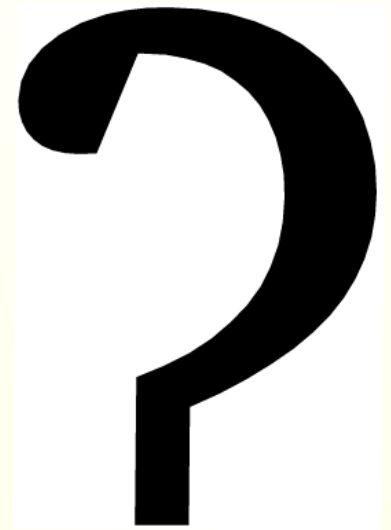


How is ATM fraud
happening



Chip and PIN is Broken

Dr Steven J. Murdoch
University of Cambridge

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

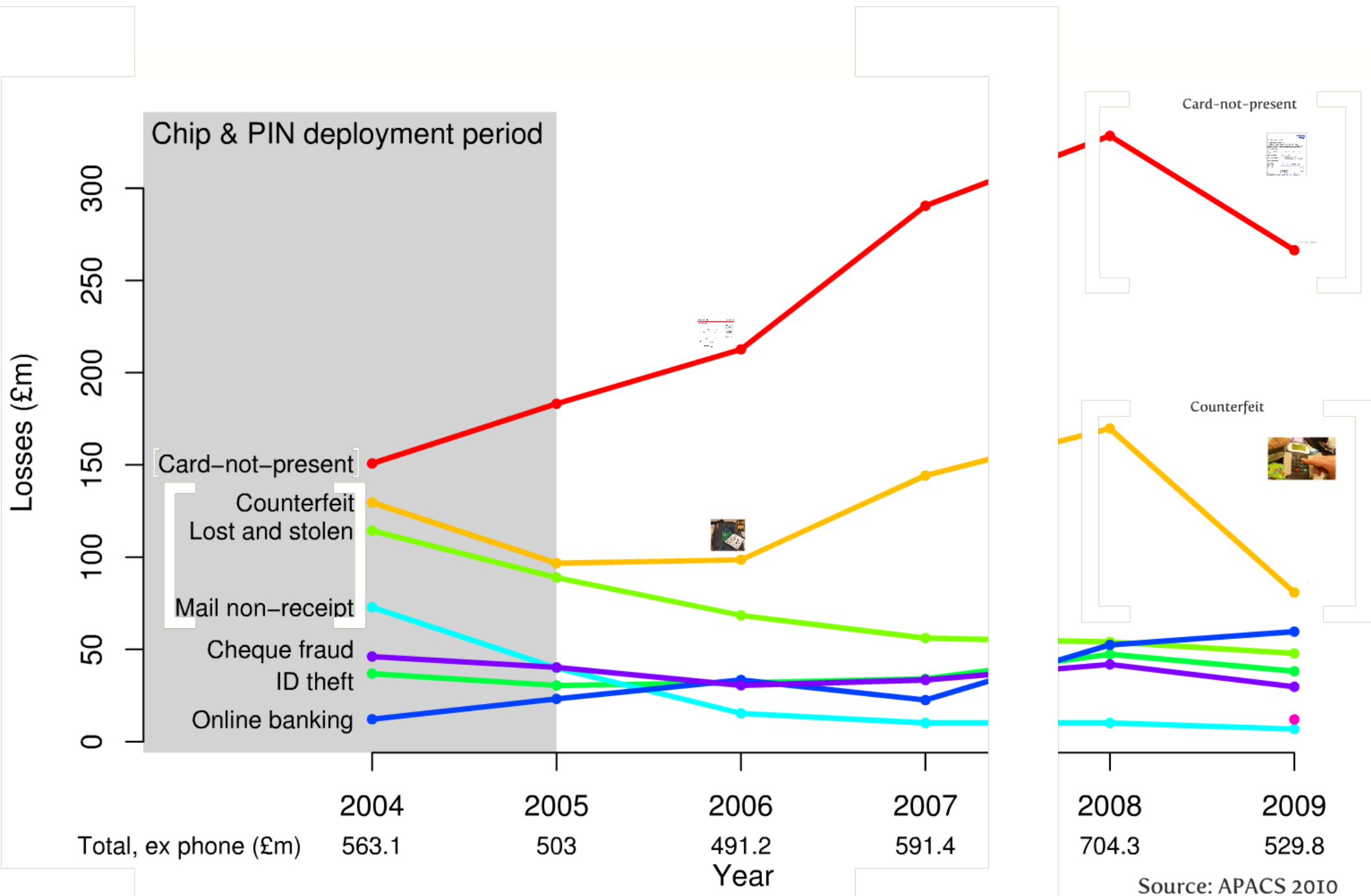
Many customers claim that their
card has been stolen and used

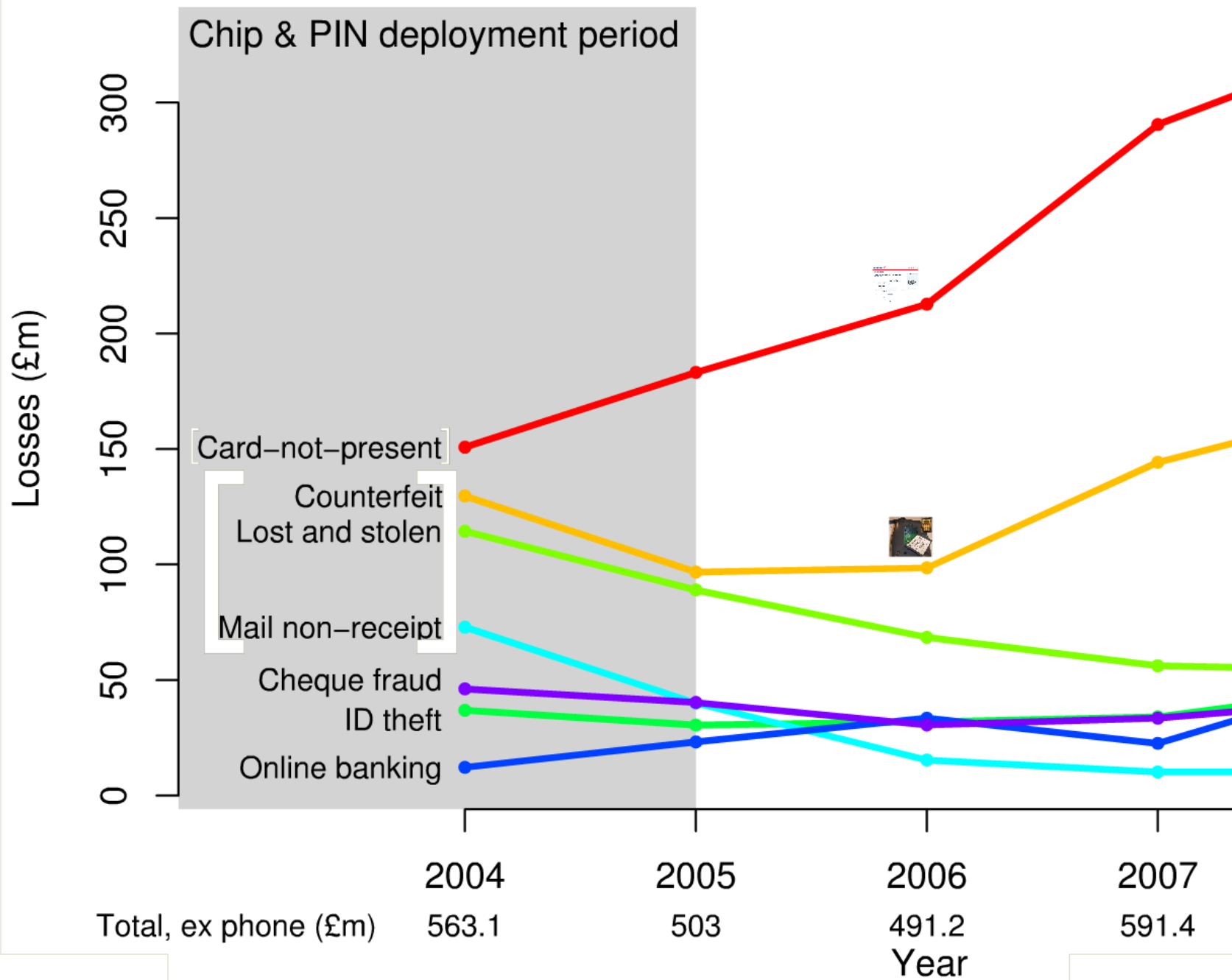
Banks claim EMV is infallible, so
victims do not get their money back

44% according to latest figures

Many o
card ha

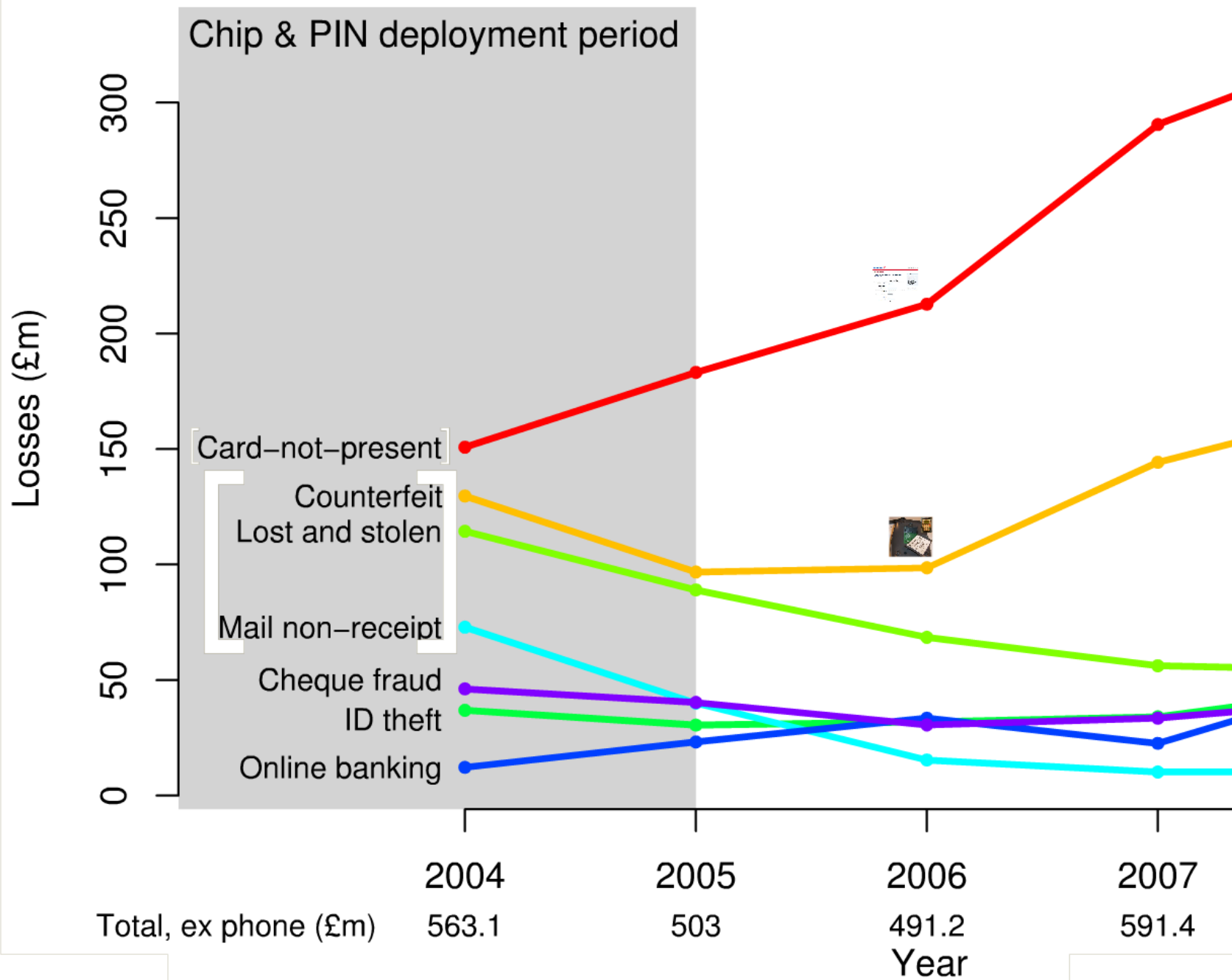
Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures





Counterfeit
Lost and stolen

Mail non-receipt

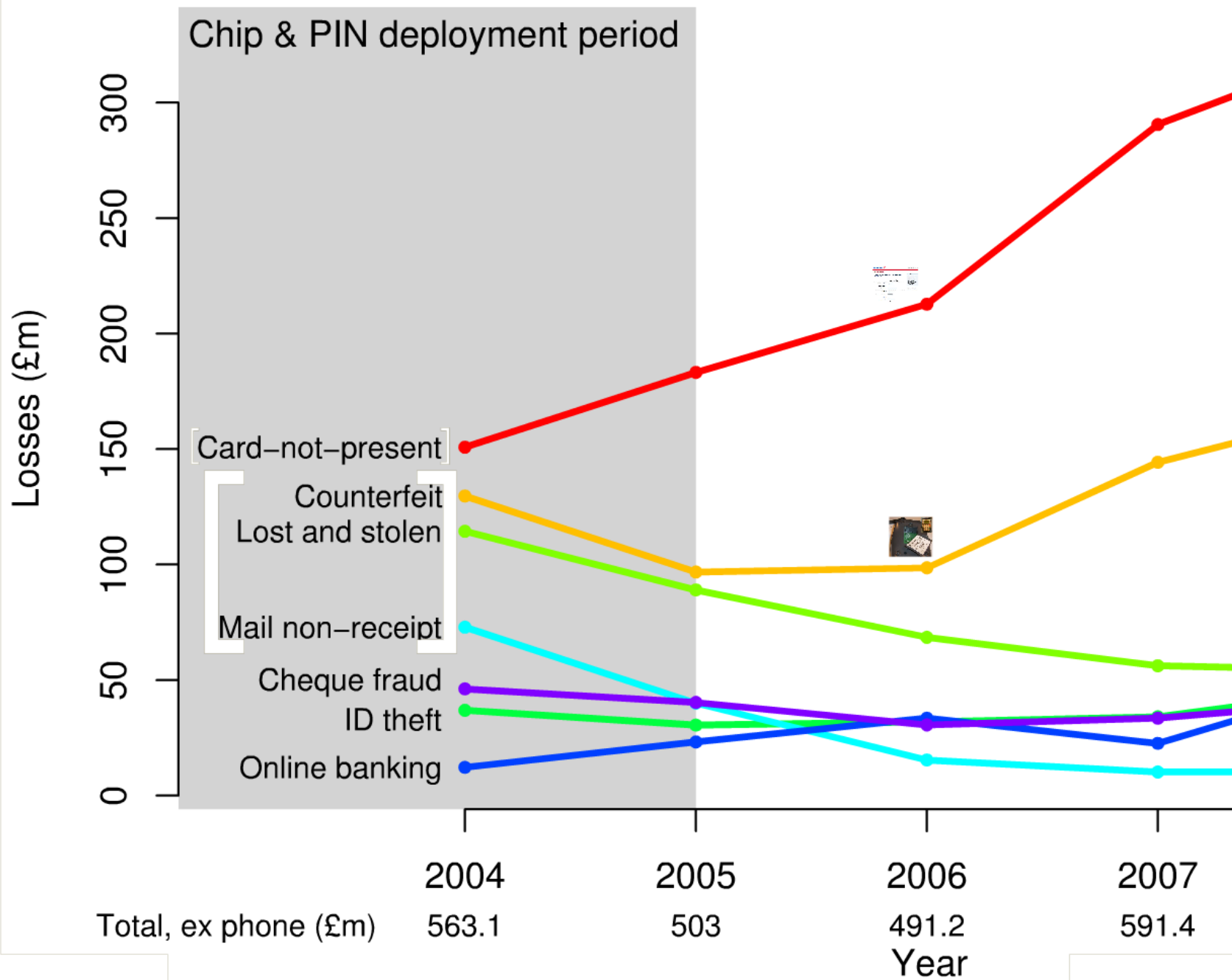




Card-not-present

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

Welcome to Card Secure Security. To activate this service, please follow the instructions below. If you have any questions, please contact your merchant or the merchant's processor.

Simply activate the online below to activate the free security service.

Card Email: COMPANY

Card State: The first 4 digits of the card number

Cardholder name as printed on the card:

Card No: 0000000000000000

Exp. M / Y: 00/00

EMV 3-D Secure: SUCCESS

By installing a new device by Jan 7, 2015 and Jan 15, 2015, you will be able to use the 3-D Secure service. For more information, please visit [http://www.visa.com/3ds](#).

3. RESPONSIBILITY

Merchant is responsible for the security of the cardholder's information.

Example of responsibilities and conditions for online purchases (example of a merchant)



Added Safety Online

Welcome to Barclaycard Secure.

You are not currently registered for this new free service.

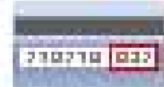
Barclaycard Secure, provided in association with Verified by Visa, protects your card when you shop online with this and other participating retailers.

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](#).

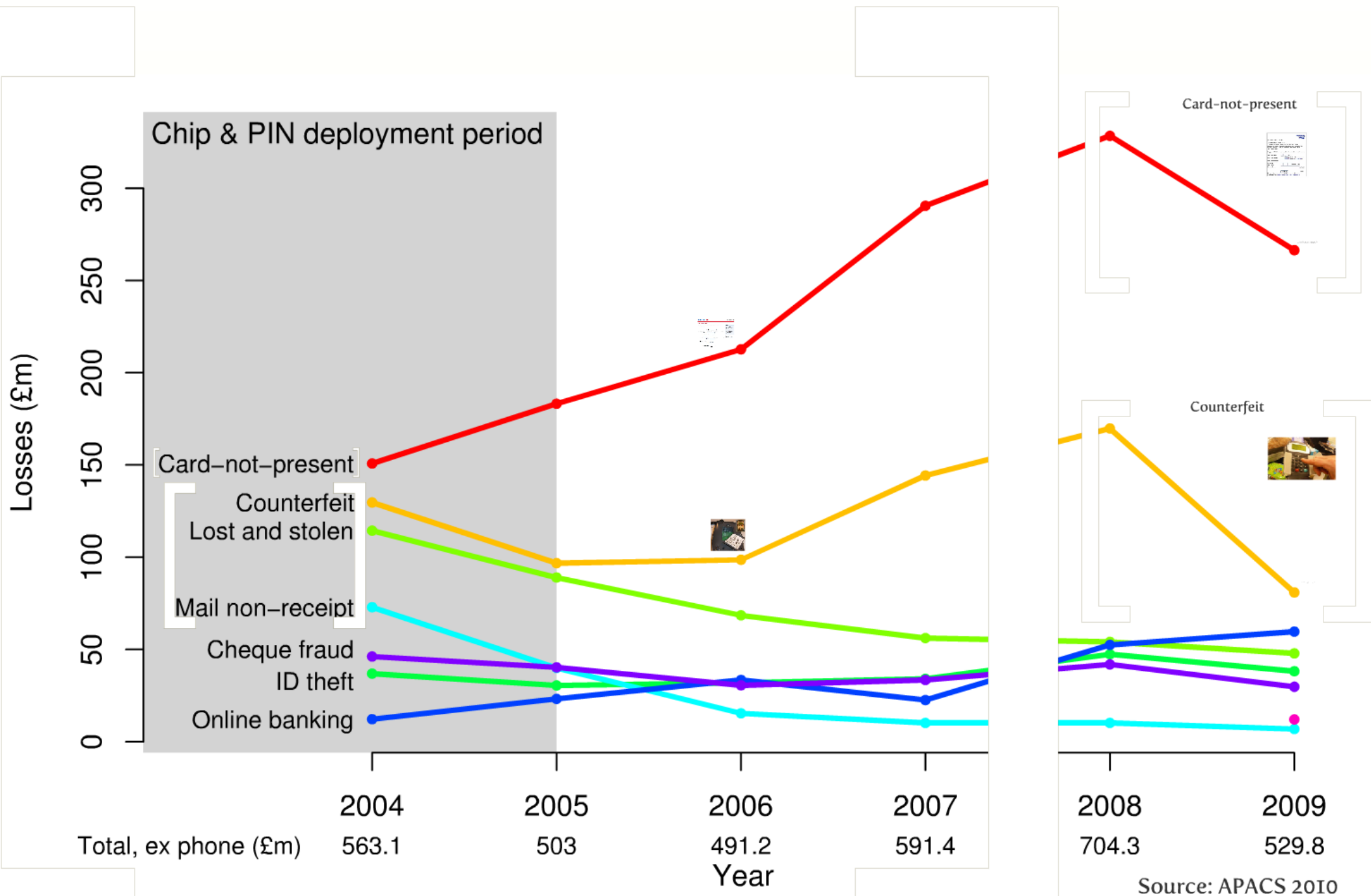
Click here to view: [Terms and Conditions of Use](#) [Privacy Policy](#).

Counterfeit



© 2010 Visa U.S.A. Inc. All rights reserved. This document is for informational purposes only and does not constitute an offer of any financial product or service.





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.

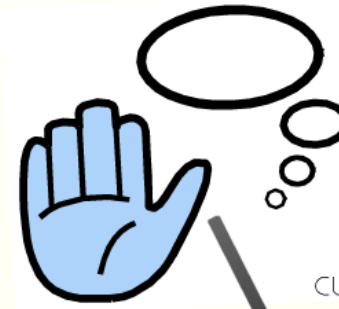
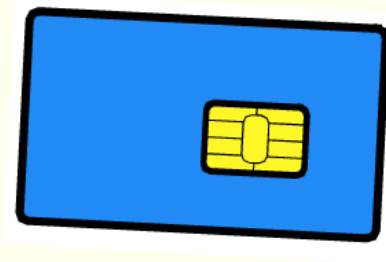
Letter denying refund for disputed transactions (American Express)

They were wrong



BBC Newsnight, February 2010

A simplified EMV transaction

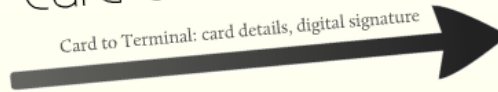


customer enters PIN

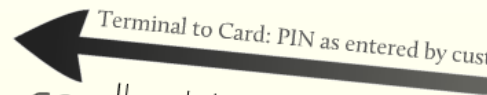


card authentication

Card to Terminal: card details, digital signature

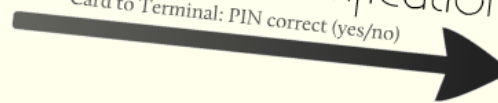


Terminal to Card: PIN as entered by customer

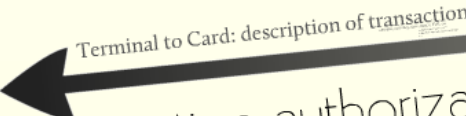


cardholder verification

Card to Terminal: PIN correct (yes/no)



Terminal to Card: description of transaction



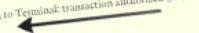
transaction authorization

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

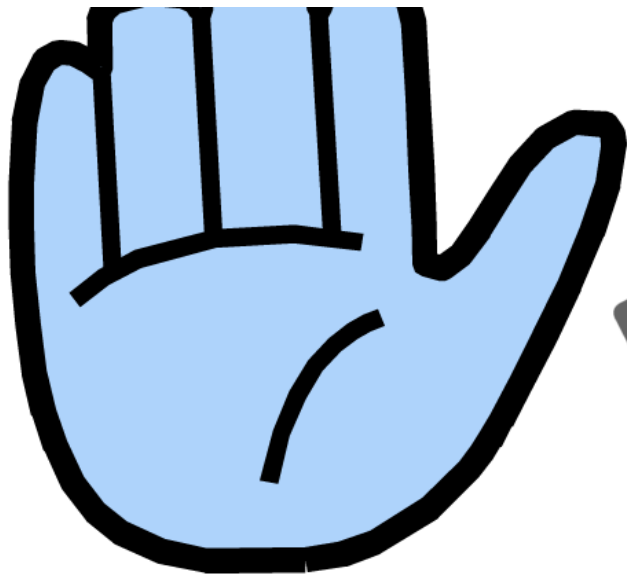
Card to Terminal: card details, digital signature



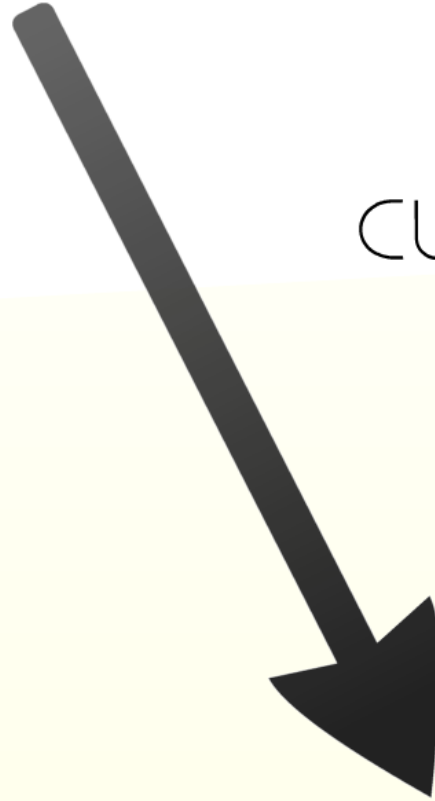
Terminal to Card: PIN as entered by customer



Cardholder



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?
* ...



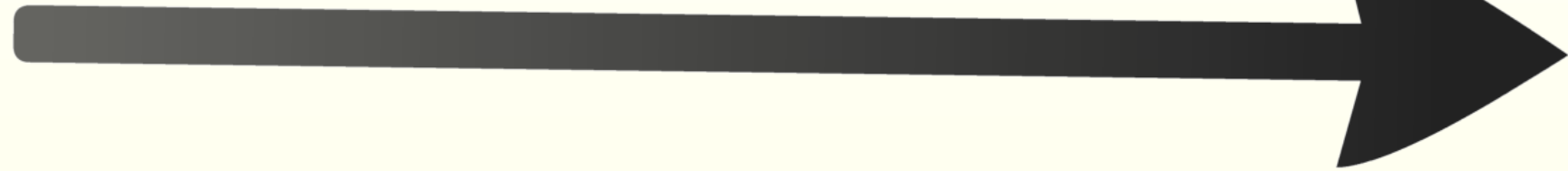
Terminal to Card: description of transaction

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



transaction authorization

Card to Terminal: MAC over transaction and other details

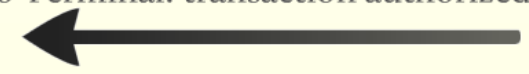


MAC and transaction sent to bank for verification



online transaction authorization

Bank to Terminal: transaction authorized (yes/no)



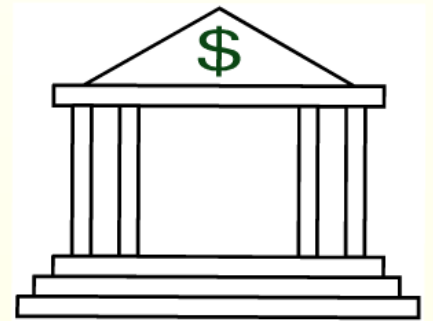
and other details



MAC and transaction sent to bank for verification



online transaction authorization



Bank to Terminal: transaction authorized (yes/no)



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?
• ...

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?
 - ...
- 

SACTIONS

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

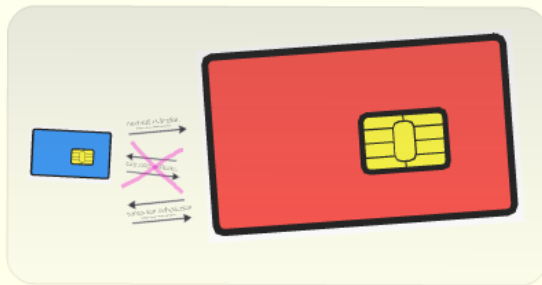
A man-in-the middle tell the card that the PIN was not required
and the terminal that the PIN was correct

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

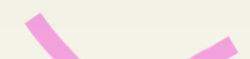
MAC and transaction sent to bank for verification
online transaction authorization

Bank to Terminal: transaction authorized (yes/no)

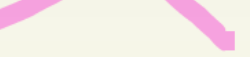




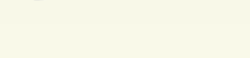
card authentication
Message relayed without modification



~~cardholder verification~~

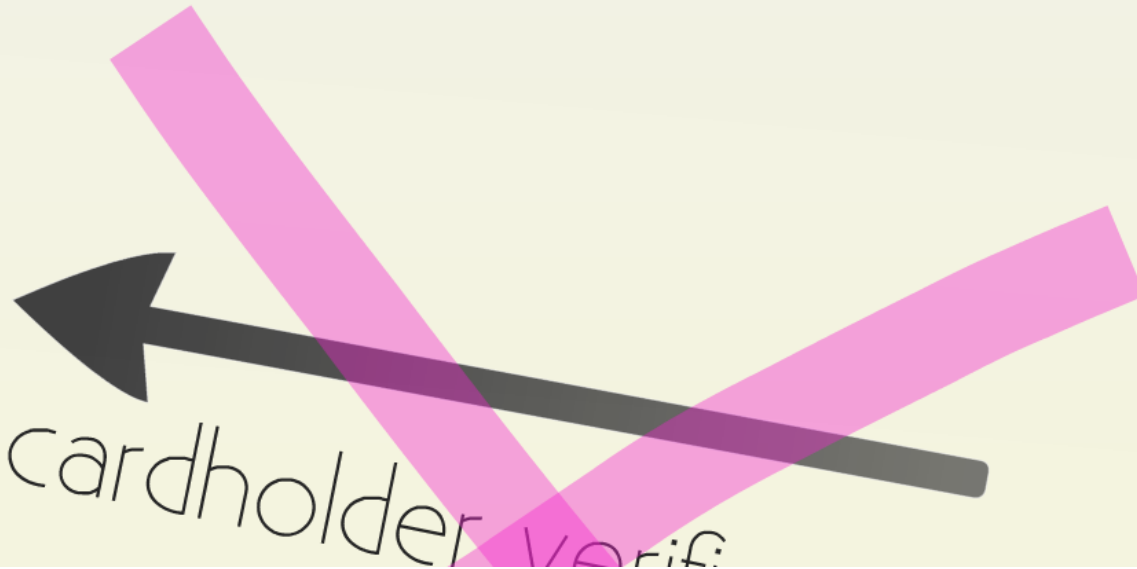
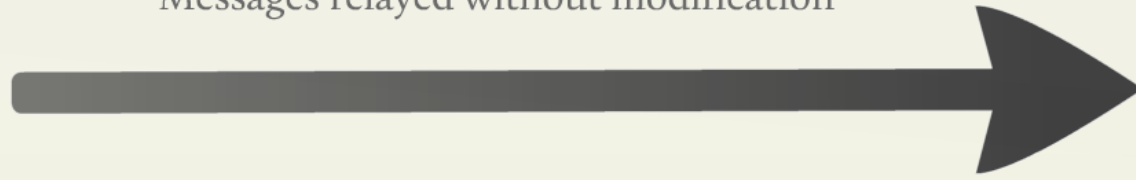


transaction authorization
Message relayed without modification

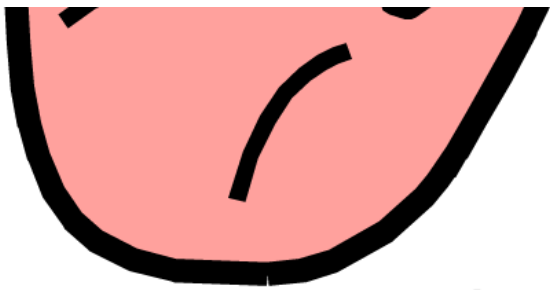


card authentication

Messages relayed without modification



cardholder verifi



criminal enters 0000



Card to Terminal: card details

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

cardholder verification

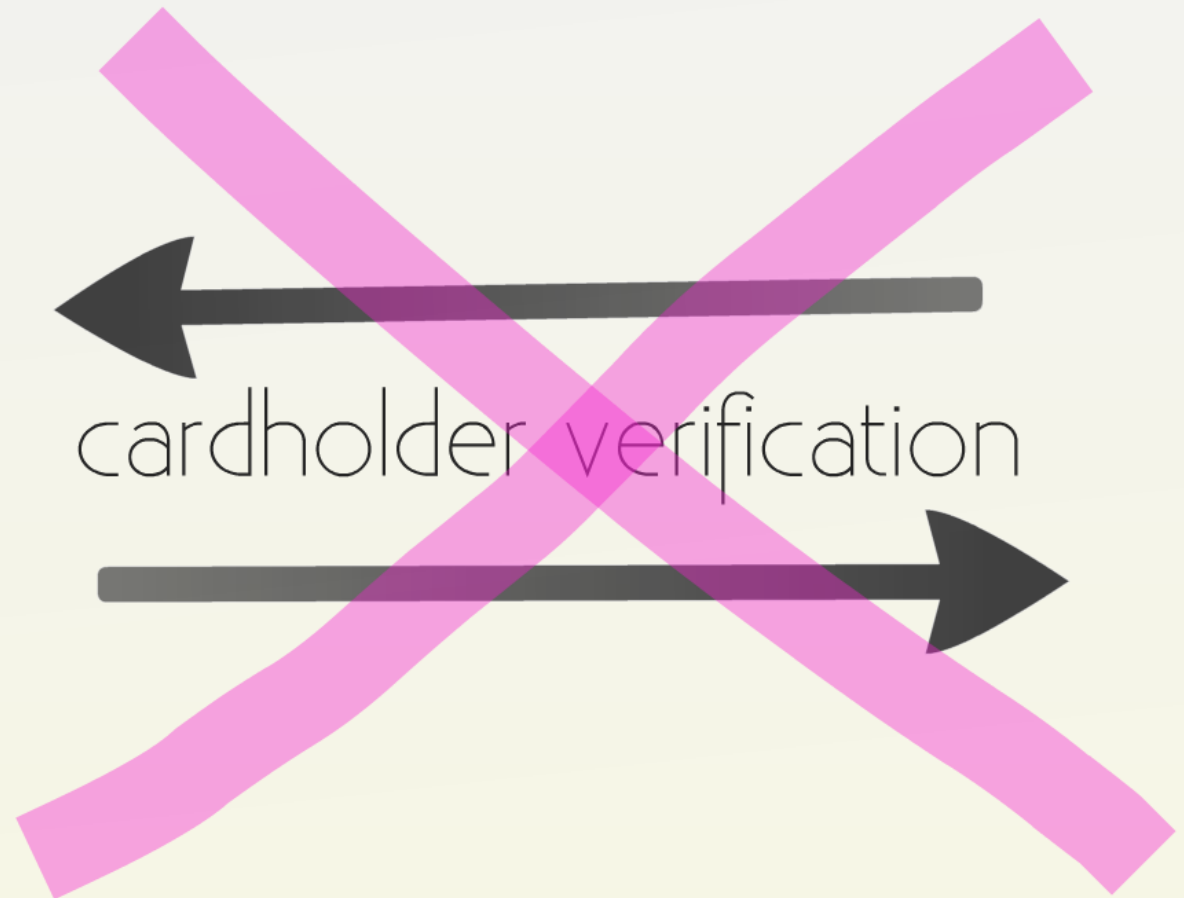
MitM to Terminal: PIN correct **yes!**

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
without modification

verification



transaction authorization

Messages relayed without modification



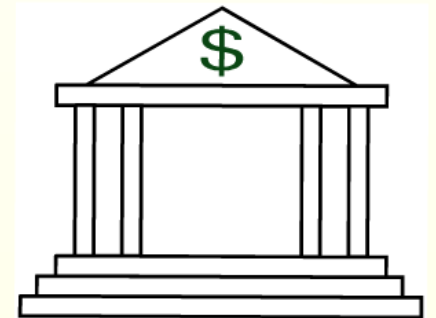
and other details



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)



ACCOUNT

late, nonce, TVR, etc

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

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

Card: N
Termina

ACCOUNT

late, nonce, TVR, etc

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

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

Card: N
Termina

"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

"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."

"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

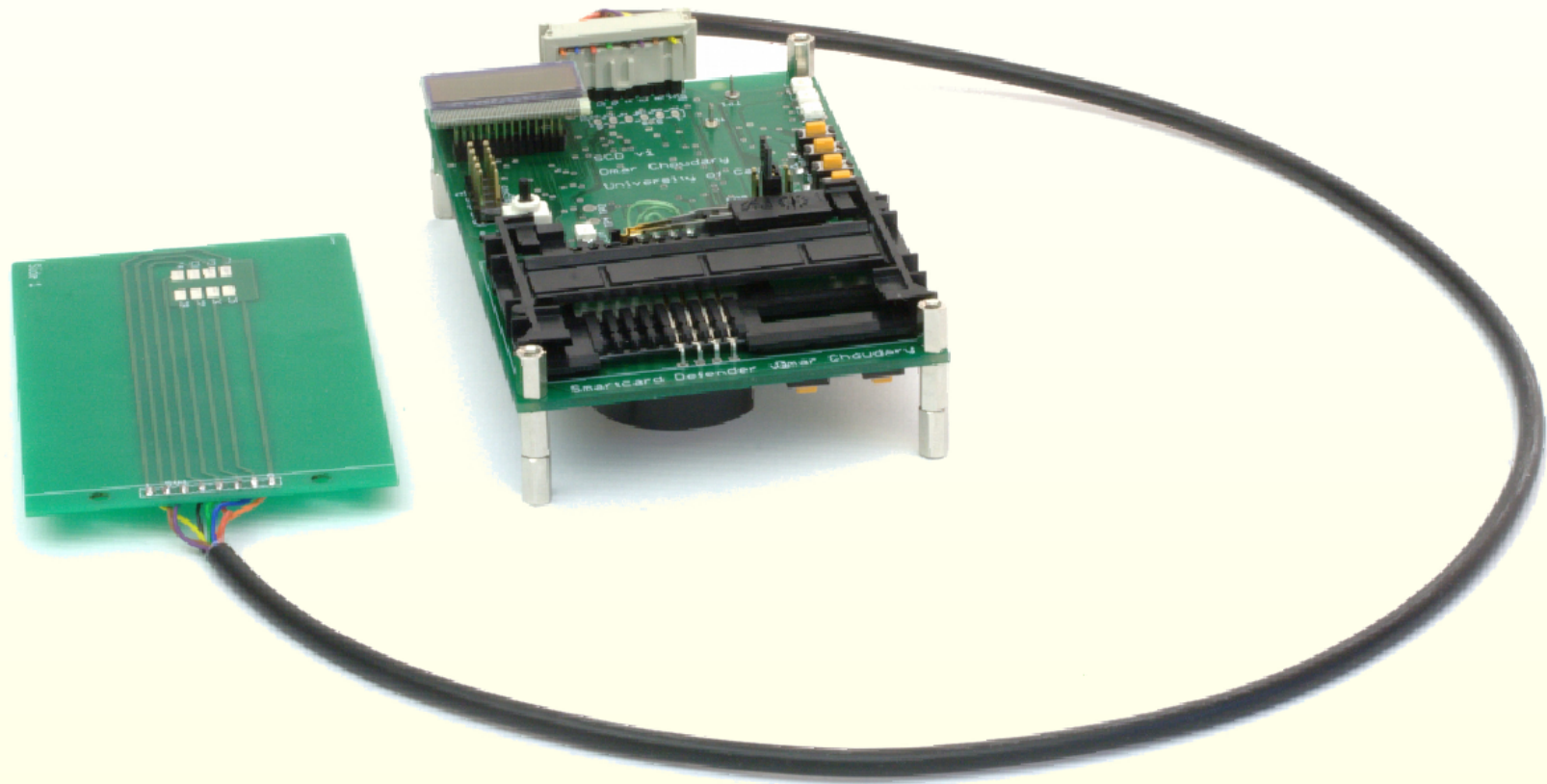
All made at [REDACTED]
[REDACTED]

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

"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



"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."

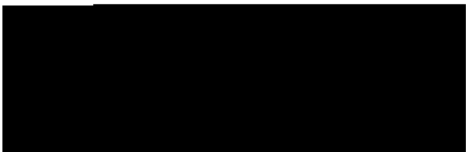
WRONG

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

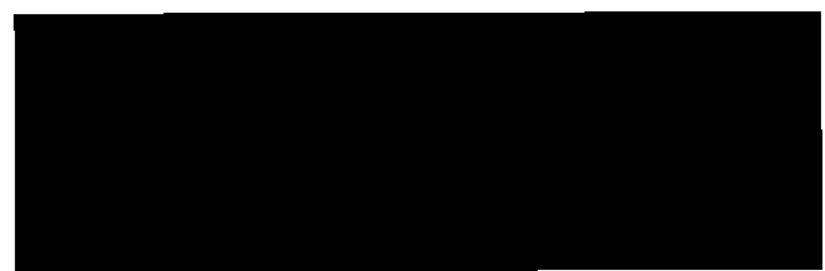
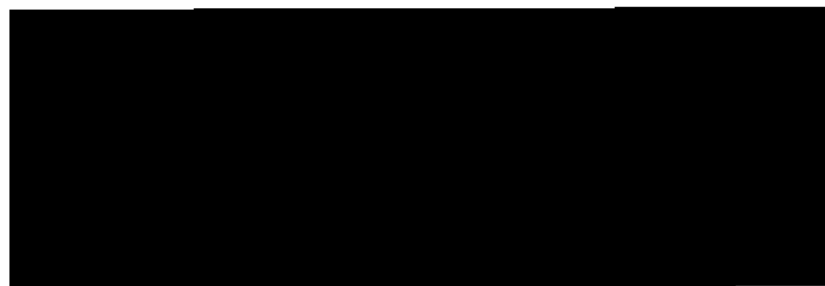


24/07/1980

11:38

KART NO

S.K.T.: 12/10



the
ver
our

EMV : A0000000031010/00A0088000/F800

APP LABEL : VISA DEBIT

CVV - no entry required, no
pad present, but no was not
entered

ORJINAL FISI SAKLAYINIZ.
MUSTERIYE 2. NUSHAYI VERINIZ.

TESEKKURLER



Many o
card ha

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

The EMV protocol and its flaws



ISSE 2010

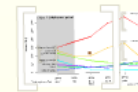
Chip and PIN is Broken

Dr Steven J. Murdoch
University of Cambridge

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

Responses

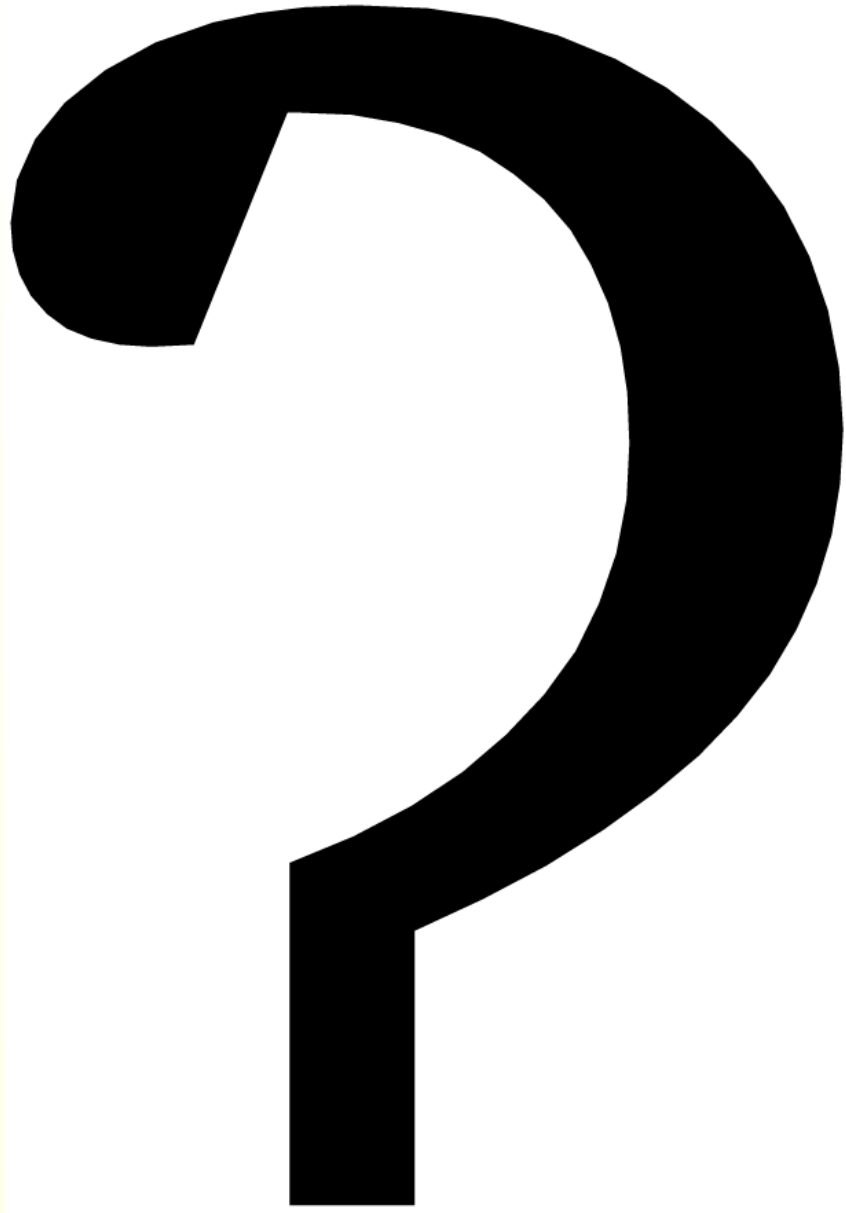
"The industry is confident that the forensic responses of such an attack is easily detectable within the data available at the time of the transaction?"



EMV



Cloud



How is ATM fraud
happening

