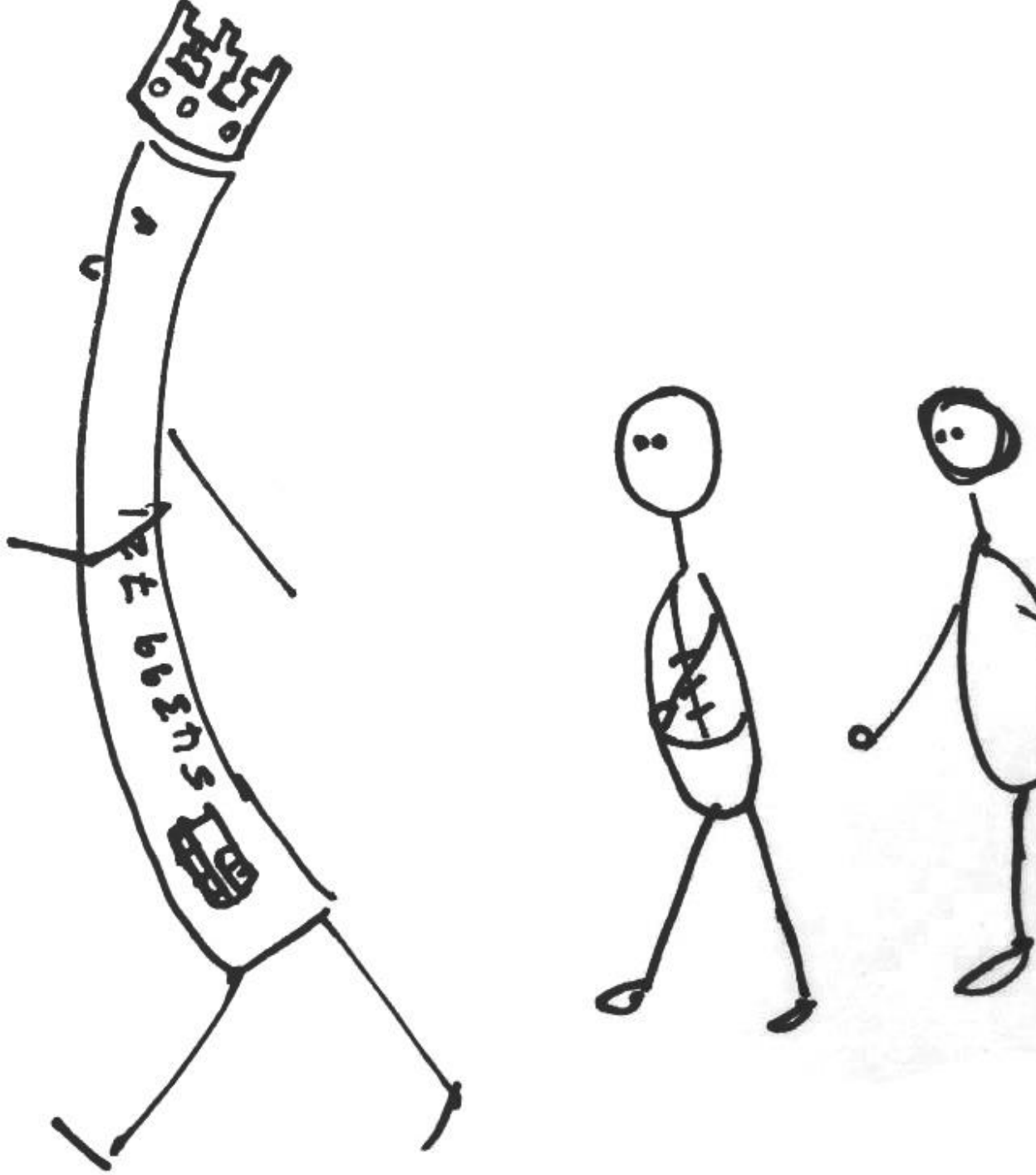
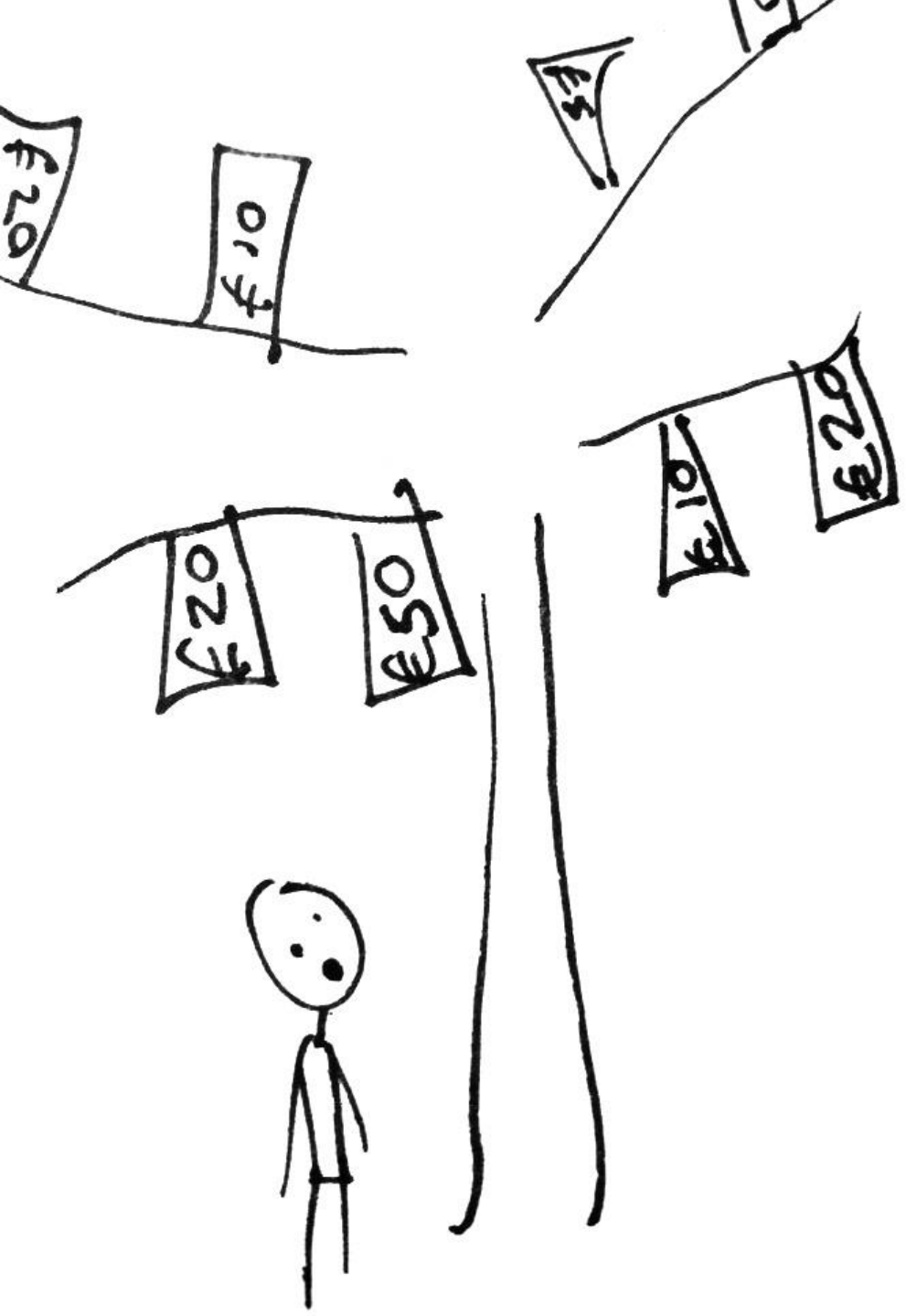
FIRST CONTACT:
New vulnerabilities in contactless payments

CYBER
R&D LAB
BY <epam> | POSITIVE

TO GOOD

To be true?





NEO BANKS

The big banking boom

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

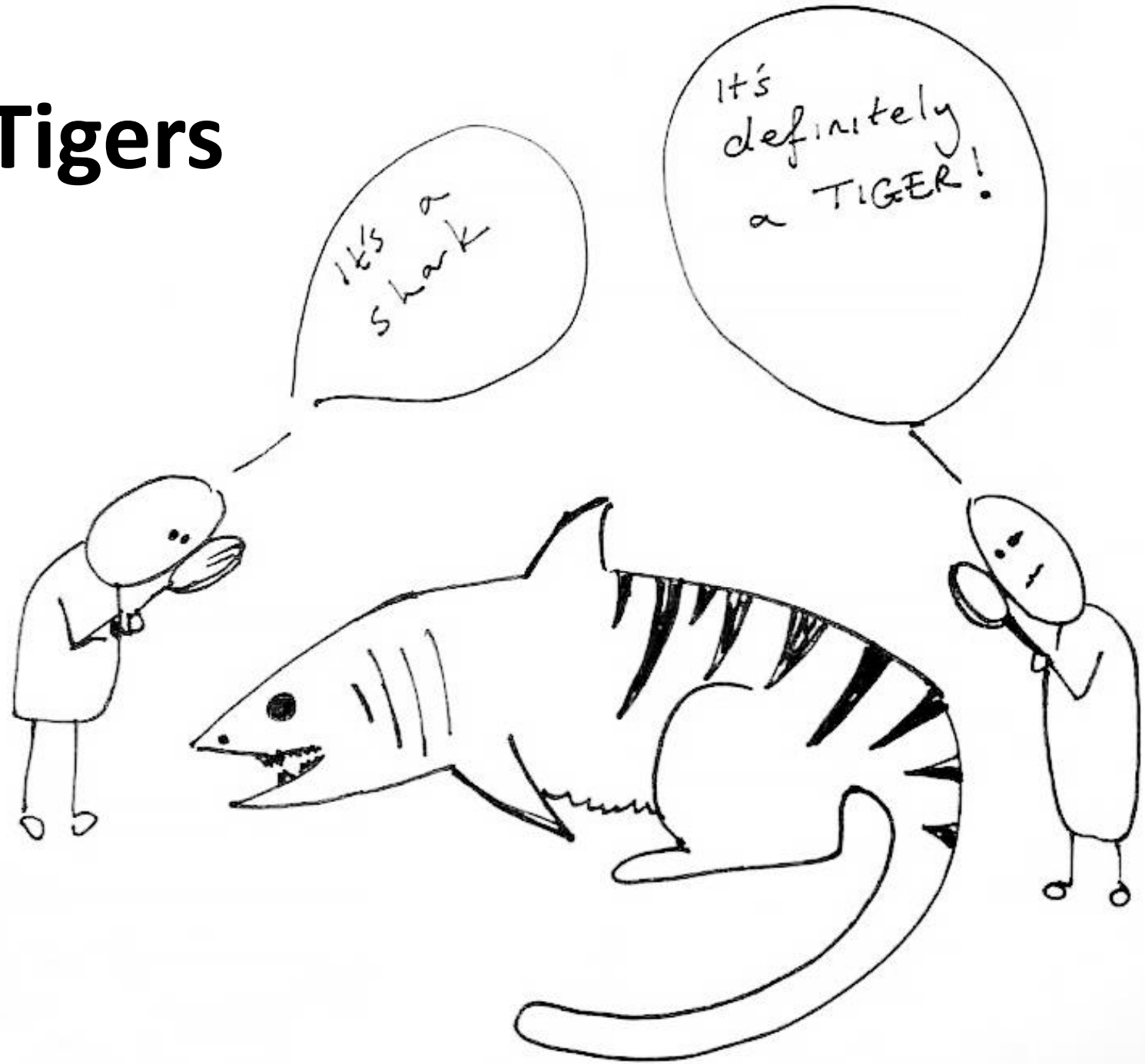
[3] UK Finance, "2018 half year fraud update," Sept. 2018, Page 12, https://www.ukfinance.org.uk/wp-content/uploads/2018/09/2018-half-year-fraud-update-FINAL.pdf

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.

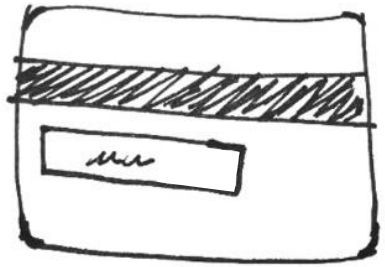
The 2018 cases, recorded between April 2017 and January 2018, represent more than half of all the reports of contactless-related fraud investigated by the City of London Police alone, which runs Action Fraud, since 2013.

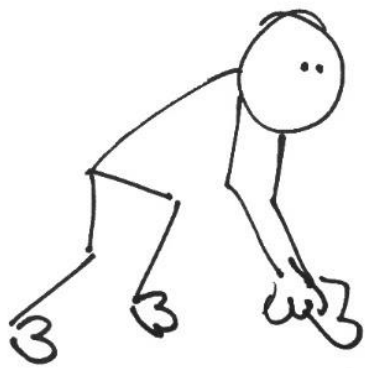
Sharks and Tigers



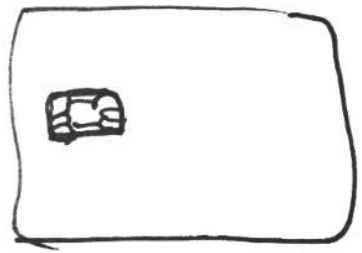
CONTACTLESS, A MODERN FORM OF PAYMENT?

1979

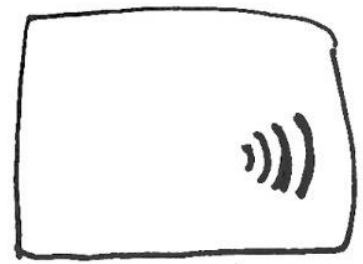


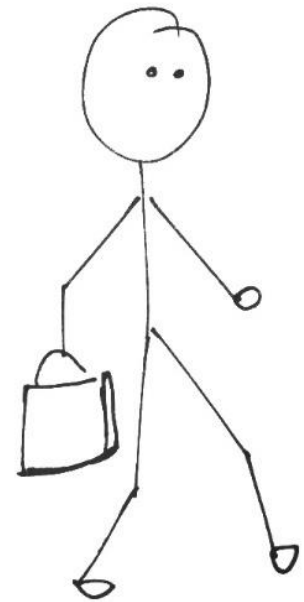


1996



2005

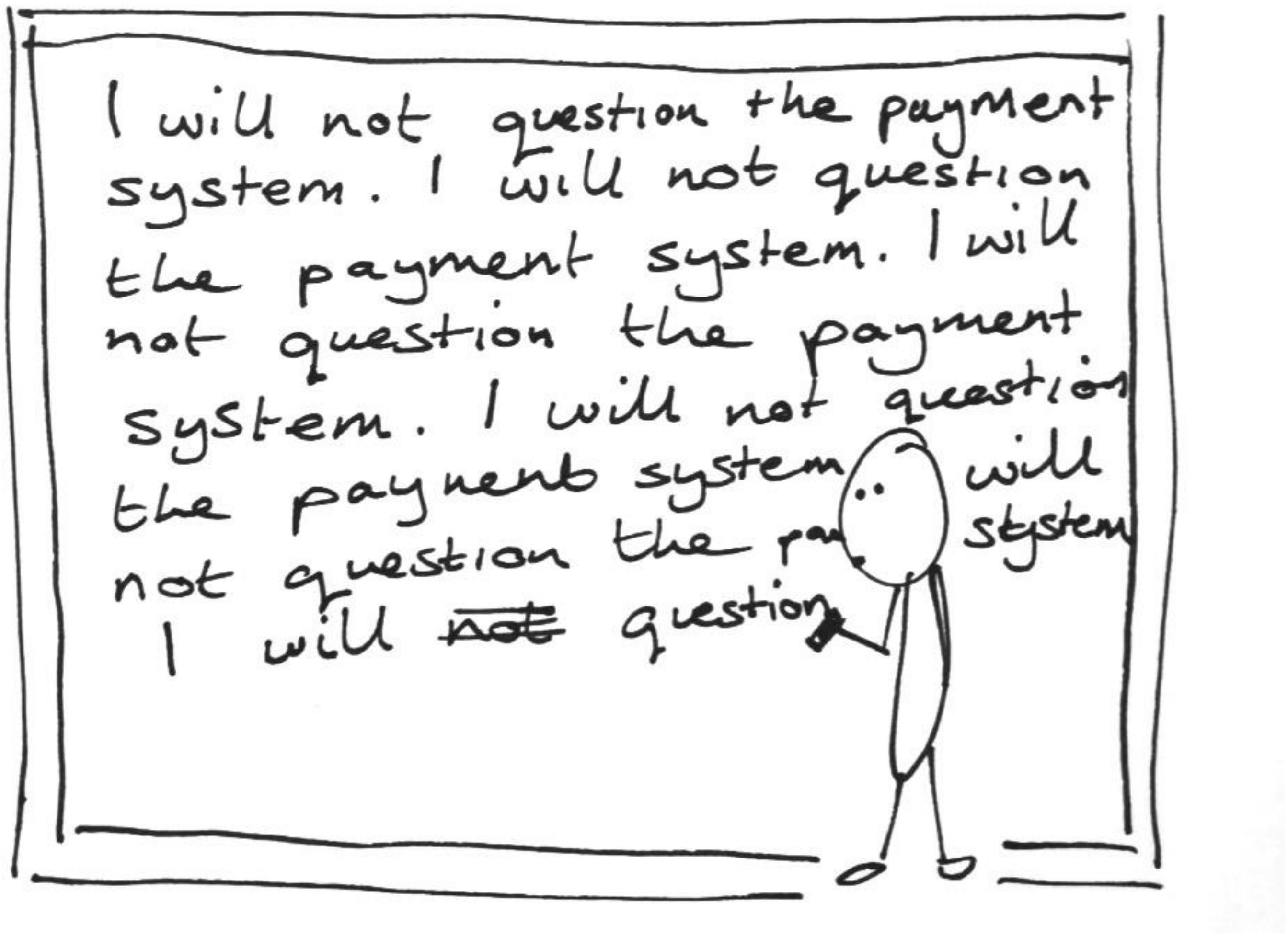




NFC is(n’t) different

- 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 STANDARDIZED?




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

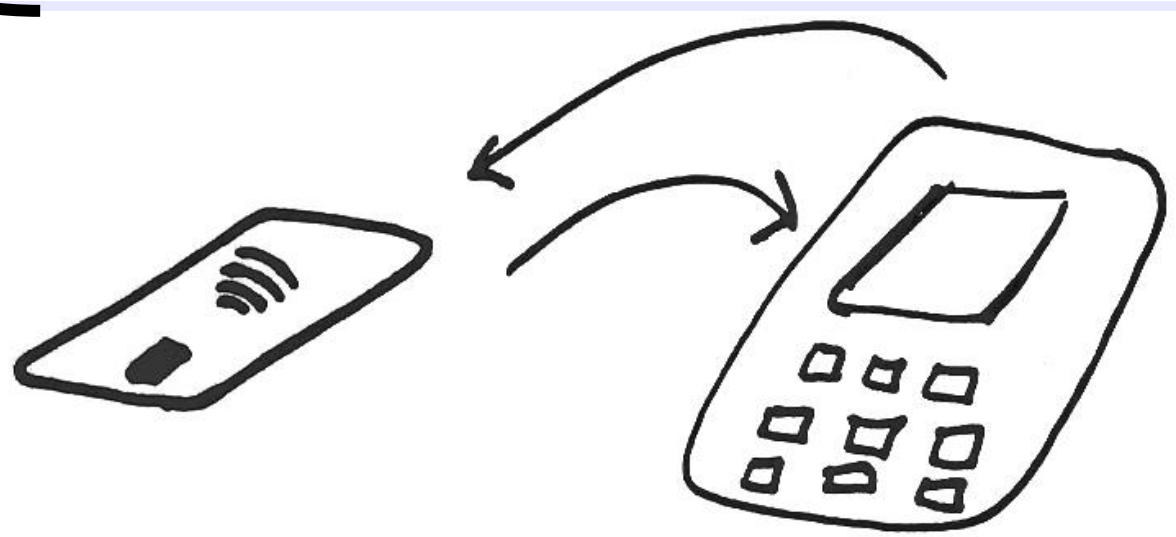
mastercard

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
```



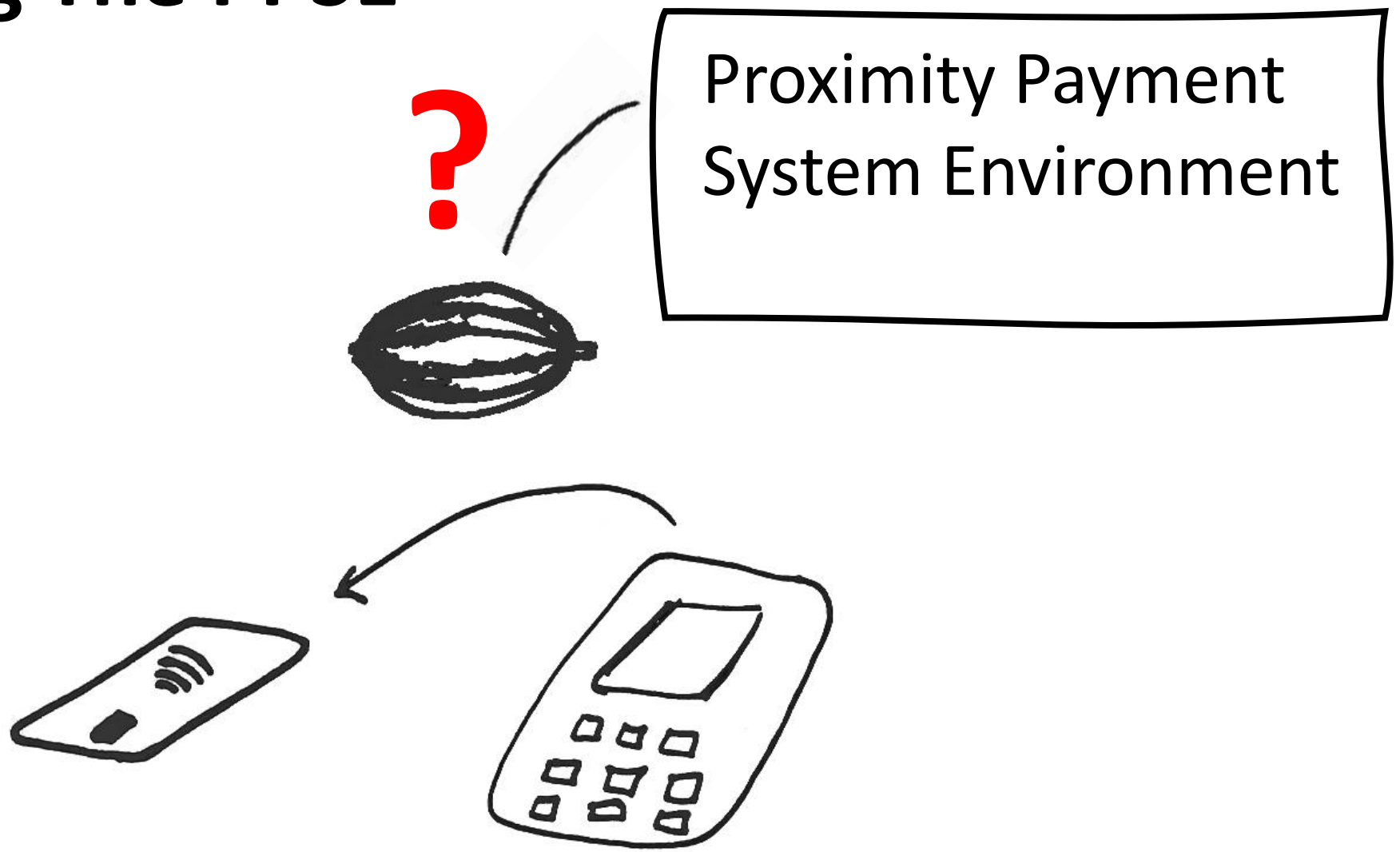
Value

2PAY.SYS.DDF

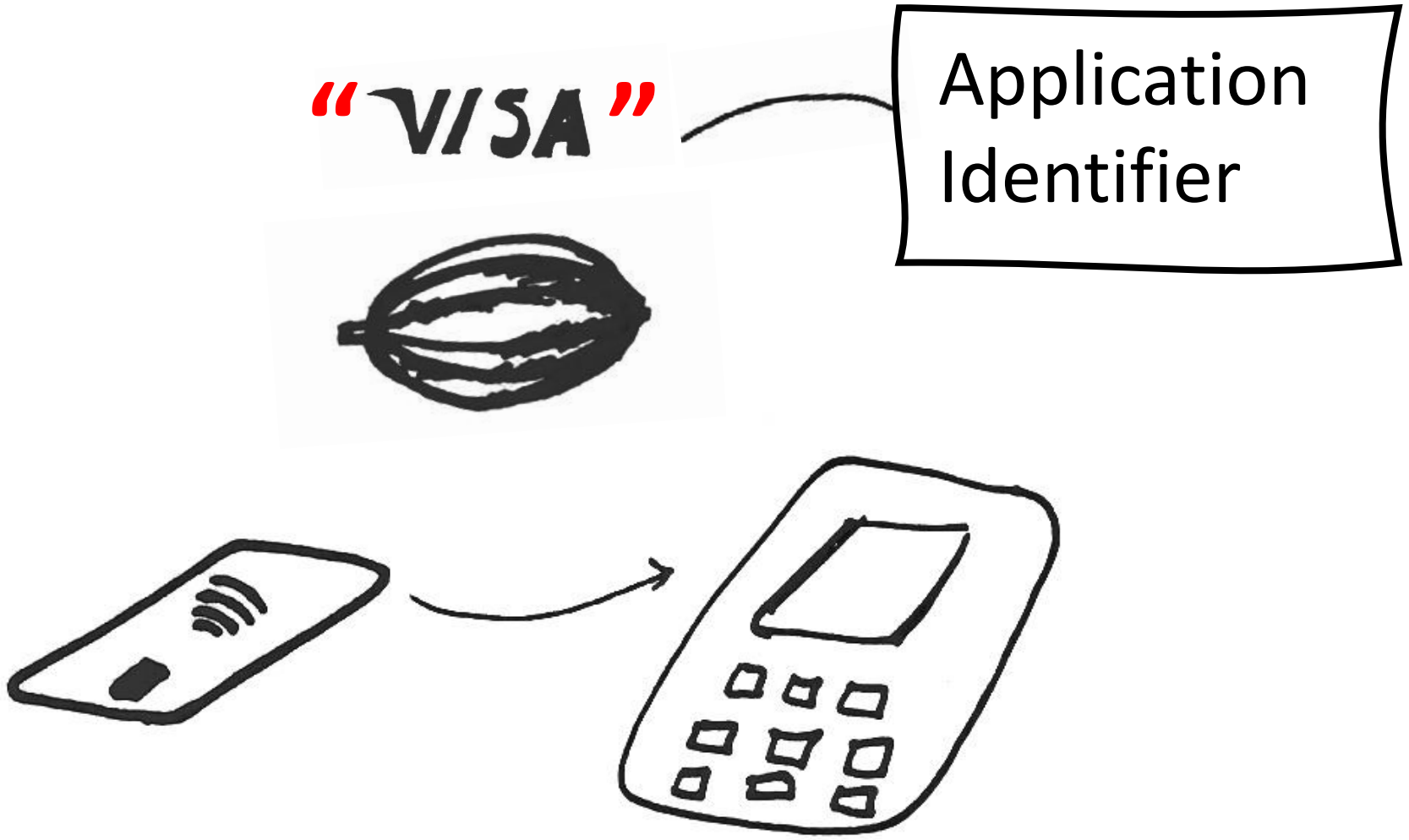
01

TLV = Tag Length Value

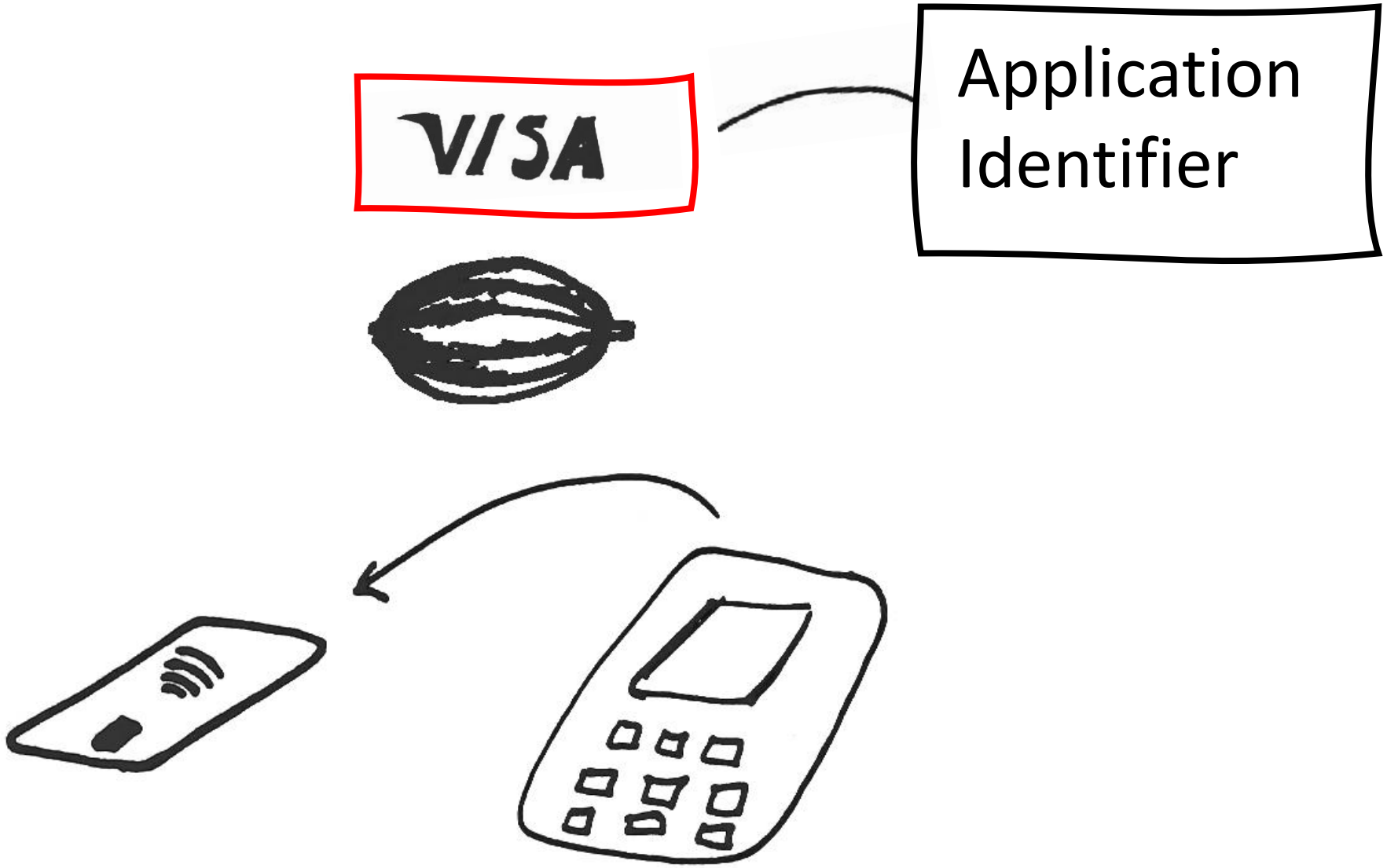
1. Reading The PPSE



2. Card responds with AID

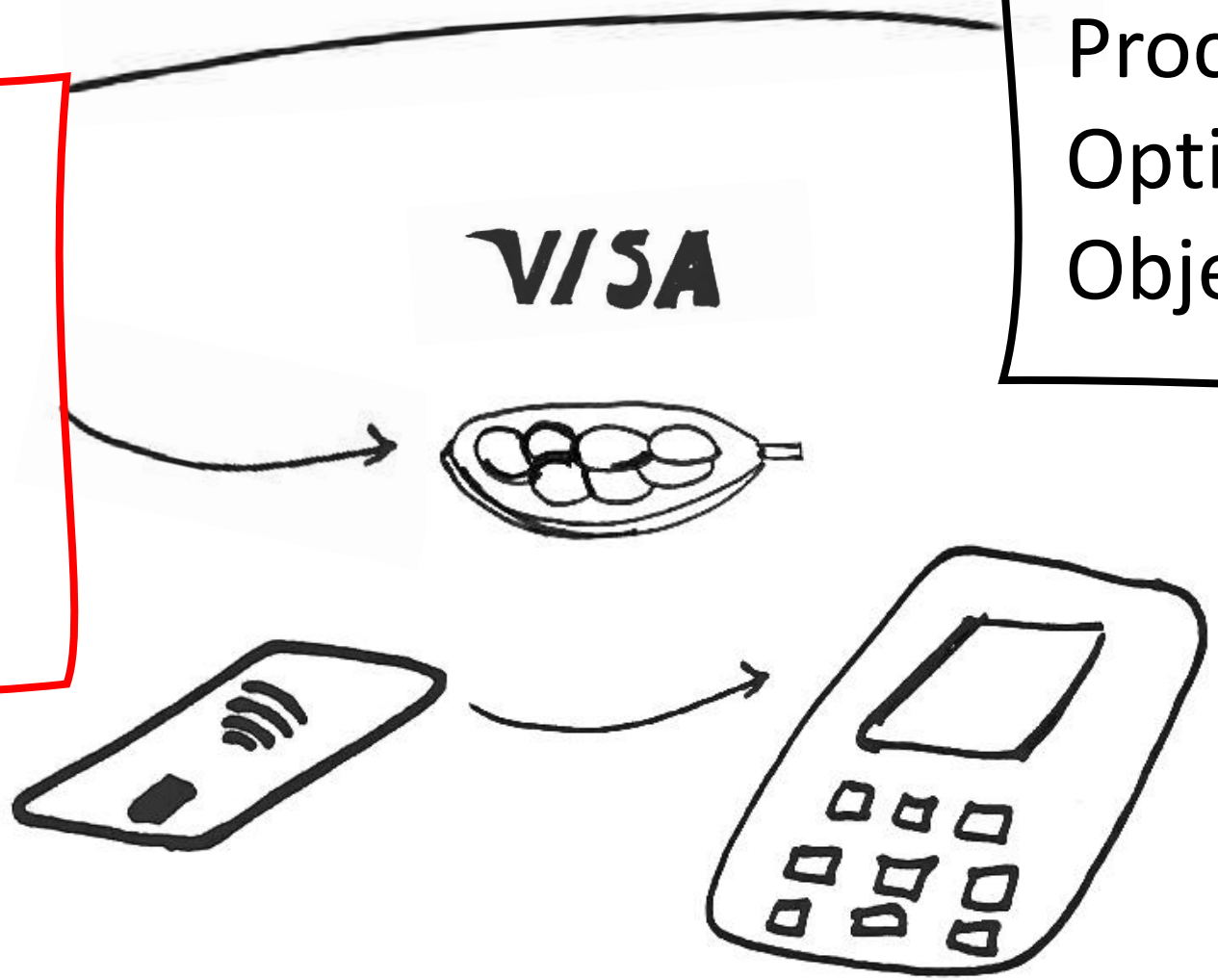


3. Terminal selects AID



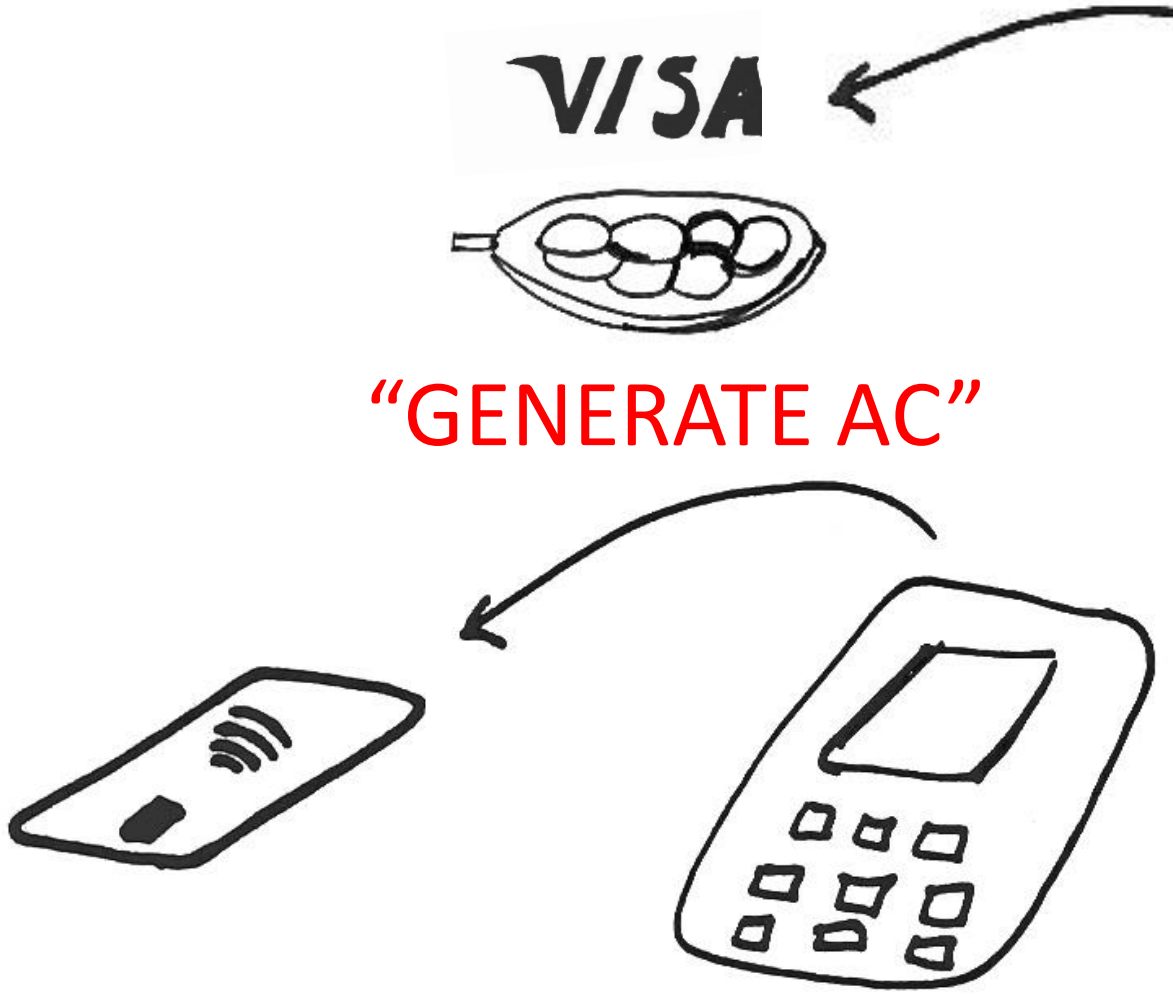
4. Card provides PDOL

Currency
Amount
UN
TTQ



Processing
Options Data
Object List

5. Terminal sends requested data



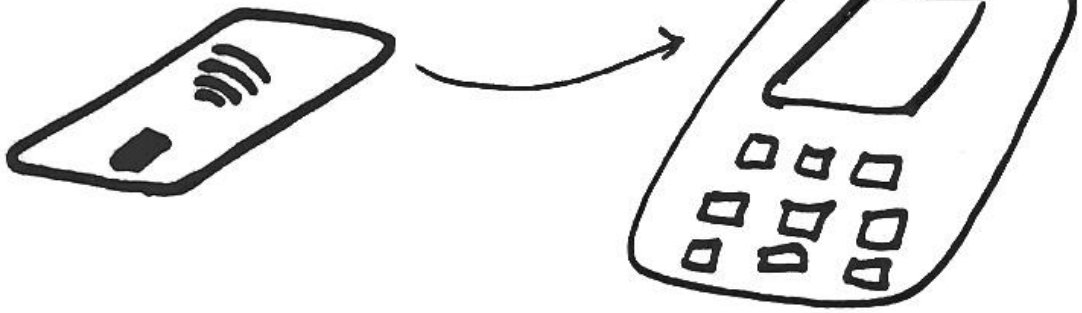
Currency
Amount
UN
TTQ

MSD?
EMV chip?
qVSDC?
CDCVM?

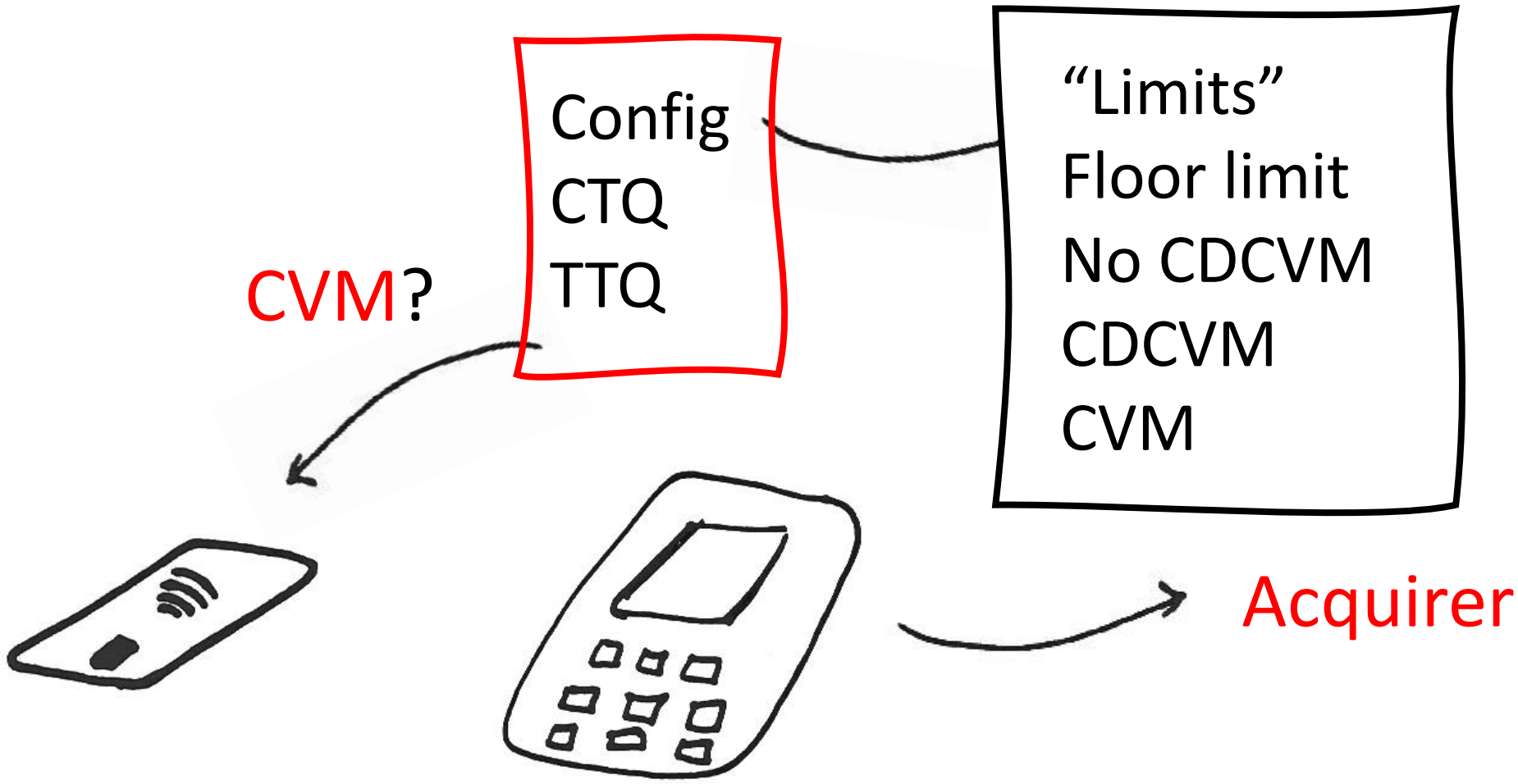
6. Card provides Application Cryptogram

ATC
Track2 Equiv
CTQ

Online Pin?
Signature?
CDCVM?

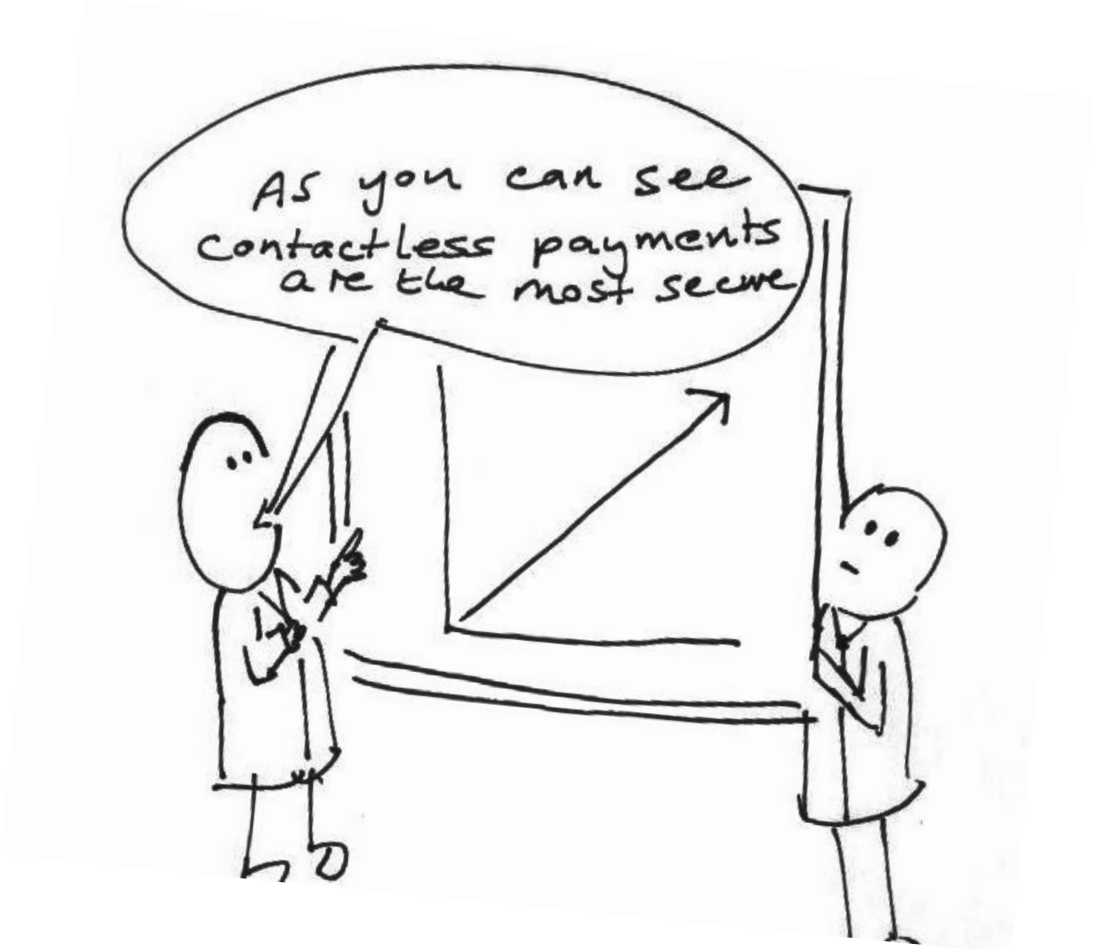


7. Terminal conducts risk analysis



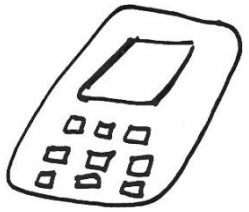
PLACEHOLDER SPEAKER TRANSITION

WHAT SECURITY MEASURES ARE IMPLEMENTED IN A TRANSACTION?



- Authentication via ODA
- Authorization via the cryptogram
- PIN for payments over Tap&Go limits

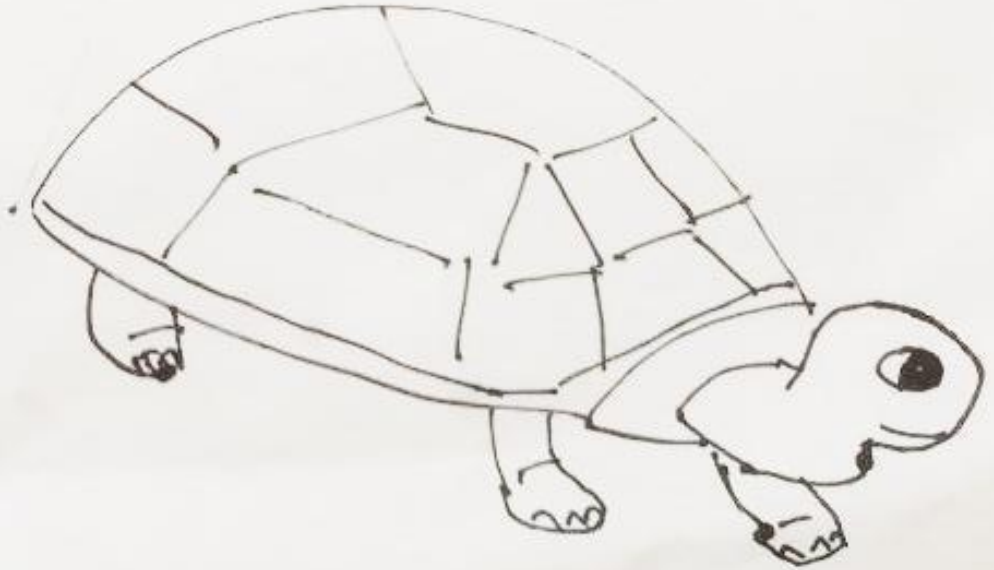
ODA



$Public_{IC}$, $Secret_{IC}$(Static)	->	Verify	**SDA**
	<-	UN - Random Number	**DDA**
$Secret_{IC}$(UN)	->	Verify	
CVMList	->		**CDA**
	<-	GenerateAC	
$Secret_{IC}$(AC,Hash(CVMList))	->		

EMV vs NFC

- MC set CDA as mandatory - 16/18 cards
- Visa disabled ODA – 0/12 cards
- MC has a set of cryptograms
  - Some of them don’t use all essential fields
- Visa has a set of cryptograms
- MC uses CVMResults, TVR, AIP fields
- Visa implemented CTQ/TTQ



VISA

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

8/12 cards

Table D-1. Data input for TC, AAC, ARQC With CVN 10/ CVN 18

Data Element
Amount, Authorized
Amount, Other
Terminal Country Code
Terminal Verification Results (TVR)
Transaction Currency Code
Transaction Date
Transaction Type
Unpredictable Number
Application Interchange Profile
ATC
Card Verification Results

- CVM List

*PIN, Signature, No CVM

- Cryptogram

*Hash(AIP, CVMResults/TVR)

- AIP

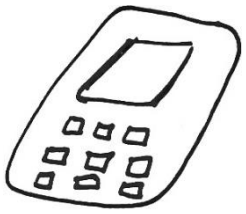
*CDA, CDCVM

CVMResults/TVR

*cardholder verification

ODA

*CDA



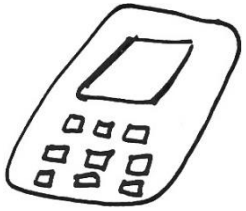
Field 55

Cryptogram

*CDA is supported

*CVM Results

VISA



TTQ

*cardholder verification

- CTQ

*PIN, No CVM, CDCVM

- Cryptogram

*Hash(Amount)

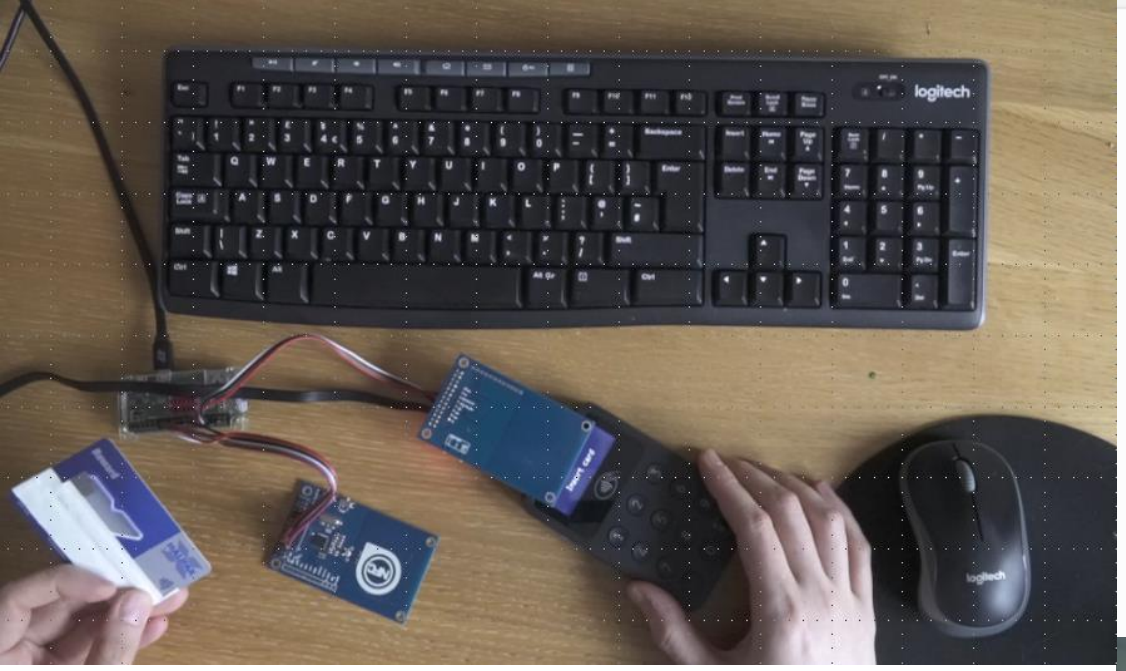
Field 55

Amount

Terminal Country Code

Online PIN

CVMResults - sometimes



EDITORS' PICK | 59,573 views | Jul 29, 2019, 06:30am EDT

Exclusive: Hack Breaks Your Visa Card's Contactless Limit For Big Frauds

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

https://leigh-annegalloway.com/presentation-materials/

Amount - £46

~~TTQ/CTQ~~

Type of payment – Mobile wallet/Card
*Field 55/Token
*Online PIN

VISA

CVM Results – not mandatory in Visa payWave
*010000 – Offline PIN (equivalent for CDCVM)

CONTACTLESS FRAUD

£1,000; Online PIN - Good
£1,000; No Field 55 - Good
£1,000; Offline PIN - Bad – CDCVM attack
£1,000; No online PIN - Bad or suspicious
£100; No online PIN - We don't know

Accepted

VISA

Visa said that card issuers are ultimately responsible for validating transactions.

Use chip every £225/€250 spent

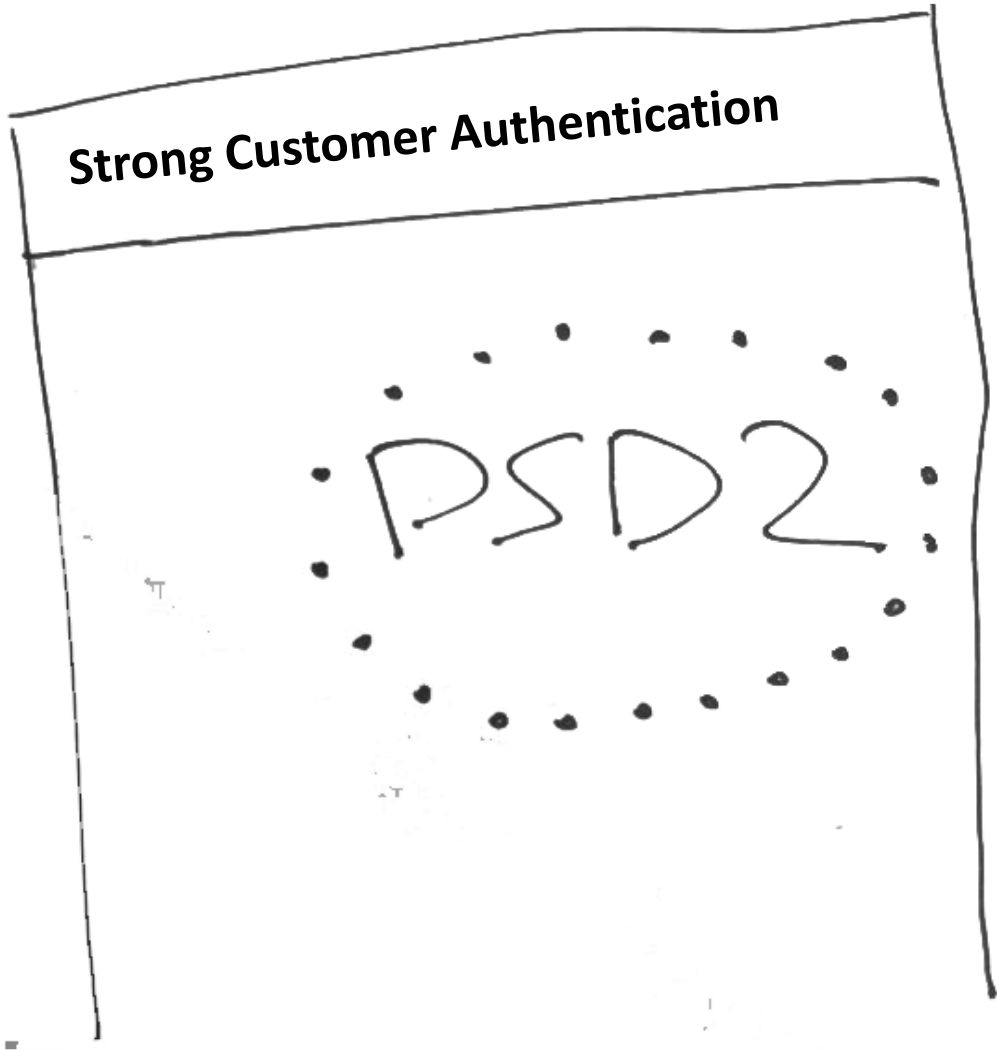
Good example of sensible limits

Applies only within the EU

Not implemented in every card

Has a lot of bypasses

https://www.cyberdlab.com/insights/card-fraud-in-a-psd2-world-a-few-examples



DIFFERENT VISA CARDS

EU cards require Online PIN

USA cards require Signature

UK cards require using chip

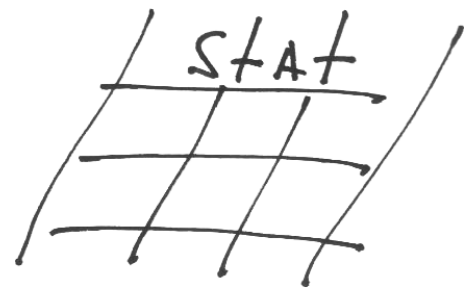
- Change CTQ to “Signature” or to “NoCVM”
- Change CTQ to “NoCVM”
- Change CTQ to “CDCVM”, also change TTQ

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

#	Card/Bank	Status	Card	PIN	Brand	Country	Vendors	AIP EMV/NFC	Replay	CVMList	CDCVM	PIN OK	CVM
1	M	r	1288		MC	UK		3900/					
2		c			MC	UK		1800/					
3		c			MC	UK		3900/					
4		i			MC	UK		3900/					
5		c			MC	UK/EU							
6		g			MC	UK/EU		3900/					
7		g			Visa	UK/EU		3C00/2000					
8		r			MC	US		.					
9		i			MC	UK		3900/					
10		i			Visa	UK		3c00/					
11		r			Visa	UK							
12		s	9006	?	Visa	UK/US		3800/					
13		v	2360		MC	UK		3900/	+				
14		v			Visa	US		1800/-					
15		v	1633		MC	US		1800/					
16		v			MC	EU		3900/					
17		g			MC	EU							
18		c			Visa	UK		3C00/					
19		i			MC	UK		3900/					
20		i			Visa	UK		3C00/					
21		v				UK/US			-				
22		i			Visa	UK		3C00/0020					
23		i			Visa	UK							
24	i	p			Visa	EU		/2000	?				
25	i	i	0124	5675	MC	EU		-/1980	+				



	Contactless	EMV
mastercard	CDA is mandatory	CDA is not mandatory (18/20)
VISA	CDA is never required	CDA is required sometimes (1/14)

Contactless

EMV

CDA is mandatory

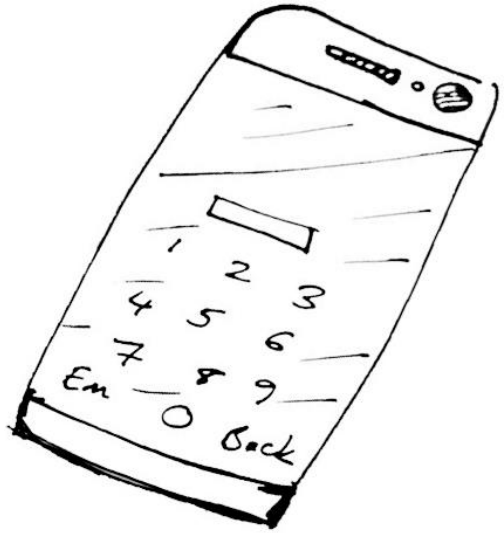
CDA is not mandatory (18/20)

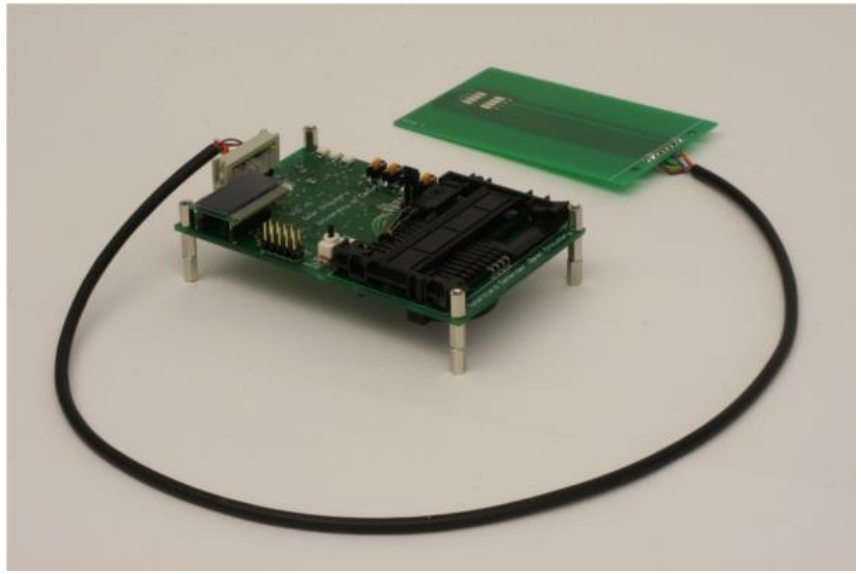
CDA is never required

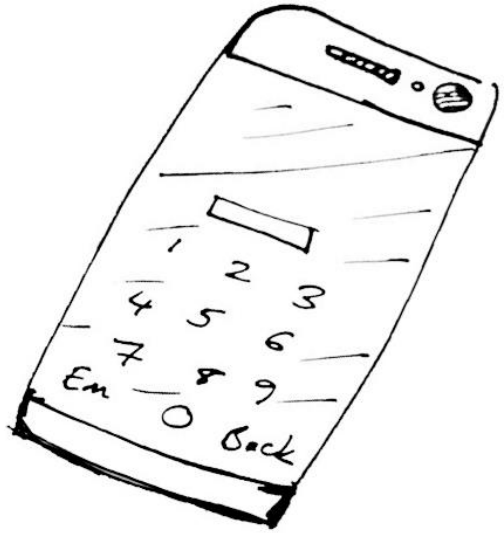
CDA is required sometimes (1/14)

Contactless

EMV







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

ATC
Track2 Equiv
CTQ

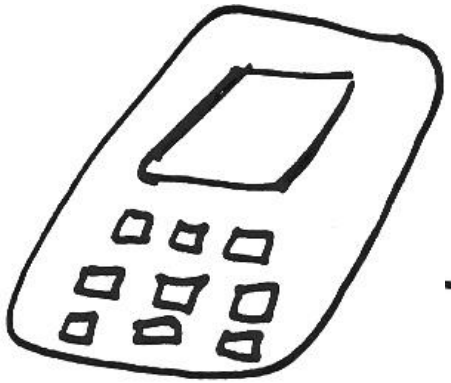
CDCVM=1

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

VISA

Currency
Amount
UN
TTQ

CVM REQUIRED=~~1~~ 0



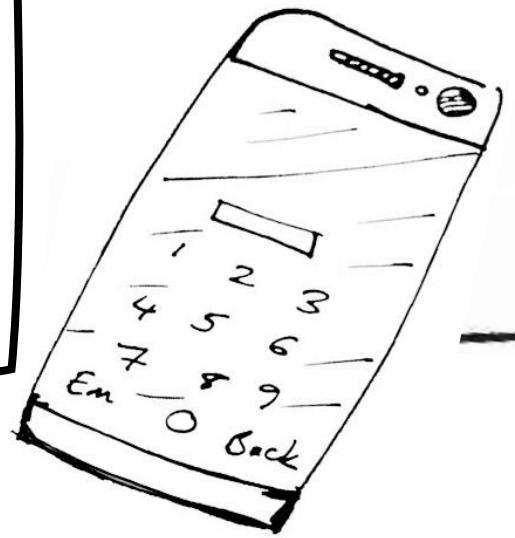
Acquirer

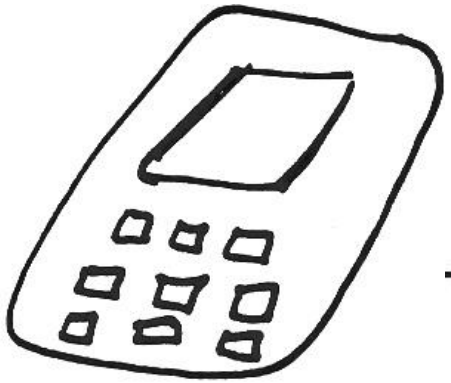
CTQ “CDCVM Performed” value is always 1 for consumer devices

CDCVM=1

Currency
Amount
UN
CVMResults

CVM REQUIRED=~~1~~ 0



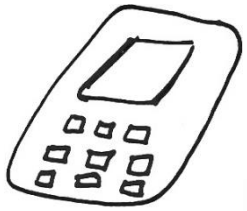


Acquirer

mastercard

ODA

*CDA



- CVM List Location

*PIN, Signature, No CVM

VISA

Currency £
Amount 10
UN AAAAAAAA

ATC
Track2 Equiv

mastercard

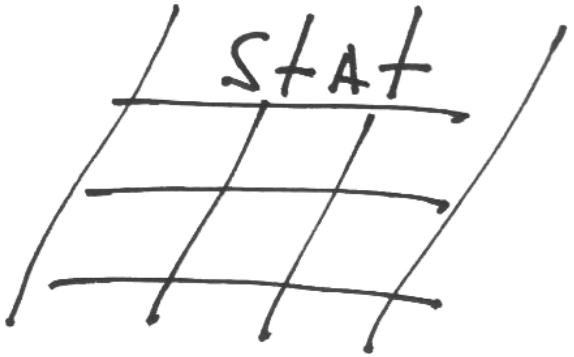
Currency £
Amount 10
UN AAAAAAAA

ATC
Track2 Equiv

Currency £
Amount 10
UN AAAAAAAA

ATC
Track2 Equiv

HOW MANY ARE AFFECTED?



It's not a
VISA/MC issue

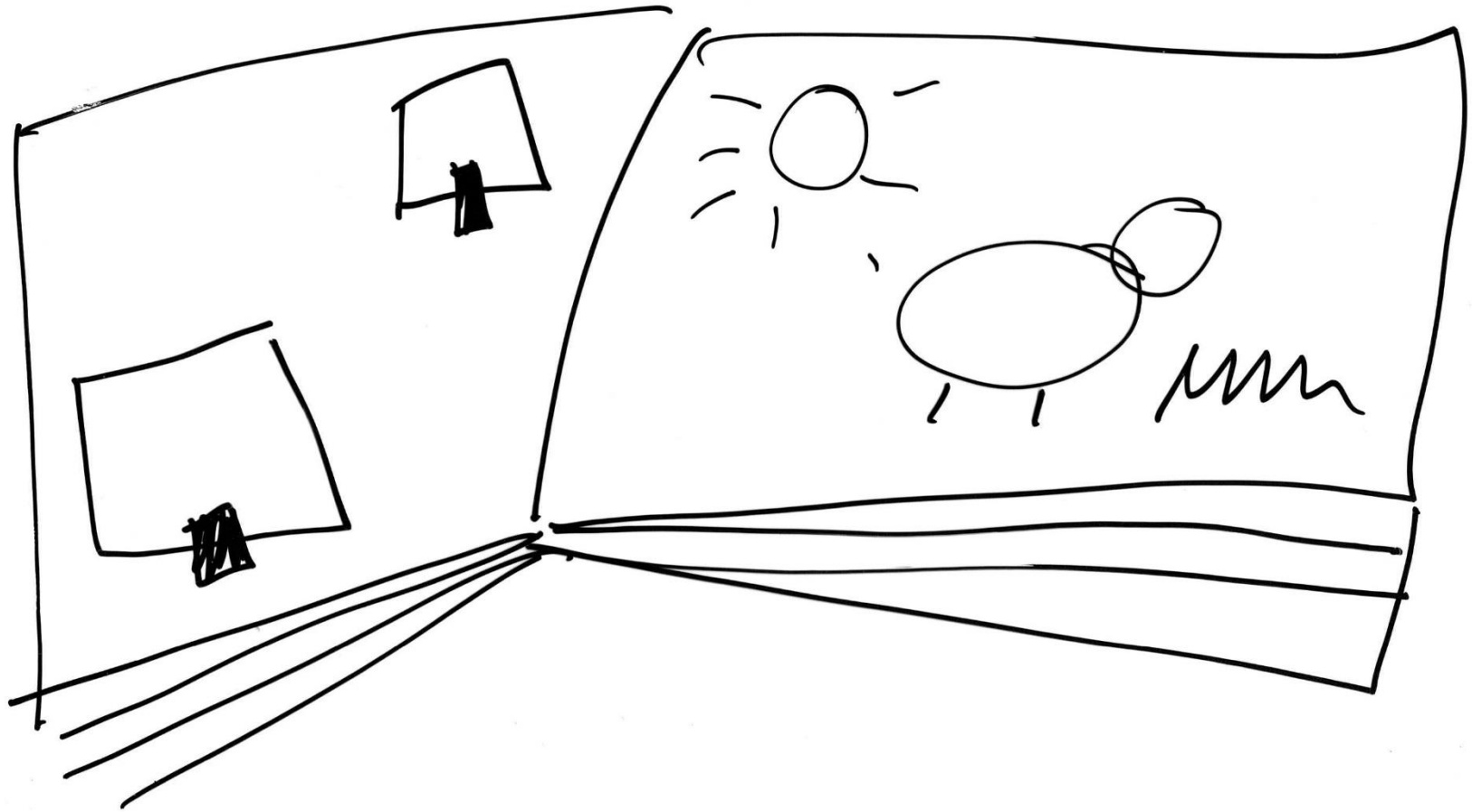
21 MC
10 VISA cards*

* UK, EU, US, Asia

11 MC
7 VISA
allow replay

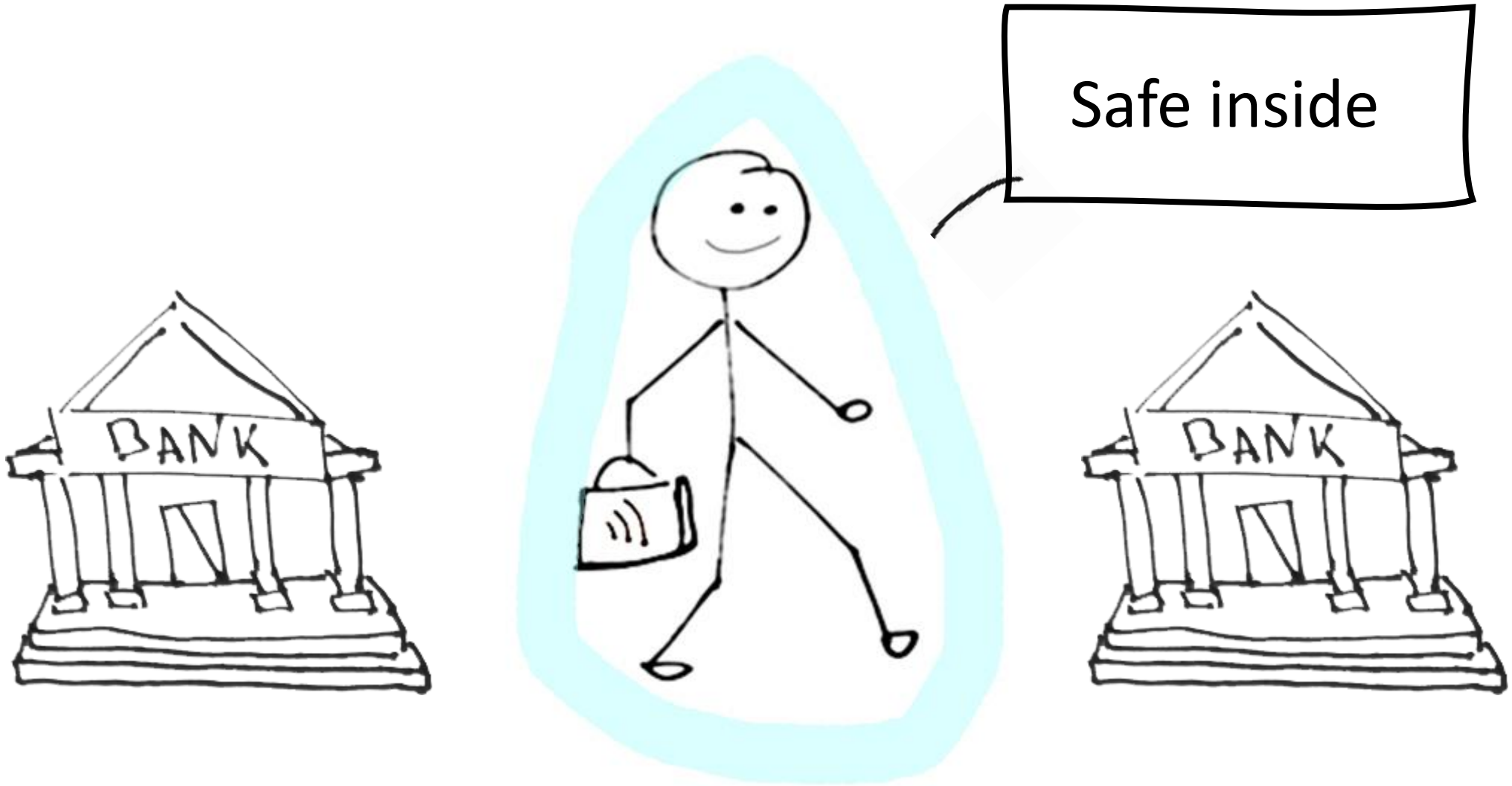
Max delay - 11d
Max replays - 12

CONCLUSIONS



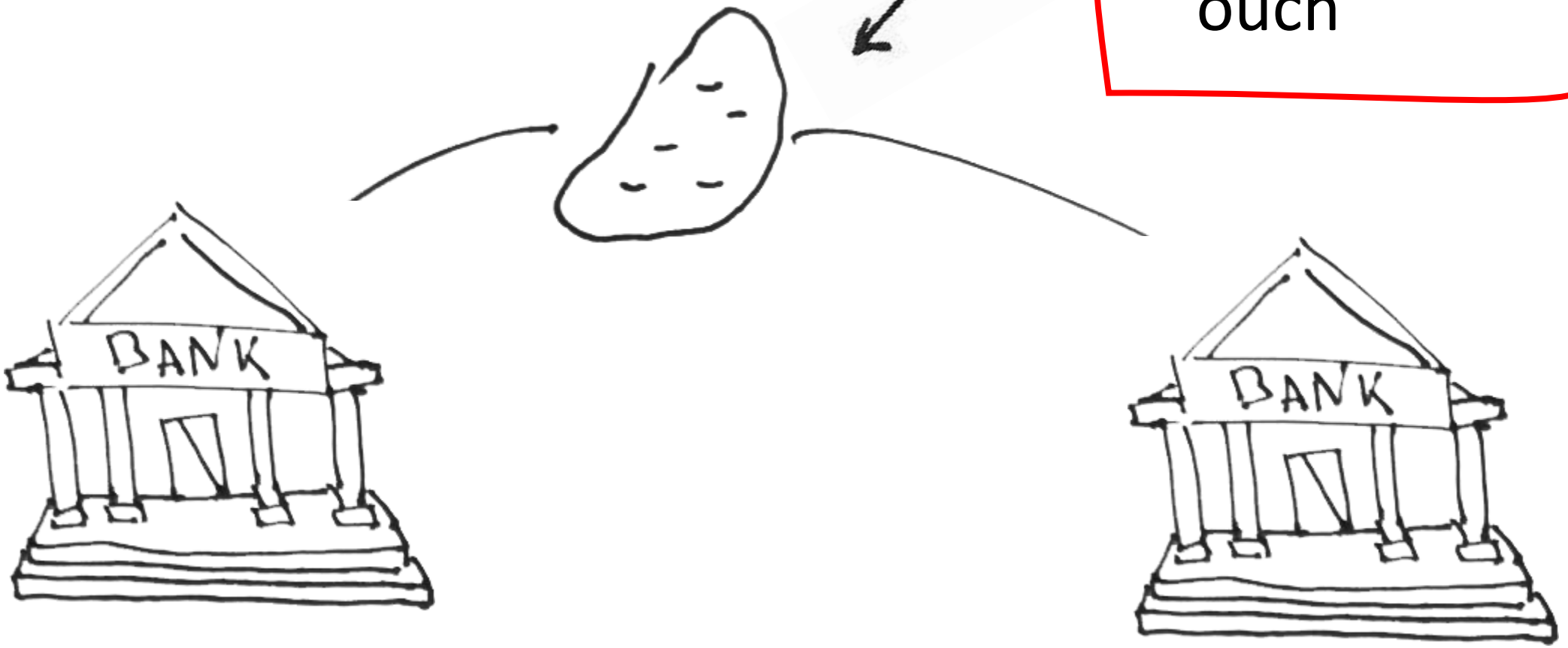
57 cards:
EU
USA
UK
Asia

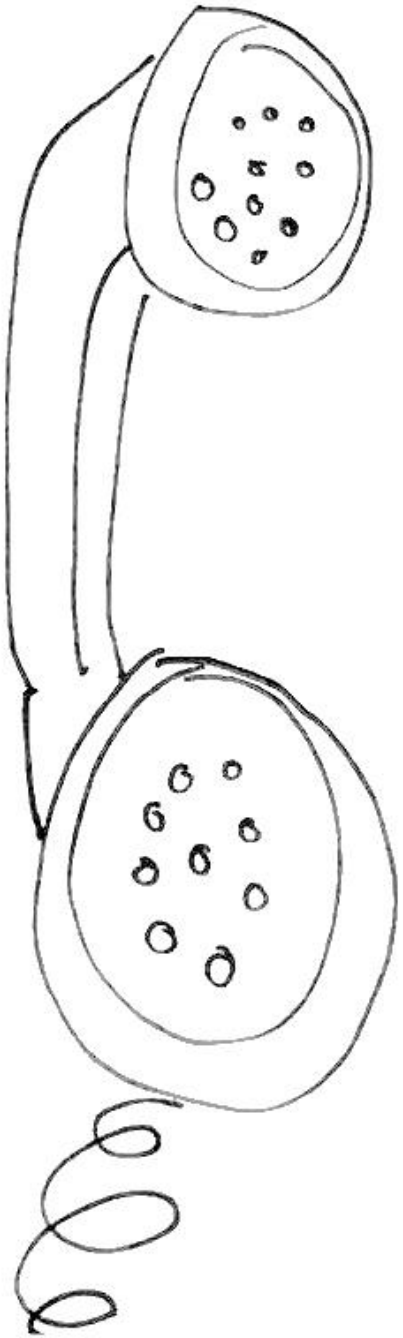
THE GOOD NEWS



BLAME GAME

Hot potato
“ouch”





PAYMENT RESOURCES

securingpayments.com

leigh-annegalloway.com

cyberdlab.com

Whitepaper available here

CONTACT

@a66ot

@L_AGalloway