



Electronic Payments, Technology, Risk, Security, Compliance



Nicolas T. Courtois



Cryptologist, Data Security and Smart Cards expert



- University College London, UK

Roadmap

- enquiry about the nature of money:
 - gold → electronic records
- electronic payment technology (bank to bank)
- compliance and personal / financial data protection
 - EU has much higher standards for personal data,
 - US has lawyers (!!!)
 - limitations / liability / encryption / access control
- bank cards,
 - security, fraud
- compliance: credit card data, most recent trend:
 - PCI DSS compliance: forbids to store certain data

Intro



Payment Technology: Evolution

Money

Key invention
in human history:

money



- here is some money for your research

Two Main Functions of Money

1. Store Value

2. Allow Payment

(3. Unit of Account)

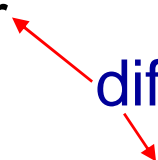
⇒ progressive separation
of the two functions 1. 2.

⇒ Both money and payments becomes more
“virtual”...

Evolution of Money – Store Value

- Precious natural resources: salt etc
- Gold, Silver, Other Metals => Coins
- Paper Money
- Money as **Electronic Record**
+ Legal Protection + Government Guarantee
- Future: Cryptographic E-Cash?

Evolution of Payments

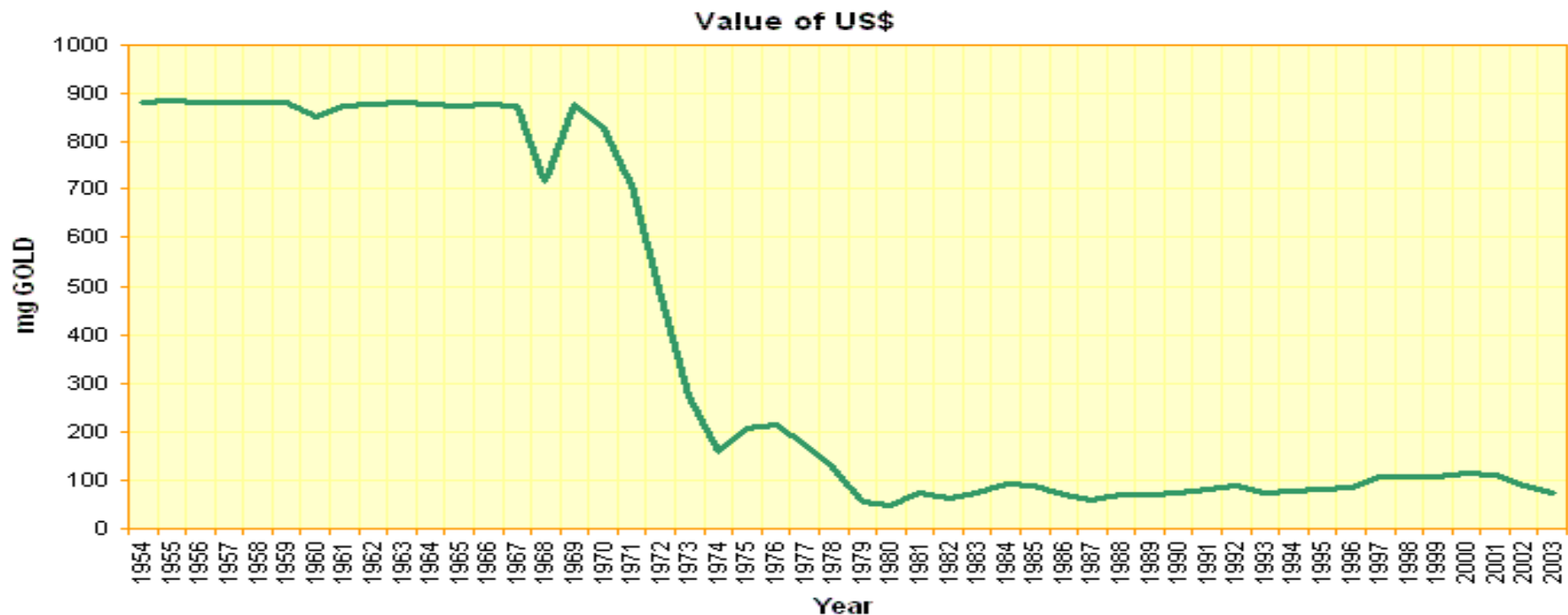
- Physical Cash (Bank Notes, Coins) = M0
 - Cheque = Check Books
 - Electronic Bank Transfer 20 days => 15 min...
 - **E-Purse Systems:** geldkarte, London Oyster
 - **Bank Cards**
 - **Contact-less Bank Cards**, e.g. MasterCard PayPass:
 - Future: Cryptographic E-Cash...
- difference?
- 

Gold = “Global Single Currency”??

Most countries abandoned the gold standard during the Great Depression,

– one of the earliest was the Bank of England [1931].

Much later, in 1971: the United States abandons it. Nixon Shock



***Problems with Gold

Gold would make the work of central bankers impossible.

Problems with gold:

- the quantity of gold does not change, while the global GDP grows.
- the supply of money would be at the mercy of exogenous factors
- and foreign countries (!).
 - some countries have vast gold mines (Russia), other vast reserves (US).
 - they will be able to make money out of thin air, and provoke inflation at a global level (they will be able to devalue the currency of other sovereign nations at will).
- Storage of gold is VERY costly.
- Gold has primary usages (Jewellery, chemistry, electronics).
 - Primary users of gold would be priced out. Bad for the economy.

“Fiat Money”

Def:

Government-issued money not convertible for anything particular
(E.g; gold, goods etc).

Its value is controlled by the monetary policy
and managed by the central bank.

increasingly independent from governments now,
but subject to (much slower) legislative regulation.



What Is Money?

each central bank has its own definitions!



+ liquid

- **M0: Monetary Base**

- Cash: bank notes + coins
- reserves hold by banks with BoE
- government money hold at BoE

⊆

M0 = monetary base
= narrow money =
reserve money =
central bank money

- **M1: Demand Deposit Accounts**

- available at any moment,
- can withdraw/deposit any amount

⊆

M1-M0 = private
money = checkbook
money = "debt
money" = money @
commercial banks

- **M2: Time Deposits (@bank)** up to few years

⊆

- **M3/M4:** not quite official status anymore:

repurchase agreements + Money

- Market Funds (not @bank, not insured) + debt securities up to 2 years + some other liquid assets...

- liquid

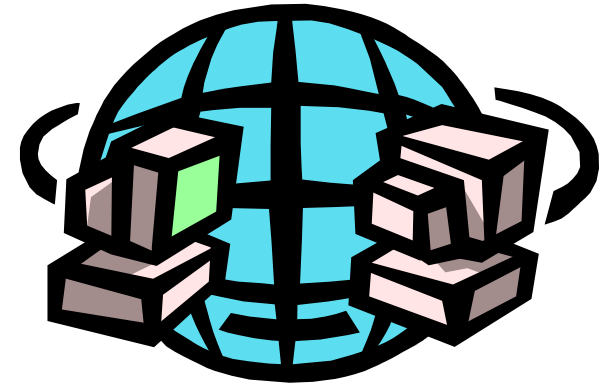
broad
money
=M4

Side Remark

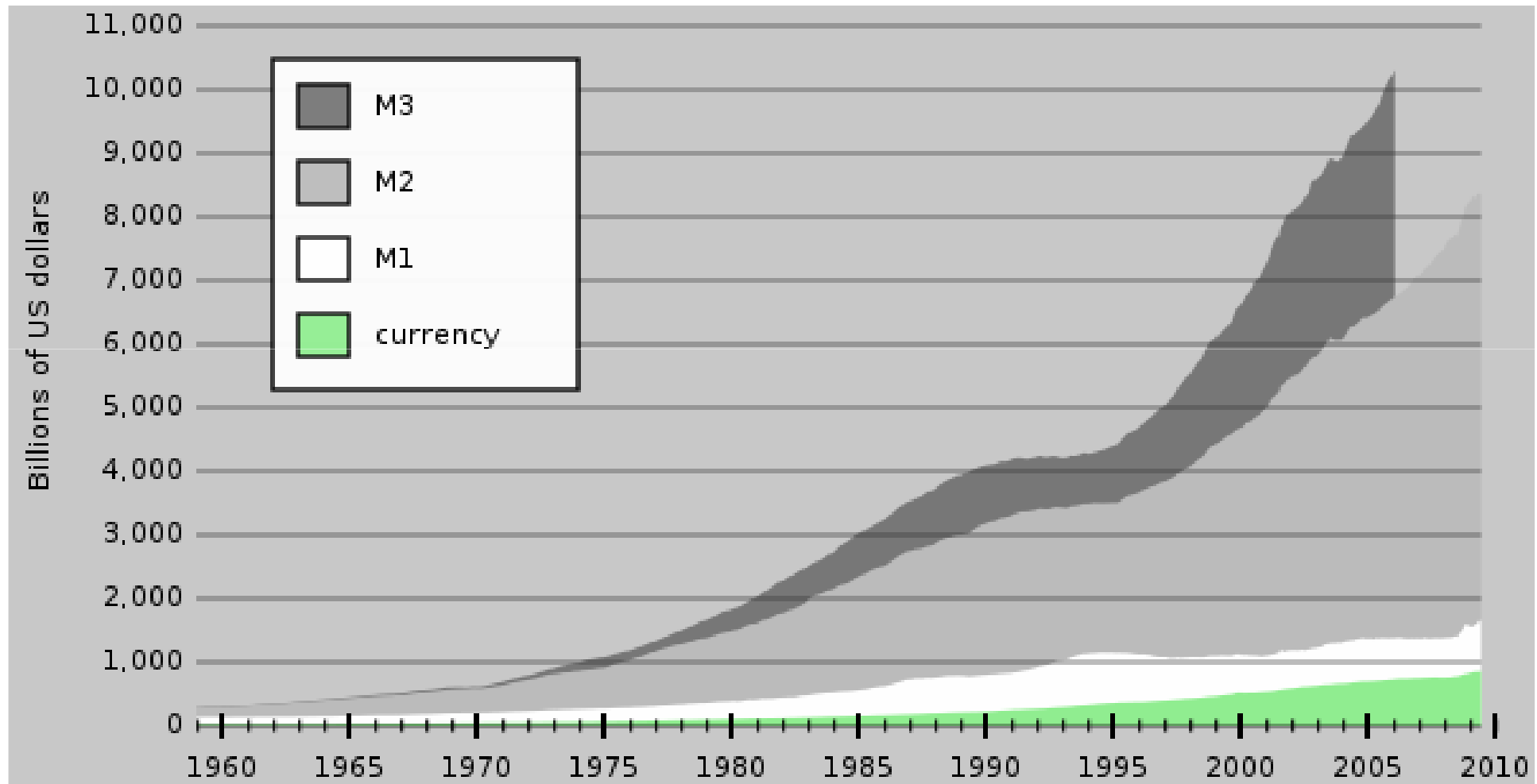
Most money is now just an electronic record.
Nothing else.

Huge potential for

- identity fraud,
- disruption,
- data loss,
- electronic forgery,
- conspiracy to defraud
 - e.g. against the bank, like fraud on credit applications,
- selling financial data for profit
- etc etc..



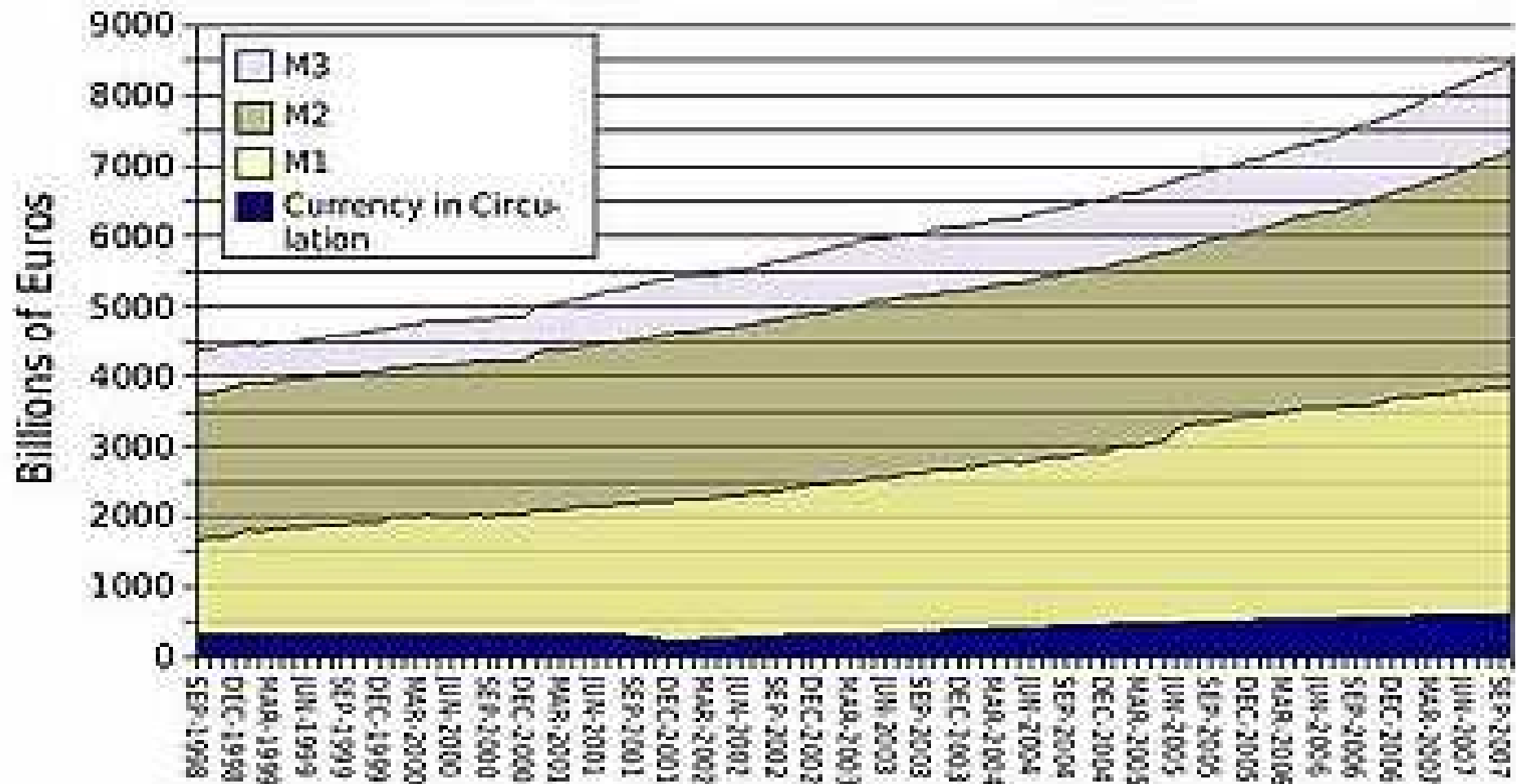
Money In Existence - US



**half is held overseas

Money In Existence - EU

Euro Money Supply Sept1998-Oct2007 (seasonally adjusted)



Where Does Money Come From?



Creation of Money

M0: Central Bank Monetary Base

central bank controls its quantity strictly

2009 BoE: quantitative easing 200 G£



M1: Demand Deposit Accounts

commercial banks **create** money each time they issue loans

fractional reserve system, e.g. 10 %



In fact 10 % leads to a multiplier of 10x

$$m = \frac{1}{R}$$

*License to Print Money?

Banks hold a “banking license”
from the government.

They collectively, in one given country,
have a monopoly for the creation of M1 and M2 money through the cycle of
successive loans and deposits.



Money created out of thin air?
Not quite. Prudence is required.

- It depends on the supply of borrowers willing and able to pay back these loans + interest.
- It depends if the government is willing to bail out the banks when they go bust (!)

*Money Reserves

Deposits: is our money ever hold by the bank?
almost never happens.



A commercial bank holds some reserves.

- Cash in vaults.
- Cash inside ATMs.
- Deposits with the central bank

Obligation to hold only (?) or as much as(!)
a fraction of their deposits as a reserve.

*What About Time Deposits?

M2-M1:

No reserves are required
against time deposits or savings accounts.

So any bank **can** create an infinite amount of money
if they loan money from Time Deposits to people
that will deposit them in other Time Deposits.

- in practice the quantity of M2 remains moderate:
 - how do you prevent people from putting the money into Demand Deposits? M1 is subject to reserve requirements!
 - bank regulators should prevent M2 from growing too much.
 - » Liquidity management at T+X years

***Financial Innovation

Interesting:

In 1997-2007, in the US,
the quantity of M2 money increased by 84%,
yet total banking system reserves decreased by 10%.

Miracle of “innovative banking”.

- for example banks created deposit accounts for 1 day, for which they didn't have to hold reserves.

**Destruction?

- Central Banks do also destroy the money at occasions:
 - the recent 200 billions of quantitative easing: they announced they will withdraw a big part of these later on!
 - Thus restoring the value of £ outside the UK.
- Commercial banks have however **no incentive** to ever destroy it. And they never do.
 - known as ‘banking reflux’. Source of inflation.

***Ever Growing Monetary Expansion

Fact: Banks only create the money for the principal of loans.

- so where does the money for interest payments come from?
 - either the central bank prints it (new M0)
 - or it must come from other loans! (new M1)
- Then, **if** people don't default on their loans, the monetary supply must double after typically about 14 years...

– All perfectly OK if there is always economic growth.

- But imagine that the recession is really bad and the real GDP is really much lower. Money in circulation remains.
 - » the obvious conclusion is that the Western banking system cannot survive if the economic growth stops, because the technology/productivity stops improving etc etc.

Cost of Money



Costs of Running the Cash Money System

Paid by the taxpayer in some indirect way.

Cost of printing + wear and replacement costs + fixed costs + distribution costs.

- 0.05 \$ / note in the US.
- UK: 2,3 billion notes in circulation, total cost = 100 M£.
 - Note: overheard at BoE: about 4 p per note
 - Coins: some made at loss: 1 p coin costs 1.7 p to manufacture (!!)

Extra costs almost certainly not accounted for:

- Cost of holding gold and foreign currency reserves
 - very large, pure opportunity costs
- Security costs: policing the fraud, checking if real, etc.
- Foreign policy: who can prevent Iran from printing US dollars?

Legal Aspects



Legal Tender

Law: Legal Tender = Forced Tender

Cannot refuse cash as a payment of debt (or tax).

- anyone refusing such monies for their whole value can be prosecuted (!)
 - Penal offence in France!
 - US: all Federal reserve notes are legal tender.
 - UK: very narrow meaning:
 - means only that, a debtor cannot successfully be sued for non-payment.

Can refuse in a bus, restaurant, vending machine.

Example: 50 £ notes are very frequently refused.

UK: Only 1,2,5£ coins are legal tender in the UK.

Bank notes aren't. Pay exact amount of a debt in 1£ coins – this cannot be refused or you don't have to pay.

Cash is Anonymous => Suspicious

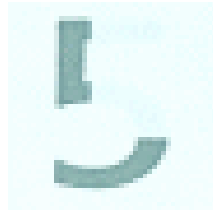
Banks cannot refuse cash payment of debt.

But in most countries they report all 'larger' cash payments to authorities.

Legal Protection

- Legally **OVER-PROTECTED** in most countries.
For centuries. Very heavy criminal penalties.
- Bank Cards: also over-protected.since very recently
(2001+ in France, 2005+ in the UK). Credit card fraud = **0.15 %** typically.
- Paypal fraud: **0.20 %**.
- Money on your Oyster card – not money,
 - not a proof of deposit not even a proof of pre-payment
 - TfL will be the only judge if credit is valid or not.
 - does NOT enjoy any similar level of legal protection,
 - business between me and TfL.

**Security Features



Fighting Counterfeit Money

Very heavy criminal penalties.

- Using it is always the crime.
 - ≤ 10 years in the UK [Forgery and Counterfeiting Act 1981]
- Buying, owning or using equipment or materials that could be used to manufacture counterfeit currency:
 - ≤ 5 years. [Proceeds of Crime Act 2002]
- In contrast, it is 100% legal to make a perfect Van Gogh painting.
 - And sell as a “perfect copy of Van Gogh”.

Counterfeit Cash:

1 in 4 Million banknotes in the UK is false.

SURPRISINGLY LITTLE.

Quickly reported (90% by retailers, 10% police) and withdrawn.

Forged Notes and Serial Numbers

Average of about 500 M forged bank notes per year.

- Compare to billions of notes in circulation – very little.
- Few billions of £ of profits.
- Big variations, gangs come and go each year.
 - In 2002 half of notes forged were £20,
 - In 2004 only £20 notes were forged => All £20 notes withdrawn in 2010.

Frankly nobody forges £50 notes, yet everybody looks at them with suspicion.

BoE: Only 10 to 12 different serial numbers per each criminal production!

Yet BoE so far does NOT publish these serial numbers.

There is no black list. (other means of detection seem secure enough).

But really for strange reasons. They could and they should.

Payment - UK

Payment

- Cash payment.

- Alice

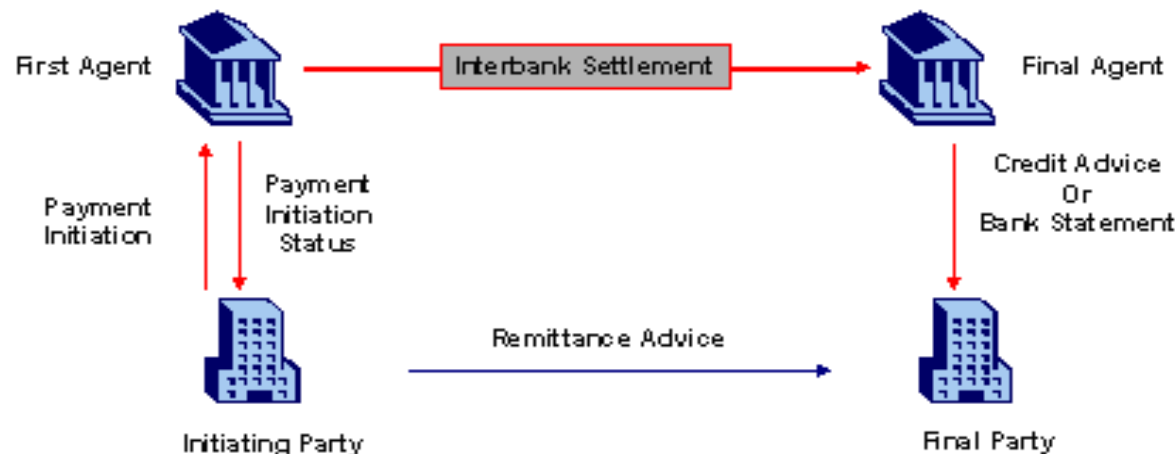
- M1 deposit → M0

Bob

→ M1 deposit

- Electronic Payment.

- M1 → M1 - deposit in another bank.



Cash Money

Usage is declining.

All cash in circulation was 6% of GDP in 1970.

About 3% today.

In recent 2 years

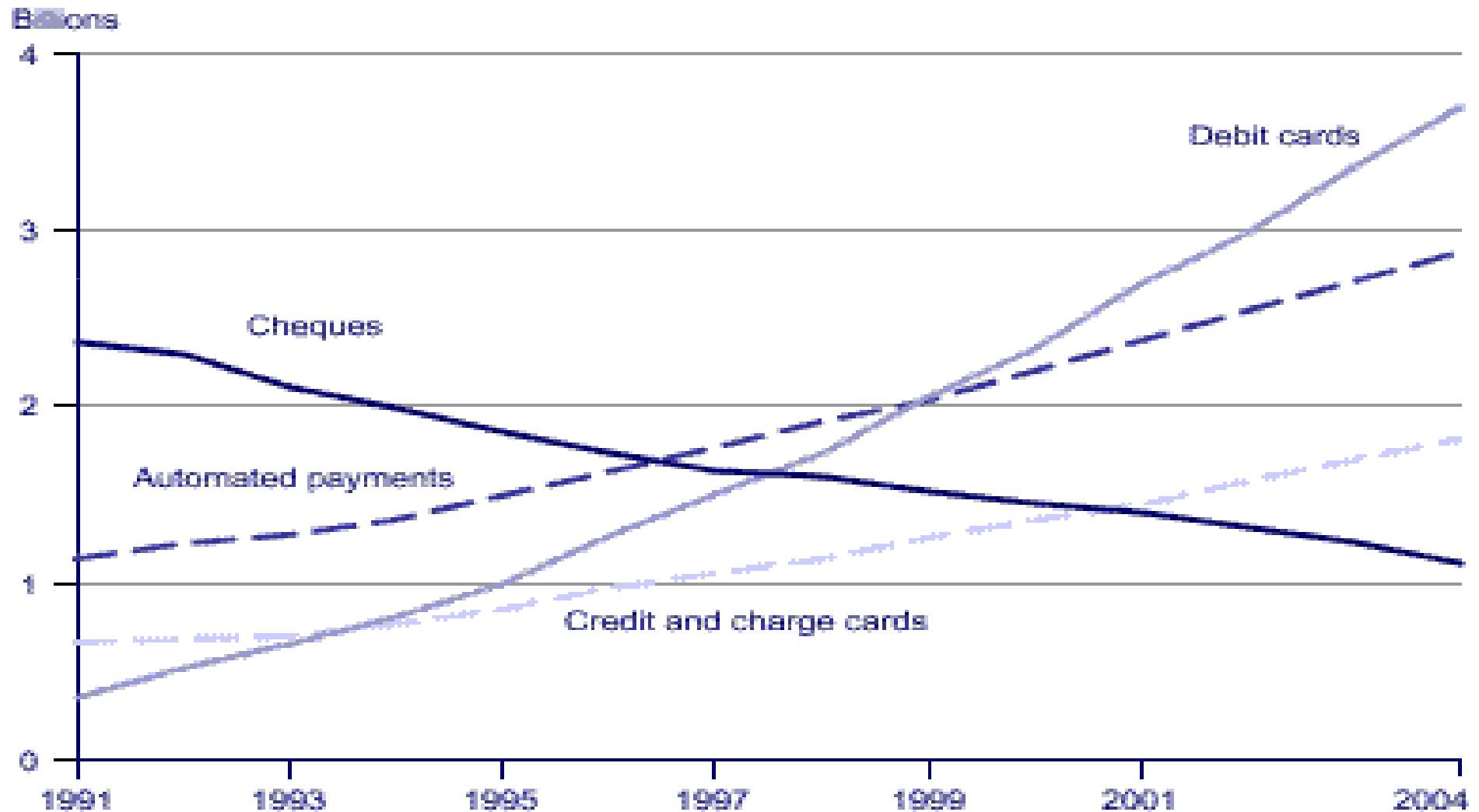
- the payment usage is further declining,
- BUT due to low interest rates, people keep MORE cash at home

Cheque Usage



UK: existed for 352 years.

Steady decline since 1990.

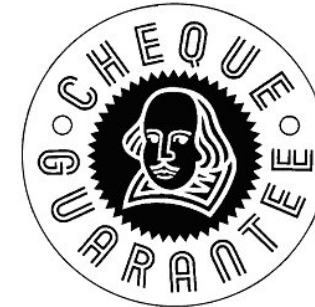


**Cheque Guarantee Cards

UK-specific scheme – UK has no ID cards.

Existed since 1969.

will close in 2011



- A stand-alone card.
- Or hologram at the back of your debit card.



Terminal Decline

Problem: cheques are **insecure**,
very **costly to process**, and banks
find themselves bearing most costs.



It is official:

In Dec. 2009 the UK Payments Council Board
has agreed to **close** the UK
central cheque clearing house by 2018.

Electronic Payment

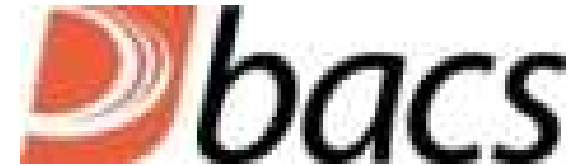
Two basic scenarios:

- Bank A → → → Bank B
 - Cheque
 - “Wire Transfer”
 - Debit card payments
- With another (third) company
 - Payments with credit cards
 - With delayed payment (like 56 days) and revolving credit aspects
 - PayPal = Single Sign-On system
 - competitors:
 - BT Click and Buy
 - Google Checkout



UK Electronic Bank-to-Bank Payment

- BACS – 3 working days,
 - Bankers' Automated Clearing Services
 - created in 1968, magnetic tapes transported between banks(!)
 - since 1983: uses telephone lines (BACSTEL)
 - since 2003: uses Internet (BACSTEL-IP)
 - known as “inefficient and archaic”
- CHAPS: same day system,
 - Clearing House Automated Payment System
 - Company established 1984
 - Expensive: banks charge you like £30 per transfer.
 - Guaranteed to be received on the same day
 - Also use in direct B2B payments
- FPS: Fast Payments Service. May 2008.
 - 24/7, close to real-time service (like 15 min)
 - able to handle lots of small payments too (like 1p)



Choice?

Most people have no choice.

Systems remained very very slow for years,

- banks used “the float” at their discretion...
 - In 2001 wire transfers in the UK still took **4.2 days** on average,
 - 34 days with certain UK banks, 2nd worst in the EU after Italy, source: EU commission
- today banks, with available technology and after many government and EU interventions, will automatically use FPS when available for a given sort code.

http://www.ukpayments.org.uk/sort_code_checker/



Types of Payments

- Immediate one-time payments
- Standing orders
- Return payments (for example if bank account was closed or changed)

http://www.ukpayments.org.uk/sort_code_checker/



Running Fast Payments Service [2008-now]

- The network is run by a company called VocaLink
- The clearing is managed by the CHAPS clearing house
- Daily volume: >5M transactions, >1 G£



Payment - EU and Global



Payments in the EU



2002: creation of the
European Payments Council (EPC)
== private consortium run by banks.

A Single European Payment Area (SEPA): self-regulatory
initiative about technical harmonization of (electronic)
payment systems.

EU: The Payment Services Directive (PSD)
(2007, UK implemented it in Nov 2010).

Payment Services Directive (PSD) - Regulation

A piece of government/EU industry regulation.



Goal: create a single European payment space

Intention(?):

lower prices – maybe prevent banks from charging £30 for every wire transfer, because systems are fully automated now...

- only pushed that far inside the € zone. Since 2003, banks must charge the same price in the whole € zone, as in the home country.

Payment Services Directive



What was done in practice:

- lower barriers for entry for competitors,
 - in particular easier “authorization”: institutions authorized to handle payment business in the UK (not only banks but so called authorized payment institutions, e.g. e-money issuers), can do business in any EU country!
 - smaller businesses can handle payments with registration only, cannot “passport” to another EU country though...
- compliance: establish common standards
 - also common rules for liability for fraud,
- handle refunds
- mandate transparency of prices and charges
- access to payment systems must be non-discriminatory (!)

***What Was NOT Done So Far

- Neither by bank self-regulatory body (EPC) nor by the EU Commission (PSD Directive).
- so far there is no pan-European electronic payment infrastructure
 - (all is handled through existing international systems)

Global Payment and Clearing

UK CHAPS is connected to the **Target** system
(**T**rans-**E**uropean **A**utomated **R**real-time **G**Gross
Settlement **E**xpress **T**ransfer **S**ystem)

- connects 16 EU countries and their real-time gross settlement (RTGS) systems.
- runs over the SWIFT network mainly

Global Payment and Clearing

The consortium of ECB + 27 EU central banks have created the **Target2** system, running since 2007.

2 countries: Sweden and UK have opted out!



Global Infrastructure Backbone - Swift

Swift - Society for Worldwide Interbank Financial Telecommunication.

They handle inter-bank **communication networks (only)** worldwide.

Belgian cooperative company. Owned by member financial institutions. Two 'secret' data centers (Netherlands + US).

Swift is the originator of most current standards and encoding conventions in financial messages. Later becoming ISO standards. Example: IBAN.

>50 % world's GDP transits here, \$2 trillion / day,

- but they don't do transaction, don't settle or clear payments.
- Just a telecom company transmitting messages and guaranteeing their authenticity and confidentiality.
 - » payments are handled by banks themselves with a variety of bilateral, national and international payment, settlement and clearing systems.

Swift and Data Security

Swift – they do provide:

1. cryptographic **authenticity** of messages (since the 70s)
 - their business model was trusted third party, remember digital signatures did not exist at that time
2. **encryption** was added much later,
 - as cryptography was only deregulated in the late 1990s
 - all traffic is decrypted in Swift's central systems, then encrypted again
 - do cooperate with law enforcement authorities, no comment policy
3. **cryptographic key management**:
 - bilateratal (diplomatic suitcase) until 2008.
 - now changed, new RMA protocol.

Swift and Data Security



Swift – is audited once per year:

- compliant with the (quite old) US norm SAS 70.
 - concerns business procedures and internal controls.
 - cf. Information security management, ISO 17799 and 27002.
- Swift are known for having some quite robust procedures:
 - Example: [Segregation of Duty / Dual Control](#): two security officers: [left security officer](#) and [right security officer](#). Both must cooperate to allow certain operations.
- This SAS 70 audit report is however not public.
- And it doesn't cover much.
 - SAS 70 = internal controls: a small subset of today's SOX compliance
 - the 'accounting' company SAS 70 never had any expertise at all in any of the technical aspects of data security...

Swift Personal Data Protection Compliance

Swift US data centre is also certified 'Safe Harbor compliant'.

- Safe Harbor certification scheme is a streamlined process run by US Dept. of Commerce in cooperation with the EU,
 - for US companies to comply with the EU Directive 95/46/EC on the protection of personal data.
 - EU commission officially says it is OK but it was controversial if safe harbour really does comply with the directive.
 - swift promised will however stop mirroring their data in the US asap.



Risk and Fraud



Interesting Statistics



In English-speaking banking industry,

- 1% of all staff are sacked each year because they **have embezzled** some money
- **no method known to predict which staff will go bad.**
 - it seems that people turn bad due to some specific reasons, such as alcohol, drugs, gambling or divorce, but these really cannot be predicted in advance.
- if it is a **senior** people that go wrong, banks go into great lengths to hide this fact from the public opinion...

“if a senior people go wrong”? The Bigger, The Better



In 1938 a large US drug and chemicals company has collapsed.

20 % of recorded assets and inventory was nonexistent:

- the President + three brothers with key positions.
- they have set up several fake companies abroad + bogus shipping company + a fake bank.
 - the auditors did not notice anything, all the accounts looked OK.
 - No one could check if assets (money in banks, stocks of raw material) do really exist...

Good Bye \$\$\$...



Conspiracy will always work(!!!). Example.

Paul Stubbs, a password reset clerk at HSBC conspired with “somebody” inside one of the HSBC’s customers, AT&T to change the password that AT&T used to access their bank account remotely.

- the password was reset
- “somebody” used it to transfer \$20 M to offshore bank accounts
 - the money was never recovered!
- a vulnerable young man, the court took mercy on him and he got away with 5 years...
 - now if he still has the money (who knows?), for each hour spent in prison, he will earn 600 dollars

Data Security and Compliance

Swift and Data Security



Swift – is audited once per year:

- compliant with the (quite old) US norm SAS 70.
 - concerns business procedures and internal controls.
 - cf. Information security management, ISO 17799 and 27002.
- Swift are known for having some quite robust procedures:
 - Example: [Segregation of Duty / Dual Control](#): two security officers: [left security officer](#) and [right security officer](#). Both must cooperate to allow certain operations.
- This SAS 70 audit report is however not public.
- And it doesn't cover much.
 - SAS 70 = internal controls: a small subset of today's SOX compliance
 - the 'accounting' company SAS 70 never had any expertise at all in any of the technical aspects of data security...

Swift and Data Protection Compliance

Swift US data centre is also certified 'Safe Harbor compliant'.

- Safe Harbor certification scheme is a streamlined process run by US Dept. of Commerce in cooperation with the EU,
 - for US companies to comply with the EU Directive 95/46/EC on the protection of personal data.
- EU commission officially says it is OK but it was controversial if safe harbor really does comply with the directive.
 - Swift promised they will however stop mirroring their data in the US asap.



2 Types of Data:

Frequent distinction between:

- **Personal** Data (name, address, family details etc...)
 - More related to privacy...
- **Financial** Data: account number, credit history, etc...
 - More related to security and fraud...

But in fact...

Both types of data are used by criminals.

Scope of « Personal Data »?

“any information relating to an identified or identifiable natural person ('data subject')”

- seems every data is personal data???

A more precise notion is

[as appears in US standards, e.g. NIST]

Personally Identifiable Information (PII) = def

- Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

EU Data Protection Directive

95/46/EU [1995]:

must implement measures ...

to protect **personal data** against:

- unauthorized disclosure or access,
- Weak and not very specific...
 - Do we encrypt the data?

EU: Data « Controller »

Art 2D: **Controller** = person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

- Doesn't have to be in the EU. It is sufficient that the data **or** the “data subjects” **or** the computer equipment used to process the data is inside the EU (!)

Obligations for the controller:

- **Each member state must** set up a data protection supervisory **authority**.
- The controller **must notify** the supervisory authority **before** he starts to process data. The notification contains at least the following information (art. 19):
 - the name and address of the controller and of his representative, if any;
 - the purpose or purposes of the processing;
 - a description of the category or categories of data subject and of the data or categories of data relating to them;
 - the recipients or categories of recipient to whom the data might be disclosed;
 - proposed transfers of data to third countries;
 - a general description of the measures taken to ensure security of processing.
- This information is kept in a public register.

Trans-Border Flows of Data

OECD Guidelines

on the Protection of Privacy and Transborder Flows of Personal Data, [1999]:

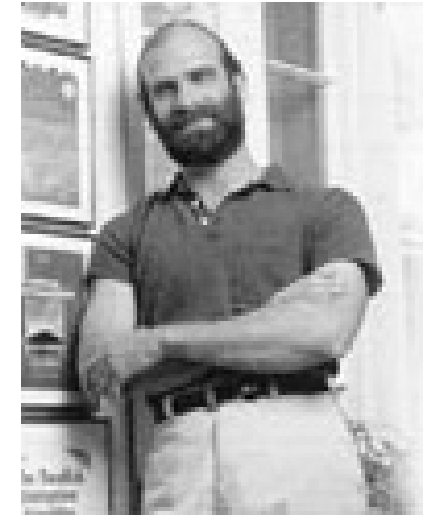
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

7 principles:

1. Notice
2. Purpose
3. Consent
4. Security
5. Disclosure—data subjects should be informed
6. Access
corrections
7. Accountability
data collectors

hold

Introducing Friends



Bruce Schneier
the “security guru” worldwide
[according to The Economist]
and high-profile industry consultant



A quote from Schneier

Cryptogram Newsletter, 15 February 2005,

..."As long as the banks are **not responsible** for financial losses from fraudulent transactions over the Internet, banks **have no incentive to improve security**. But if banks are held responsible for these transactions, you can bet that they won't allow such shoddy security."

And Yet Another from Schneier

Wired News October 6, 2005, "A Real Remedy for Phishers",

..."lawmakers need to do more than create new punishments for wrongdoers - they need to create **tough new incentives** that will effectively **force financial companies** to change the status quo and improve the way they protect their customers' assets. "

Innovation ← the US [again]

Some interesting things has happened in the last years...

- US approach:
let it happen, then maybe sue them. [Liability](#).
- EU approach:
protect, forbid, [Regulate](#)...

Both are methods of FORCINGLY promoting “GOOD” BEHAVIOUR.

Different approach, same objective.

Bank Laws and Regulations (mostly US)

Gramm-Leach-Bliley Act [GLBA]

1999, a.k.a. Financial Modernization Act

⇒ requires financial institutions
(and subcontractors) to adopt
strict privacy measures
relating to **customer data**.

Gramm-Leach-Bliley Act [GLBA]

1. **The Financial Privacy Rule:** regulates collection and disclosure of **all non-public personal financial information**: (e.g. is client ?, account balance)
2. **The Safeguards Rule:** defines safeguards to protect **customer data records**.
3. **The Pretexting Provisions:** specifically protect consumers from obtaining data under false pretenses.

A Setback - Recent Court Ruling:

[w.r.t. The Safeguards Rule]: - 20/02/2006

- An employee of Brazos had customer information on a laptop computer he was using at home. The computer was stolen, and a customer sued them [Minnesota].
- The judge dismissed the lawsuit and ruled that “[GLBA] **does not require that any nonpublic personal information stored on a laptop computer should be encrypted.**”

Schneier comment posted two days later:

we as a society need to force companies to encrypt personal data about us. Companies won't do it on their own -- the market just doesn't encourage this behavior -- so legislation or liability are the only available mechanisms. **If this law doesn't do it, we need another one.**

2005 “Data” Pearl Harbour

Wachovia and Bank of Am. crime ring:

- manually built a database of the 676,000 accounts (8 % of all New Jersey residents): names + social security numbers obtained by regular bank employees at work
(=> did 500 searches a day instead of 50)
- the information was sold to more than 40 collection agencies and law firms...

2005 “Data” Pearl Harbour (3)

Bank of America Tapes lost:

- the addresses and account numbers for 1.2 Million US government employees including 60 U.S. senators.

☹ Did not encrypt anything...

? Maybe the data are hard to access... Not sure how serious it is.

2005 “Data” Pearl Harbour (4,5,6)

From Schneier we learn also that:

- ChoicePoint sold personal data on 145,000 people to criminals
- LexisNexis exposed personal data on 300,000 individuals
- And Citigroup lost data on 3.9 million individuals

2005 “Data” Pearl Harbour (7)

Bruce Schneier, New York Daily News, June 23, 2005

“The epidemic of personal data thefts and losses...”

“...Real reform is required to solve these problems...”

- “reduce the amount of personal information collected, limit how it can be used and resold,
- require companies that mishandle our data to be liable for that mishandling...”

And (8), BTW, and it is not funny...

Why nothing like this have happened in Europe ?

Because of SB1386 (later about this).

Now in the US, such incidents **HAVE** to be **MADE PUBLIC**.

=> Must have happen in Europe...
and nobody knows...

Tougher Breach And Disclosure Regulations

California Security Breach Act [SB1386]

[July 2003] Designed to fight identity theft, huge plague in the US (not in Europe..), 214 K complaints/year.

The Act stipulates that **if there's a security breach** of a database containing **personal data**, the responsible organization **must notify each individual** for whom it maintained information.

Violation fines: up to 25 K\$ / day / person / prohibition violated !!!

California Security Breach Act [SB1386]

Many people interpreted this law as follows.

- You must ENCRYPT the data, otherwise you face huge negative PR impact.
- More than 18 states have passed related laws.
- Many people hoped that it would become a federal law.

The Devil Strikes Back...

...the federal bill, cleverly titled the **Data Accountability and Trust Act**, or **DATA**.
Lobbyists attacked the legislation in two ways...

- 1) the definition of personal information:
 - your full name -> DISCLOSURE
 - your first initial, middle name, last name, social Security number, bank account number, address, phone number, date of birth, mother's maiden name and password – DOES NOT HAVE TO BE DISCLOSED
 - "personal information" is defined as "an individual's first and last name in combination with ..." certain other personal data.

TOTALLY OUTRAGEOUS.

The Devil Strikes Back...

Lobbyists attacked...

2) went after the definition of "breach of security."

if a company loses a backup tape containing millions of individuals' personal information, it **doesn't have to** disclose **if it believes** there is no "significant risk of identity theft."

...the company could point to a study that showed the probability of fraud to someone who has been the victim of this kind of data loss to be less than 1 in 1,000 -- which is not a "significant risk" -- and then **not disclose** the data breach at all.

The Devil Strikes Back...

Even worse, this federal law pre-empts the 23 existing state laws -- and others being considered -- many of which contain stronger individual protections.

So while DATA might look like a law protecting consumers nationwide,
it is actually a law **protecting companies with large databases** from state laws protecting consumers.

The Devil Strikes Back...

Schneier final word:

“We can at least **hope that** ...

Congress will refrain from ...

[...passing bad bills that override good state laws...]

...and helping criminals (!).

DATA

Not a law yet, the House passed it in Dec 2009,
now with the Senate...

Current text:

- spirit of disclosure left, much weaker obligations
- penalties were capped at \$5 million

UK and Breach Disclosure

On August 13th 2007 the House of Lords issued a report on “Personal Internet Security”. Recommends [after Schneier]

- a data security breach notification law to be voted
- legal liability for damage resulting from security flaws.

MA Leads the Pack- 2010

Mass. 201 CMR 17 Law. Effective Jan 1st 2010.

- applies to any business that handles Massachusetts residents' sensitive data **regardless of where that business is located.**
- If an incident occurs, organizations are required to alert the Office of Consumer Affairs and Business Regulation (OCABR) **and** the Attorney General **and** the affected party.
- The law also requires that when a company reports a breach that it also provide details of the steps that have been taken to prevent a breach from occurring again.

Plastic Money - Cards

Excessively High Fraud → Near 0 in 5 Months

US, Germany etc: 0.08 %,

Malaysia in 2001: 0.74 %,

=> chip card introduced quite LATELY in 2005

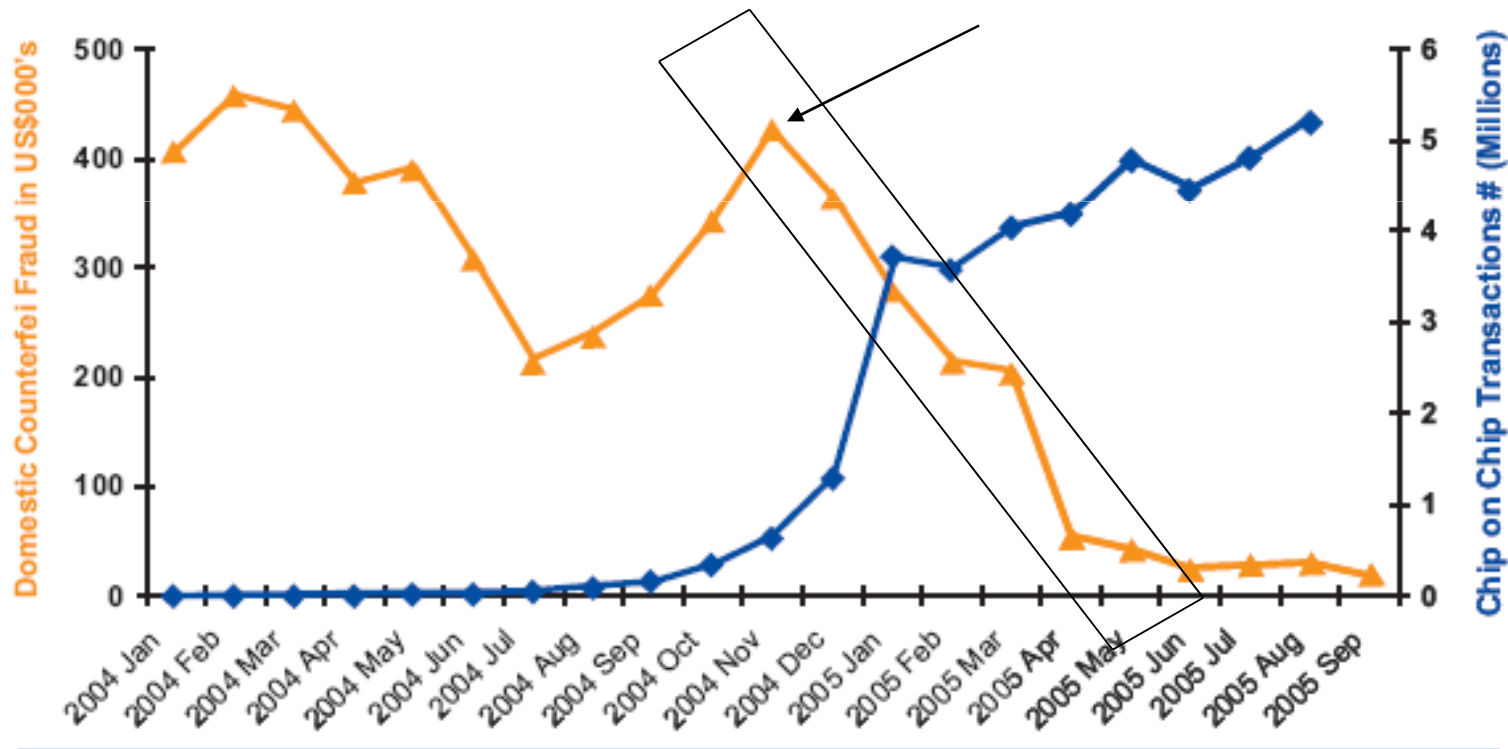


Figure 1: Malaysia's Domestic Counterfeit Fraud in a growing chip environment

UK Card Fraud

In 2000: one of the fastest growing crimes in the UK

Chip and PIN was introduced because
it was projected 1 B£ in 2010?

Plastic card fraud losses on UK-issued cards 1996-2005
Figures in grey show percentage change on previous year's total

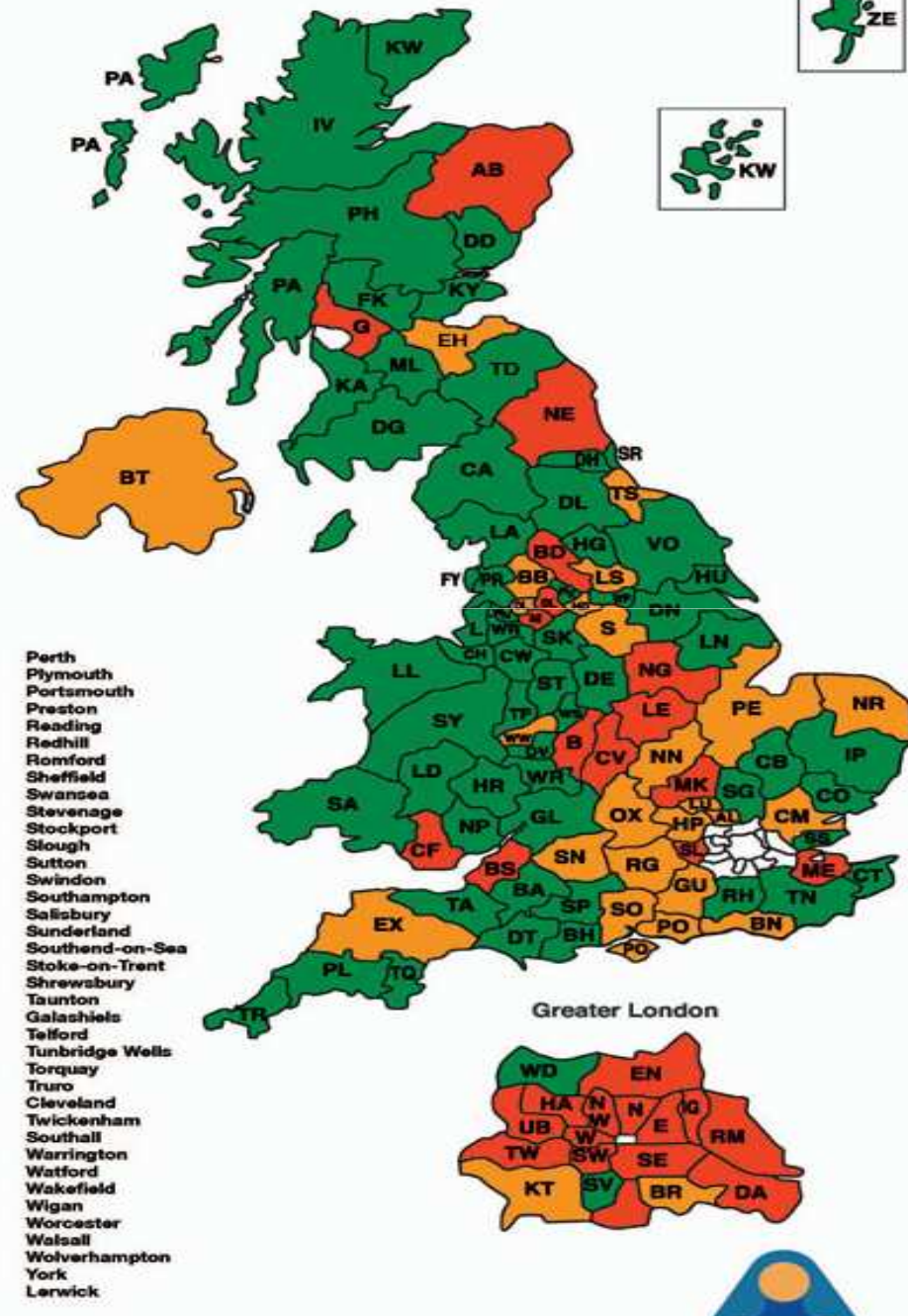


UK Card Fraud Geography

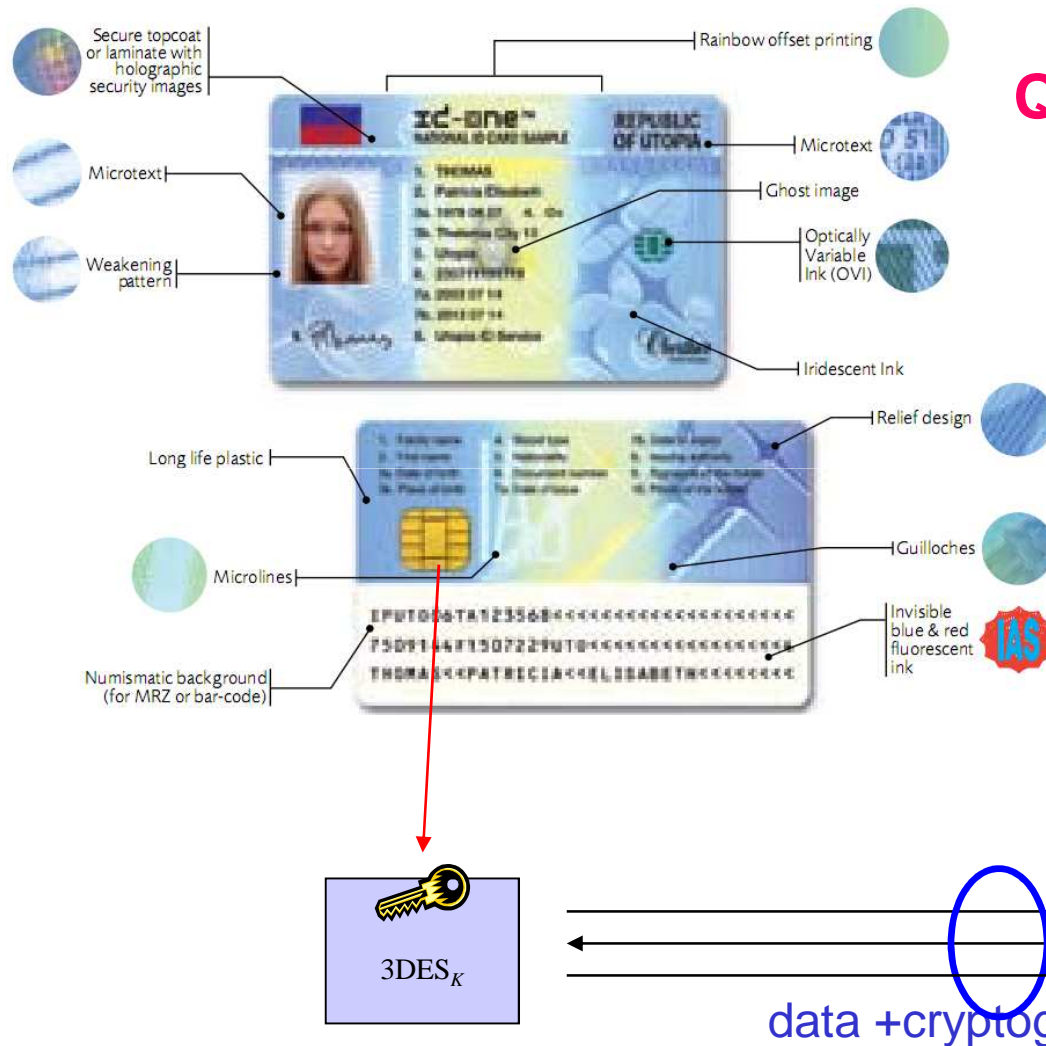
UK CARD FRAUD HOTSPOTS

AB Aberdeen
AL St Albans
B Birmingham
BA Bath
BB Blackburn
BD Bradford
BH Bournemouth
BL Bolton
BN Brighton
BR Bromley
BS Bristol
BT Belfast
CA Carlisle
CB Cambridge
CF Cardiff
CH Chester
CM Chelmsford
CO Colchester
CR Croydon
CT Canterbury
CV Coventry
CW Crewe
DA Dartford
DD Dundee
DE Derby
DG Dumfries
DH Durham
DL Darlington
DN Doncaster
DT Dorchester
DY Dudley
EH Edinburgh
EN Enfield
EX Exeter
FK Falkirk
FY Blackpool
G Glasgow
GL Gloucester
GU Guildford
HA Harrow
HD Huddersfield
HG Harrogate
HP Hemel Hempstead
HR Hereford
HU Hull
HX Halifax
IG Ilford
IP Ipswich
IV Inverness
KA Kilmarnock
KT Kingston-Upon-Thames
KW Kirkwall
KY Kirkcaldy
L Liverpool
LA Lancaster
LD Llandrindod Wells
LE Leicester
LL Llandudno
LN Lincoln
LS Leeds
LU Luton
M Manchester
ME Medway
MK Milton Keynes
ML Motherwell
NE Newcastle upon Tyne
NG Nottingham
NN Northampton
NP Newport
NR Norwich
OL Oldham
OX Oxford
PA Paisley
PE Peterborough

PH Perth
PL Plymouth
PO Portsmouth
PR Preston
RG Reading
RH Redhill
RM Romford
S Swansea
SA Stevenage
SG Stockport
SK Slough
SM Sutton
SN Swindon
SO Southampton
SP Salisbury
SR Sunderland
SS Southend-on-Sea
ST Stoke-on-Trent
SY Shrewsbury
TA Taunton
TD Galashiels
TF Telford
TN Tunbridge Wells
TQ Torquay
TR Truro
TS Cleveland
TW Twickenham
UB Southall
WA Warrington
WD Watford
WF Wakefield
WN Wigan
WR Worcester
WS Walsall
WV Wolverhampton
YO York
ZE Lerwick

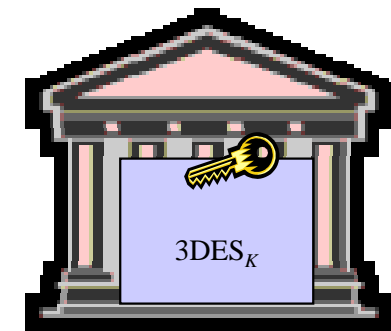


Lots of New Security Features...



Q1. Secure Payment Card?

Q2. Secure Payment Transaction?



data + cryptograms

Security of Chip Cards

Security varies depending on offline/online transactions

5 Protections:

1. Visual: hologram, special font, UV, h. signature...
 - CVV2 code also at the back (3-4 digits)
2. Cardholder verification with a PIN code,
 - Online verification – ATM withdrawals, magstripe only.
 - Offline POS - PIN verified by the card.
3. Static RSA signature, inside the chip
(B0':VS,VA, EMV:SDA functionality).
4. 3DES cryptogram generation by the chip. Authenticates individual transaction by a MAC (symmetric signature).
(CAI with B0', ARQC with EMV)
5. NVM stores all transactions for about the last 3 months...
 - + EMV: cards are updated online, so that clones can be detected also in this way...

Cardholder / PIN

On-card PIN verification function.



PIN

not encrypted except in some EMV DDA cards



Y/N

not authenticated except in EMV DDA cards

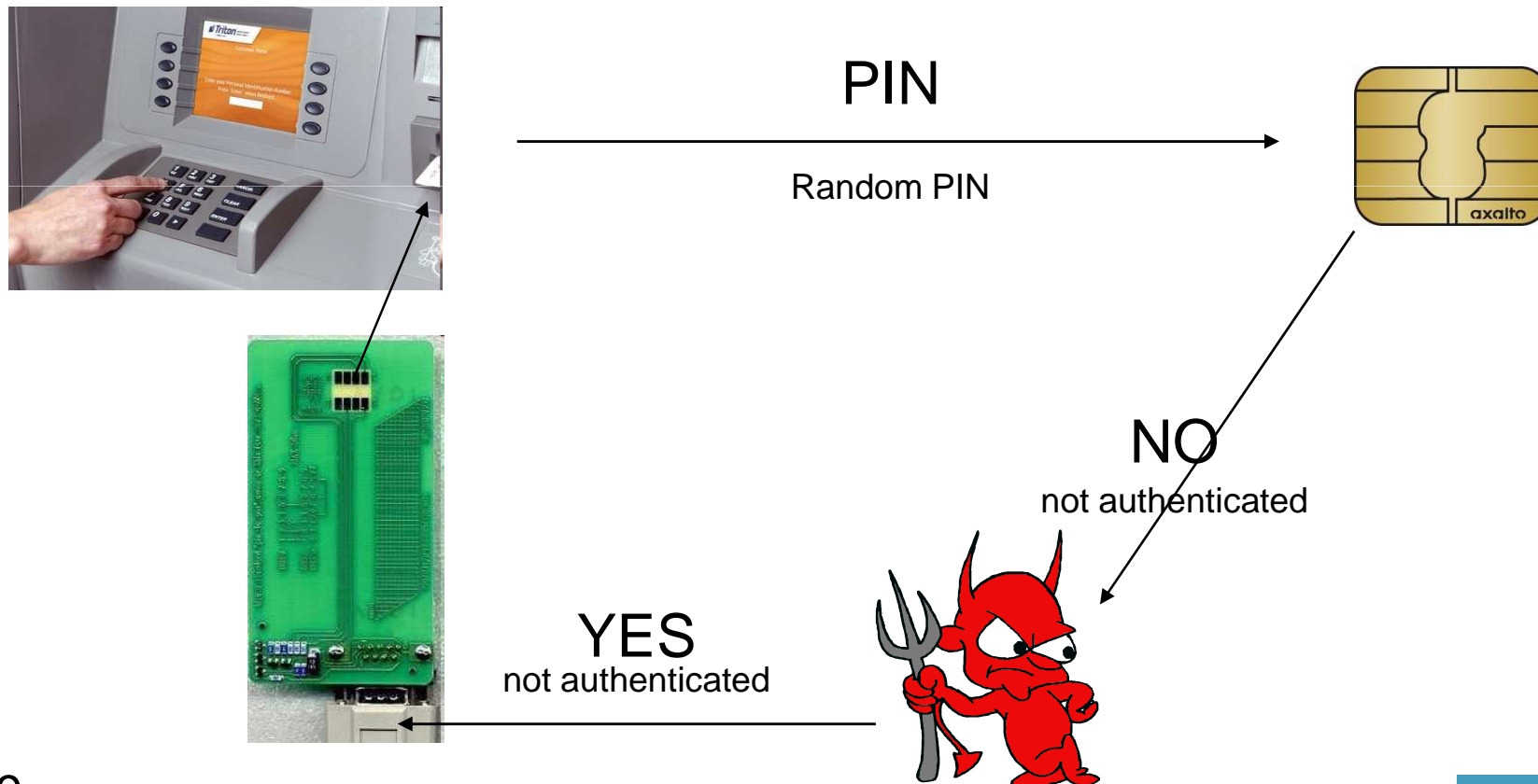
Yes Card Attacks

- Works in offline terminals



Online Yes Card Attacks

Connect between the card and the reader,
change NO -> YES



Conclusion

The “Yes” MUST BE digitally signed.

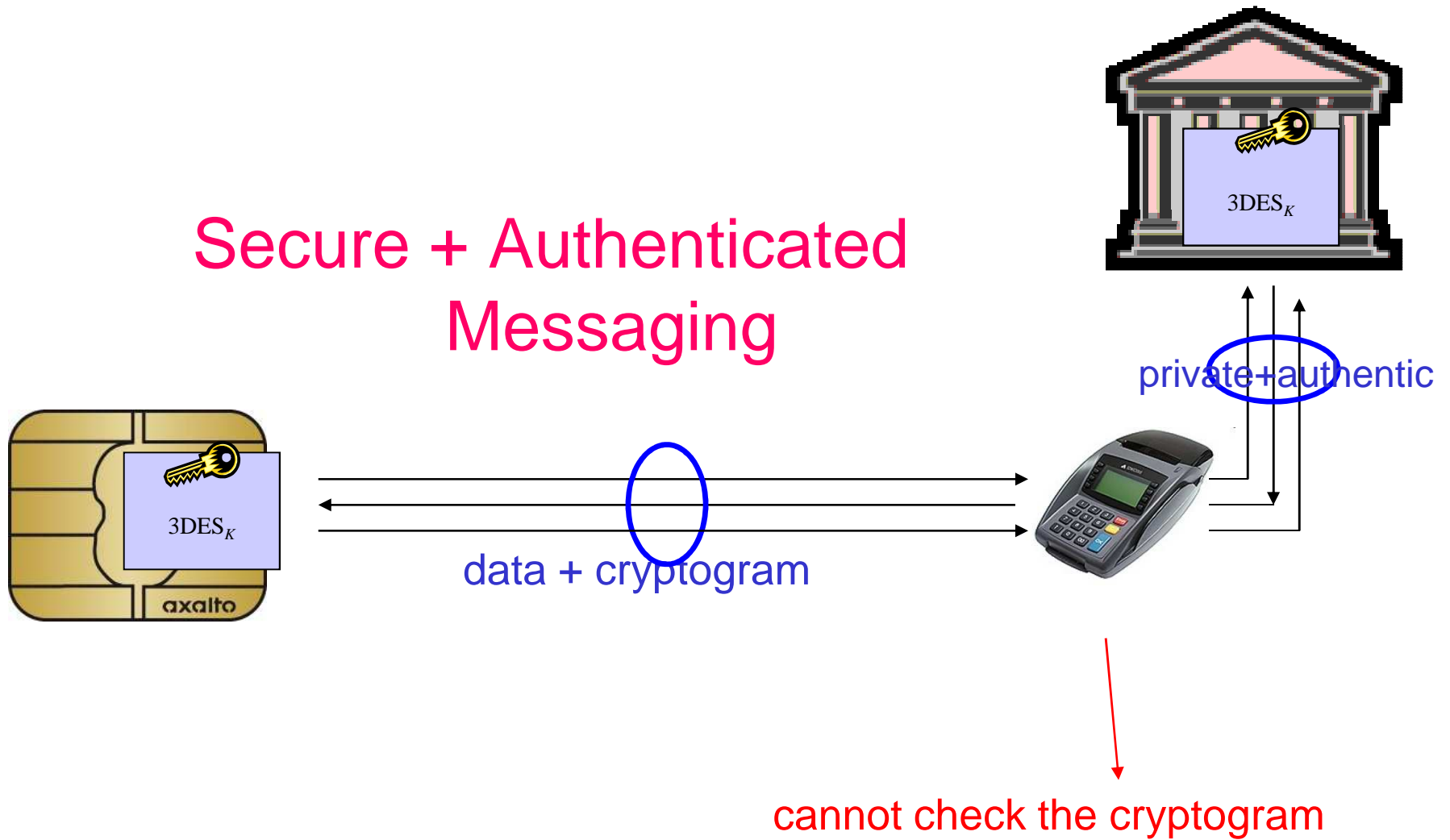
Time to use it.

- Current cards (DDA chips) are powerful enough to allow this.
 - Banks were extremely negligent in not making it obligatory so far.

Security of Individual Bank Transactions

Each transaction is certified by the card by a MAC (Message Authentication Code), a “secret key signature” of the transaction.

Secure + Authenticated Messaging



Beyond Cryptograms

Problem: the MAC, a “secret key signature” of the transaction can only be checked in the with a real-time connection to the Issuer bank.

Needed: public key signature:

- Everyone can verify
- Non-repudiation: even the bank cannot forge this certificate.
- Now exists: in the EMV specifications.

Plastic Money - Fraud

Problem

New technology usually decreases fraud on average.
However. Liability is shifted on the customer.

In the UK banks will be entirely liable for fraud due to forged handwritten signatures, BUT there is no legal protection for victims of electronic fraud.

Example: UK banks have also recently changed the voluntary code of practice “the Banking Code” to make customers liable for fraud if they do not have up-to-date anti-virus and firewall software.

Liability Shift

With MagStripe: bad technology

⇒ banks must take responsibility for fraud



CHIP and PIN:

⇒ less fraud, but when it occurs the customer will be held responsible!

Security Economics - UK

Extracted from paper “Information security Economics and Beyond” by Ross Anderson and Tyler Moore[Cambridge].

“In the USA, banks are generally **liable** for the costs of card fraud; when a customer disputes a transaction, the bank must either show she is trying to cheat it, or refund her money. In the UK, the banks had a much easier ride: they generally **got away** with claiming that their systems were ‘secure’, and telling customers who complained that they must be mistaken or lying. “Lucky bankers,” one might think; yet UK banks spent more on security and suffered more fraud. This may have been what economists call a moral-hazard effect: UK bank staff knew that customer complaints would not be taken seriously, so they became **lazy and careless, leading to an epidemic of fraud**.”

Fraud is Hidden

Ross Anderson et al.: [www.cl.cam.ac.uk/research/security/banking/ped/]

Criminals are already using tampered terminals to forge bank cards. [...] Detailed information on criminal activity has been kept out the public domain by the “sub judice” rules.

=> obligation of secrecy in matters under trial



Also the UK Parliament has a “sub judice” rule:

- MPs and Lords can be prevented from bringing up matters awaiting adjudication in a court of law...



*Fraud is Hidden

[...] what happens to the whole credit card merchant system, when no one cares to prosecute the thieves anymore? Well....that day is already here[...]

[...] police stations, instructed to do so by the Home Office, have been turning away the victims of bank card fraud and other financial crimes[...]

Yes!



From April 2007 (related to new Fraud Act) on-line financial fraud can no longer be reported to the police directly. It first has to be reported to the financial institution concerned.

It is now the responsibility of banks to **decide** which offences to pass on for investigation.

These are no longer recorded except by the financial industry itself that is interested in:

- Hiding some fraud...
- Passing other fraud on the customer...
- Covering up for internal problems
- They can profit from fraud: at the end of the day it is included in the price of the card + profit margin.

From DCPCU Web Page [2010]

“a special police unit fully sponsored by the banking industry”



“The DCPCU is unable to take reports of crime from members of the public.

If you are a victim of card fraud you should report it to your card company as soon as possible.”

So Maybe We Should Sue the Bank?

In the UK if you sue the bank and lose,
you have to pay bank's legal fees.
(this will be typically about £100 K)

Germany: cap on the fees.



Sue the Bank? [contd.]

In the UK the banks just have to convince themselves that they are right.

- They DON'T believe university experts(!).

The Financial Ombudsman [UK]:

also assumes that the log files transmitted them to the bank must be authentic [of course], refused to transmit them to 3rd party experts.

They say “PIN was used”,
but there is no evidence it was.

Banks destroy the evidence (the chip).



****Black-List Yourself**

(advocated by Bruce Schneier in the US,
though circumstances that are different).

Equifax operates the Protective Registration Service on behalf of CIFAS,
the UK's Fraud Prevention Service.

Anyone affected by this incident can contact Equifax on 0870 010 2091 and
a notice will be placed on their credit file indicating that data has been
stolen and that they may therefore be at risk of identity fraud.

There is a one-off cost for this service of £11.75.

Most people don't want to do that, because they want to be able to use their
credit card...

*Fraud for Different Types of Cards

Card Fraud Rates In Basis Points

Security Mechanism	Card Type	Basis Points
Mag-Stripe & Signature	UK Credit Cards	15 * 0.01 %
Mag-Stripe & Online Authorization	Visa US Credit Cards	6
Mag-Stripe with PIN	Europay Maestro Cards	3
Smart Card with PIN	Belgian Debit Cards	1

Source: [Lafferty Publications](#), September 2001

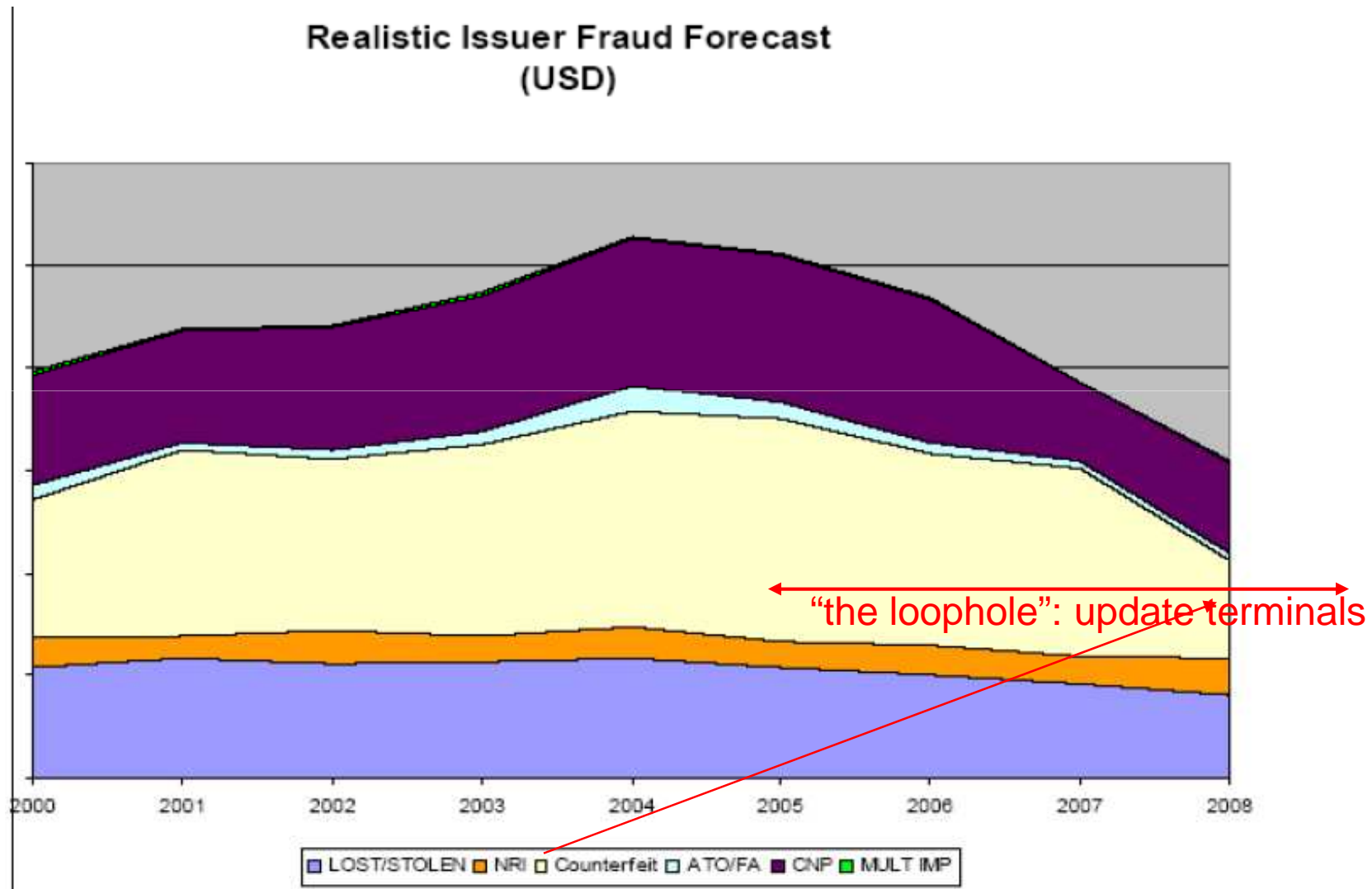
*Chip and PIN vs. Magstripe

Card Type	Volume	Security Mechanism
Belgian Debit	0.02%	Smart Card & PIN
CB (France)	0.04%	Smart card & PIN
Maestro (Europay)	0.06%	Mag-stripe & PIN
UK Debit	0.14%	Mag-stripe & PIN
Visa EU Credit	0.04%	Mag-stripe & signature
Visa USA Credit	0.06%	Mag-stripe & signature
Europay Credit	0.1%	Mag-stripe & signature
Canada Credit	0.15%	Mag-stripe & signature
UK Credit	0.16%	Mag-stripe & signature
Cartes Bancaires Abroad	0.47%	Mag-stripe & signature

Popular Fraud Classification

- **L/S** = Lost / Stolen
- **NRI** = Non-Receipt of Issue = Mail Theft
- **Counterfeit** = copy of magnetic stripe or cloned chip etc...
- **ATO/FA** = Account Take-Over, Fraudulent Application == Identity Theft
- **CNP**: Card Not Present = Unauthorized use of the card number on the Internet

MasterCard Fraud Forecast



Official UK Fraud Figures [2010]

Card Fraud Type – on UK issued credit and debit cards	2005	2006	2007	2008	2009	+/- (08/09)
Phone, internet and mail order fraud (Card-not-present fraud)	£183.2m	£212.7m	£290.5m	£328.4m	£266.4m	-19%
Counterfeit (skimmed/ cloned) fraud	£96.8m	£98.6m	£144.3m	£169.8m	£80.9m	-52%
Fraud on lost or stolen cards	£89.0m	£68.5m	£56.2m	£54.1m	£47.9m	-11%
Card ID theft	£30.5m	£31.9m	£34.1m	£47.4m	£38.2m	-20%
Mail non-receipt	£40.0m	£15.4 m	£10.2m	£10.2m	£6.9m	-32%
TOTAL	£439.4m	£427.0m	£535.2m	£609.9m	£440.3m	-28%

Malaysia Fraud: Fall Yes, But Also Shift

“Counterfeit” segment only: fell from 0.16 % in 2000-2004 to 0.03 % in 2006. BUT other segments increased.

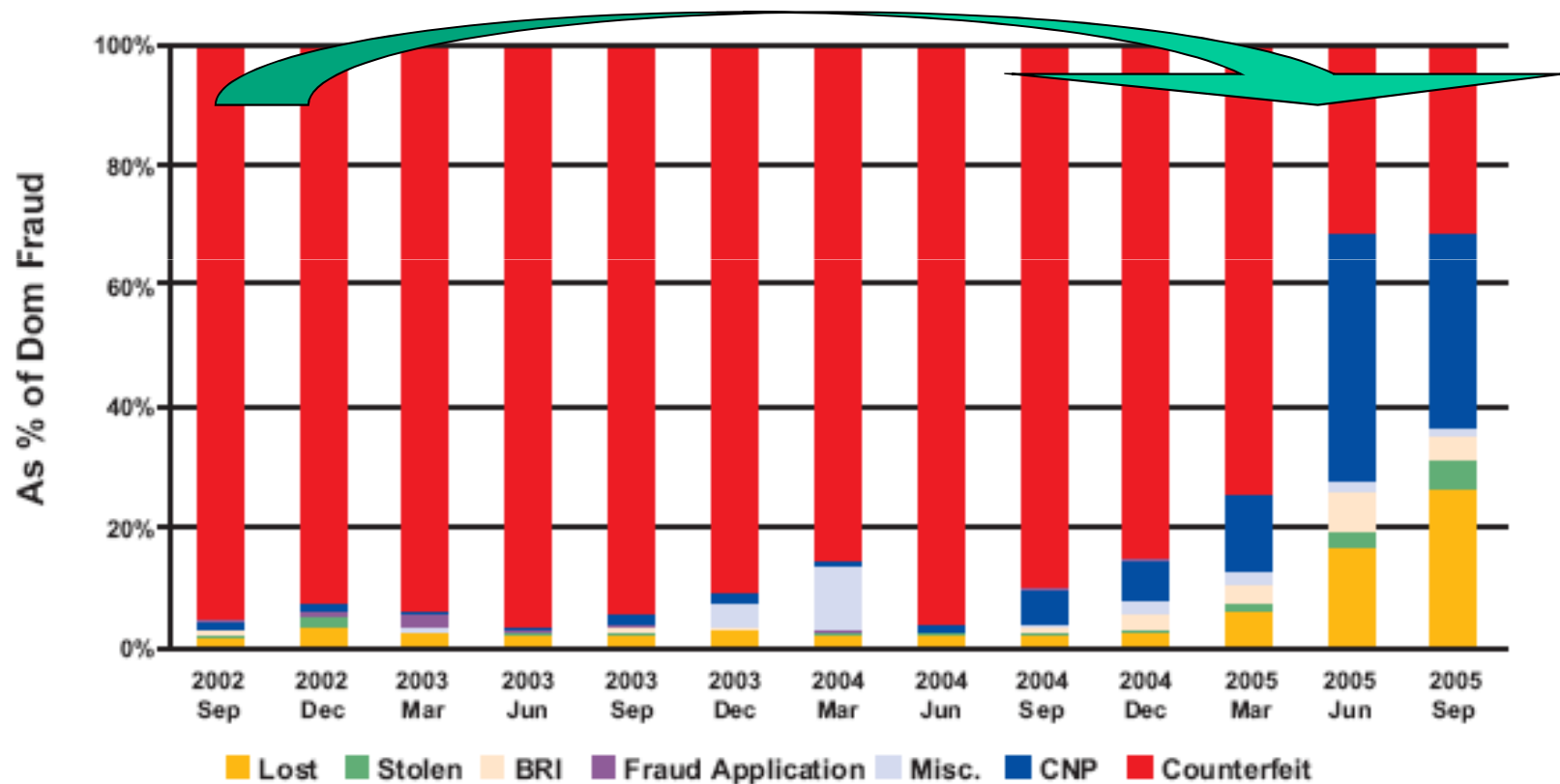


Figure 3: Malaysia's Domestic Fraud Types as % of Contribution

Plastic Money - Compliance

Who is in Charge?



UK: who is responsible for the security of bank card transactions:

- VISA/Mastercard.     
- PCI Standards Council 
- UK Payments  
- GCHQ   



Schneier about 2005 “Data” Pearl Harbour

Bruce Schneier, New York Daily News, June 23, 2005

“The epidemic of personal data thefts and losses...”

“...Real reform is required to solve these problems...”

- “reduce the amount of personal information collected, limit how it can be used and resold,
- require companies that mishandle our data to be liable for that mishandling...”

In this Schneier Quote we See:

Two main ideas to improve security:

LIMITATIONS

- “**reduce** the amount of personal information collected, limit how it can be used and resold,

LIABILITY

- require companies that mishandle our data to be **liable** for that mishandling...”

PCI - DSS



PCI Data Security Standard



PCI – DSS Requirements [contd]

They define 12 main requirements.

Build and Maintain a Secure Network

- firewall configuration to protect cardholder data
- do NOT use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- protect stored cardholder data
- **encrypt** transmission across open networks

Maintain a Vulnerability Management Program

- use and regularly update anti-virus software
- develop and maintain secure systems and applications

PCI – DSS Requirements

Implement Strong Access Control Measures

- **restrict access** to cardholder data to need-to-know
- assign a unique ID to each person with computer access

Restrict physical access to cardholder data

- regularly Monitor and Test Networks
- track and monitor all access to network resources and cardholder data
- regularly test security systems and processes

Maintain an Information Security Policy

forbidden to
store after
authorization

Restrictions in PCI-DSS

	Data Element	Storage Permitted	Protection Required	PCI DSS Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiry Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN/PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with the PCI DSS requirements for general protection of the cardholder environment. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Who Has to Comply?

Q: Can a coffee shop with random employees be trusted???

Notion of “Merchant Level”

- based on transaction volume and acceptance method.
- less compliance requirements at lower Merchant Level.

Fact: All merchants and all service providers that store, process, or transmit cardholder information are required to comply with the PCI DSS requirements.

Penalties?

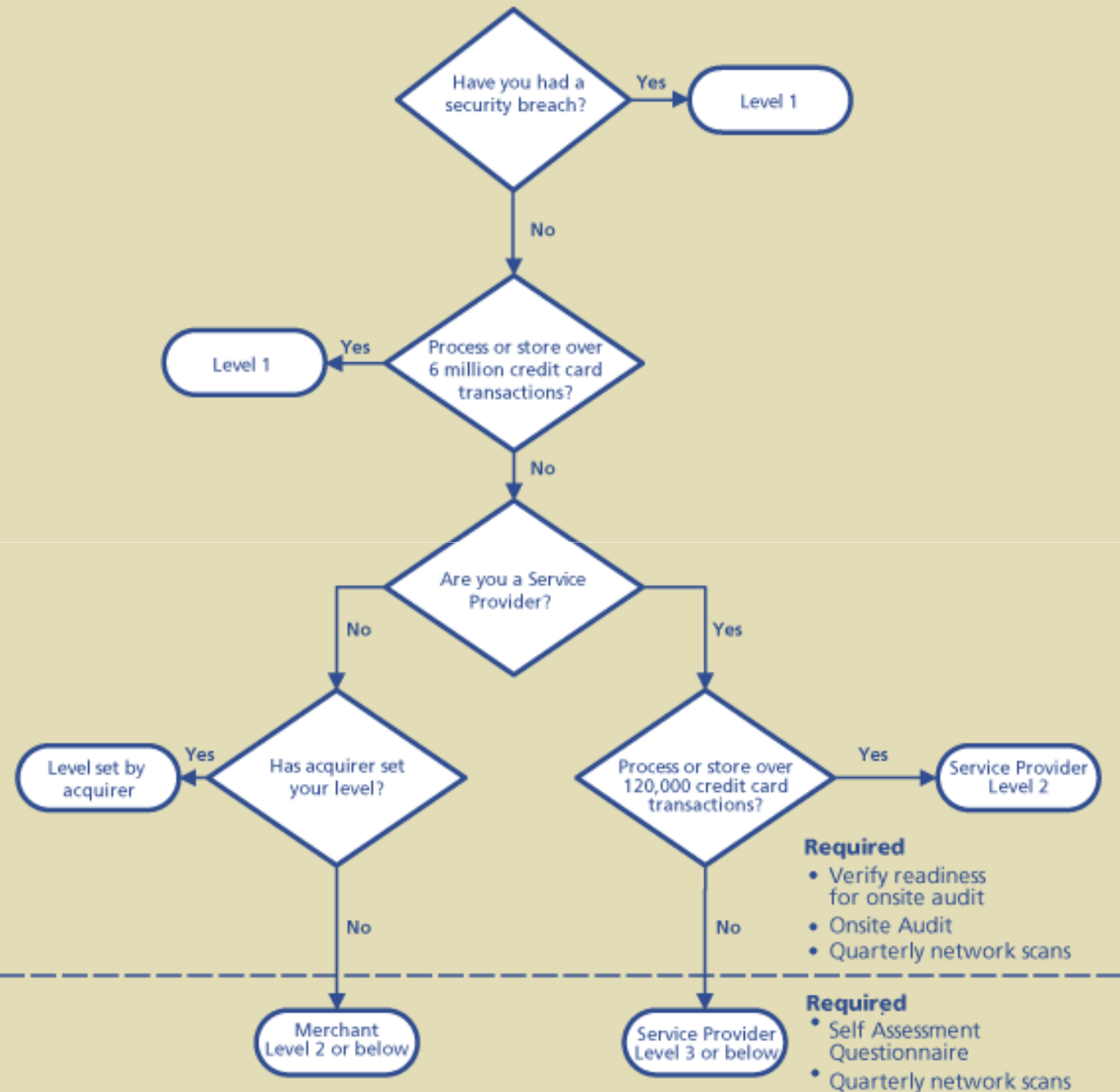
Regulation needs “teeth”. Merchant’s compliance is enforced by payment card associations = Visa/MasterCard etc.

- A written contract/agreement, enforced by national law.
- Fines: card companies can and have fined members tens of thousands of dollars per month if they fail to implement.
- Threat of termination of card processing services.
- New laws:

NEW!

- Minnesota MS 356E.64, effective August 1, 2008,
 - prohibits persons and entities conducting business in Minnesota from retaining data from the magnetic strips on payment cards, as well as security codes and PINs from such cards, for more than 48 hours after a card transaction is approved.
- Three other US states have similar state bills pending.
- Texas law HB 3222, effective January 1, 2009:
 - accept payment cards => must comply with ALL PCI DSS requirements.
- short lived victory: it is expected that data security bills pending in the federal Congress will preempt these laws.

Merchant Levels



Compliance Cost [source of jobs!]

Level 1: Probably very expensive.

- ⇒ **A.** Annual On-site Security Assessment
== 2-3 days on-site audit by a Qualified Security Assessor (QSA)
recognized for a given country. [e.g. Verisign, BT, etc].
To become one [5000 USD, strict selection]:

https://www.pcisecuritystandards.org/qsa_asv/become_pa-qa.shtml

Lost of requirements, background checks, insurance, stable business, ...

[...]must have demonstrated **competence in cryptographic techniques**, to include cryptographic algorithms, key management and rotation processes, and secure key storage[...]

Levels 23:

- **B.** Annual Self Assessment Questionnaire (like an exam: MCQ)

General obligation - all levels 123:

- **C.** must allow an external company to scan their network (!!!) 4 times per year. ASV = Approved Scanning Vendor,
e.g. BT Counterpane, Qinetiq, Symantec, McAfee, Whitehat security)

Level 4: Your bank MAY ask you to do **B** and **C** [their decision].

Known Incident [US, c. 2004]

CardSystems [processing company for VISA and AmEx]:

Network intrusion => up to 40 million (at least 239 000) credit card accounts compromised:

all magnetic stripe data [PAN, name, Exp.+ CVV codes]

- ☹ Did not encrypt anything...
- ☹ Did hold all their old data since 1998...
- ☹ Both VISA and Amex announced they were terminating their contracts...