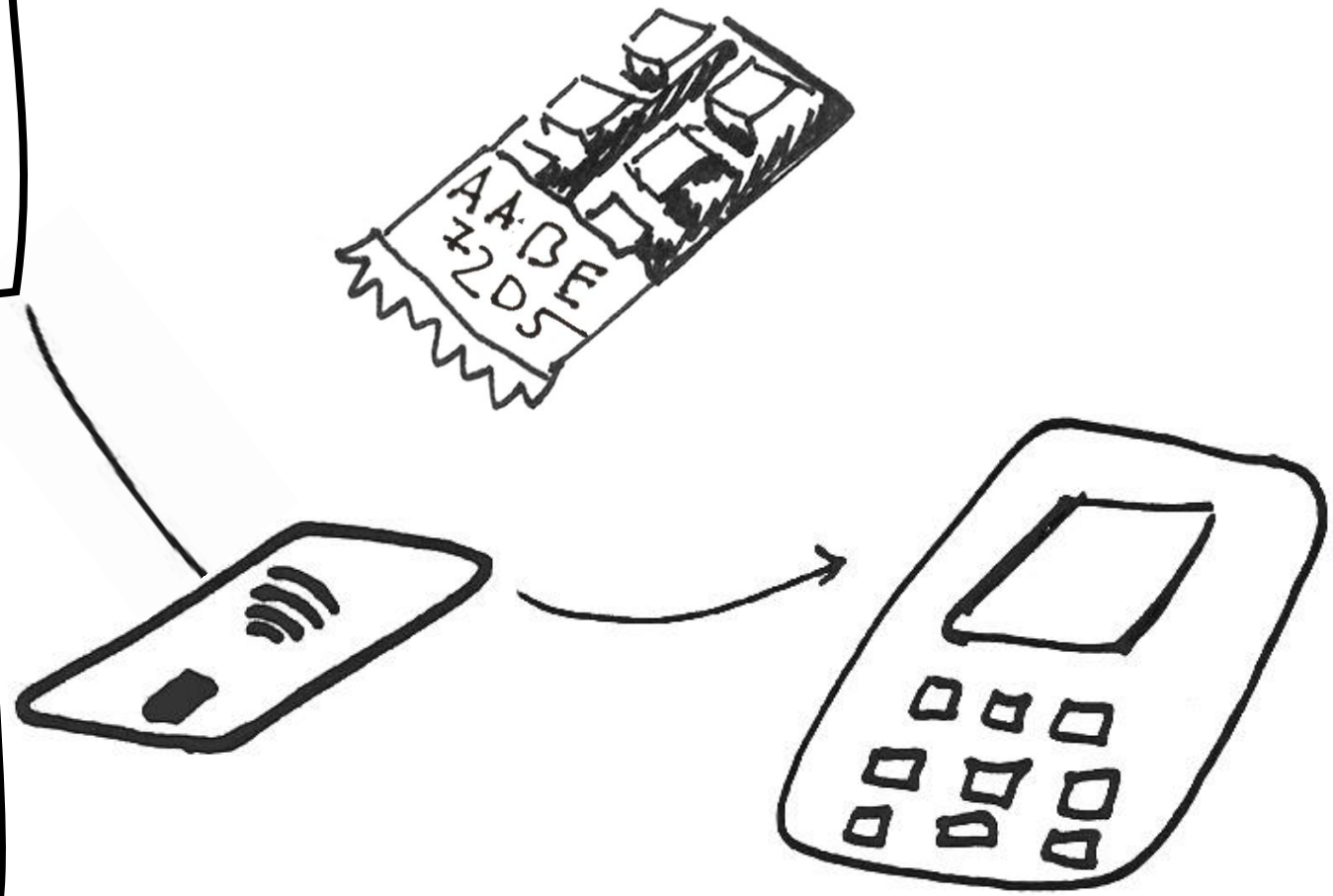
mastercard

ATC

Track2 Equiv

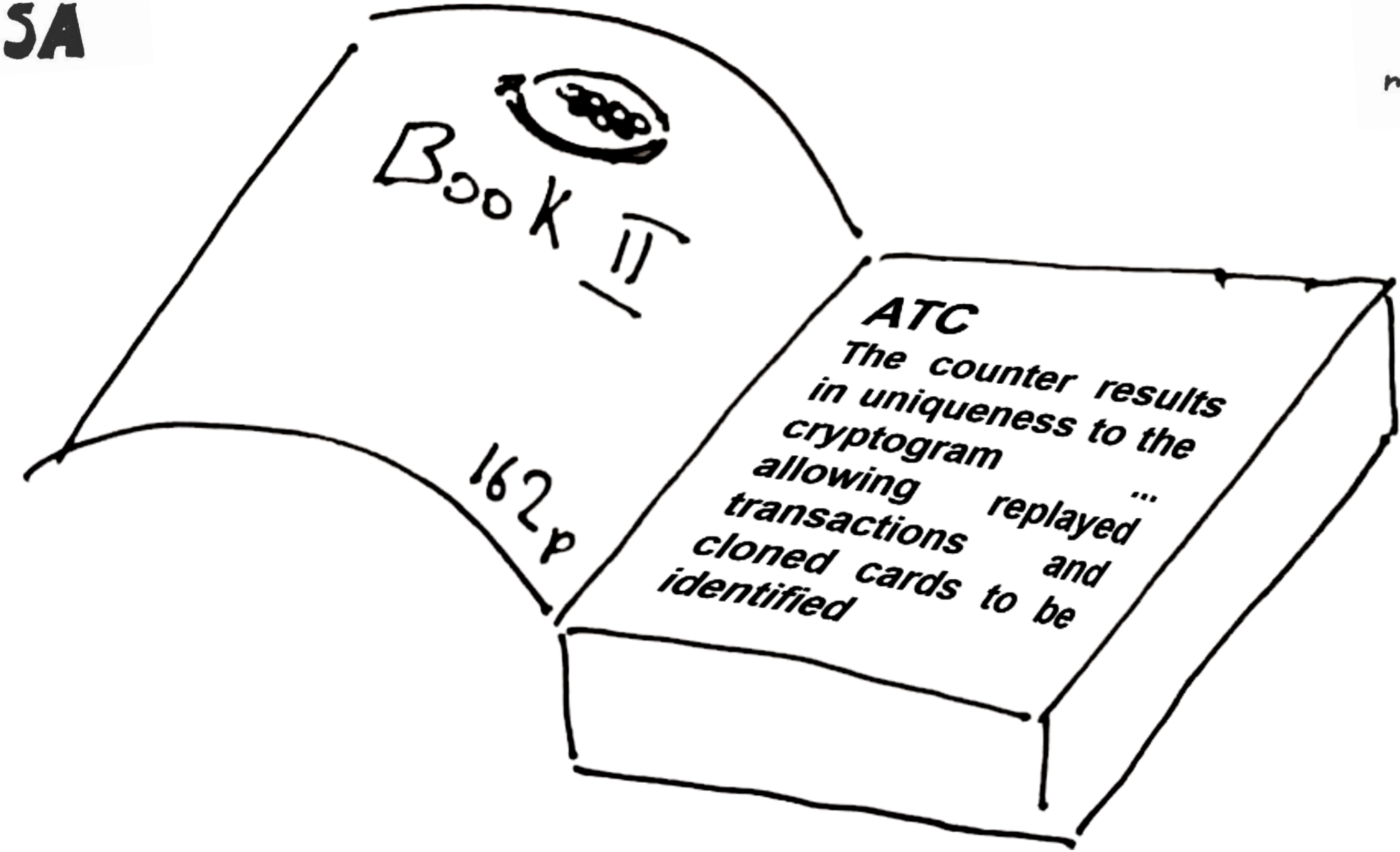
CTQ

ATC increments with each transaction



VISA

mastercard



VISA

Currency £
Amount 10
UN AAAAAAAA

ATC
Track2 Equiv

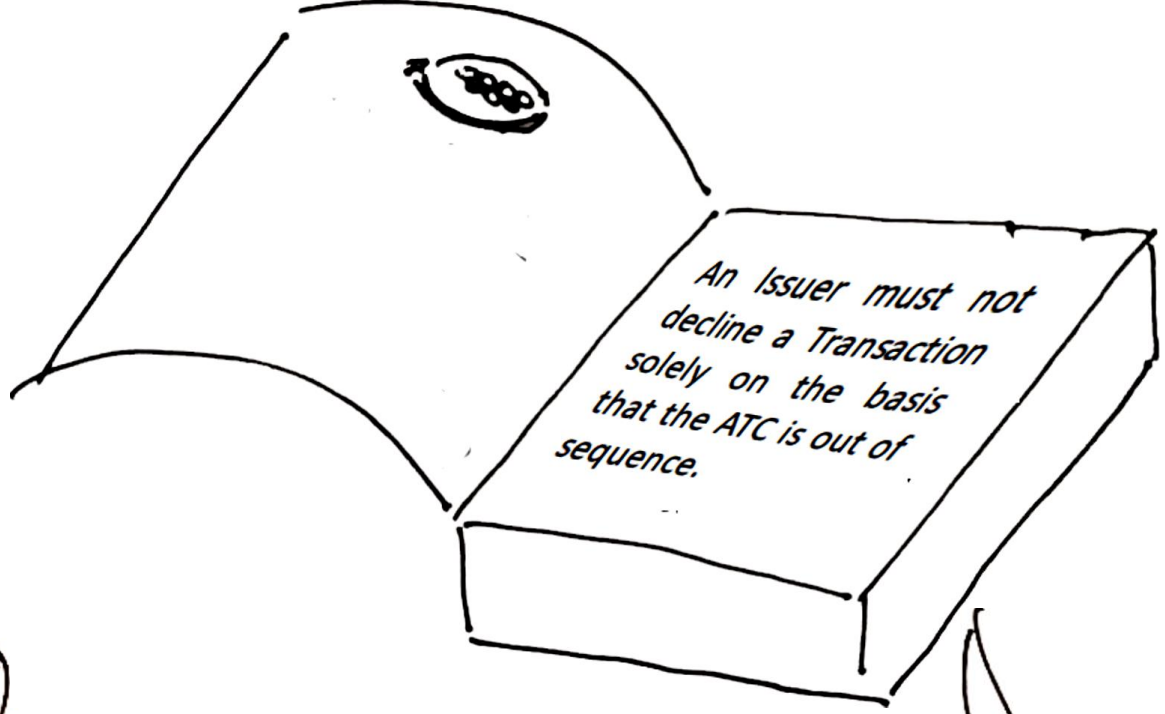
Currency £
Amount 10
UN AAAAAAAA

ATC
Track2 Equiv

Currency £
Amount 10
UN AAAAAAAA

ATC
Track2 Equiv

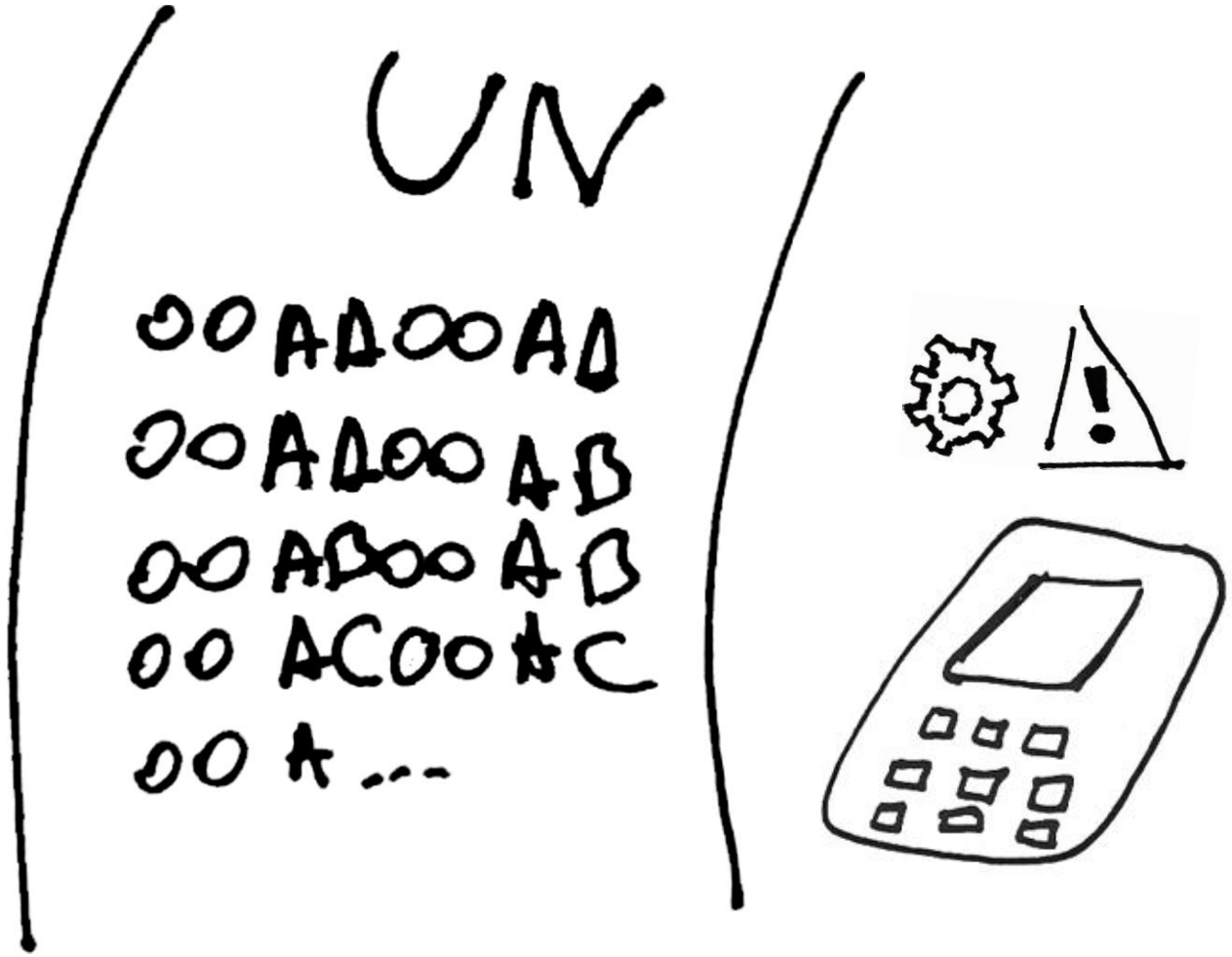
VISA



mastercard

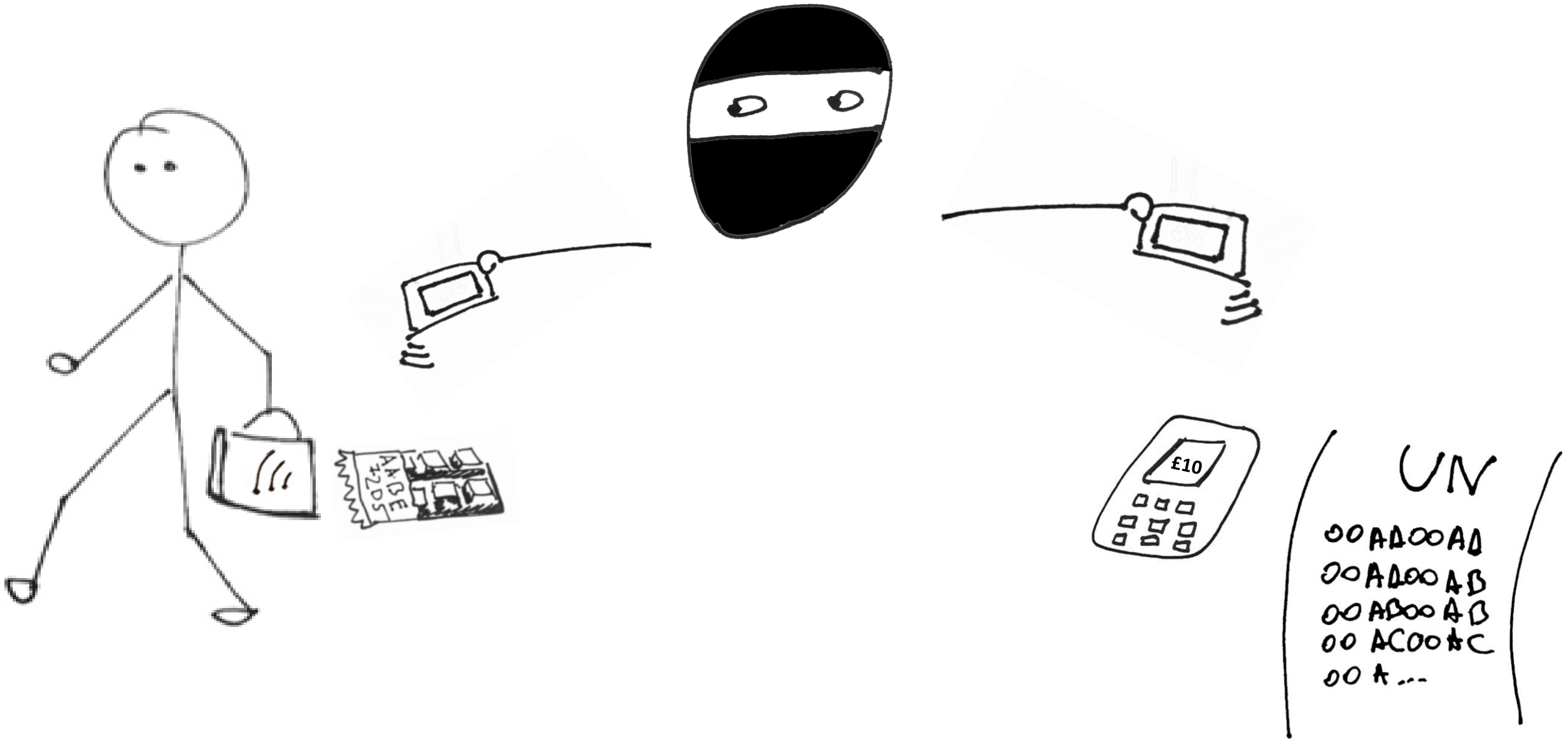
Block ATC jumping
Block equal ATC

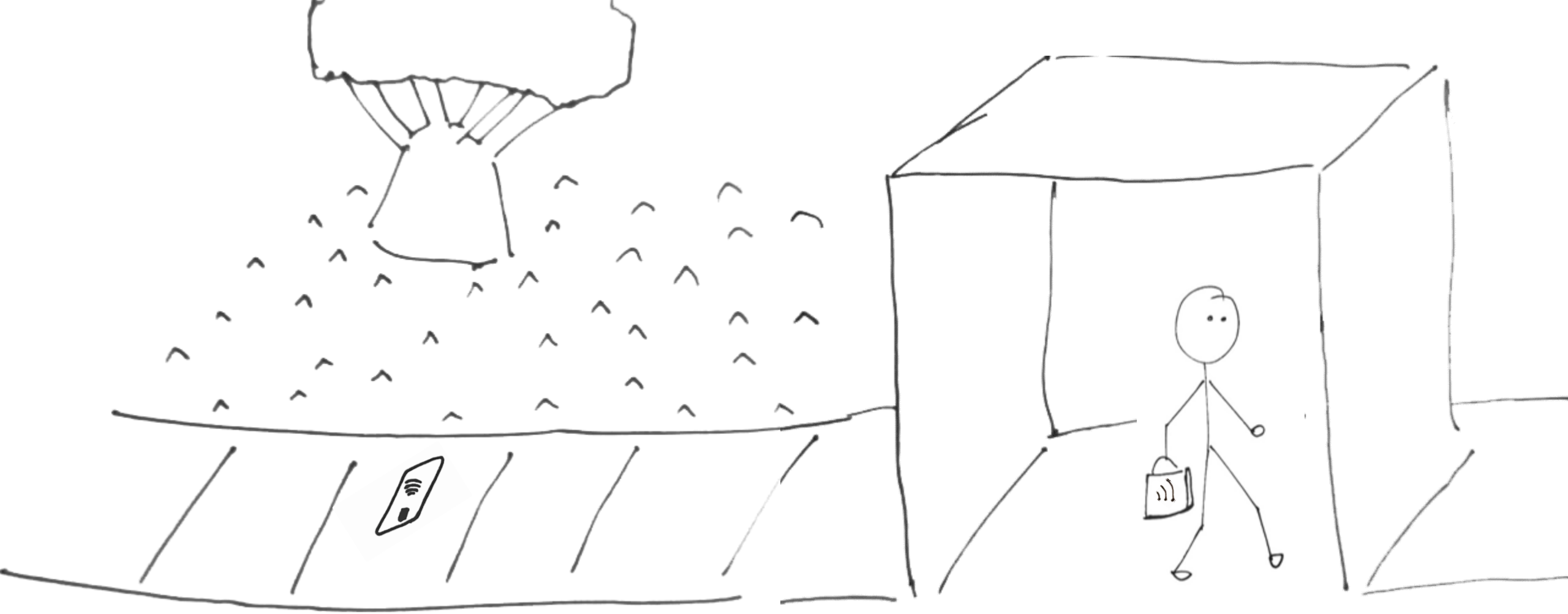
Allow ATC jumping
Allow equal ATC


UN
OOADOOAD
OOADOOAB
OOADOOAB
OO ACOO*C
OO *...


Tag 84: A0000000031010
Tag 5A:
Tag 5F34: 01
Tag 9F26: FD4E04DB0FC91EE5
Tag 9F02: 000000001112
Tag 9F03: 000000000000
Tag 9F1A: 0643
Tag 5F2A: 0643
Tag 9A: 190725
Tag 9C: 00
Tag 9F37: 08AA60AA
Verifone
VX 520

STEAL A CARD OR A TRANSACTION?


£10
UN



HOW MANY ARE AFFECTED?

It's not a
VISA/MC issue

21 MC
10 VISA cards*

* UK, EU, US, Asia

11 MC
7 VISA
allow replay

Max delay - 11d
Max replays - 12

SCA for contactless

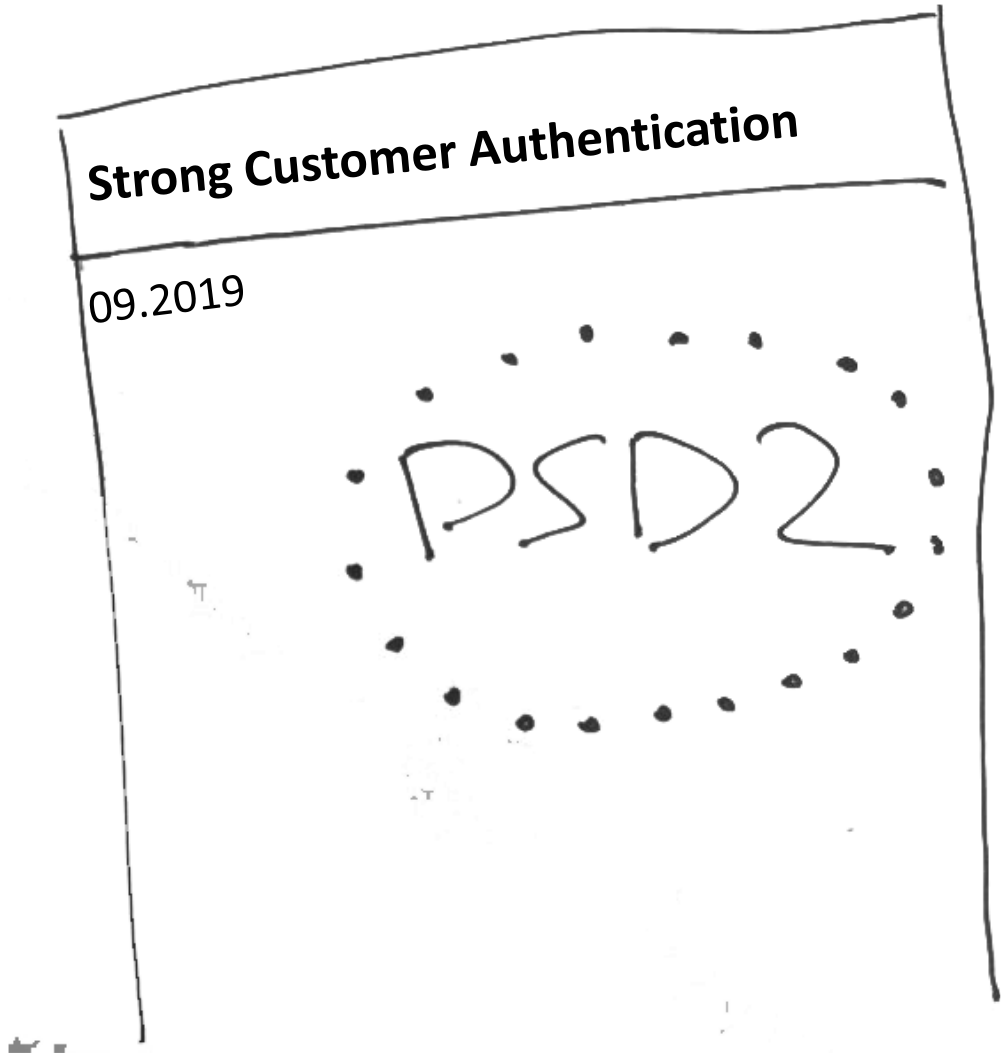
Two-factor authentication

Insert card and use PIN

Should be made occasionally

Cumulative limits (£150)

Issuing bank is in charge



How to bypass SCA cumulative limits

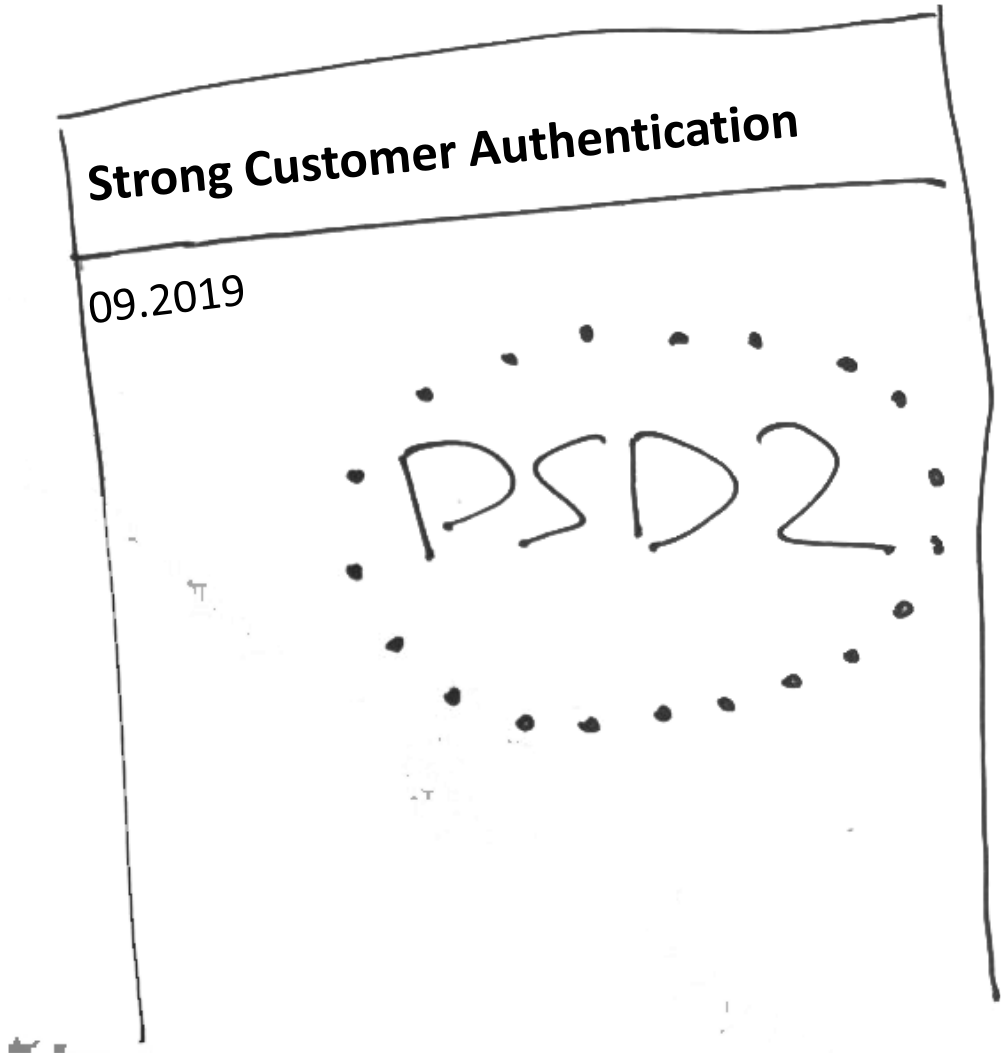
Change the type of transaction

Contactless becomes EMV

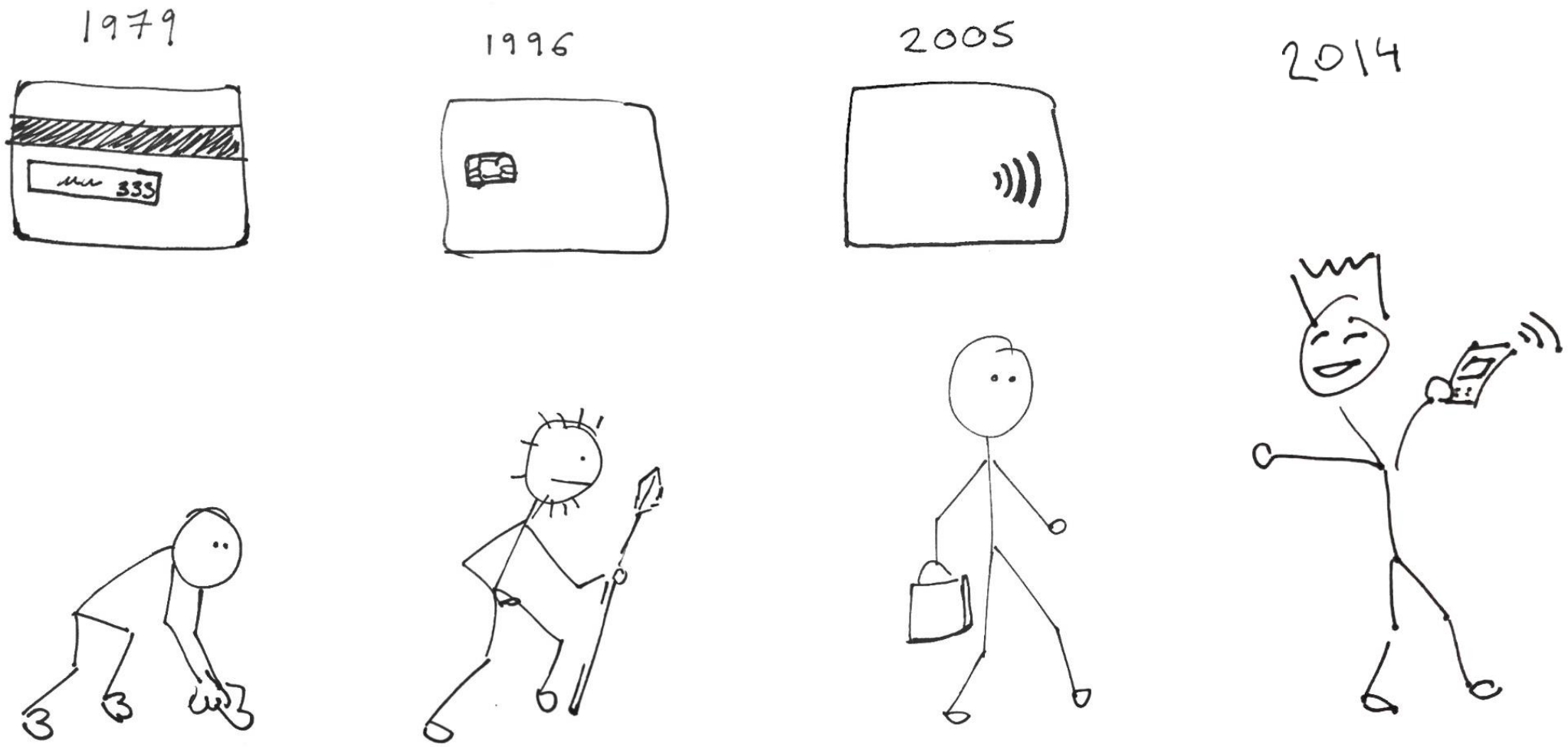
Pretend to be a phone

With CDCVM flag

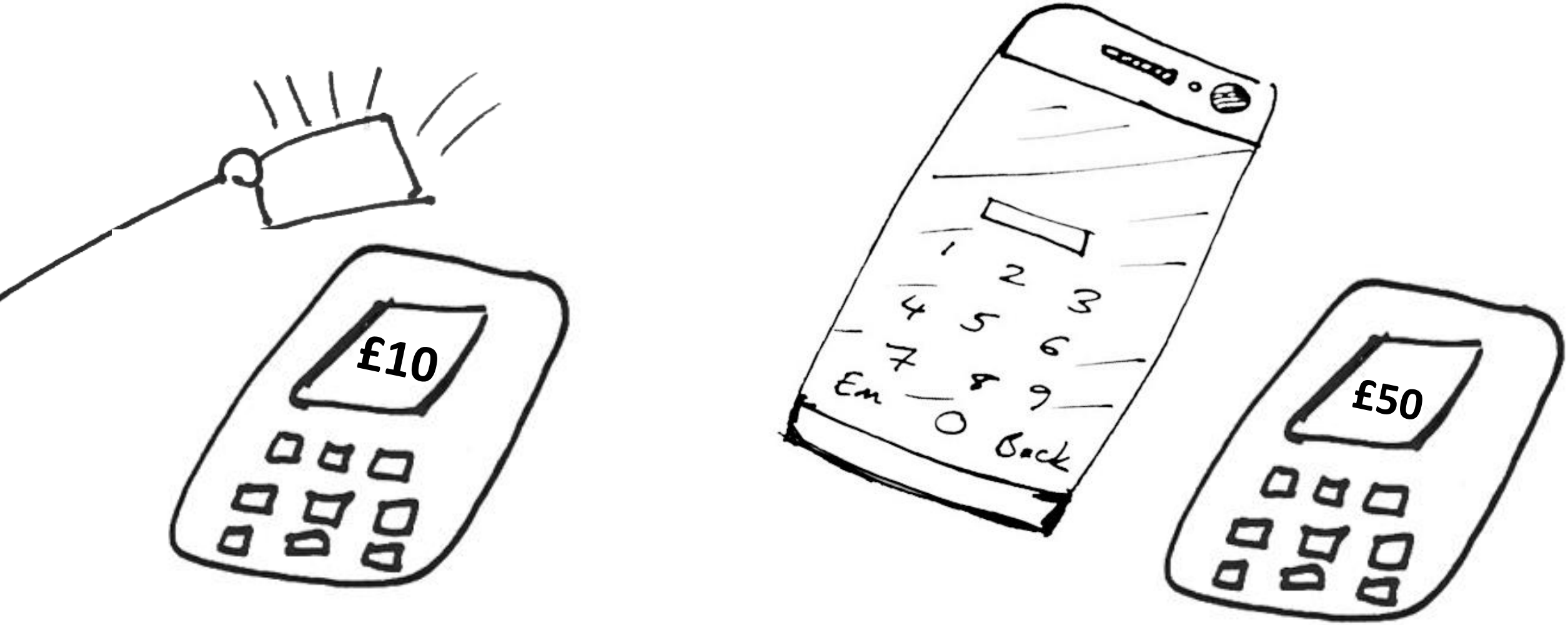
Be a phone



WHAT ABOUT CONSUMER DEVICES?



GPAY HAS A VULNERABILITY FOR VISA



CTQ “CDCVM Performed” value is always 1 for consumer devices

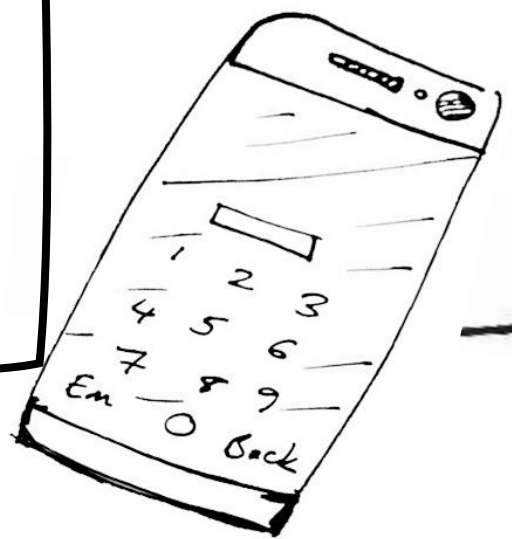
ATC
Track2 Equiv
CTQ

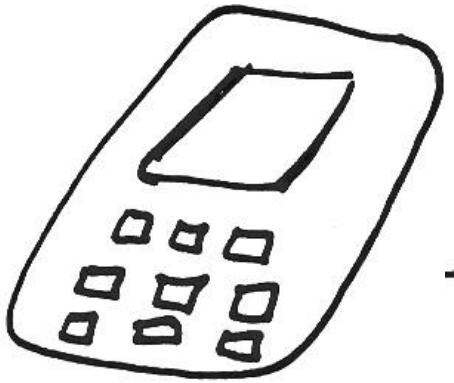
CDCVM=1

1. Change TTQ “CVM Required” value from 1 to 0

Currency
Amount
UN
TTQ

CVM REQUIRED=~~1~~ 0

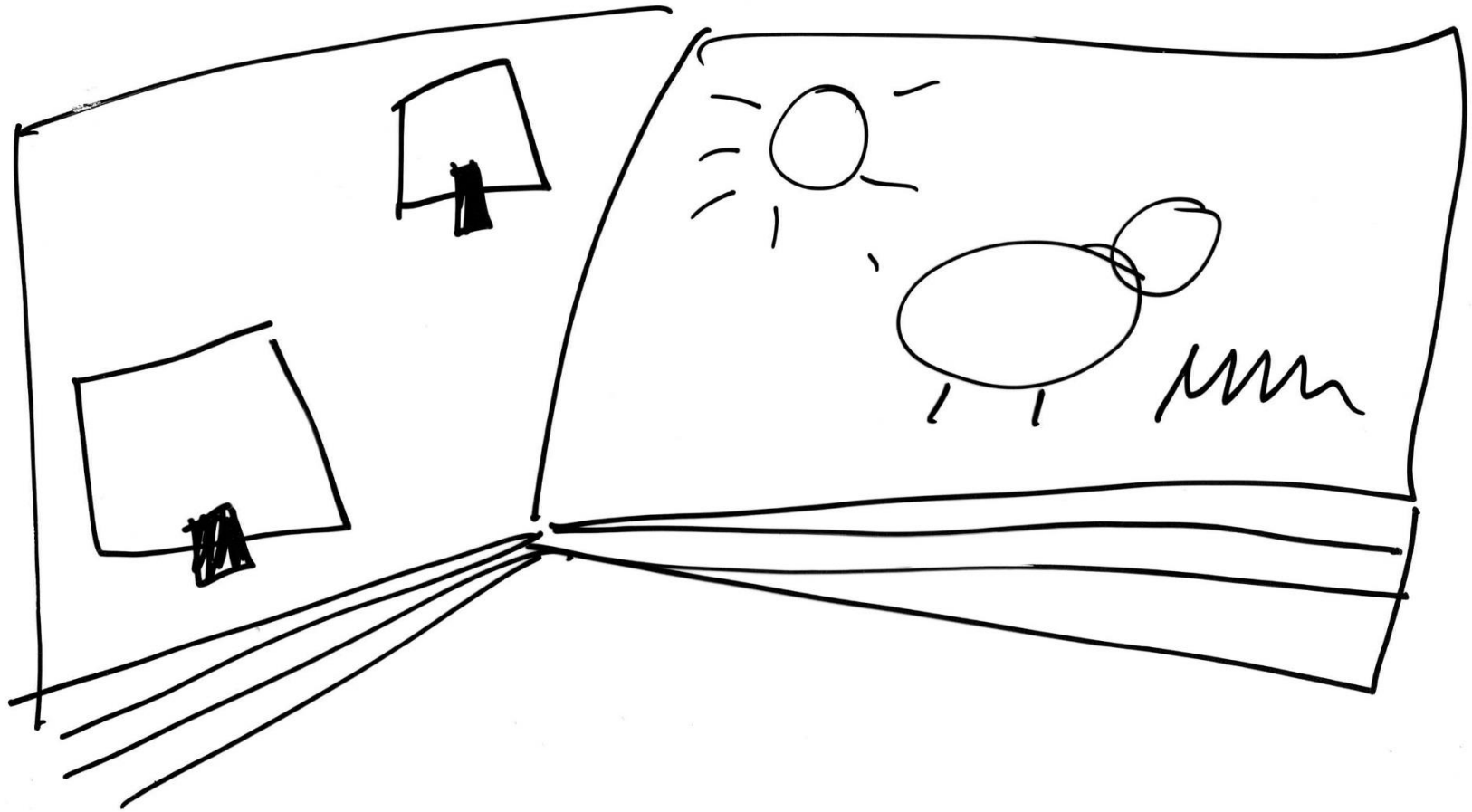




Acquirer


logitech
Connected to
Samsung Galaxy J3 ...
logitech

CONCLUSIONS

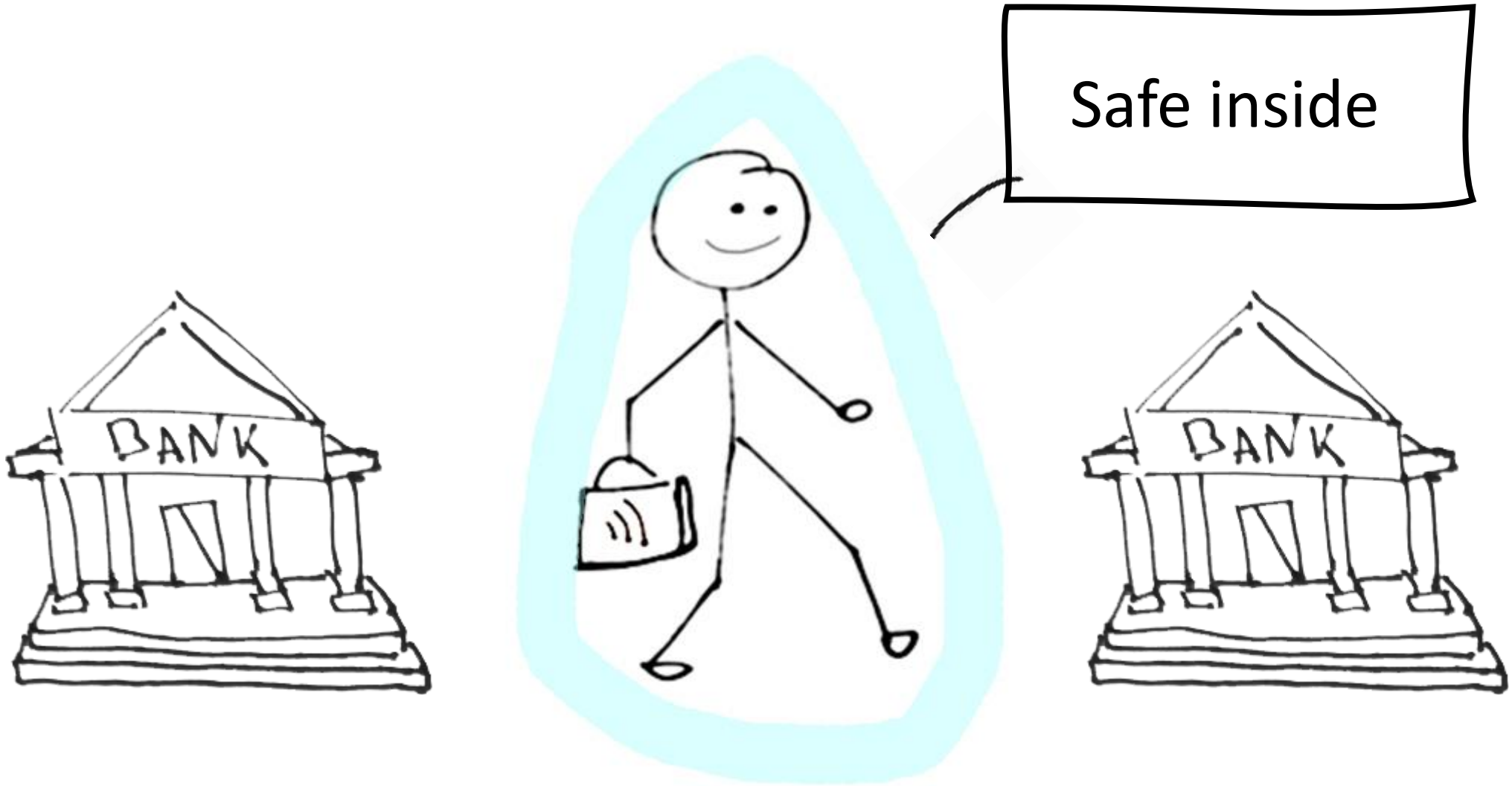


U.S. ALSO AFFECTED

$50.00 – No CVM
$10,000.00 - CDCVM

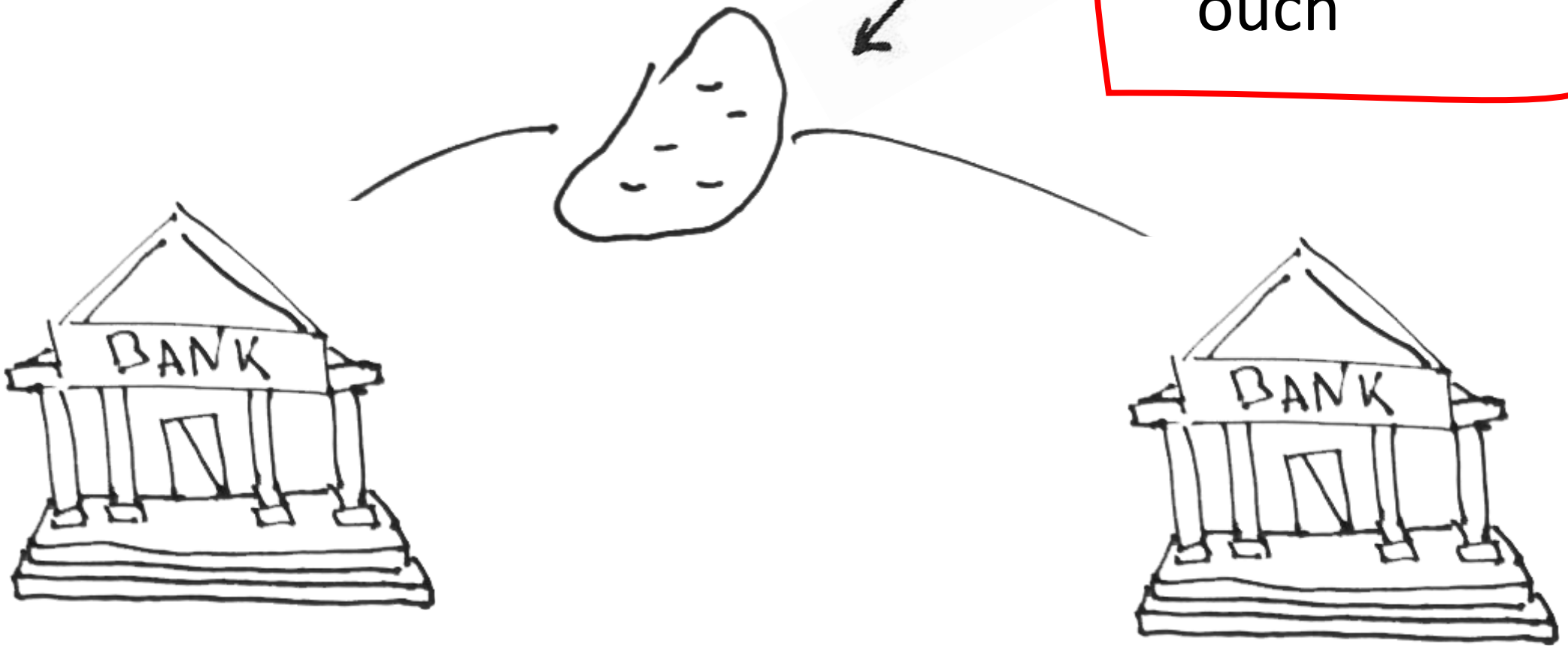
https://www.paypalobjects.com/webstatic/mobile/pph/sw_repo_app/us/miura/m010/prod/7/contactless.cfg

THE GOOD NEWS



BLAME GAME

Hot potato
“ouch”



IN CONCLUSION

Three vulnerabilities

Visa will not issue a fix

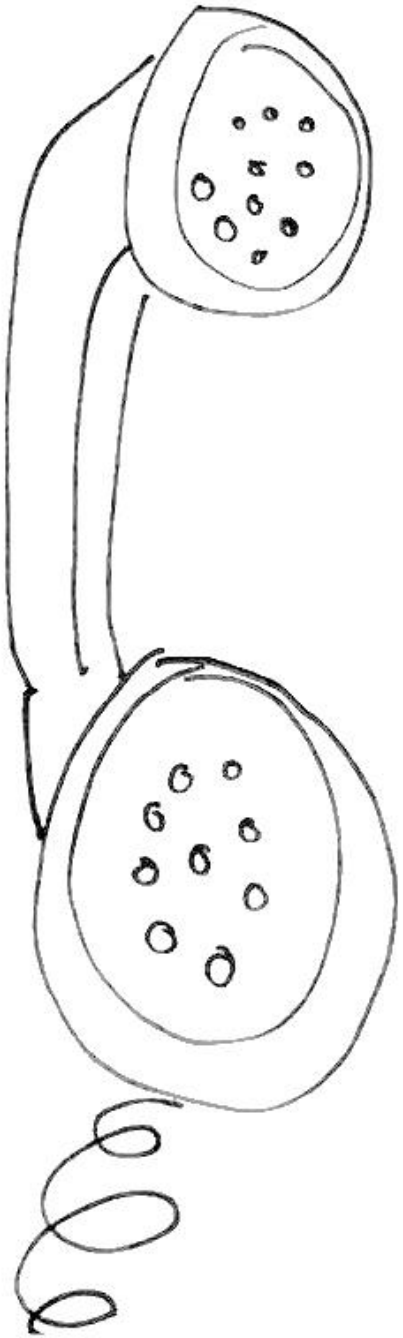
Google will not issue a fix

Contactless, less secure than CHIP

Not all card brands are the same

Contactless fraud is real

Someone has to pay…who will it be?



NEXT STEPS

- AmEx
- WeChat
- Secure Elements
- HCE

PAYMENT RESOURCES

securingpayments.com

leigh-annegalloway.com

Whitepaper available here

Illustrations (mostly)

CONTACT

@a66ot

@L_AGalloway