

www.lightbluetouchpaper.org

Chip and PIN is Broken

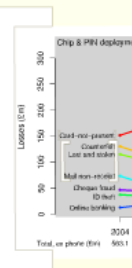
Steven Murdoch

work with Saar Drimer,
Mike Bond, Omar Choudary,
Ross Anderson

Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios.

nses

Association, February 2010



E
EuroPay

E M V

EuroPay

MasterCard

Visa

EMV is deployed or in planning in most countries
except the US, but vendors are working hard to change this

Point-of-sale and ATM

Credit and Debit

Smart card based payments

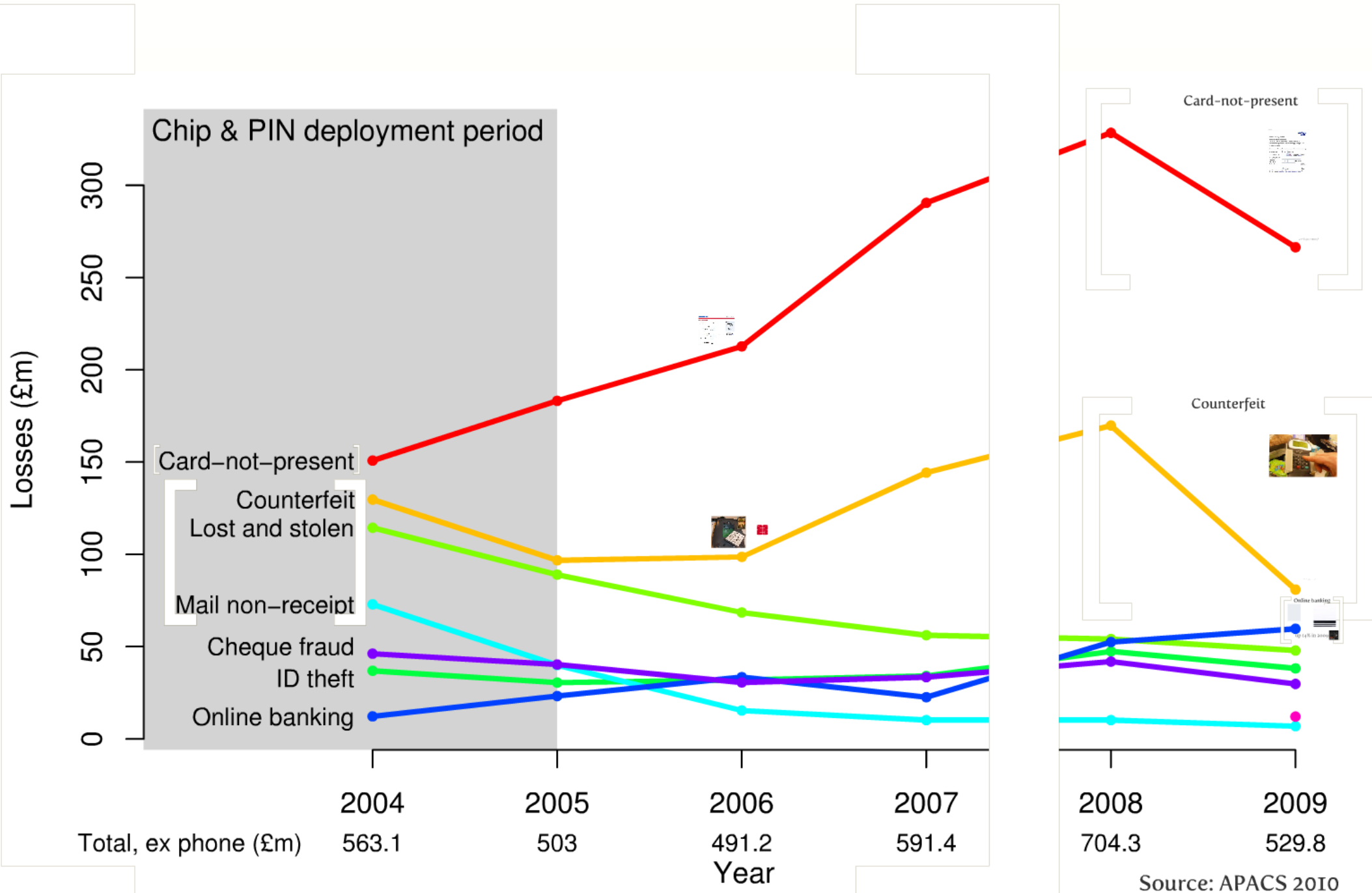
Used on 750m cards, billions
of pounds, euros, dollars

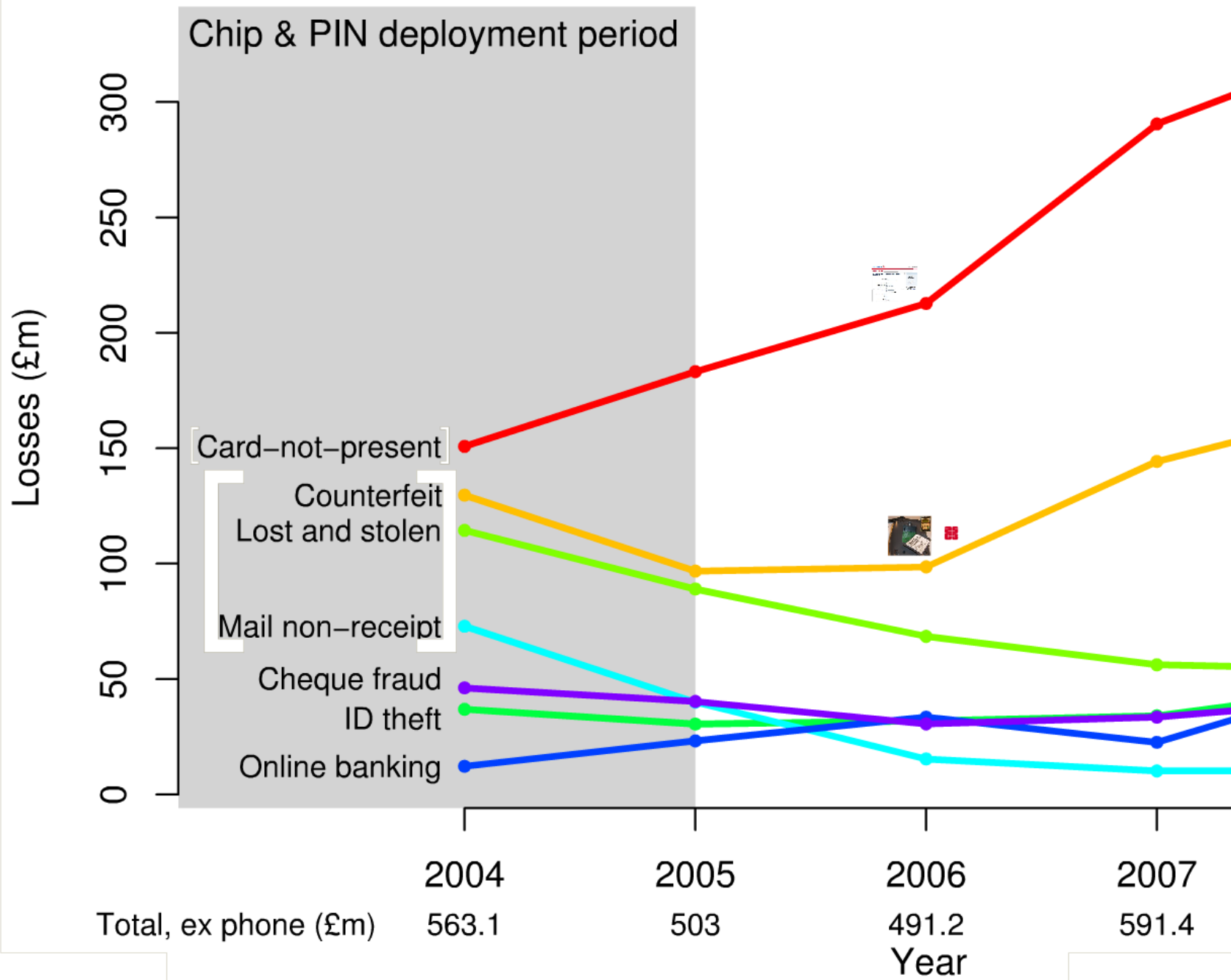
Many customers claim that their
card has been stolen and used

Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures

Many o
card ha

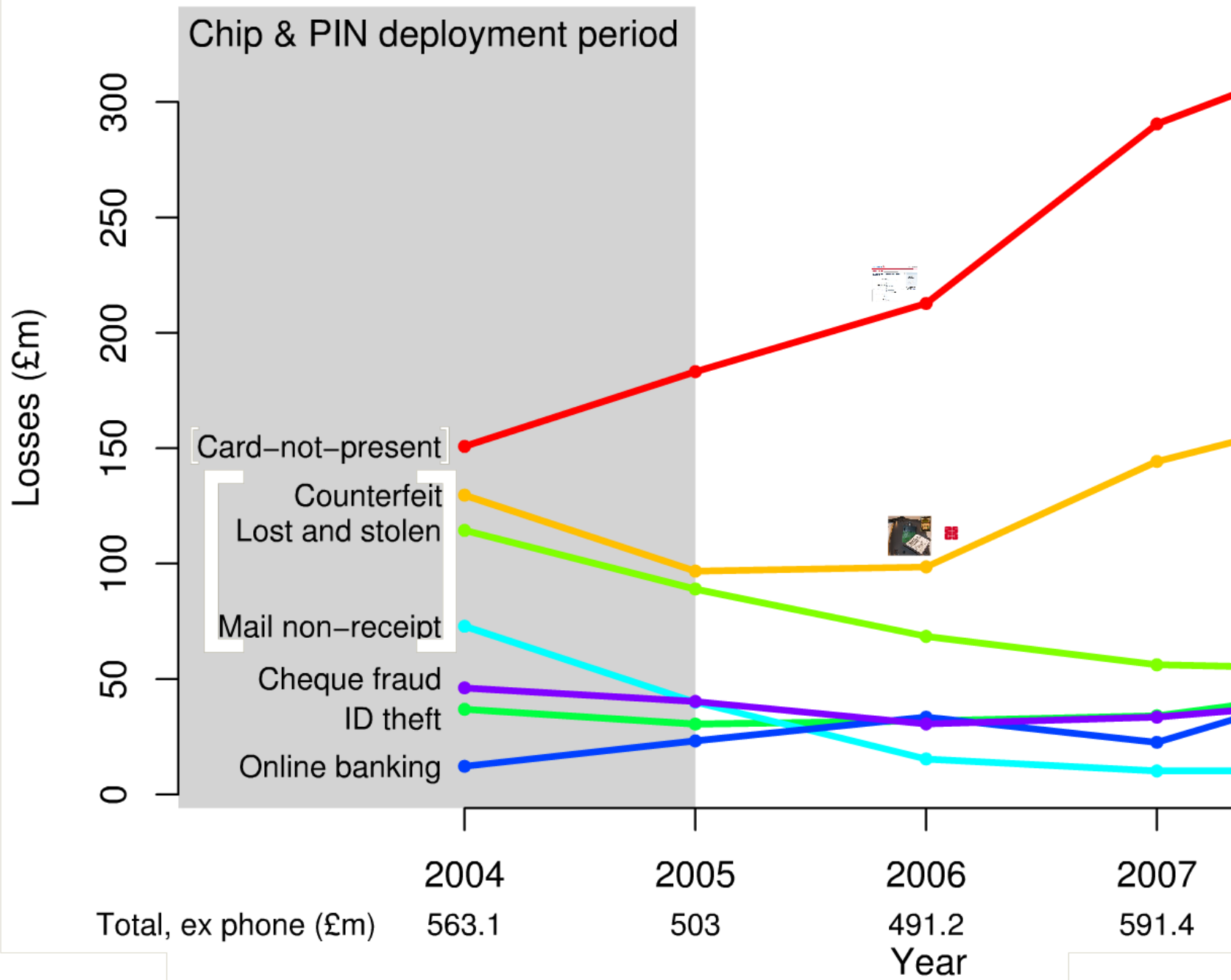
Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures





Counterfeit
Lost and stolen

Mail non-receipt



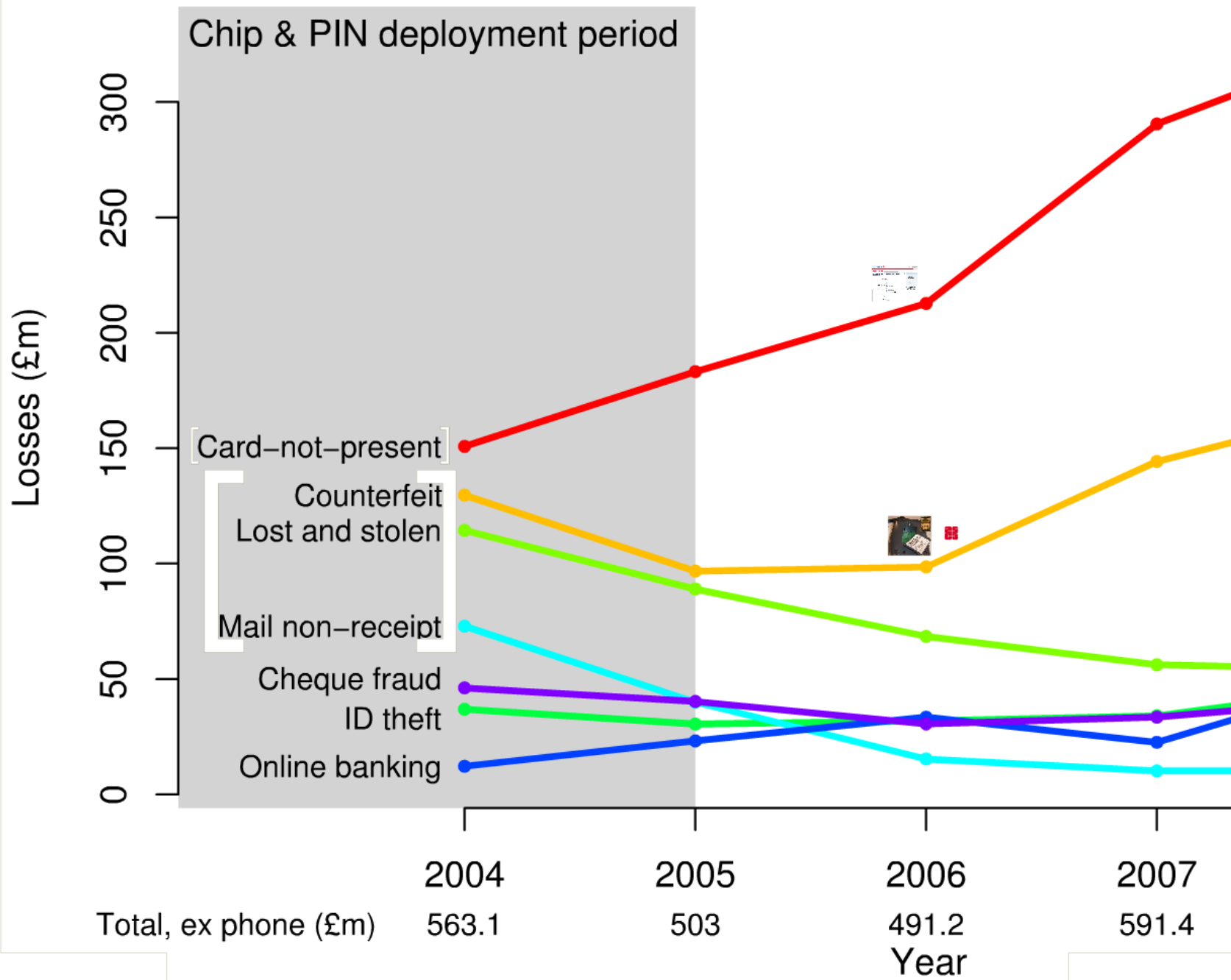


25
03

Card-not-present

Counterfeit

Lost and stolen



Security Confirmation

To continue with Online Banking, please provide the information requested below.

Passcode:
(8 - 20 Characters, case sensitive)

Date of Birth (mm/dd/yyyy): / /

Social Security Number: - -

Mother's Maiden Name:

Card Number:
(16 digits, no dashes or spaces)

Card Expiration Date (mm/yyyy): /

Card CVV2:

ATM or Check Card PIN:
(4-12 digits)

Quick Help

What do I need to know?

We use your information, only to identify you. The information is safe and secure. No one else can access it. Entering either your SSN ensures you get access to your Bank of America accounts.

Bank of America is committed to keeping your information secure with our [Online Banking Guarantee](#).

Card-not-present

Verified by VISA

Added Safety Online

With Verified by Visa, you are not currently obligated for the purchase of goods or services and you are not liable for unauthorized transactions. You will participate in the liability protection program only if you participate in the program.

Shop securely & confidently with the responsibility of Visa.

Card serial number:

Card security code:

Cardholder name:

Cardholder address:

Cardholder city:

Cardholder state:

Cardholder zip:

Cardholder phone:

Cardholder email address:

By using this service, you agree to the Terms of Use and Privacy Policy. Click on the links [Terms and Conditions](#) and [Privacy Policy](#).

RESPONSIBILITY

We are not liable for any unauthorized transactions for which we are not responsible.

Details of cardholder's liability and responsibility for unauthorized transactions are provided in the cardholder's agreement.



Added Safety Online

Welcome to Barclaycard Secure.

You are not currently registered for this new free service.

Barclaycard Secure, provided in association with Verified by Visa, protects your card when you shop online with this and other participating retailers.

Simply complete the details below to activate this free security service.

Card Expiry Date: / (MM/YY)

Card Security Code:  The last 3 digits on the back of your card ([more help](#))

Card holder name as printed on the card:

Cardholder Date of Birth: / / (DD/MM/YYYY)

Email address: [How will it be used?](#)

[Back](#)

By registering now, you agree to the [Terms and Conditions of Use](#).

Click here to view: [Terms and Conditions of Use](#) [Privacy Policy](#).

Counterfeit

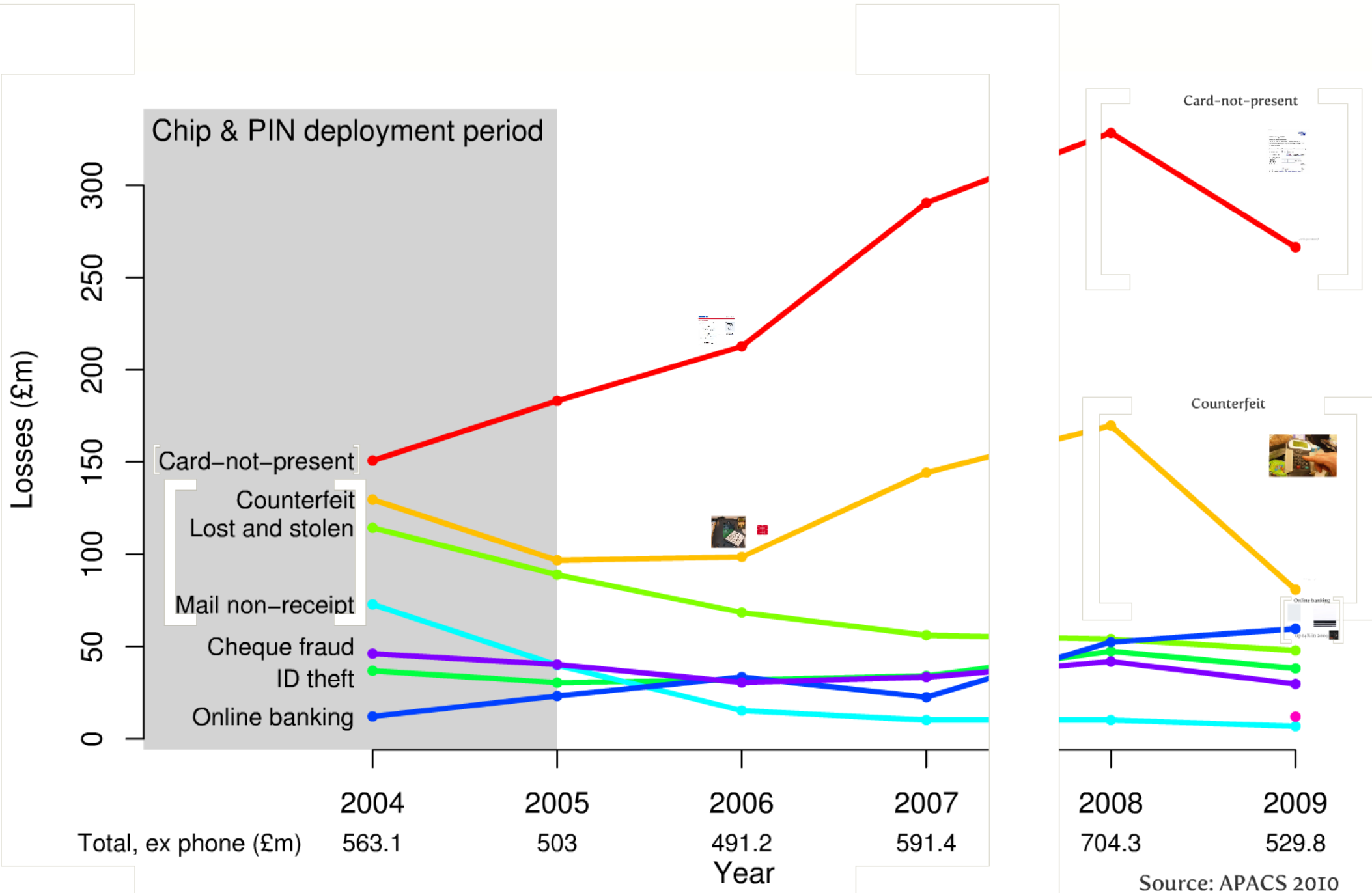


Handwritten text on a torn paper strip, possibly a signature or a note.

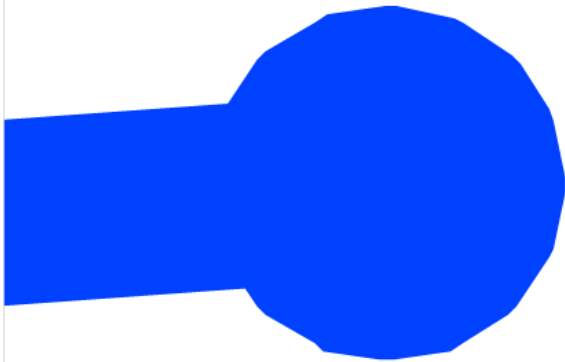
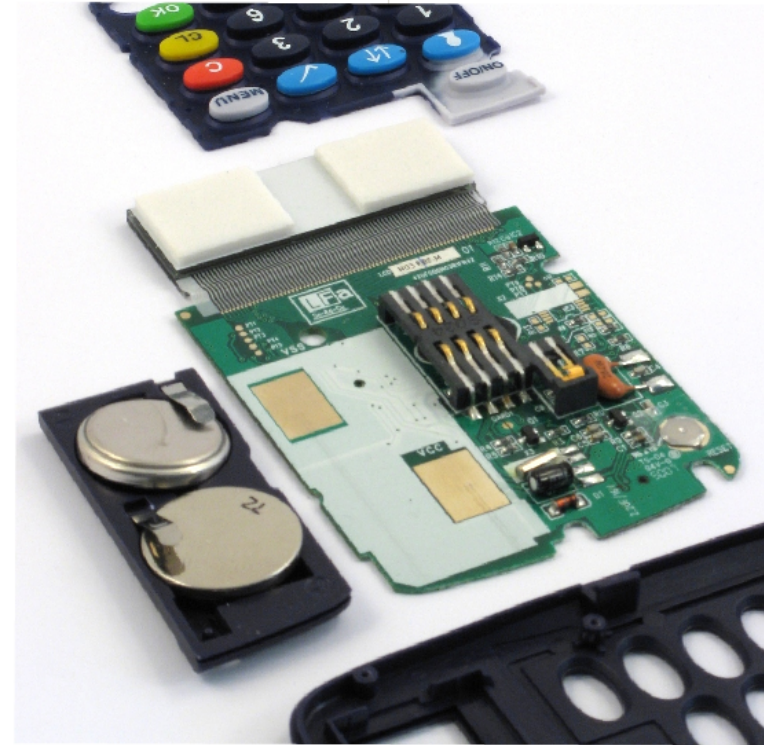
Online banking





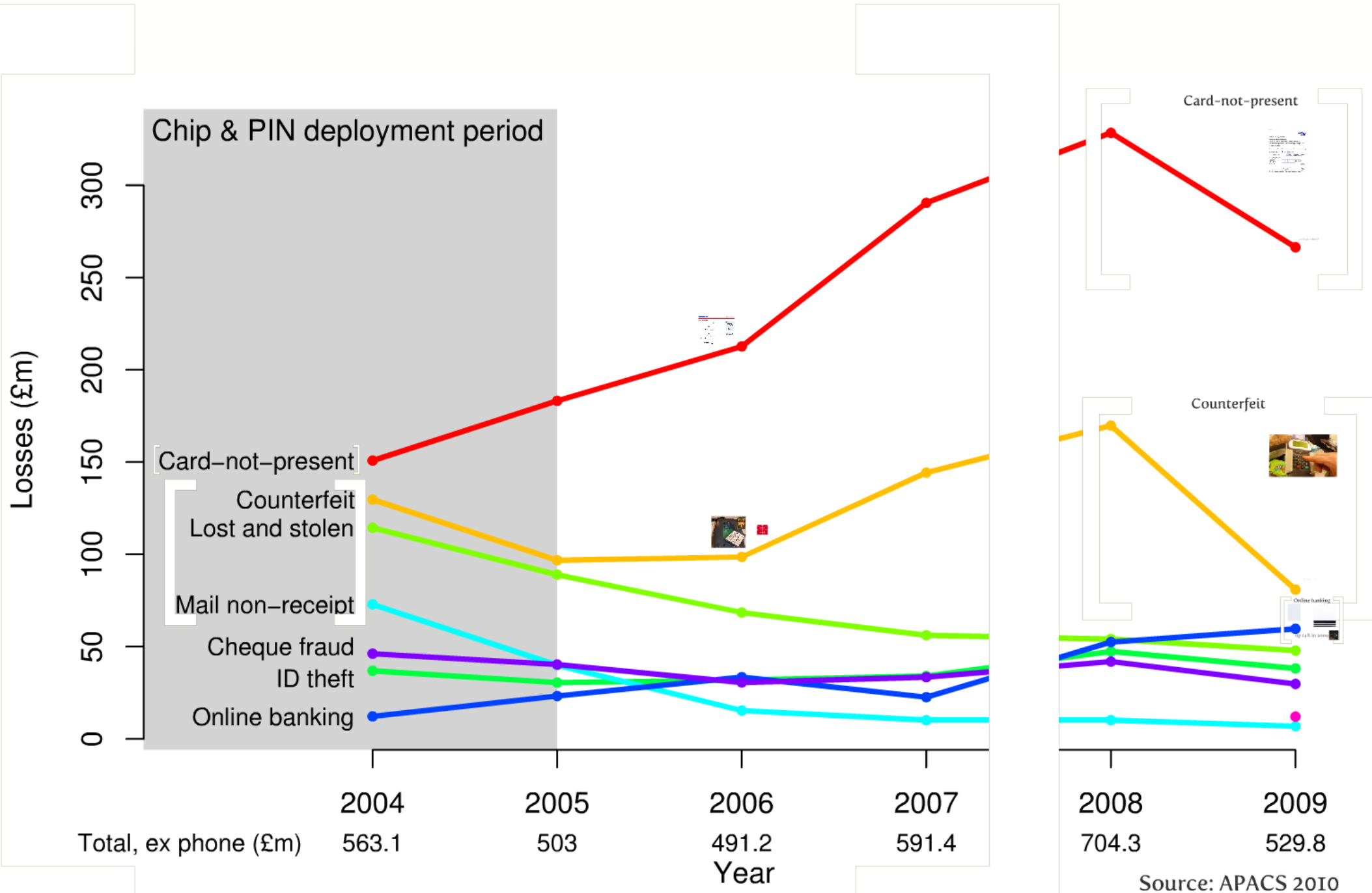


Online banking



up 14% in 2009





9. RESPONSIBILITY

You understand that you are financially responsible for all uses of RBS Secure.

Example of revised terms and conditions for online purchases (Royal Bank of Scotland)



10. Chip and PIN charges cannot be disputed as card would have been in possession when charges were put through.

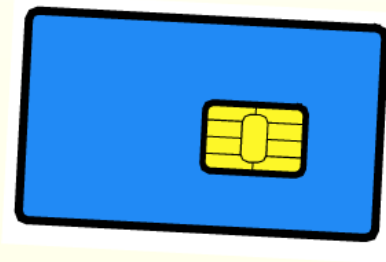
Letter denying refund for disputed transactions (American Express)

They were wrong



BBC Newsnight, February 2010

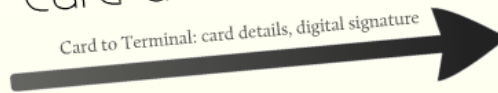
A simplified EMV transaction



customer enters PIN

card authentication

Card to Terminal: card details, digital signature



Terminal to Card: PIN as entered by customer

cardholder verification

Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction

transaction authorization

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification
online transaction authorization

Bank to Terminal: transaction authorized (yes/no)



card authentication

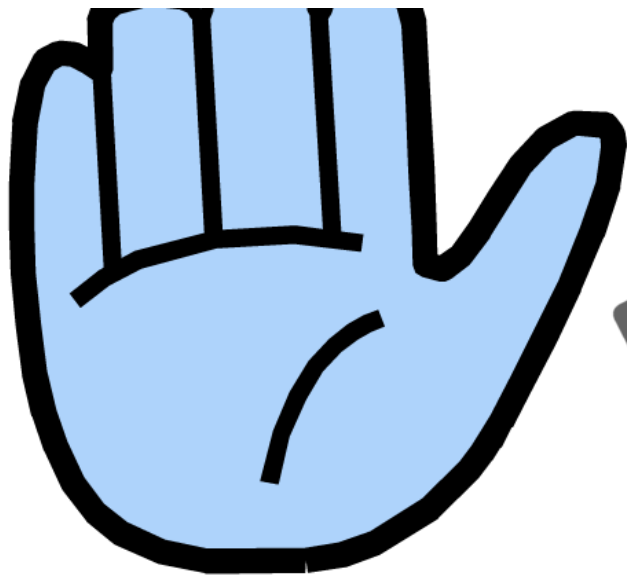
Card to Terminal: card details, digital signature



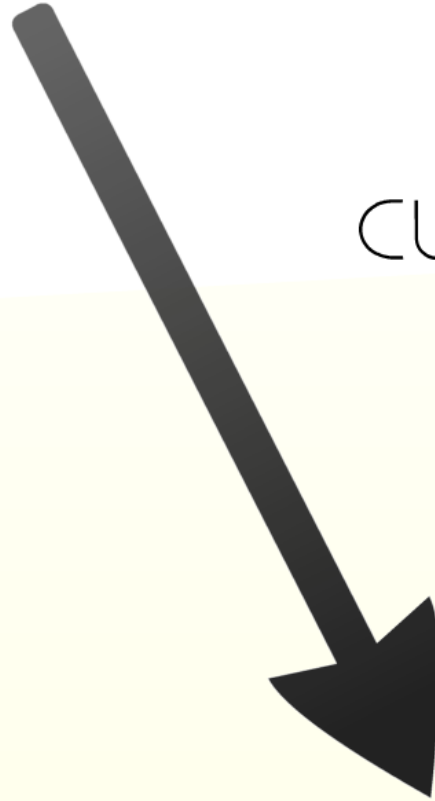
Terminal to Card: PIN as entered by customer



Cardb



customer enters PIN



Card to Terminal: card details

Terminal to Card: PIN as entered by customer

cardholder verification

Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction
amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?
• ...

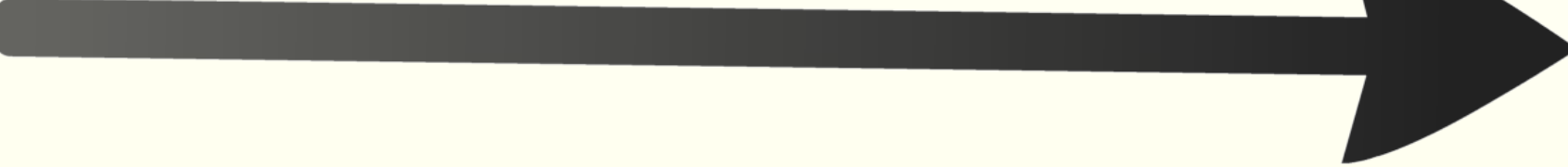


Terminal to Card: description of transaction


amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?
• ...

transaction authorization

Card to Terminal: MAC over transaction and other details




MAC and transaction sent to bank for verification



online transaction authorization

Bank to Terminal: transaction authorized (yes/no)



and other details

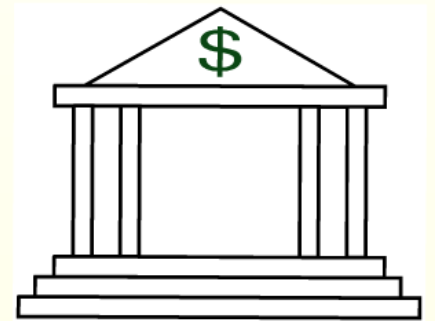


MAC and transaction sent to bank for verification



online transaction authorization

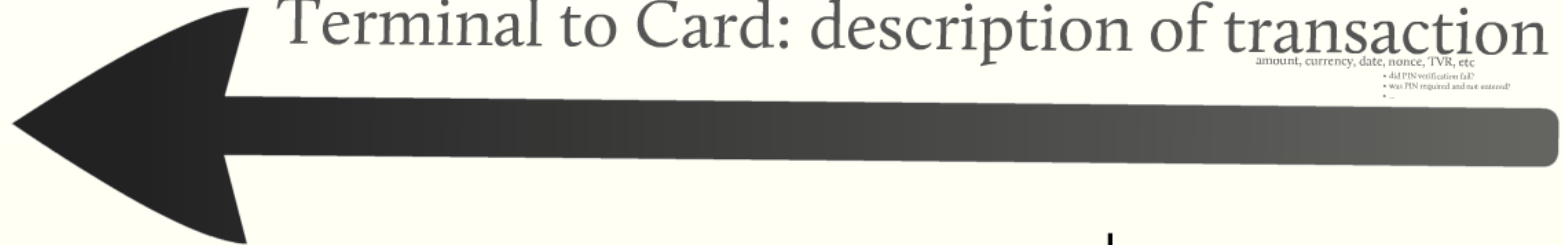
Bank to Terminal: transaction authorized (yes/no)



Card to Terminal: PIN verification
PIN correct (yes/no)

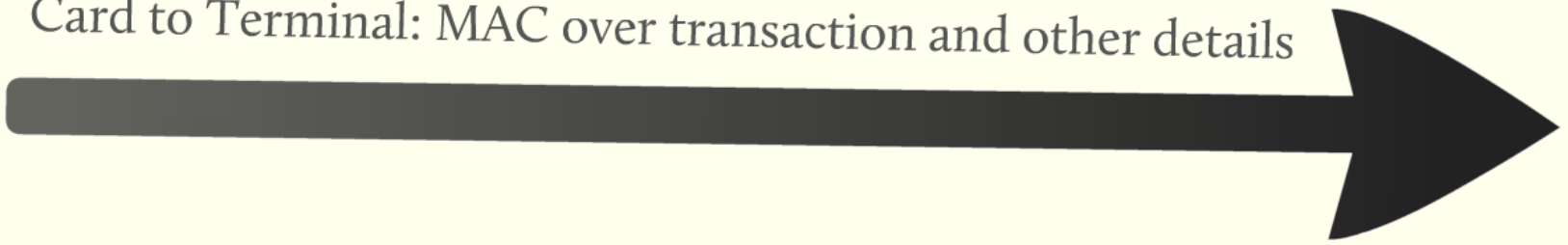


Terminal to Card: description of transaction
amount, currency, date, nonce, TVR, etc
- did PIN verification fail?
- was PIN required and not entered?
- ...



transaction authorization

Card to Terminal: MAC over transaction and other details

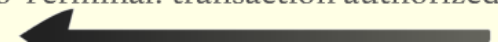


MAC and transaction sent to bank for verification



online transaction authorization


Bank to Terminal: transaction authorized (yes/no)





transaction

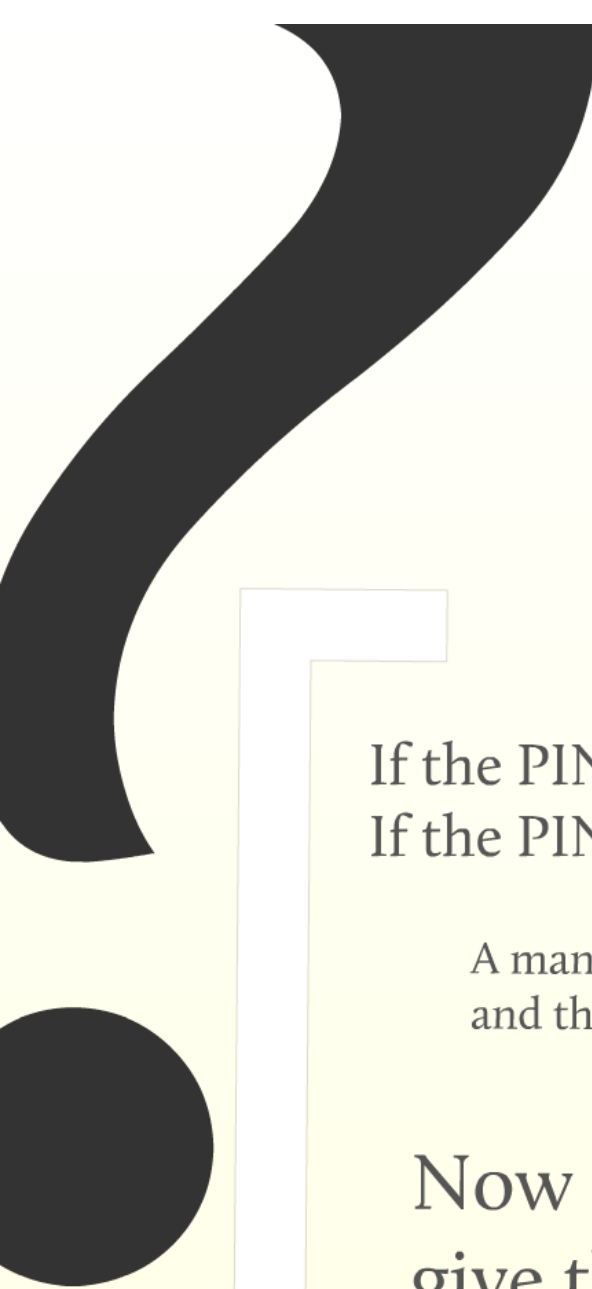
amount, currency, date, nonce, TVR, etc

- did PIN verification fail?
 - was PIN required and not entered?
 - ...
- 

Authentication

date, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...



If the PIN is not required by the terminal, the TVR is all zeros
If the PIN is entered correctly, the TVR is still all zeros

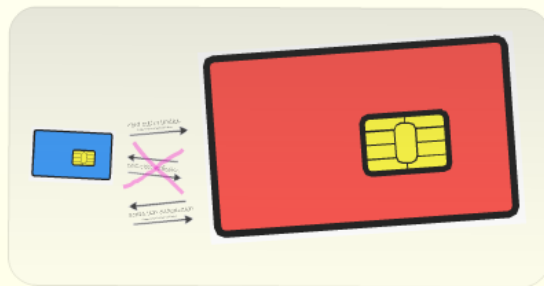
A man-in-the-middle tell the card that the PIN was not required
and the terminal that the PIN was correct

Now the criminal can use a stolen card,
give the wrong PIN to the terminal
and still have the transaction succeed

How the attack works



criminal enters 0000



card authentication

Card to Terminal: card details, digital signature

Terminal to MitM: 0000 entered by criminal

cardholder verification

MitM to Terminal: PIN correct **yes!**

Terminal to Card: description of transaction

transaction authorization

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification
online transaction authorization

Bank to Terminal: transaction authorized (yes/no)





card authentication
Messages relayed without modification



~~cardholder verification~~

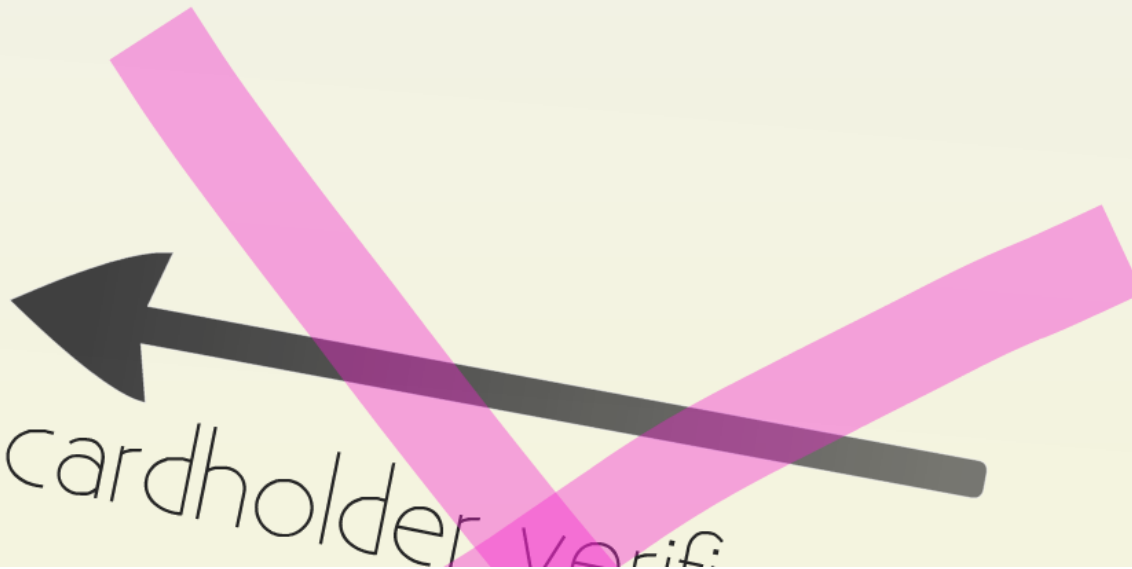
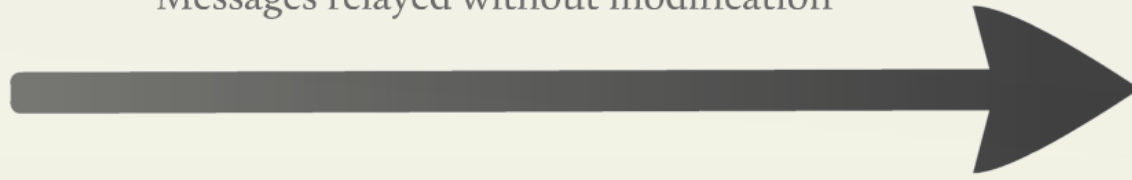


transaction authorization
Messages relayed without modification

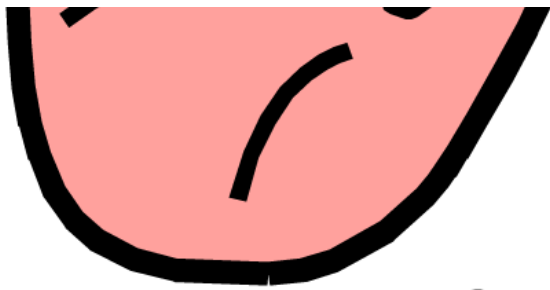


card authentication

Messages relayed without modification



cardholder verifi



criminal enters 0000



Card to Terminal: card details

Terminal to MitM: **0000** entered by criminal

cardholder verification

MitM to Terminal: PIN correct **yes!**

Terminal to Card: description of transaction
amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?
• ...

Card
Messages relayed without



cardholder verification



transaction authorization

Account modification

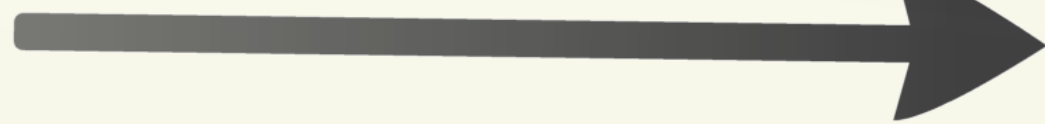


verification



transaction authorization

Messages relayed without modification



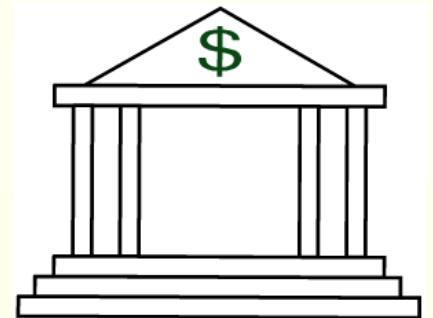
and other details



MAC and transaction sent to bank for verification



online transaction authorization



Bank to Terminal: transaction authorized (yes/no)





Terminal to Card: description of transaction

amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?

transaction authorization

Card to Terminal: MAC over transaction and other details




MAC and transaction sent to bank for verification



online transaction authorization

Bank to Terminal: transaction authorized (yes/no)



ACCURATOR

ate, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...

Card: No (not attempted)
Terminal: No (verification succeeded)

Card: N
Termina

Card: No (not attempted)

Terminal: No (verification
succeeded)

t entered?

ACCURATOR

ate, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...

Card: No (not attempted)
Terminal: No (verification succeeded)

Card: N
Termina

Card: No (not required)

Terminal: No (was entered)

WO
Mike

"When a card company receives a claim about a fraudulent transaction from a customer, they will always rely on primary evidence to review the facts of the case and would never use a paper receipt (which in fact they could only see if the customer provided the copy) for evidence as suggested."

"Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios."

Responses

UK Cards Association, February 2010

"The industry is confident that the forensic signature of such an attack is easily detectable within the data available at the time of the transaction."

December 2010

"It is the publication of this level of detail which we believe breaches the boundary of responsible disclosure. Essentially, it places in the public domain a blueprint for building a device which purports to exploit a loophole in the security of chip and PIN."

Consequently, we would ask that this research be removed from public access immediately and would hope that you are able to give us comfort about your policy towards future disclosures." UK Cards Association

"Second, you seem to think that we might cross a student's thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Examinations, of Newton, and of Darwin; concerning writings that offend the powerful is offensive to our deepest values."

Ross Anderson
University of Cambridge



"When a card company receives a claim about a fraudulent transaction from a customer, they will always rely on primary evidence to review the facts of the case and would never use a paper receipt (which in fact they could only see if the customer provided the copy) for evidence as suggested."

Response

WRONG



2

We also requested at the time of this claim, supporting documents from [REDACTED] and were provided a copy of the till receipts confirming these charges were verified with the PIN. These receipts also show the products purchase which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euro's and not for a holiday as thought by [REDACTED] at the time.

Timings and location of these charges are as follows.....

£3000.00 - 20/05/08 - 12.27pm

£4000.00 - 20/05/08 - 12.28pm

£2500.00 - 20/05/08 - 12.30pm

All made at [REDACTED]
[REDACTED]

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.

"The industry is confident that the forensic signature of such an attack is easily detectable within the data available at the time of the transaction."



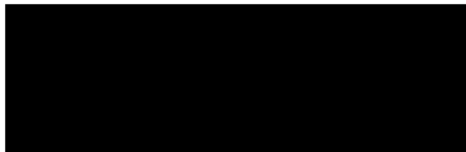
WRONG

Below is a list of the dates and times of all transactions performed in [REDACTED] from 23rd July 2009 onwards. I have also included further computerised records for your information:

Date	Amount	Retailer/ATM	Successful/Unsuccessful
24/07	211.66	[REDACTED]	Unsuccessful
24/07	3994.56	[REDACTED]	Successful
24/07	3994.56	[REDACTED]	Successful
24/07	3187.54	[REDACTED]	Unsuccessful
24/07	85.56	[REDACTED]	Unsuccessful

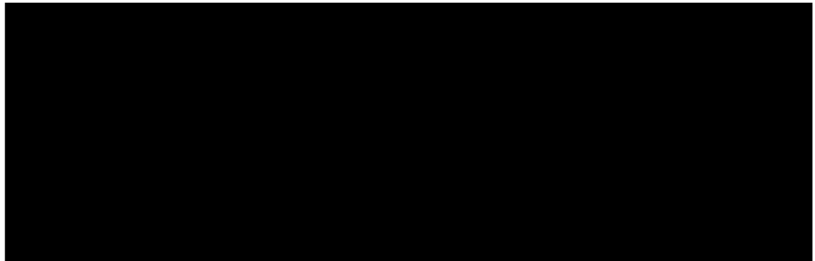
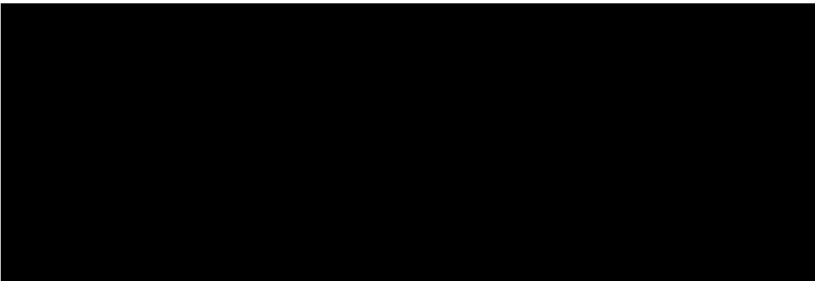
According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.

om
our



24/07/1988
KART NO

11:38
S.K.T.: 12/10



the
ver
our

EMV : A0000000031010/00A0089000/F800
APP LABEL : VISA DEBIT

EMV - no entry required, no
pad present, but no wafer
entered

ORJINAL FISI SAKLAYINIZ.
MUSTERIYE 2. NUSHAYI VERINIZ.

TESEKKURLER

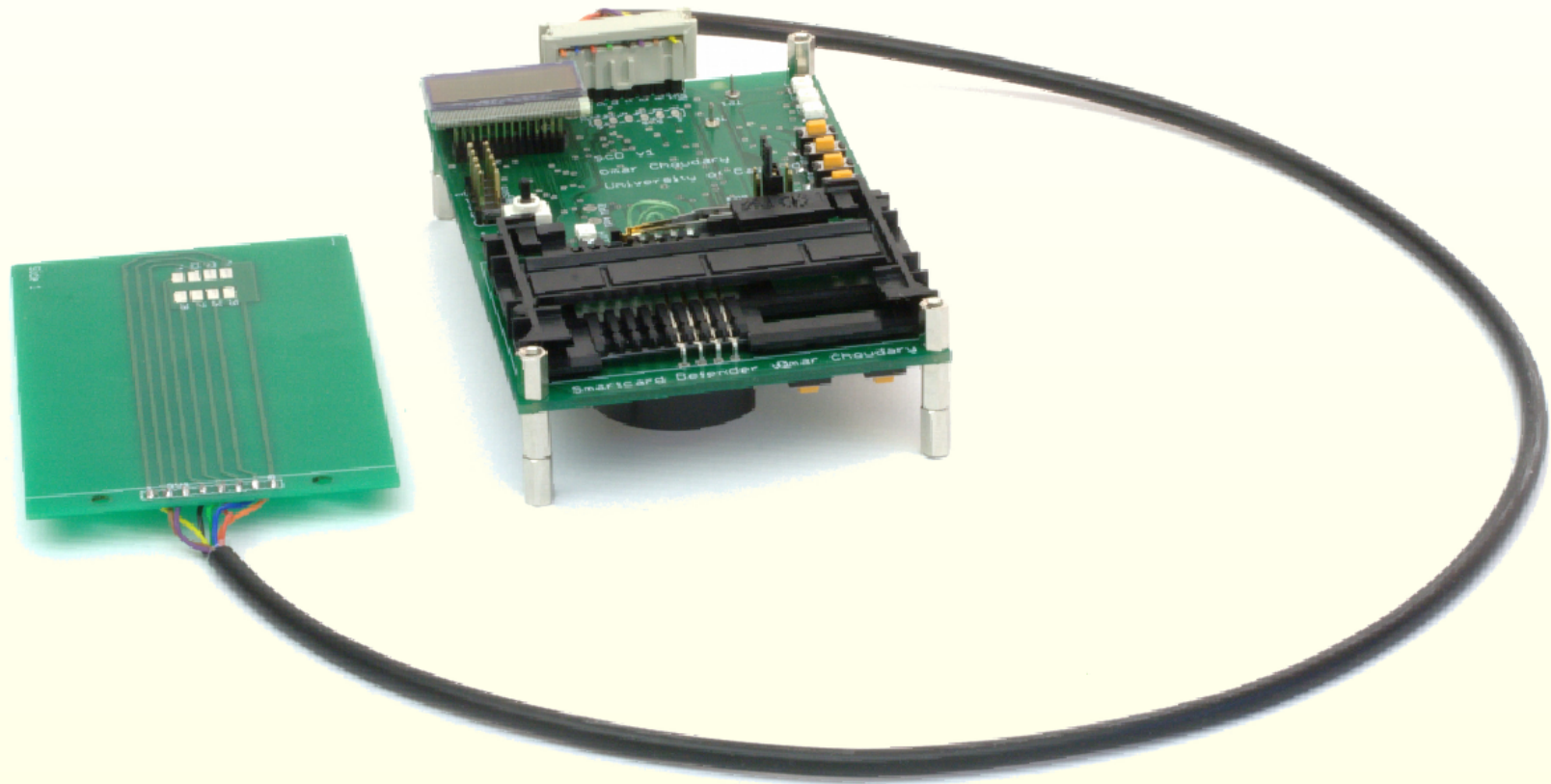


0x08 = PIN entry required, PIN
pad present, but PIN was not
entered

"Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios."^[1]



WRONG





December 2010

"It is the publication of this level of detail which we believe breaches the boundary of responsible disclosure. Essentially, it places in the public domain a blueprint for building a device which purports to exploit a loophole in the security of chip and PIN.

...

Consequently, we would ask that this research be removed from public access immediately

"Second, you seem to think that we might censor a student's thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Erasmus, of Newton, and of Darwin; censoring writings that offend the powerful is offensive to our deepest values.

"It is the publication of this level of detail which we believe breaches the boundary of responsible disclosure. Essentially, it places in the public domain a blueprint for building a device which purports to exploit a loophole in the security of chip and PIN.

...

Consequently, we would ask that this research be removed from public access immediately and would hope that you are able to give us comfort about your policy towards future disclosures."

UK Cards Association

"Second, you seem to think that we might censor a student's thesis, which is lawful and already in the public domain, simply because a powerful interest finds it inconvenient. This shows a deep misconception of what universities are and how we work. Cambridge is the University of Erasmus, of Newton, and of Darwin; censoring writings that offend the powerful is offensive to our deepest values.

Ross Anderson
University of Cambridge

UK banks attempt to censor academic paper; Cambridge University resists

315 submitted 4 days ago by sjmurdach
22 comments share save hide delete

Your Rights Online: UK Banks Attempt To Censor Academic Publication

Posted by [timothy](#) on Saturday December 25, @15:55
from the [here-are-some-rugs-for-your-eyes](#) dept.

An anonymous reader writes

"Representatives of the UK banking industry have sent a take-down notice (PDF link) to



well as his in the report throughout Europe and fundamentally flawed Cambridge University has y they will keep the

THE INDEPENDENT EDUCATION

- News
 - Opinion
 - Environment
 - Sport
 - Life & Style
 - Arts & Ents
 - Travel
 - UK
 - World
 - Business
 - People
 - Science
 - Media
 - Education
 - Obituaries
 - Video
 - Appeal
- Home > News > Education > Education News

Banks attempt to suppress maths student's exposé of chip and pin



Banks covered up a fatal flaw in Chip and PIN security

Inquirer - Nick Farrell - 1 hour ago
BLIGHTY BANKS apparently have tried to cover up a flaw in the attempting to silence the Cambridge ...
[Chip and PIN flaw that banks tried to censor: Cambridge scientist](#)
[Cambridge boffins rebuff banking industry take down request - Scientist in bank 'censorship' row](#) - The Press Association
Techworld.com - PCR-online.biz
[all 103 news articles >](#)



Archive Features Forums Newsletter RSS

< previous | next >

Bank censorship attempt rebuffed

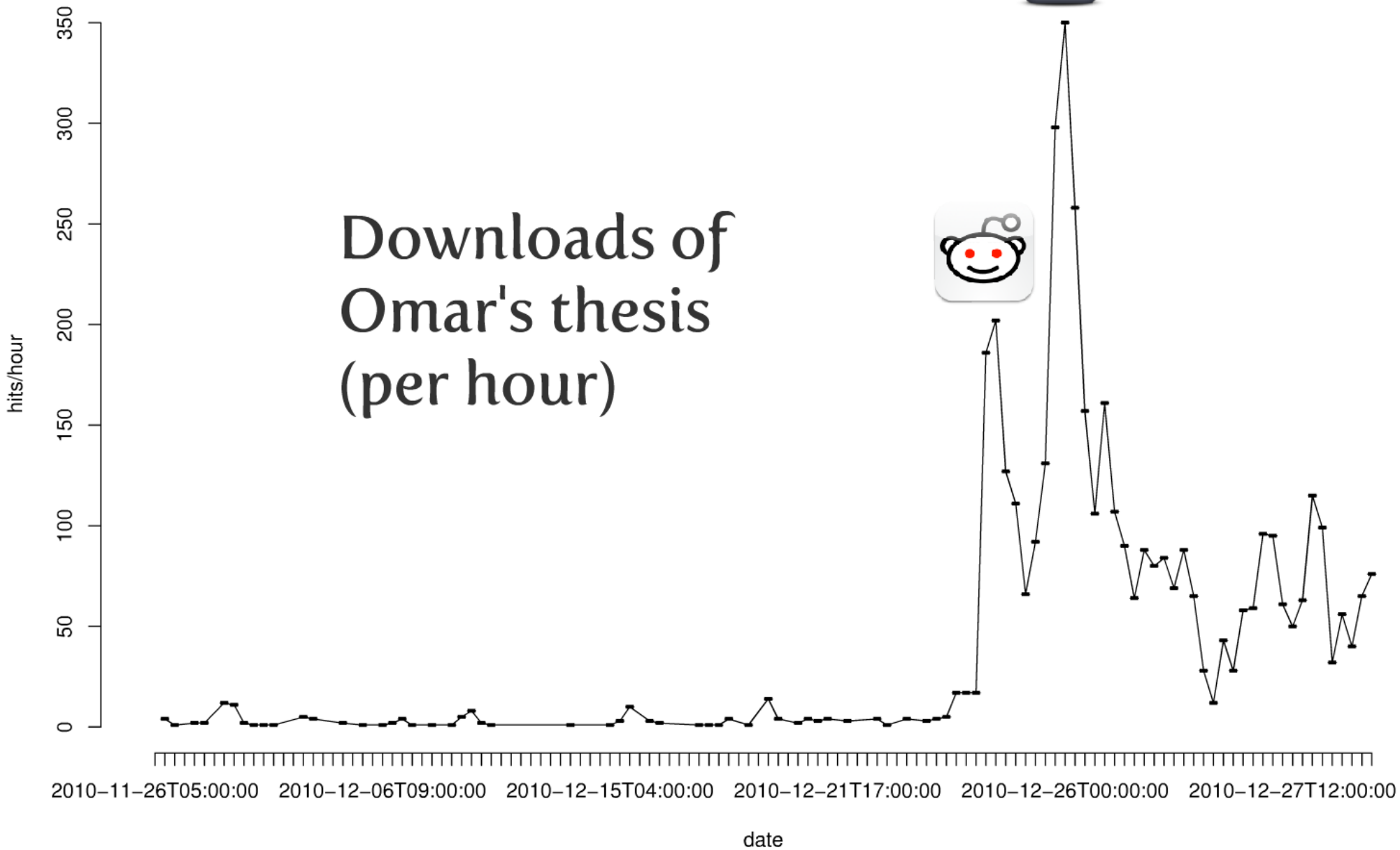
A trade association of bankers attempted to get the University of Cambridge to withdraw a thesis by Omar Choudary on the No-PIN attack on Chip and Pin. Ross Anderson has told the UK Cards Association that the paper will not be taken offline in a [robust response](#) to that request. Anderson points out that the material on the No-PIN attack has already been published by himself and others on the Cambridge University web site.



- Home
 - News
 - Sport
 - TV&Showbiz
 - Femail
 - Health
 - Science&Tech
 - Money
 - De
- News Home | World news | Headlines | Pictures | Most read | News Board

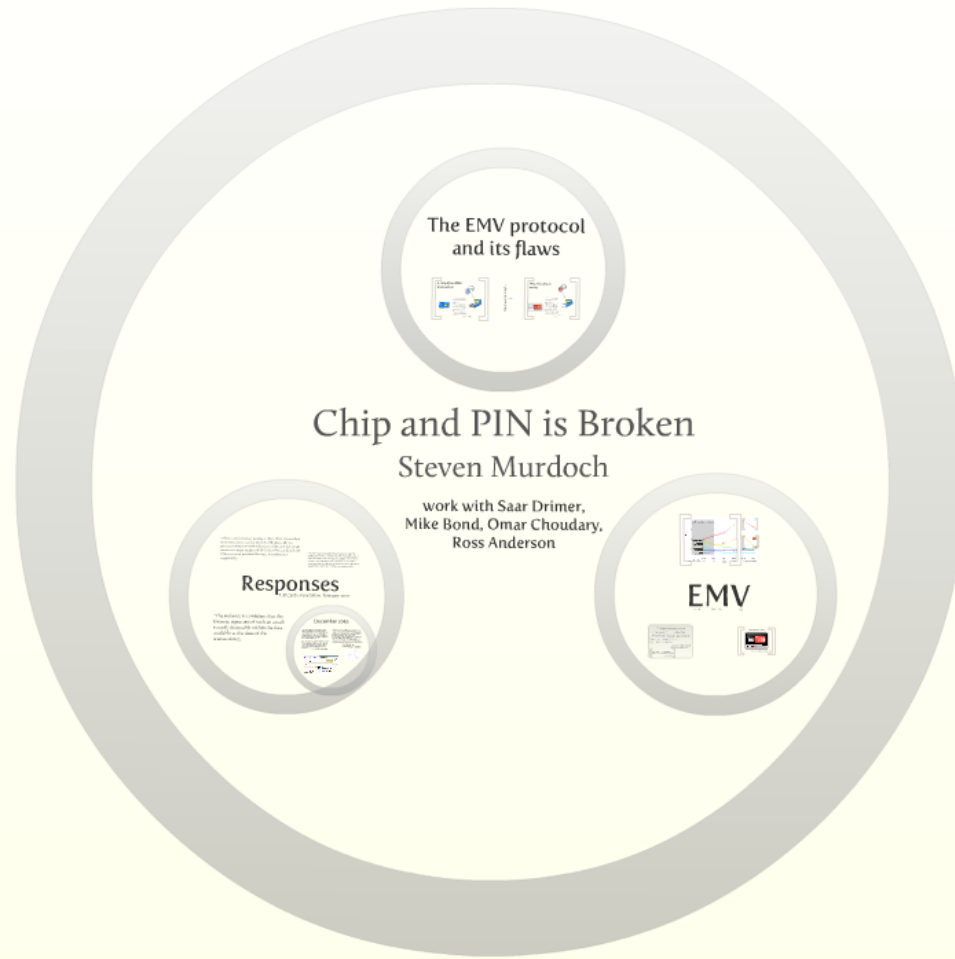
Chip and PIN flaw that banks tried to censor: Cambridge scientist exposed security failures

Downloads of Omar's thesis (per hour)



Many o
card ha

Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures



www.lightbluetouchpaper.org