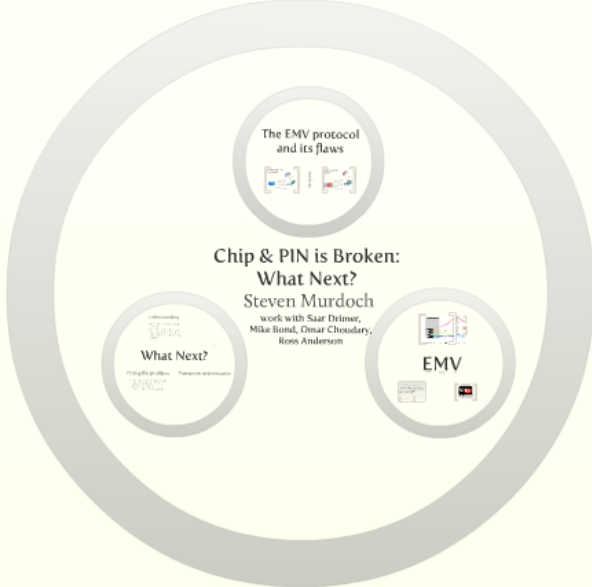


We are recording this presentation for a podcast

- to ensure the highest possible quality
- please switch off your mobile phone ringer - set your phone to vibrate - on those rare occasions with the ringer on, leaving it silent is the preferred
- if you wish to comment or ask a question, please raise your hand and wait for the meeting moderator - comments should only be recorded and we will have to bring the session to rest
- please speak clearly with the top of the microphone pointing upwards at chest height - not directly at the mic



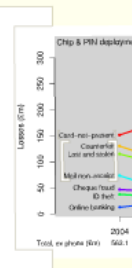
www.lightbluetouchpaper.org



Chip & PIN is Broken: What Next?

Steven Murdoch

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



What Next?

EMV

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

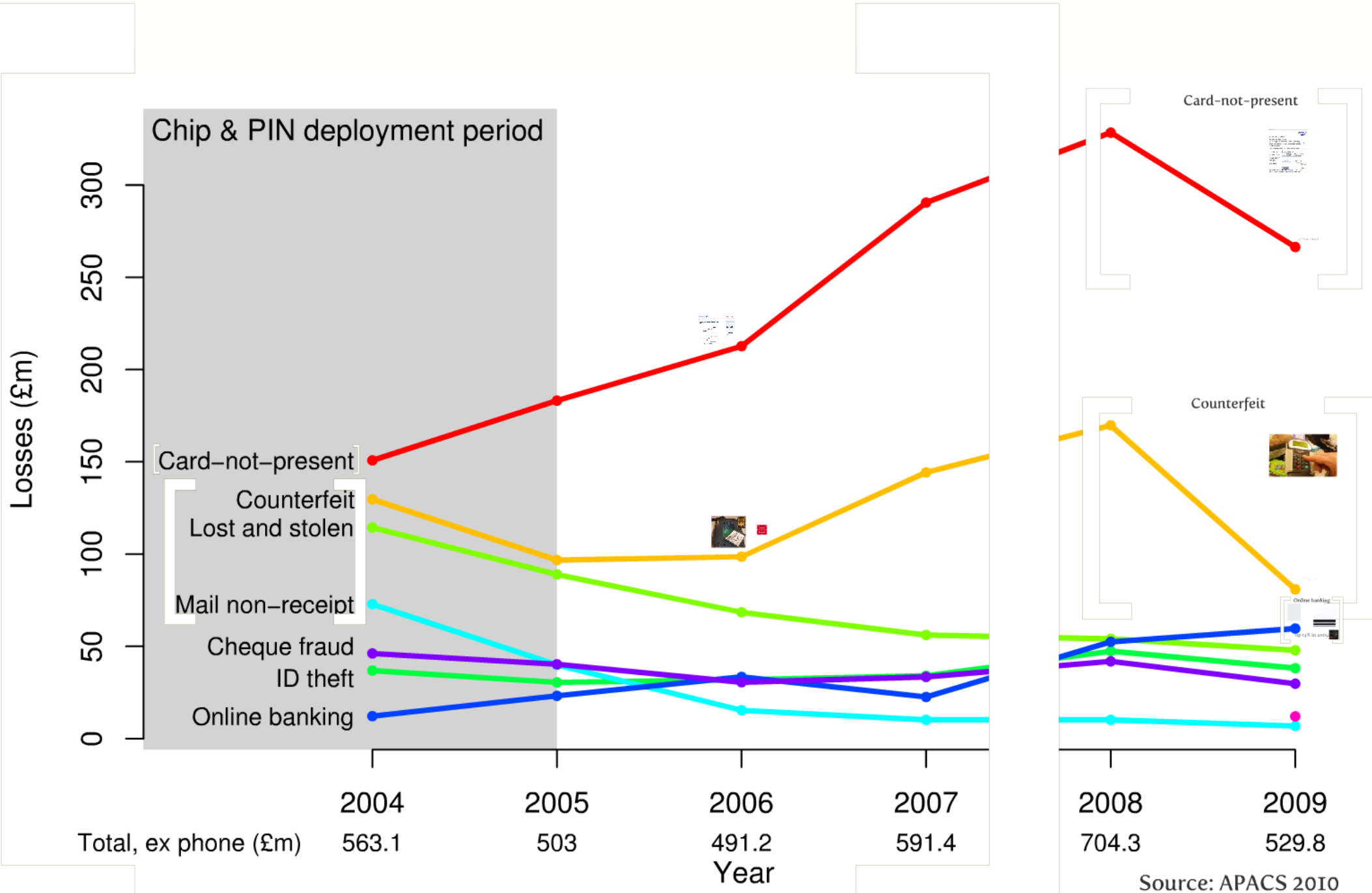
Used on 750m cards, billions
of pounds, euros, dollars

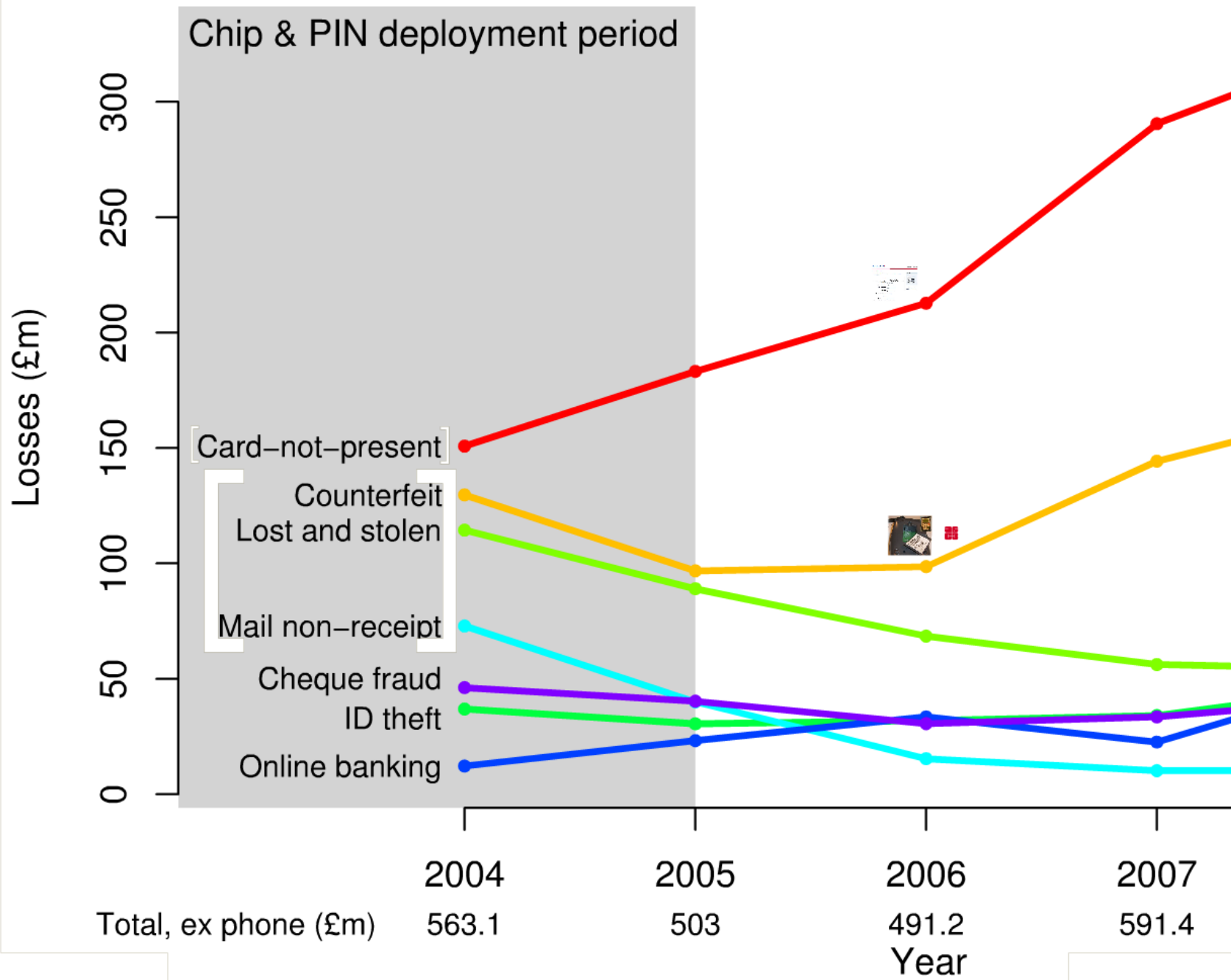
Many customers claim that their
card has been stolen and used

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

Many o
card ha

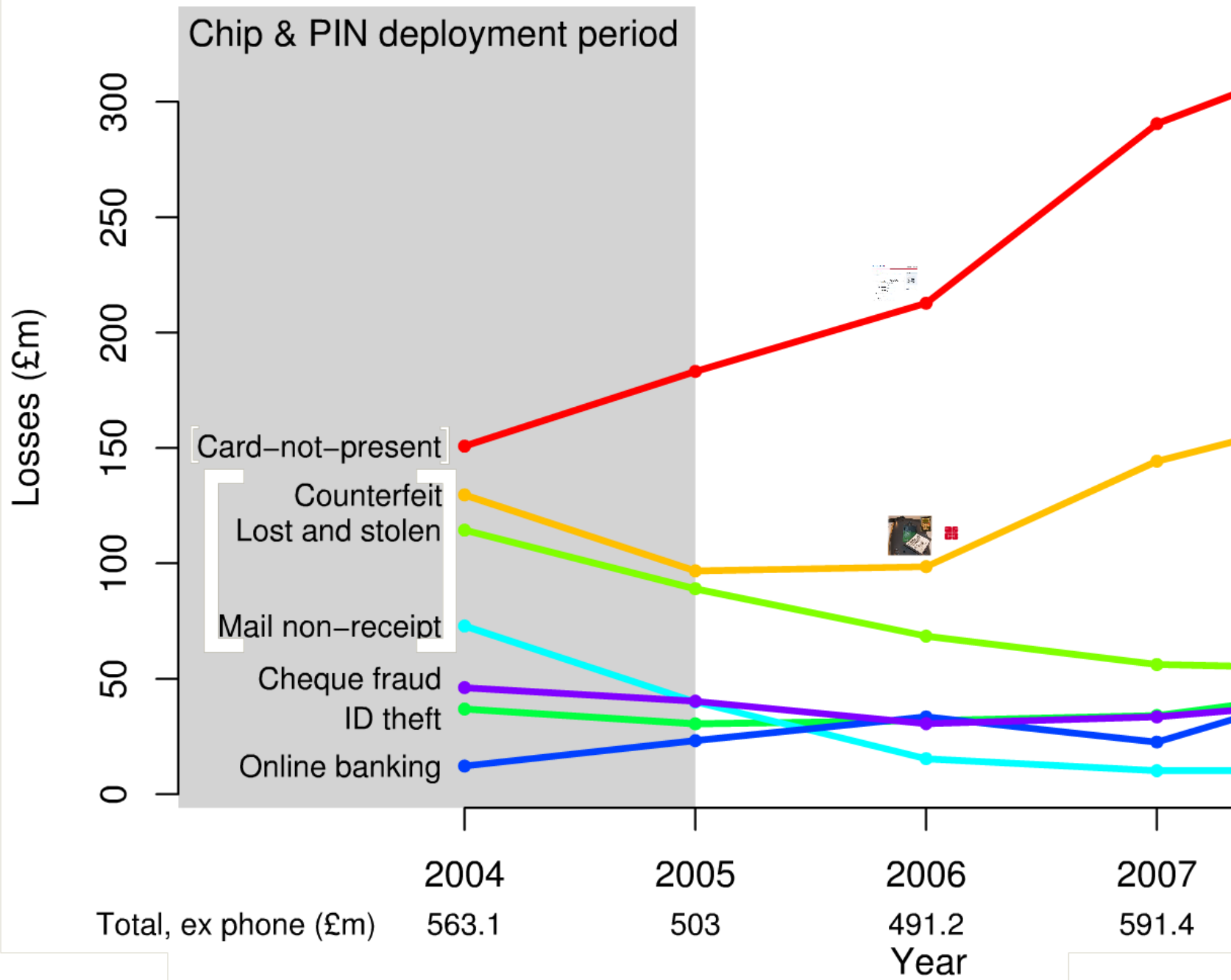
Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures





Counterfeit
Lost and stolen

Mail non-receipt



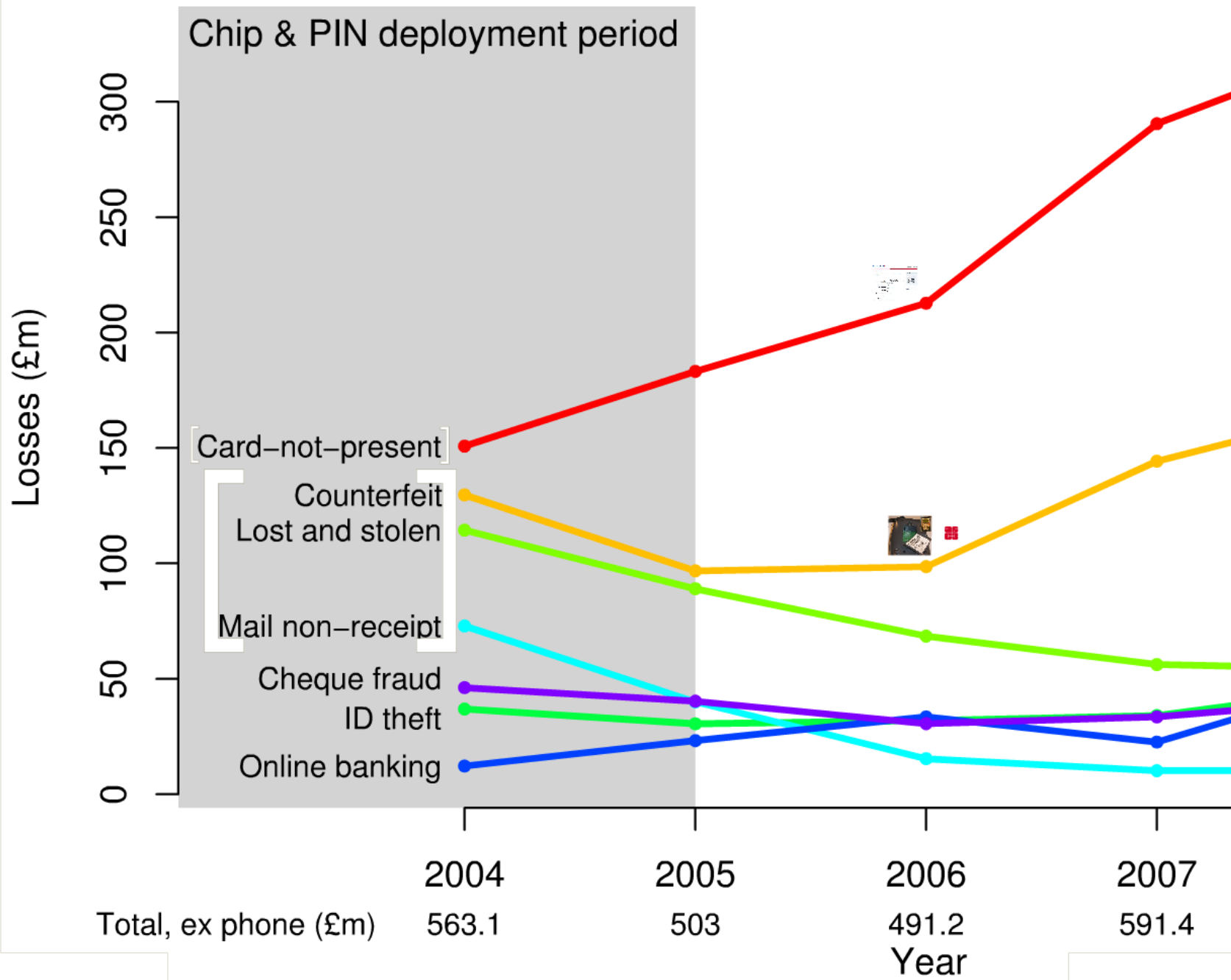


25
03

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](#).



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)

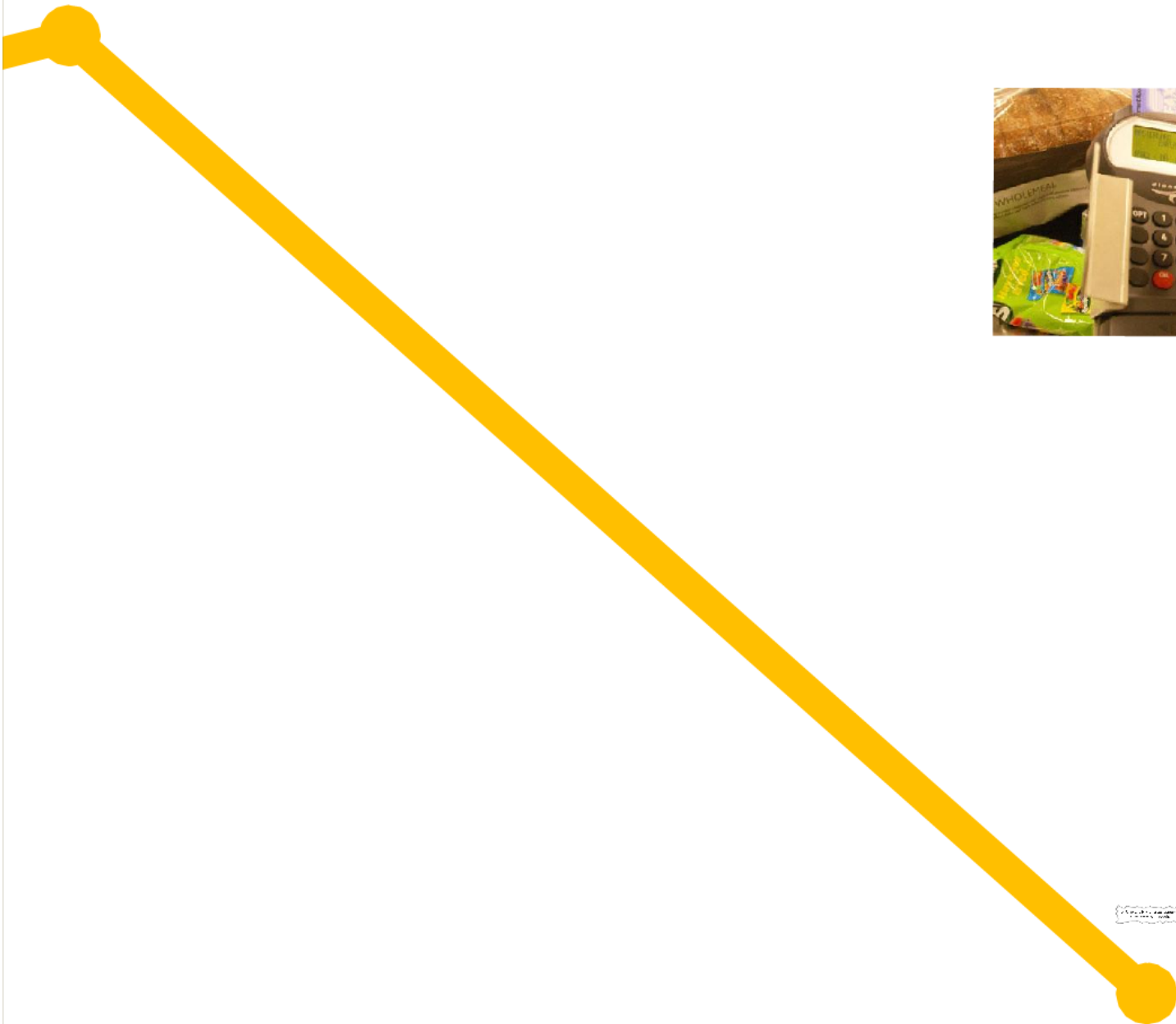
Email address: [How will it be used?](#)

[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

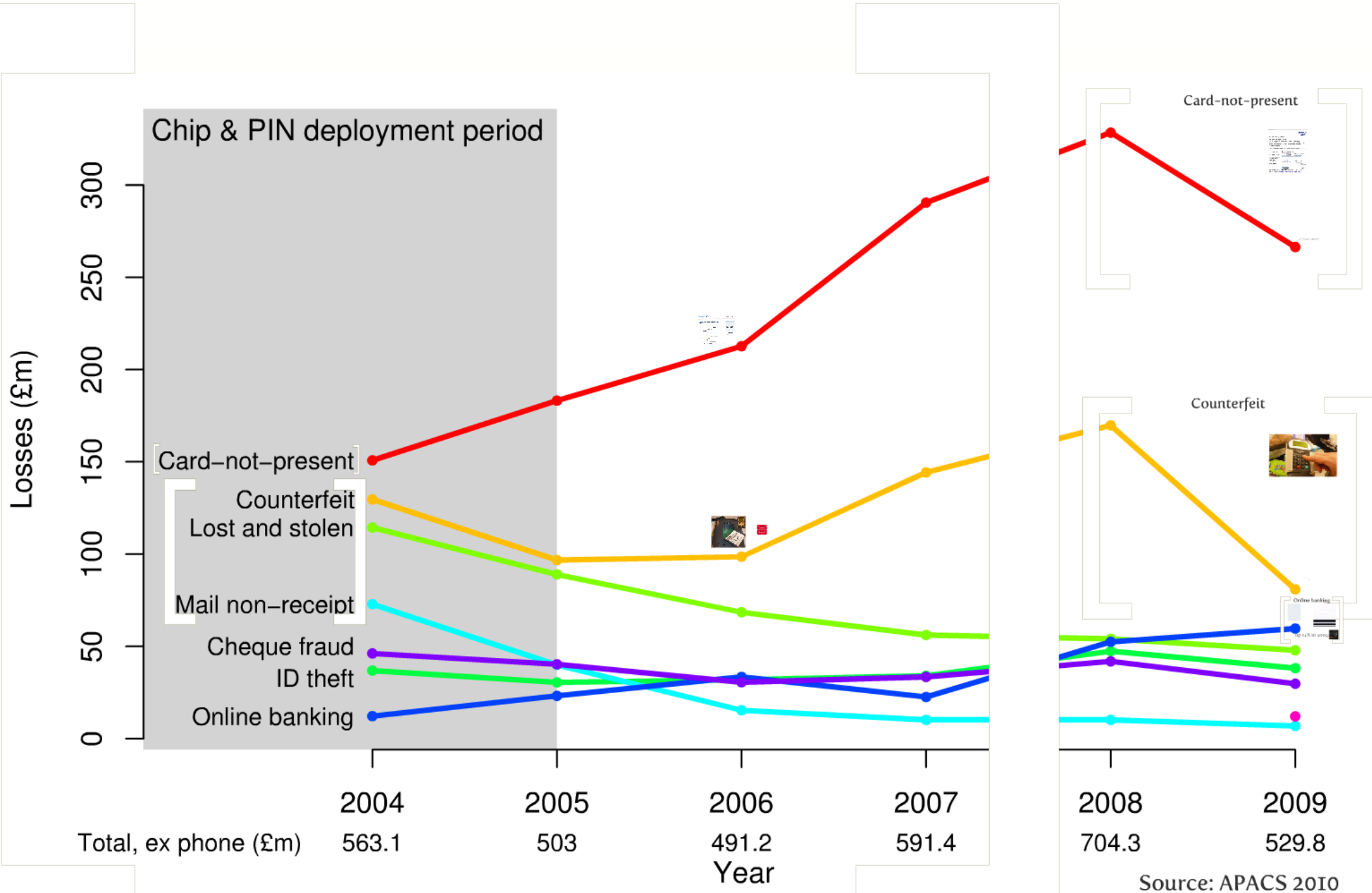


© 2011 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

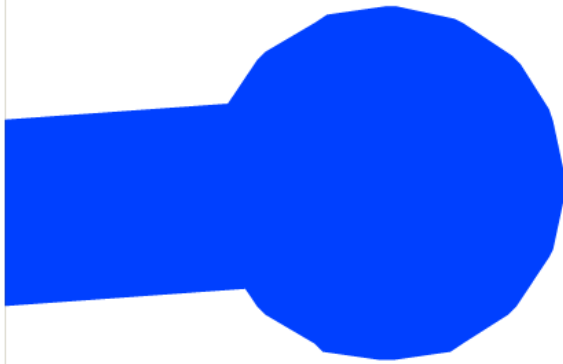
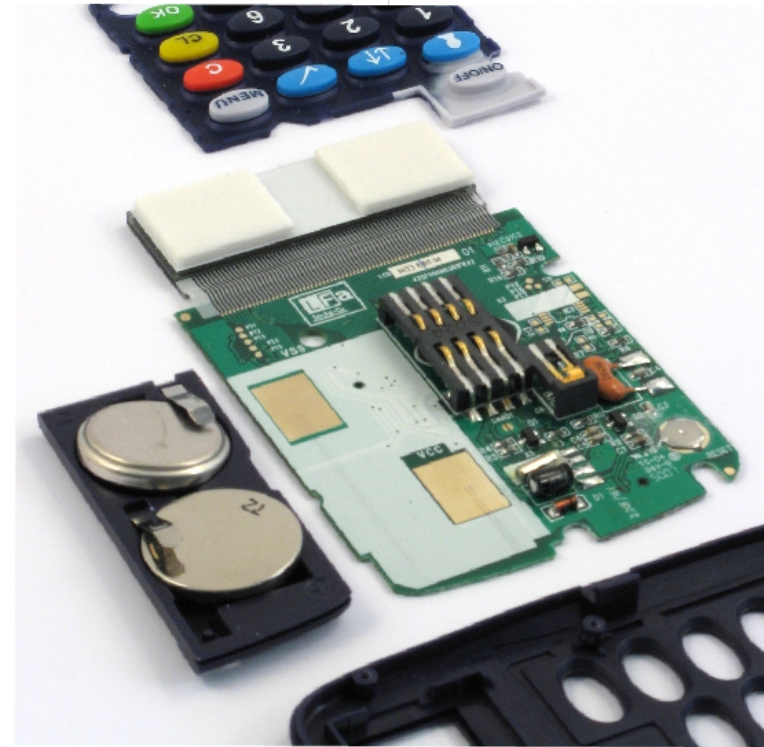
Online banking





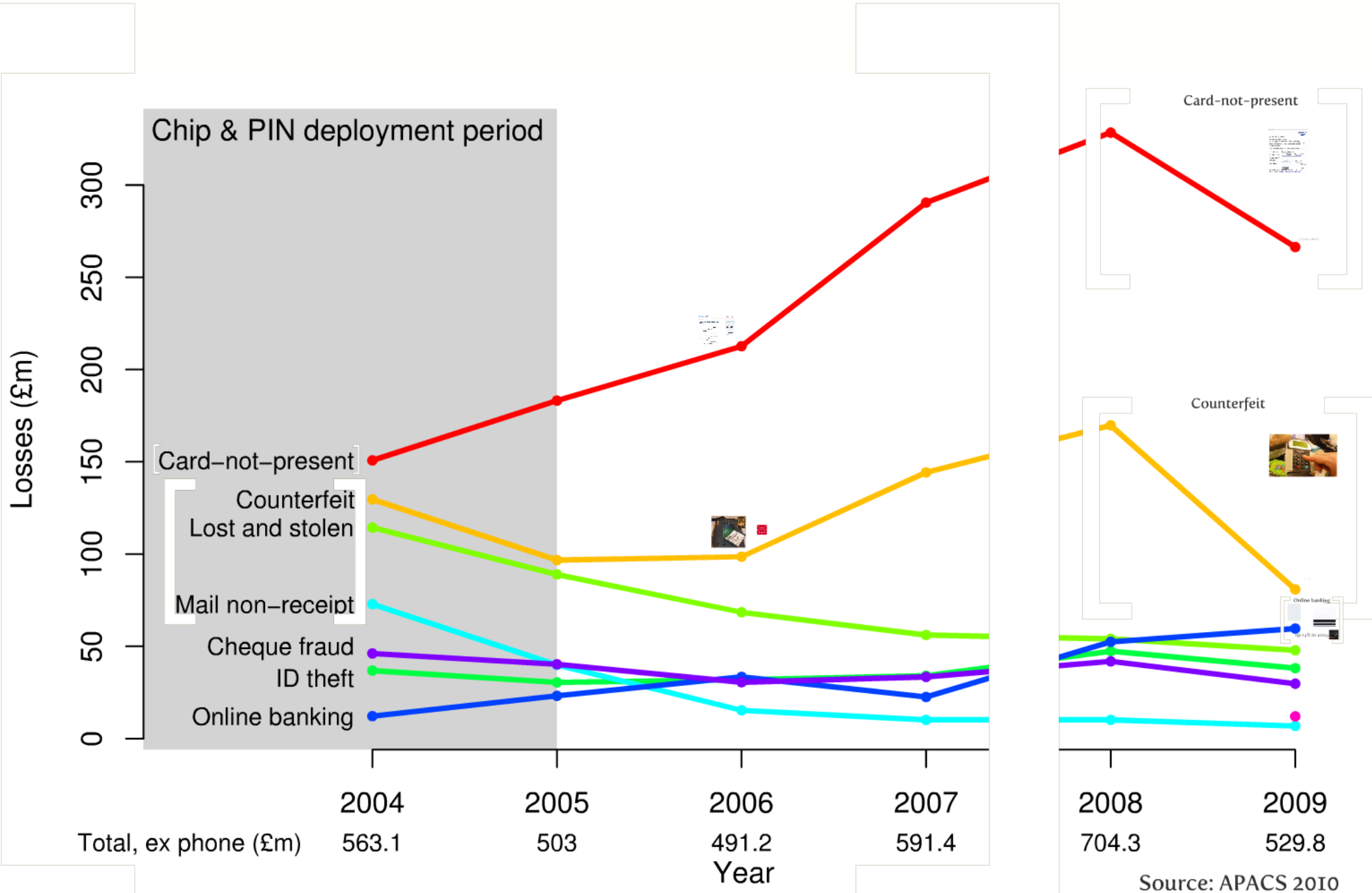


Online banking



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.

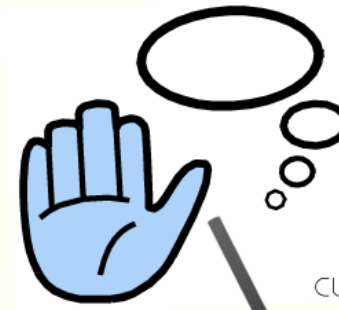
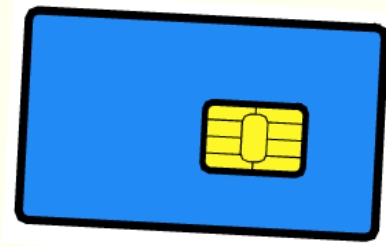
Letter denying refund for disputed transactions (American Express)

They were wrong



BBC Newsnight, February 2010

A simplified EMV transaction



customer enters PIN

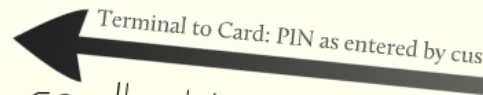


card authentication

Card to Terminal: card details, digital signature

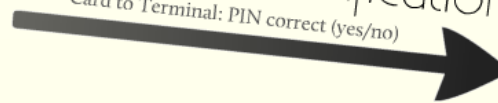


Terminal to Card: PIN as entered by customer

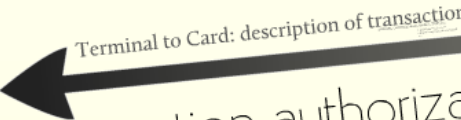


cardholder verification

Card to Terminal: PIN correct (yes/no)

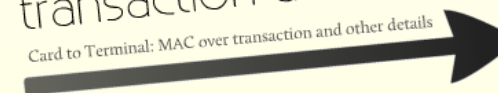


Terminal to Card: description of transaction



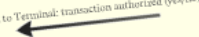
transaction authorization

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

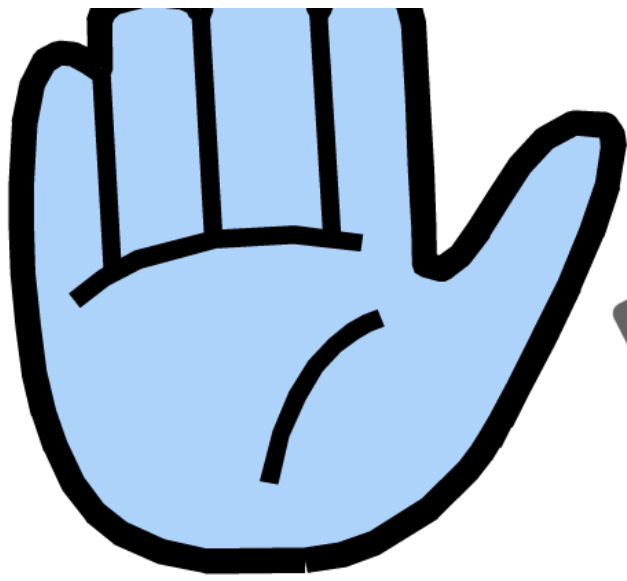
Card to Terminal: card details, digital signature



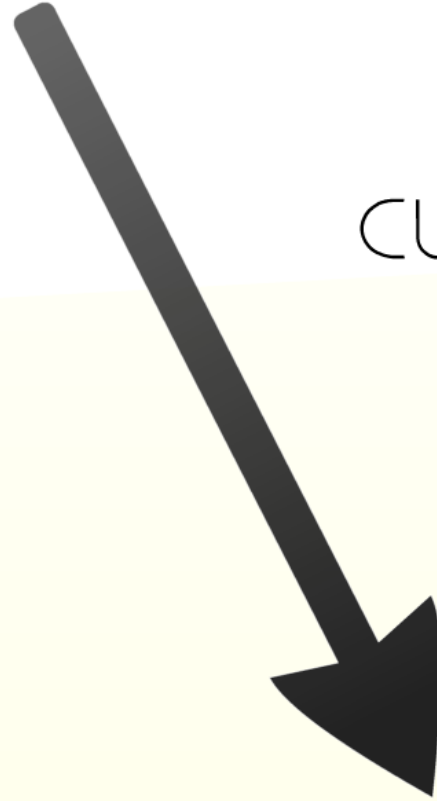
Terminal to Card: PIN as entered by customer



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?
...

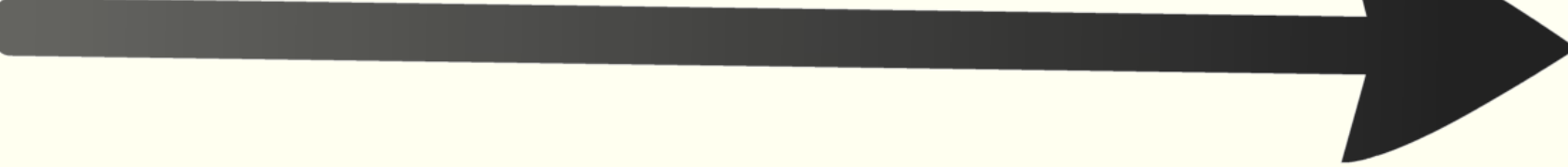


Terminal to Card: description of transaction

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)



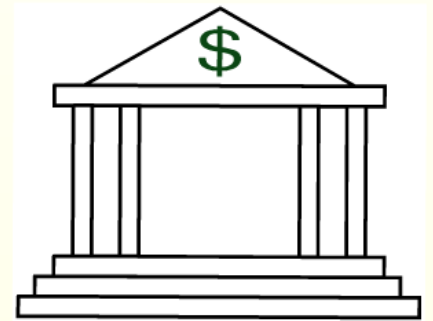
and other details



MAC and transaction sent to bank for verification



online transaction authorization



Bank to Terminal: transaction authorized (yes/no)



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

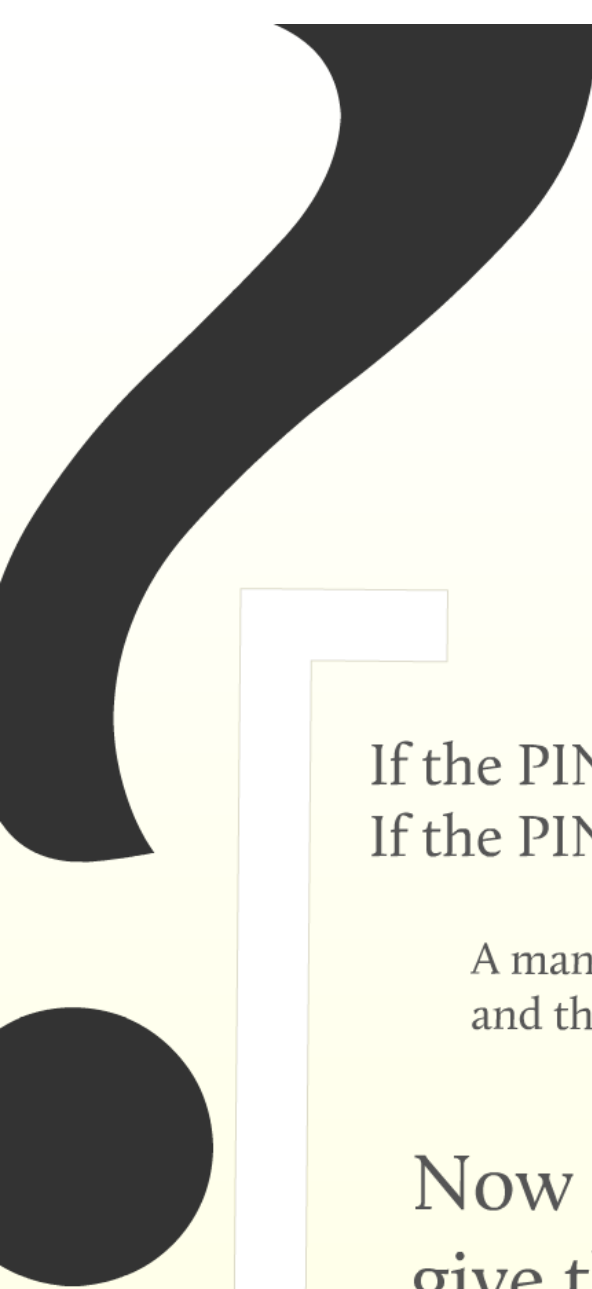
amount, currency, date, nonce, TVR, etc

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

Transaction

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

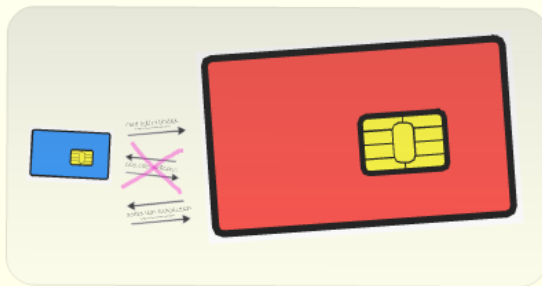
A man-in-the-middle tell the card that the PIN was not required
and the terminal that the PIN was correct

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

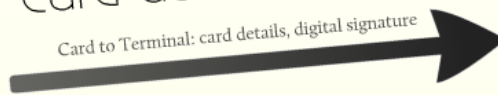


criminal enters 0000

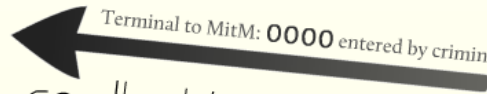


card authentication

Card to Terminal: card details, digital signature

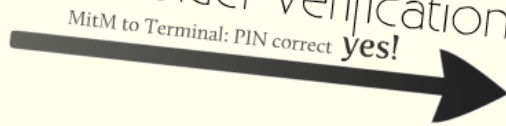


Terminal to MitM: 0000 entered by criminal

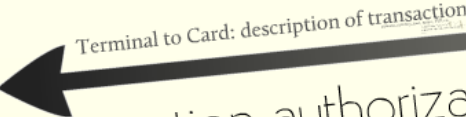


cardholder verification

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

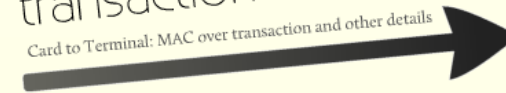


Terminal to Card: description of transaction



transaction authorization

Card to Terminal: MAC over transaction and other details



MAC and transaction sent to bank for verification

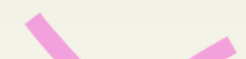
online transaction authorization

Bank to Terminal: transaction authorized (yes/no)





card authentication
Messages relayed without modification



~~cardholder verification~~

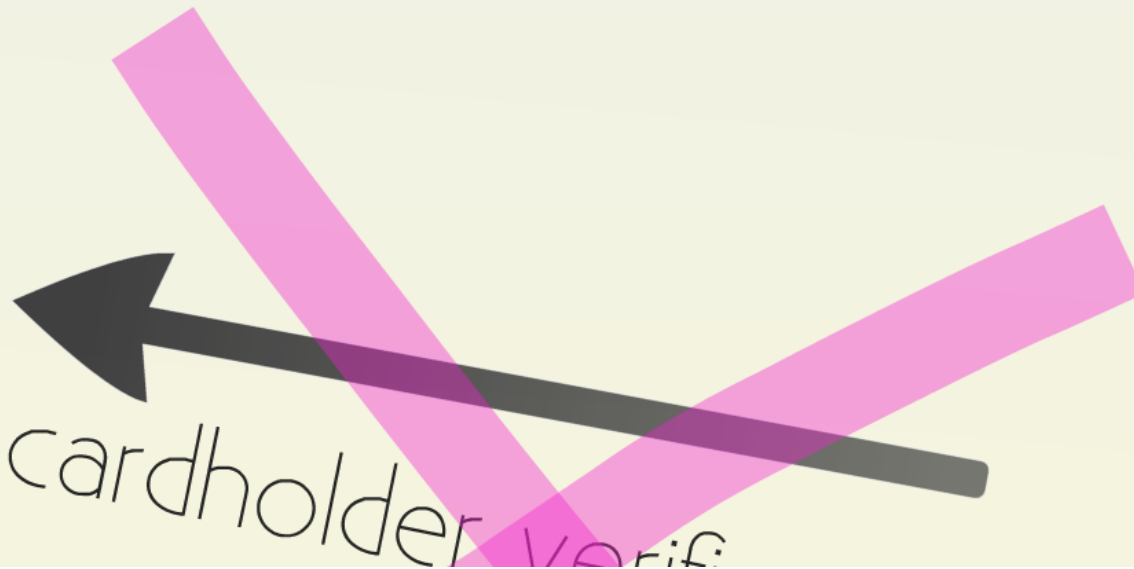
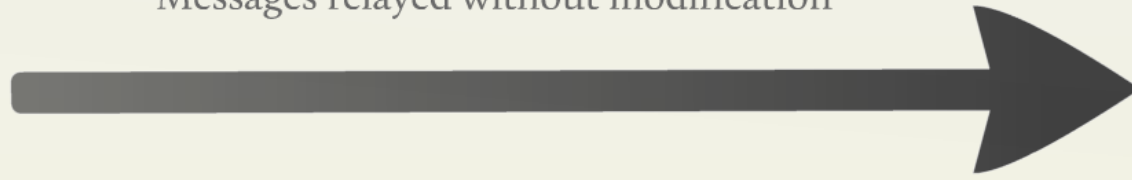


transaction authorization
Messages relayed without modification

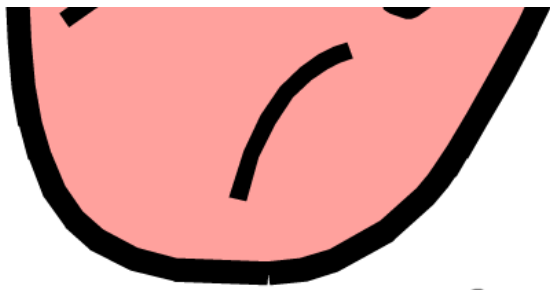


card authentication

Messages relayed without modification



cardholder verif:



criminal enters 0000



Card to Terminal: card details

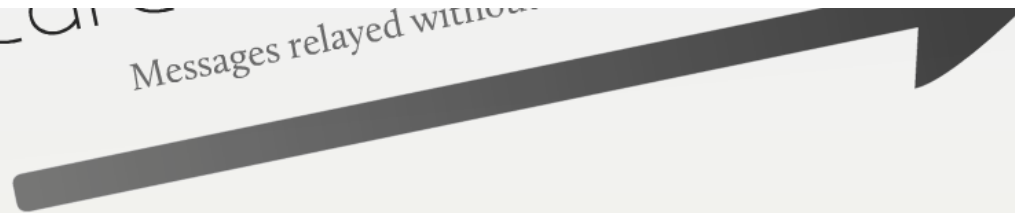
Terminal to MitM: **0000** entered by criminal

cardholder verification

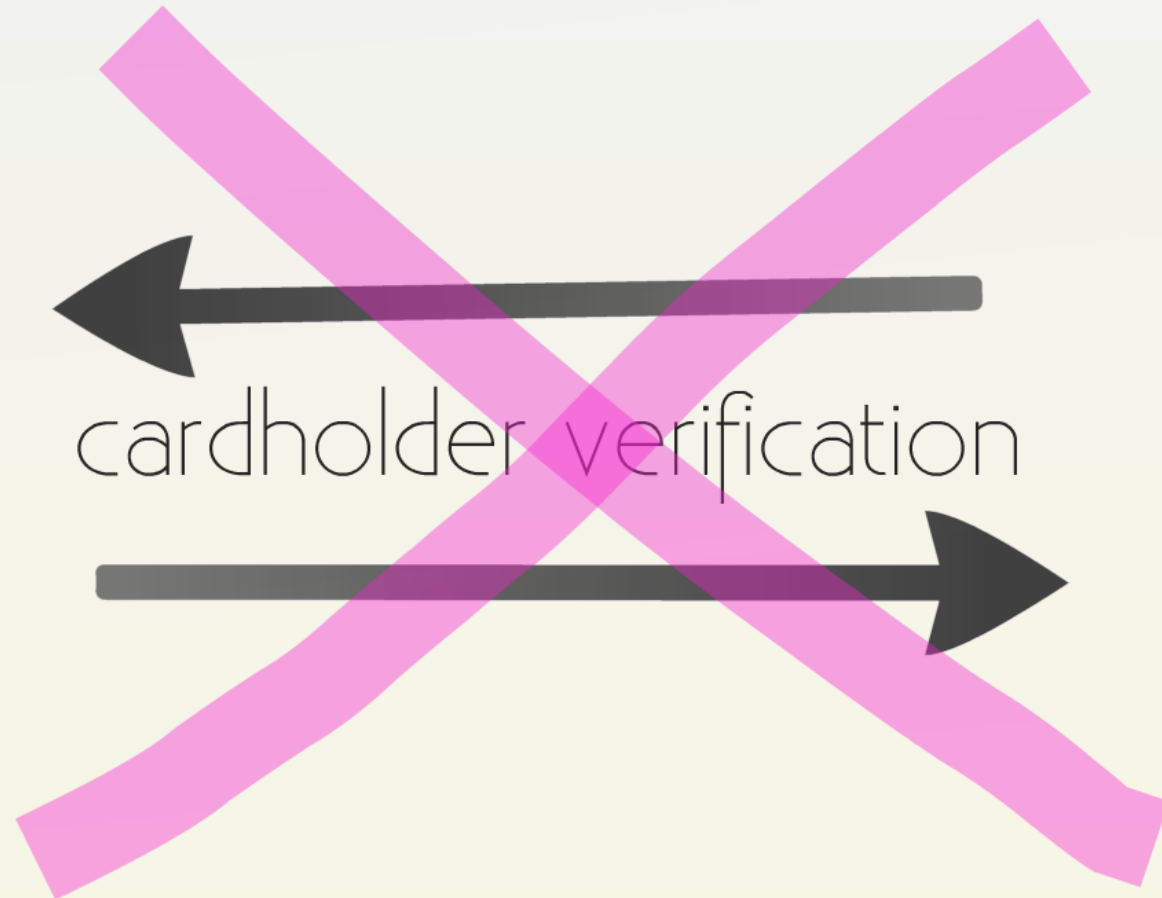
MitM to Terminal: PIN correct **yes!**

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

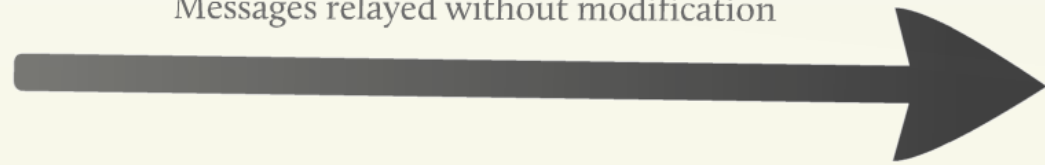


verification



transaction authorization

Messages relayed without modification



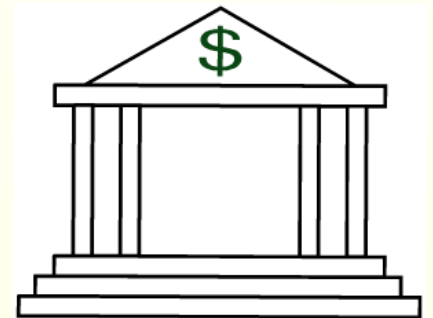
and other details



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)



ACCOUNTS

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?

ACCOUNTS

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)

Stev

wo

Mike

Online banking

- Majority of UK losses are card-not-present
- Online banking fraud is rising
- Existing 2-Factor authentication technologies are fundamentally flawed

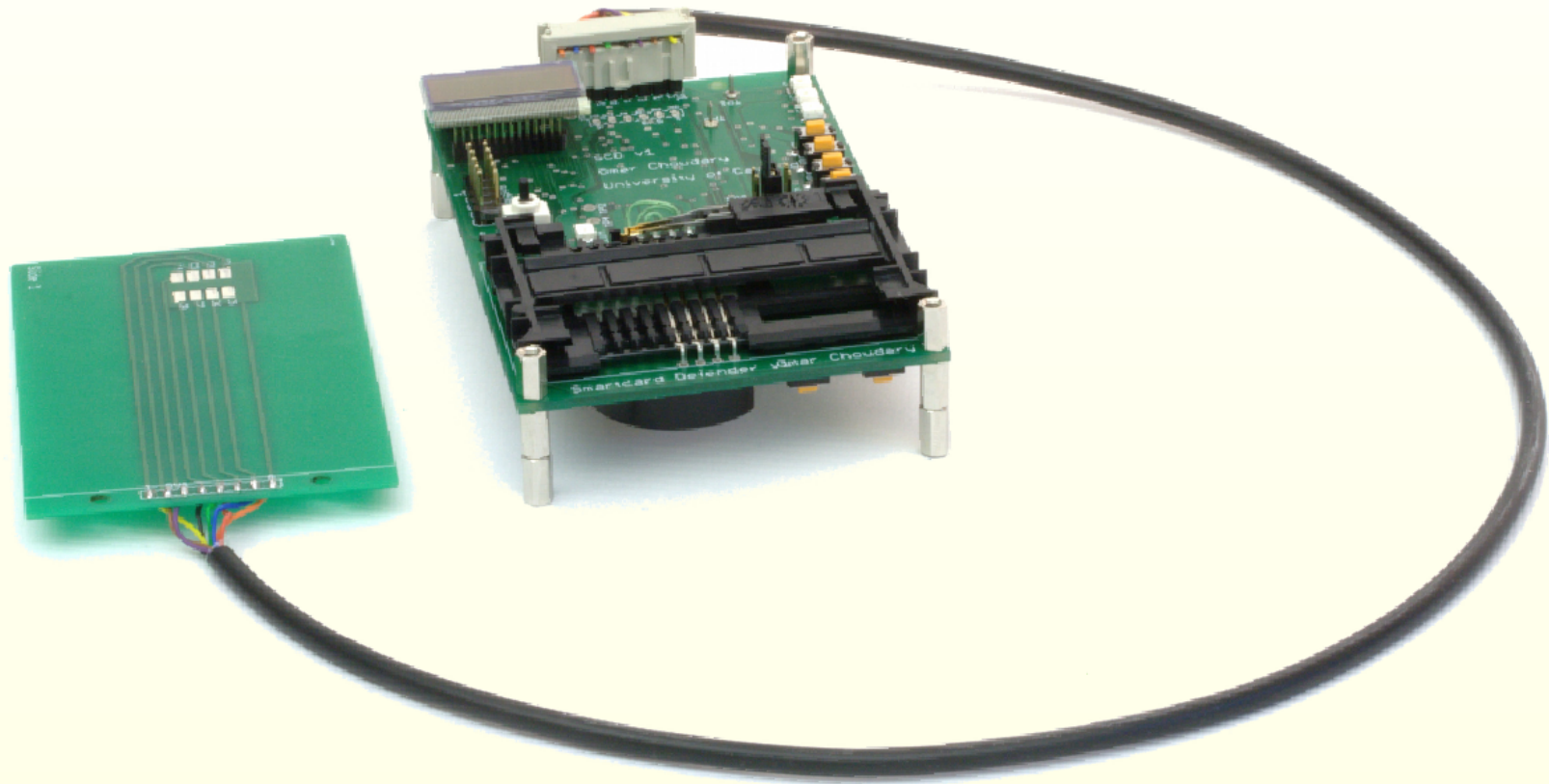
What Next?

Fixing the problem

- Techniques to fix the flaw are known
- Requires upgrading authorization system at issuing bank
- Does not require changing cards

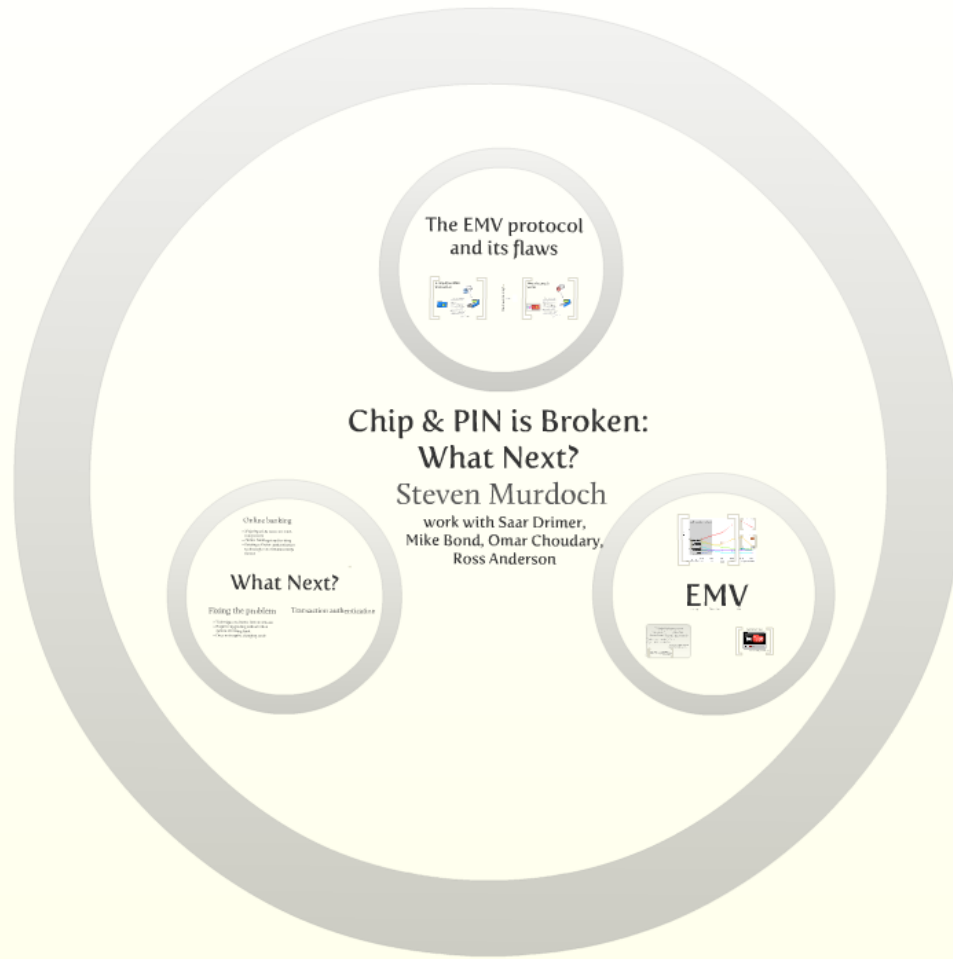
Transaction authentication

WRONG



Many o
card ha

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

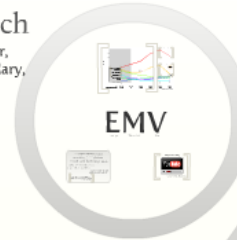


www.lightbluetouchpaper.org

Chip & PIN is Broken: What Next?

Steven Murdoch

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



www.lightbluetouchpaper.org