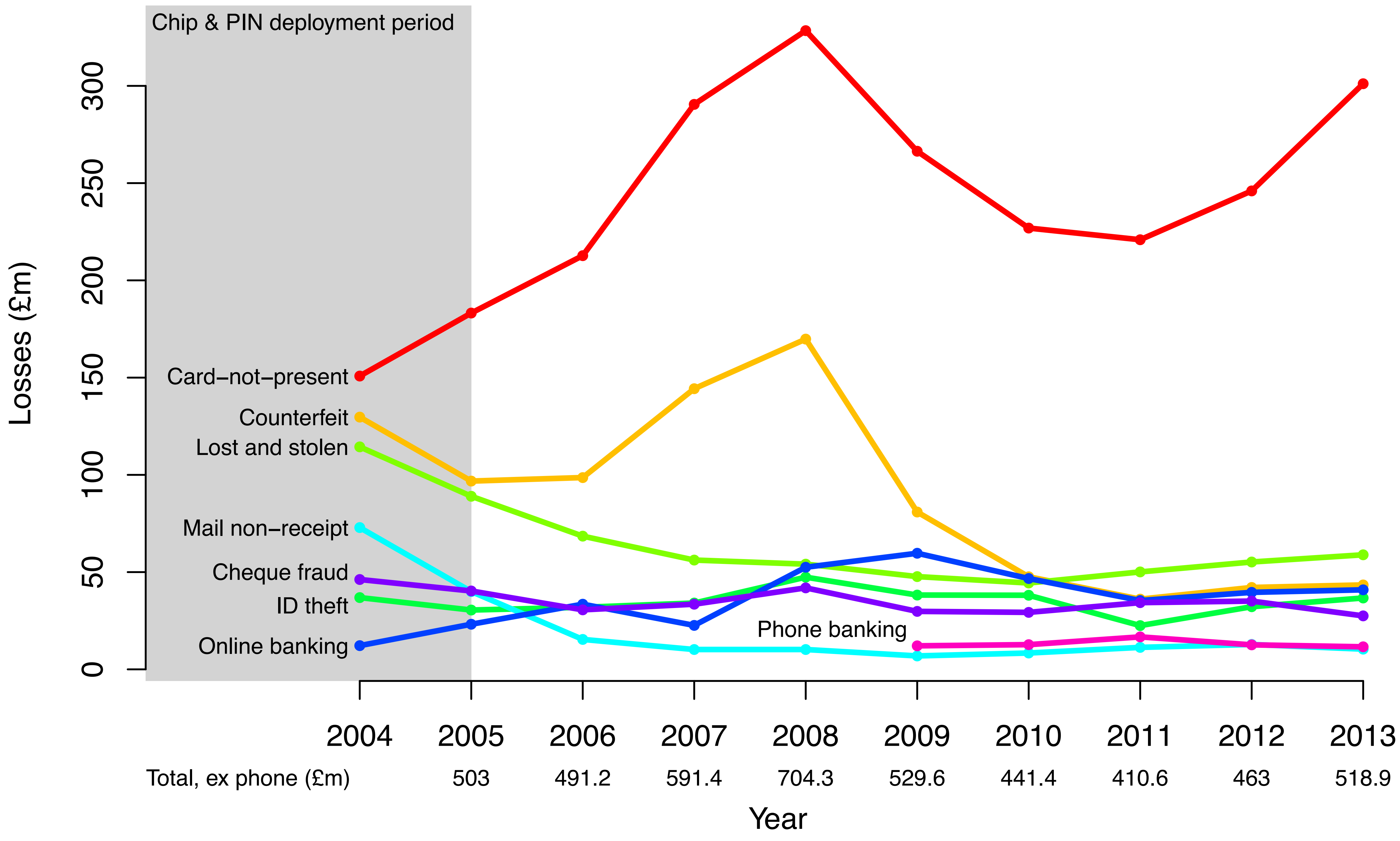
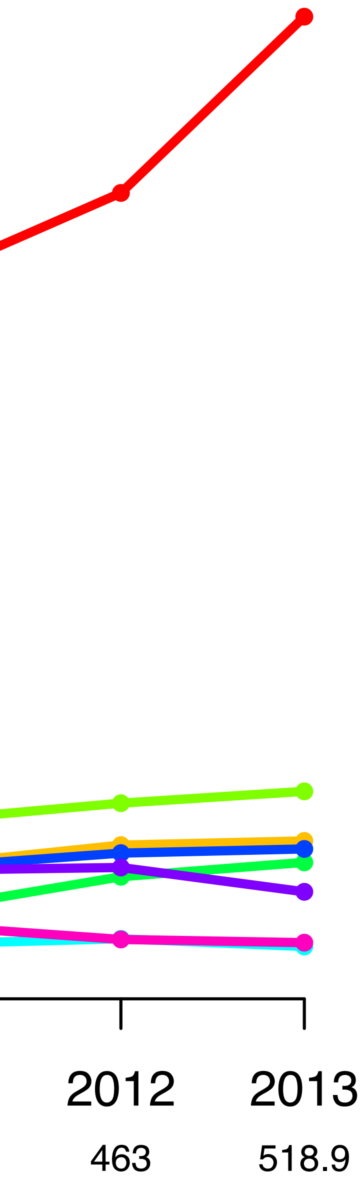
# Payment Security: Attacks & Defences

Dr Steven J Murdoch
University College London

# UK fraud is going up again



# …even types of fraud Chip and PIN was supposed to prevent



Card-not-present: up 22% to £301m

**Lost and stolen: up 7% to £58.9m**

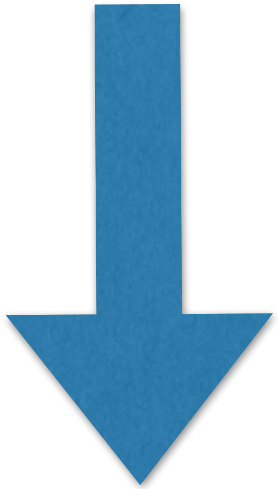
**Counterfeit: up 3% to £43.4m**

# …even types of fraud Chip and PIN was supposed to prevent

Card-not-present: up 22% to £301m

**Lost and stolen: up 7% to £58.9m**

**Counterfeit: up 3% to £43.4m**



*within total fraud figures*

**UK retail face-to-face: up 11% to £60.8m**

**UK cash machine: up 10% to £31.9m**

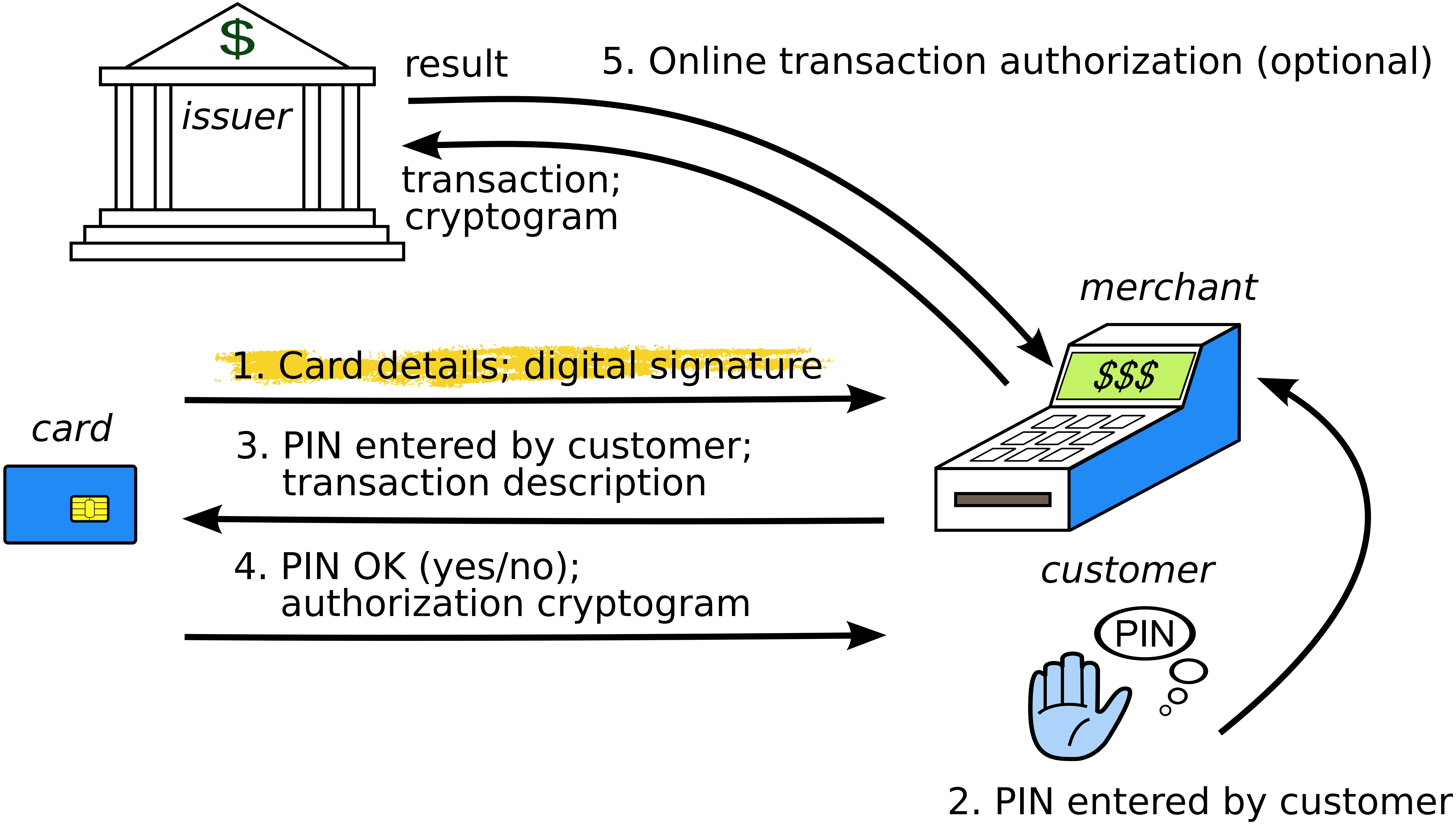
# Chip and PIN transactions have three main stages

- **Card authentication**: card proves it is real through providing a digital signature that the terminal can verify

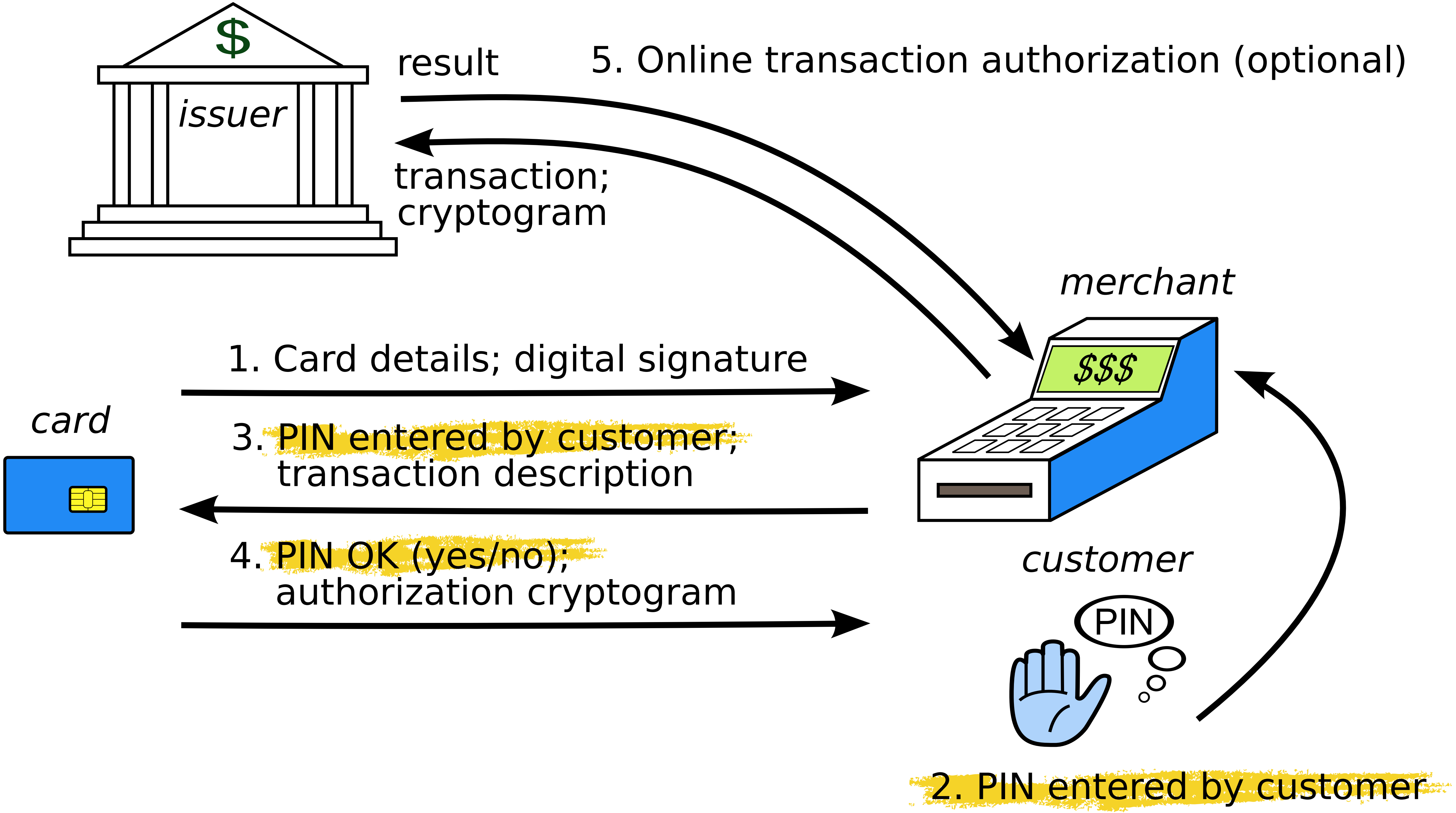
- **Cardholder verification**: card and terminal check that legitimate cardholder is present (normally by card verifying the PIN)

- **Transaction authorisation**: terminal checks with bank that previous steps have been followed and the transaction should proceed

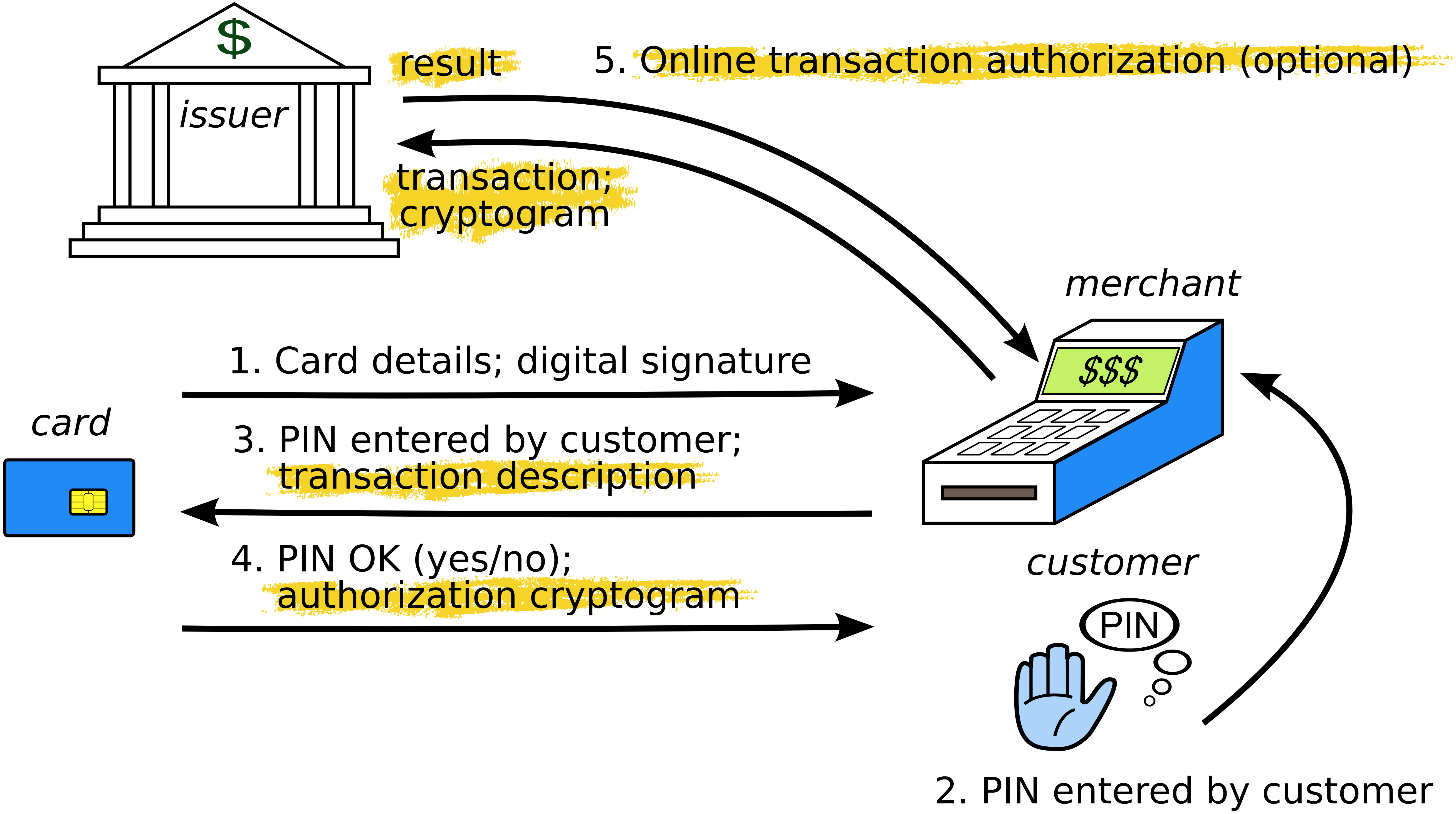
# Card authentication


issuer
$
result
5. Online transaction authorization (optional)
transaction; cryptogram
merchant
$$$
1. Card details; digital signature
card
3. PIN entered by customer; transaction description
4. PIN OK (yes/no); authorization cryptogram
customer
PIN
2. PIN entered by customer

# Cardholder verification


$
issuer
result
5. Online transaction authorization (optional)
transaction;
cryptogram
merchant
$$$
1. Card details; digital signature
card
3. PIN entered by customer;
transaction description
4. PIN OK (yes/no);
authorization cryptogram
customer
PIN
2. PIN entered by customer

# Transaction authorisation



5. Online transaction authorization (optional)

1. Card details; digital signature

3. PIN entered by customer;
transaction description

4. PIN OK (yes/no);
authorization cryptogram

2. PIN entered by customer

# Criminals have successfully bypassed Chip & PIN

Obtain static data as a result of flawed tamper resistance in Chip & PIN terminals

*then*

**Bypass card authentication** through exploiting backwards compatibility mode

Counterfeit

Steal cards

*then*

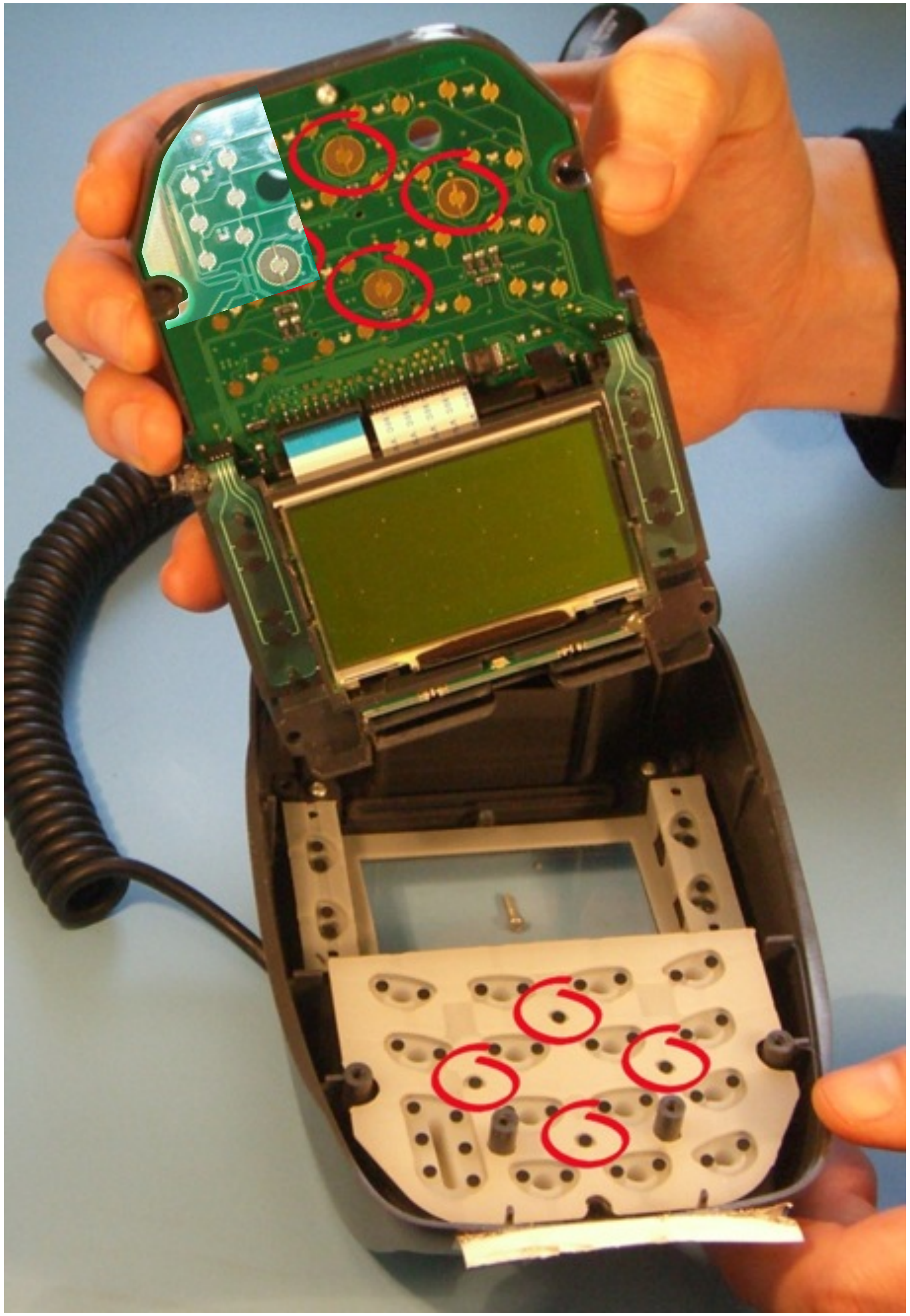
**Bypass cardholder verification** by exploiting Chip and PIN protocol flaws

Lost and Stolen

# Sensitive data is sent unencrypted between the card and the terminal

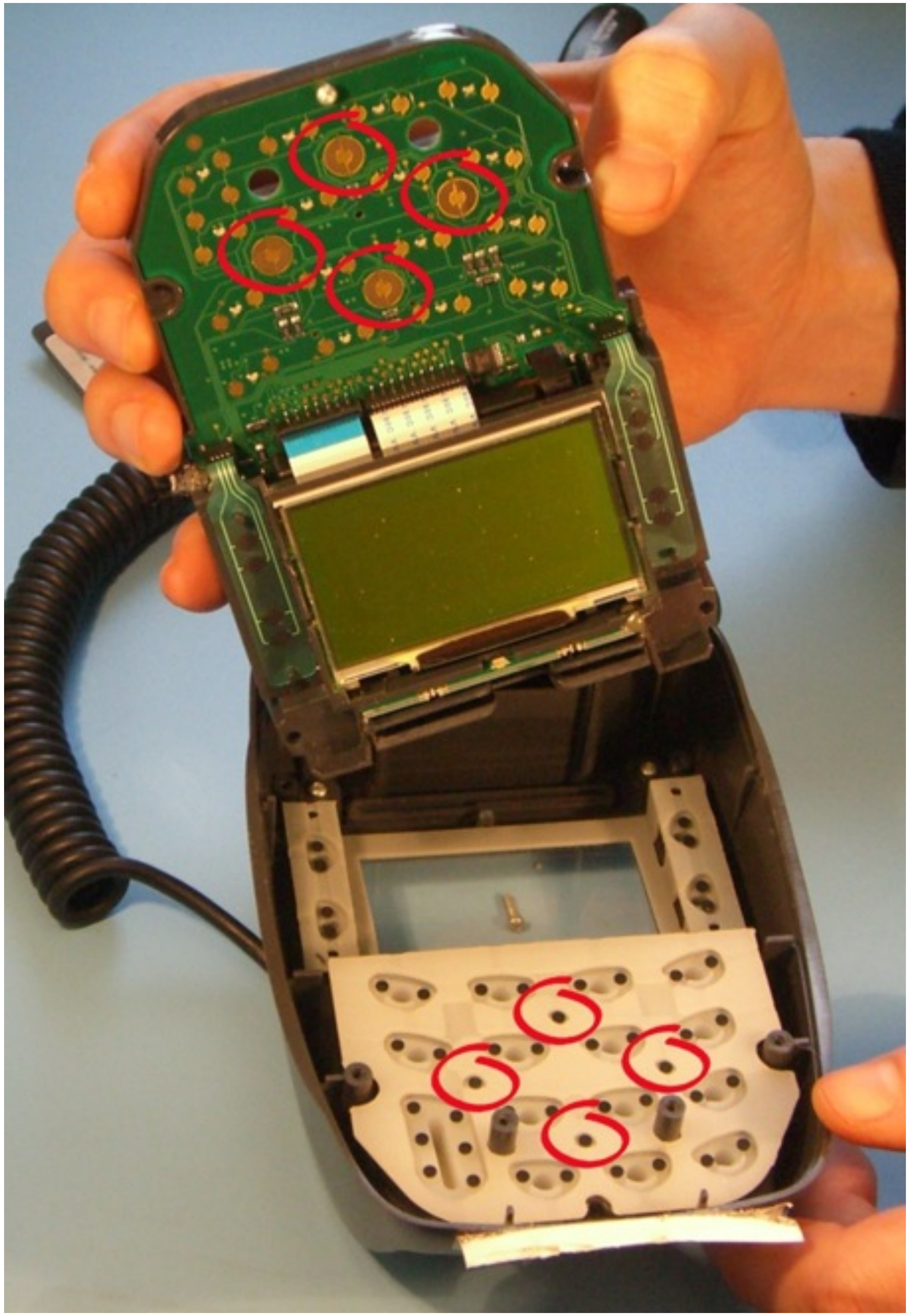
- Card number, expiry date, cardholder name …
- Copy of magnetic stripe including CVV (for some cards)
- PIN to be checked by card

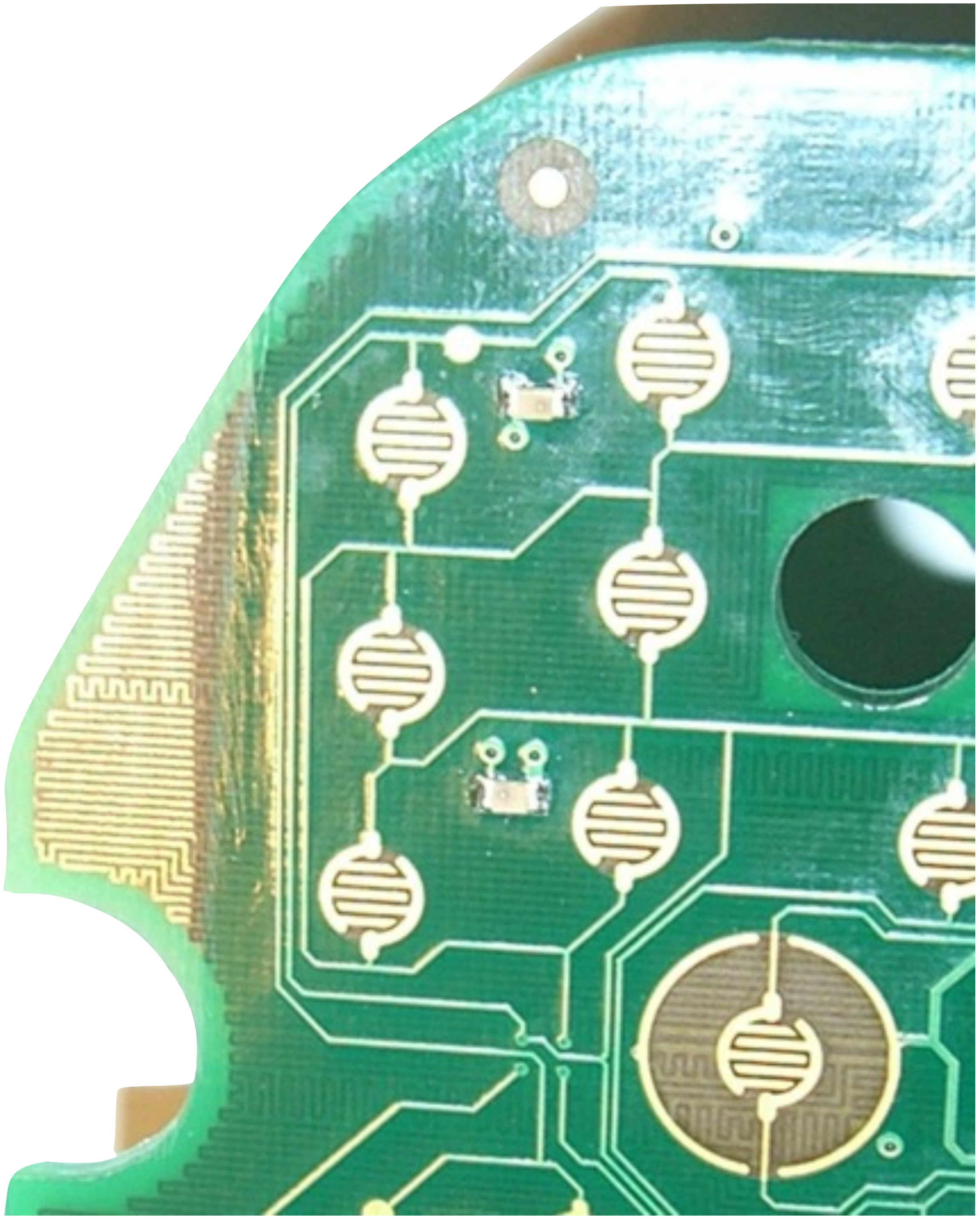
Chip and PIN terminals are supposed to protect this information against being recorded: **tamper resistance**

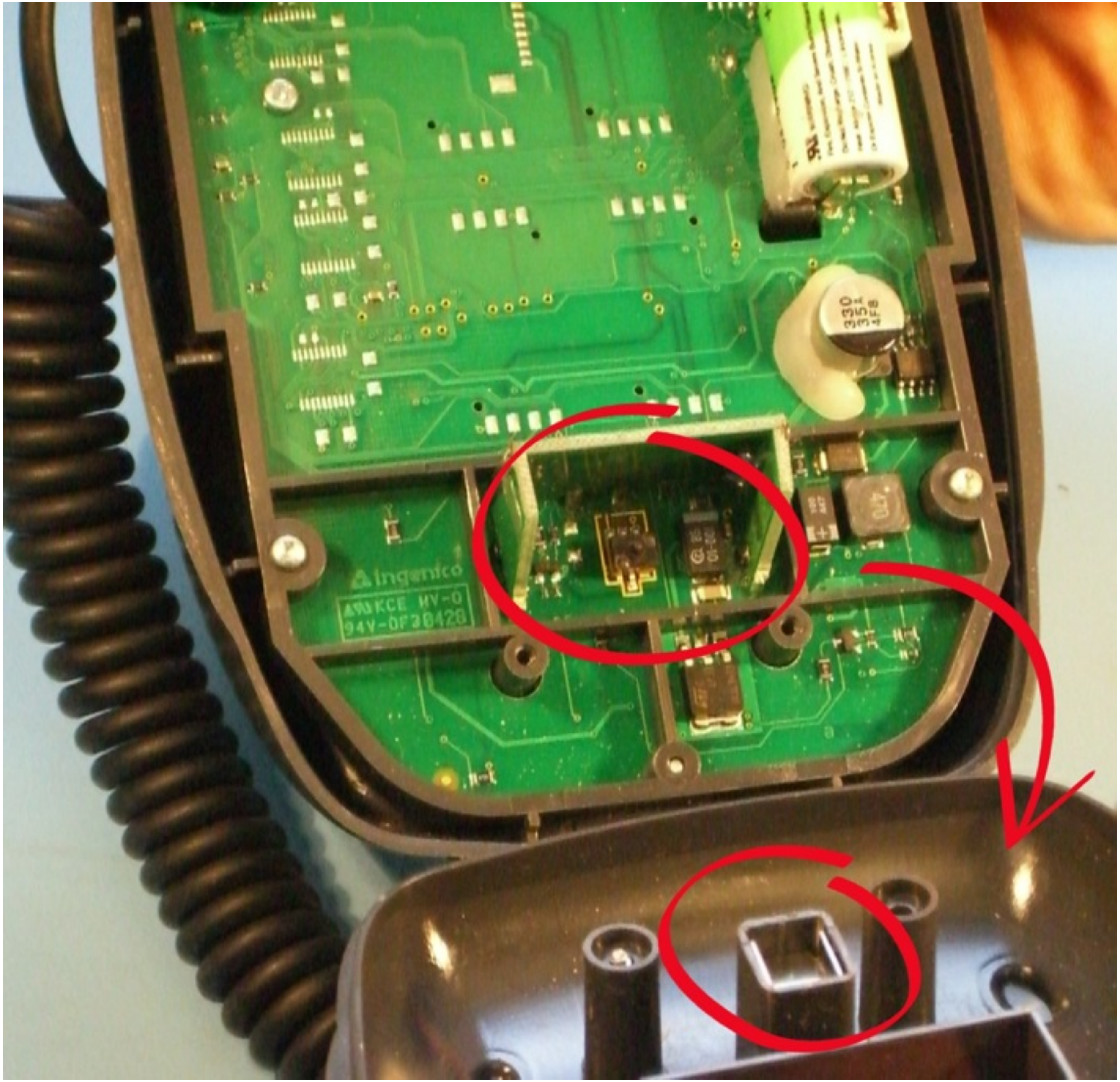


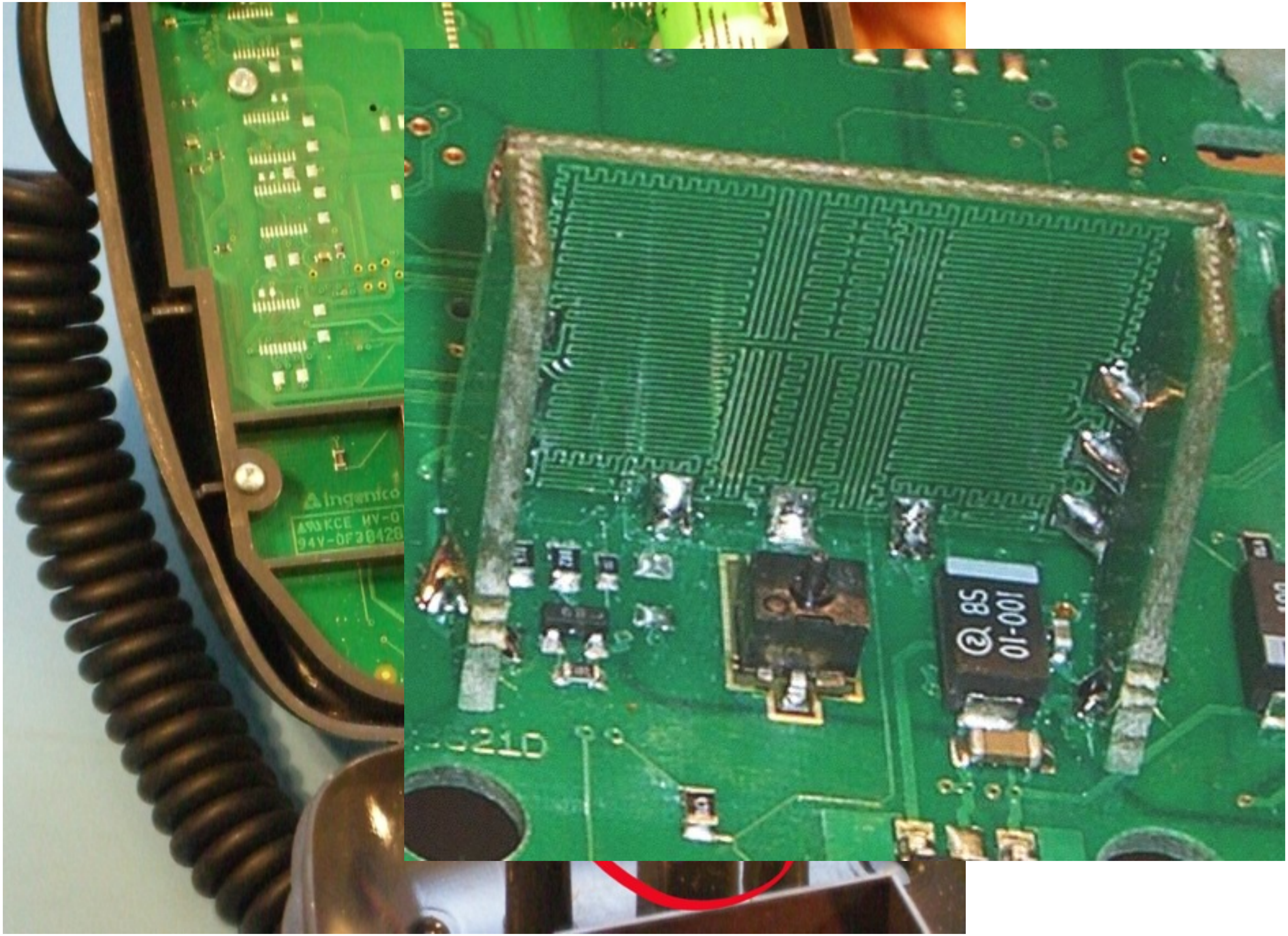
# Tamper switches

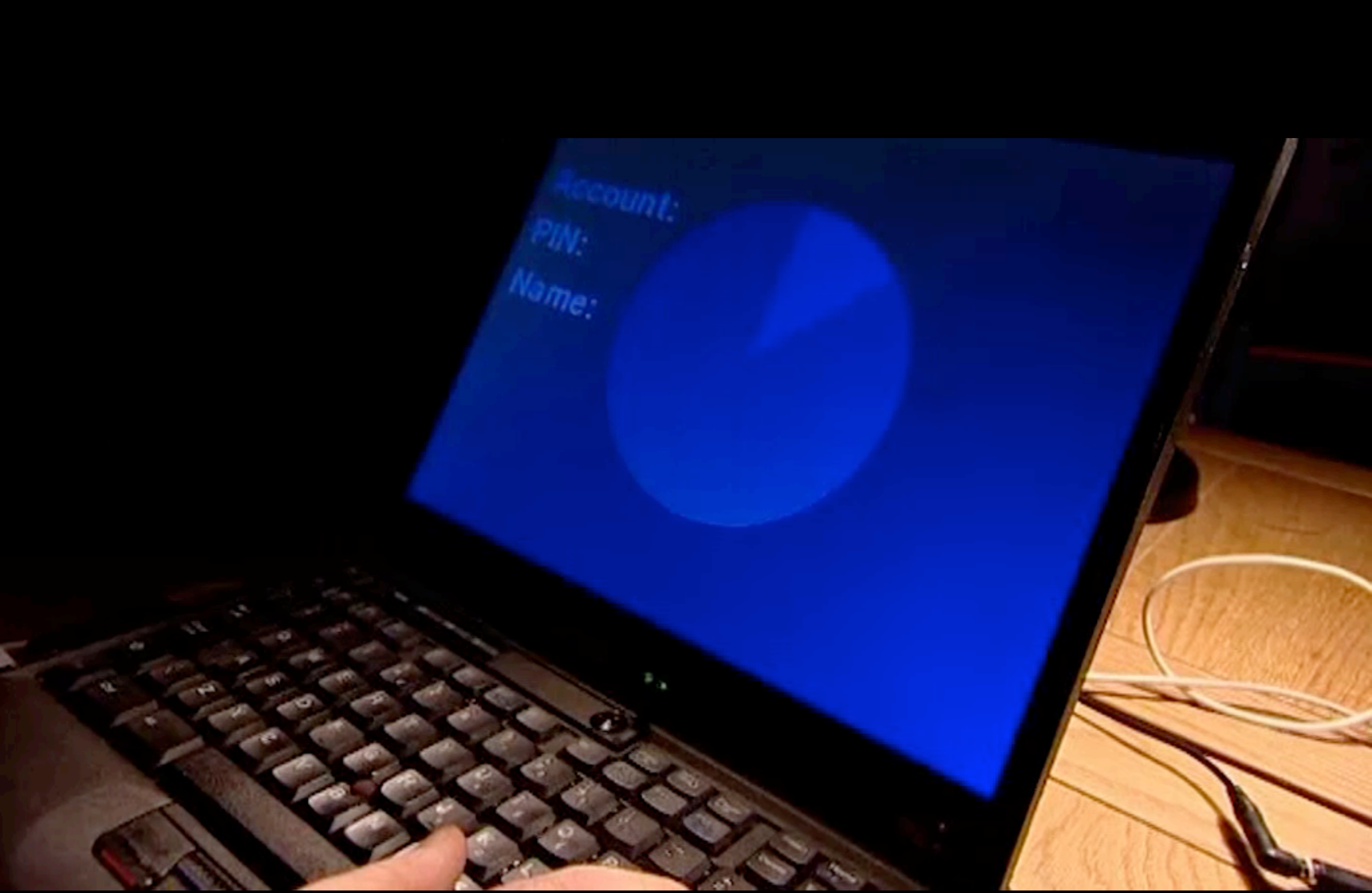
# Tamper mesh

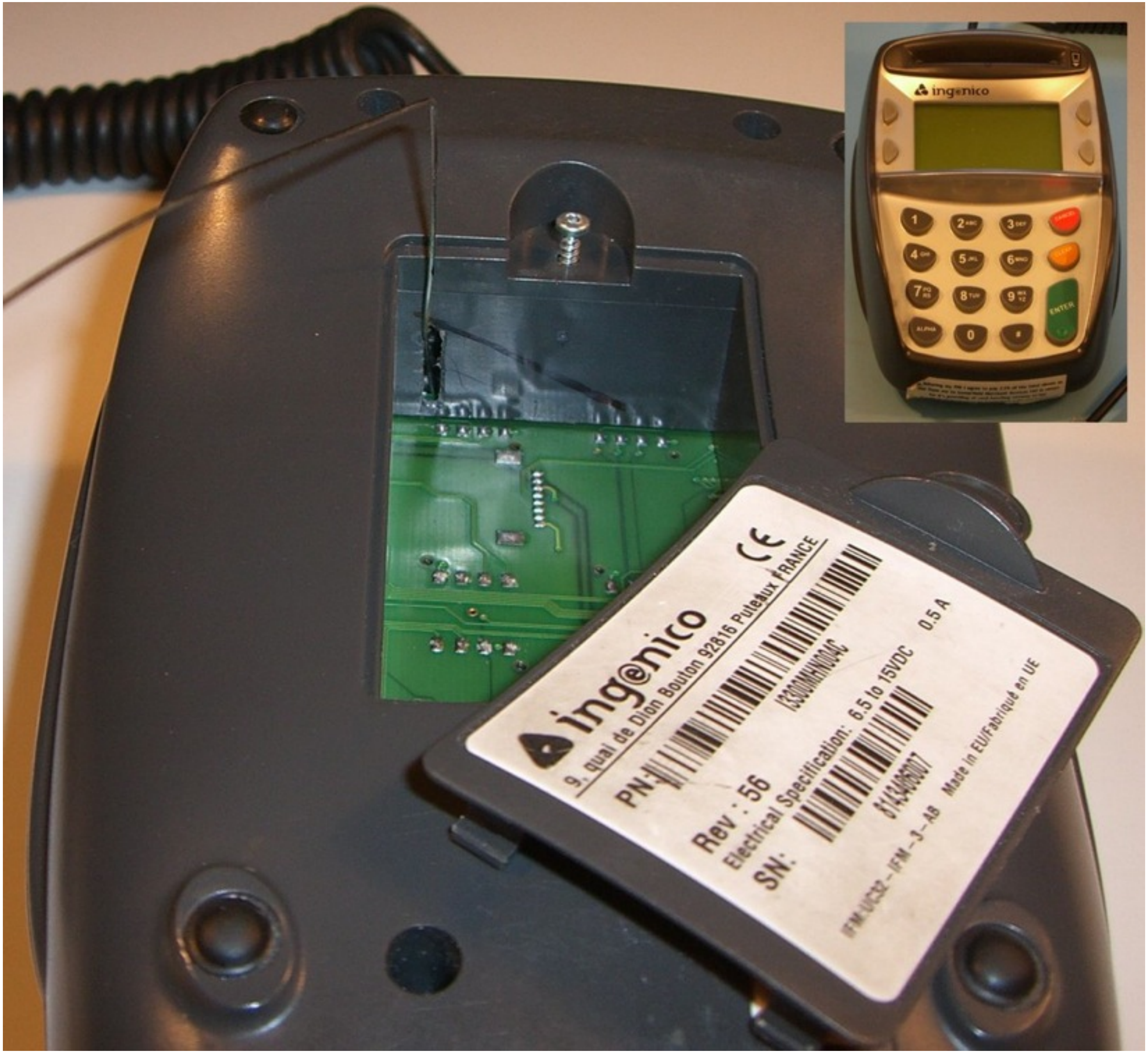





ingenico
KCE MV-0
94V-0F20428


Ingenico
KCE HV-0
94V-0F2B428
C210D
85
100-10


Account:
PIN:
Name:


ingenico
ingenico
9, quai de Dion Bouton 92816 Puteaux FRANCE
PN:
Rev : 56
Electrical Specification: 6.5 to 15VDC 0.5 A
SN:
I3300MHN00AC
01434086007
Made in EU/Fabriqué en UE
IFM-UC32-IFM-3-AB
1
2 ABC
3 DEF
CANCEL
4 GHI
5 JKL
6 MNO
CLEAR
7 PQRS
8 TUV
9 WXYZ
ENTER
ALPHA
0
#

# Criminal gets all that is needed to make a magnetic stripe card

- Card number, expiry date
- CVV
- Cardholder's PIN

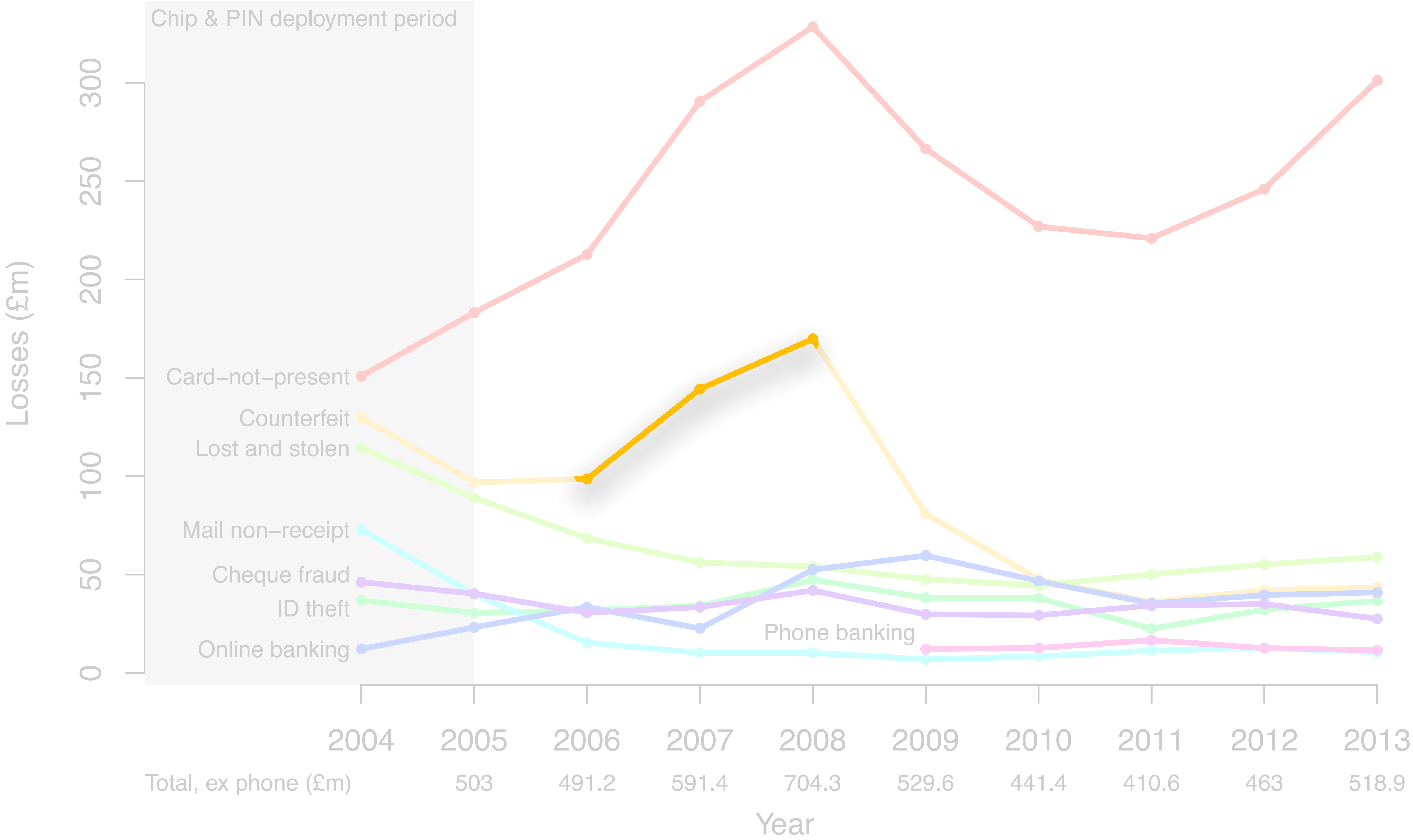
Compromising a shop terminal now gives criminals enough information to make ATM withdrawal

# Criminal gets all that is needed to make a magnetic stripe card

- Card number, expiry date
- CVV
- Cardholder's PIN

CASH

# Chip and PIN led to increase in counterfeit fraud



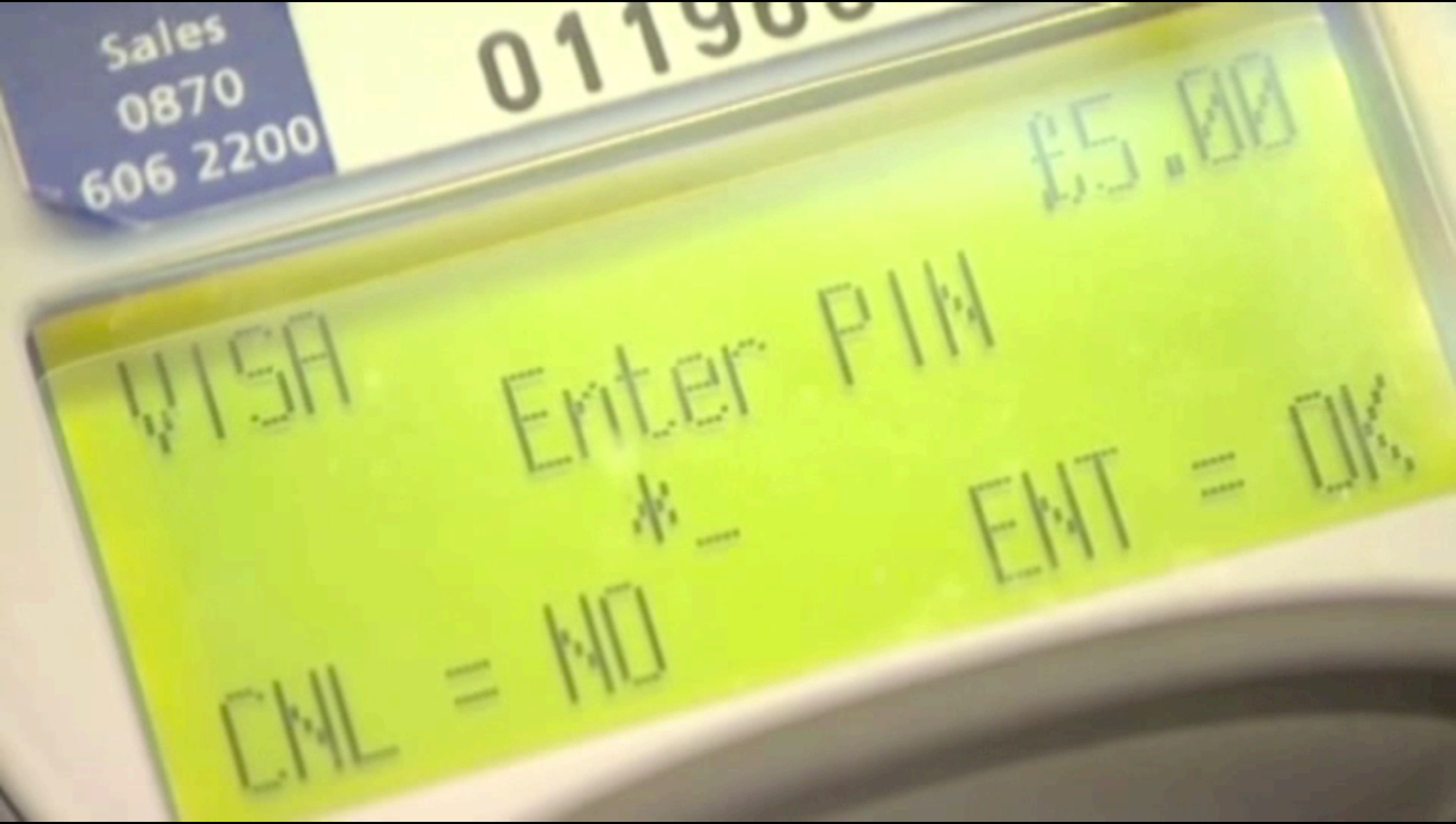
# Card is responsible for cardholder verification

- Card states ways by which cardholder verification can be performed and the preference (e.g. first PIN, then signature)

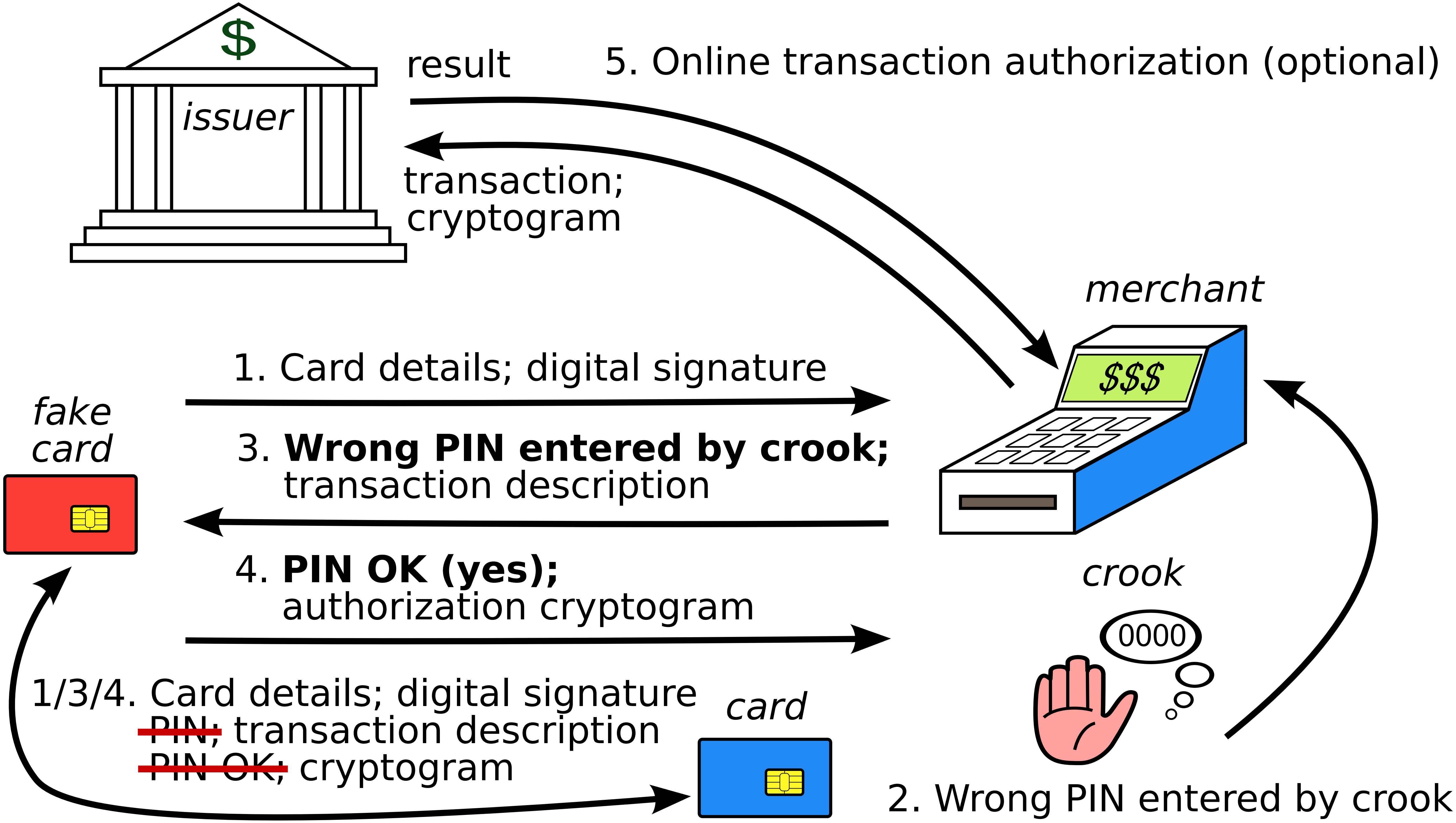
- If PIN used, terminal sends PIN to card and card checks if correct

- PIN sometimes encrypted

- Response **not encrypted or authenticated**


Sales
0870
606 2200
01198
£5.00
VISA Enter PIN
*_
ENT = OK
CNL = NO

# The no-PIN attack



result

5. Online transaction authorization (optional)

transaction;
cryptogram

1. Card details; digital signature

3. **Wrong PIN entered by crook;**
transaction description

4. **PIN OK (yes);**
authorization cryptogram

1/3/4. Card details; digital signature
~~PIN;~~ transaction description
~~PIN OK;~~ cryptogram

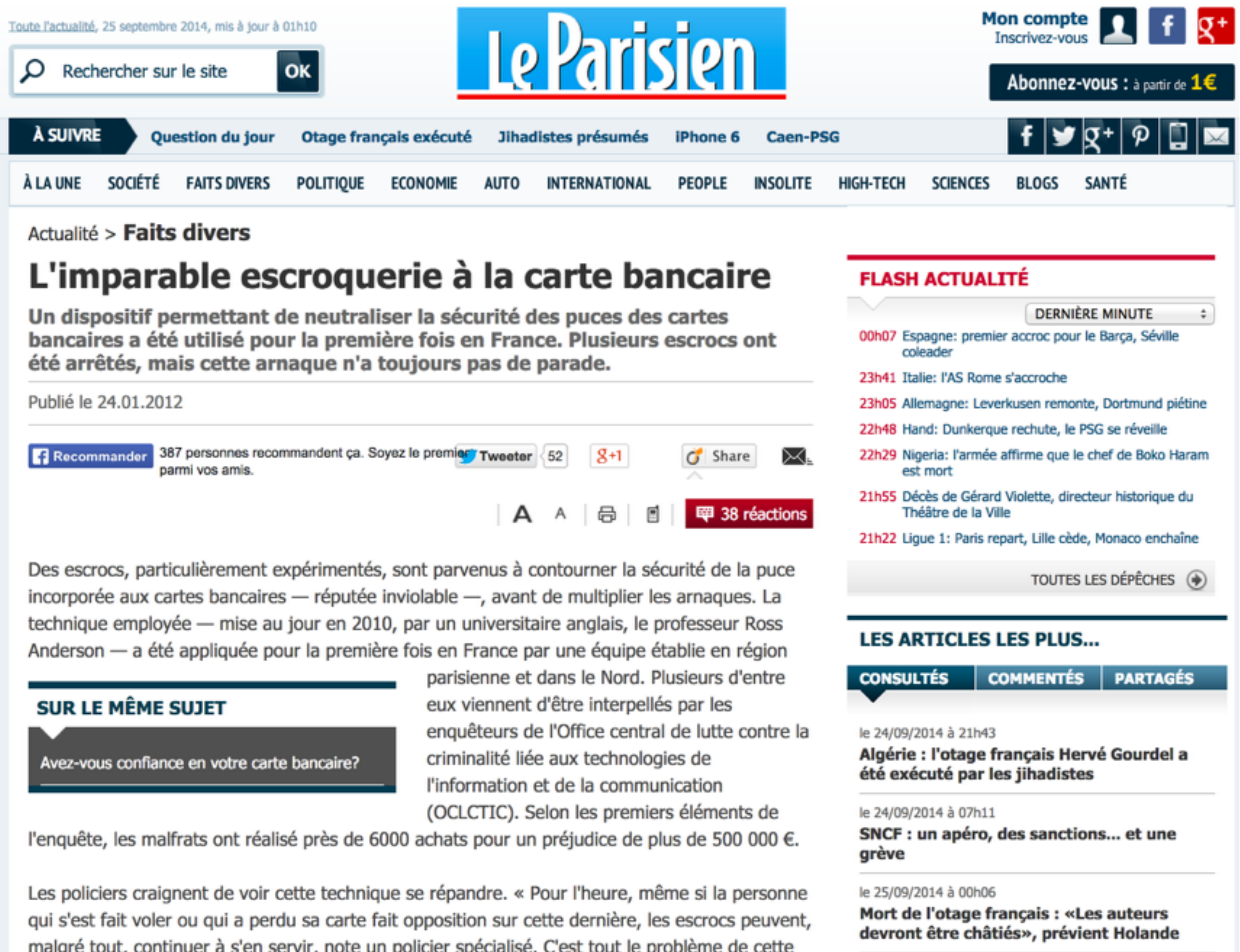
2. Wrong PIN entered by crook

# Response from industry

> “What is more, at this stage, the observations are the result of scientific research whose transposition outside laboratory conditions is complex since it would necessitate the use of highly sophisticated material.
>
> — Le GIE des Cartes Bancaires (January 2010)

> “Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks.
>
> — UK Cards Association (February 2010))

# Response from criminals



## L'imparable escroquerie à la carte bancaire

**Un dispositif permettant de neutraliser la sécurité des puces des cartes bancaires a été utilisé pour la première fois en France. Plusieurs escrocs ont été arrêtés, mais cette arnaque n'a toujours pas de parade.**

Publié le 24.01.2012

Des escrocs, particulièrement expérimentés, sont parvenus à contourner la sécurité de la puce incorporée aux cartes bancaires — réputée inviolable —, avant de multiplier les arnaques. La technique employée — mise au jour en 2010, par un universitaire anglais, le professeur Ross Anderson — a été appliquée pour la première fois en France par une équipe établie en région parisienne et dans le Nord. Plusieurs d'entre eux viennent d'être interpellés par les enquêteurs de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Selon les premiers éléments de l'enquête, les malfrats ont réalisé près de 6000 achats pour un préjudice de plus de 500 000 €.

**SUR LE MÊME SUJET**

Avez-vous confiance en votre carte bancaire?

Les policiers craignent de voir cette technique se répandre. « Pour l'heure, même si la personne qui s'est fait voler ou qui a perdu sa carte fait opposition sur cette dernière, les escrocs peuvent, malgré tout, continuer à s'en servir, note un policier spécialisé. C'est tout le problème de cette

**FLASH ACTUALITÉ**

DERNIÈRE MINUTE

00h07 Espagne: premier accroc pour le Barça, Séville coleader

23h41 Italie: l'AS Rome s'accroche

23h05 Allemagne: Leverkusen remonte, Dortmund piétine

22h48 Hand: Dunkerque rechute, le PSG se réveille

22h29 Nigeria: l'armée affirme que le chef de Boko Haram est mort

21h55 Décès de Gérard Violette, directeur historique du Théâtre de la Ville

21h22 Ligue 1: Paris repart, Lille cède, Monaco enchaîne

TOUTES LES DÉPÊCHES

**LES ARTICLES LES PLUS...**

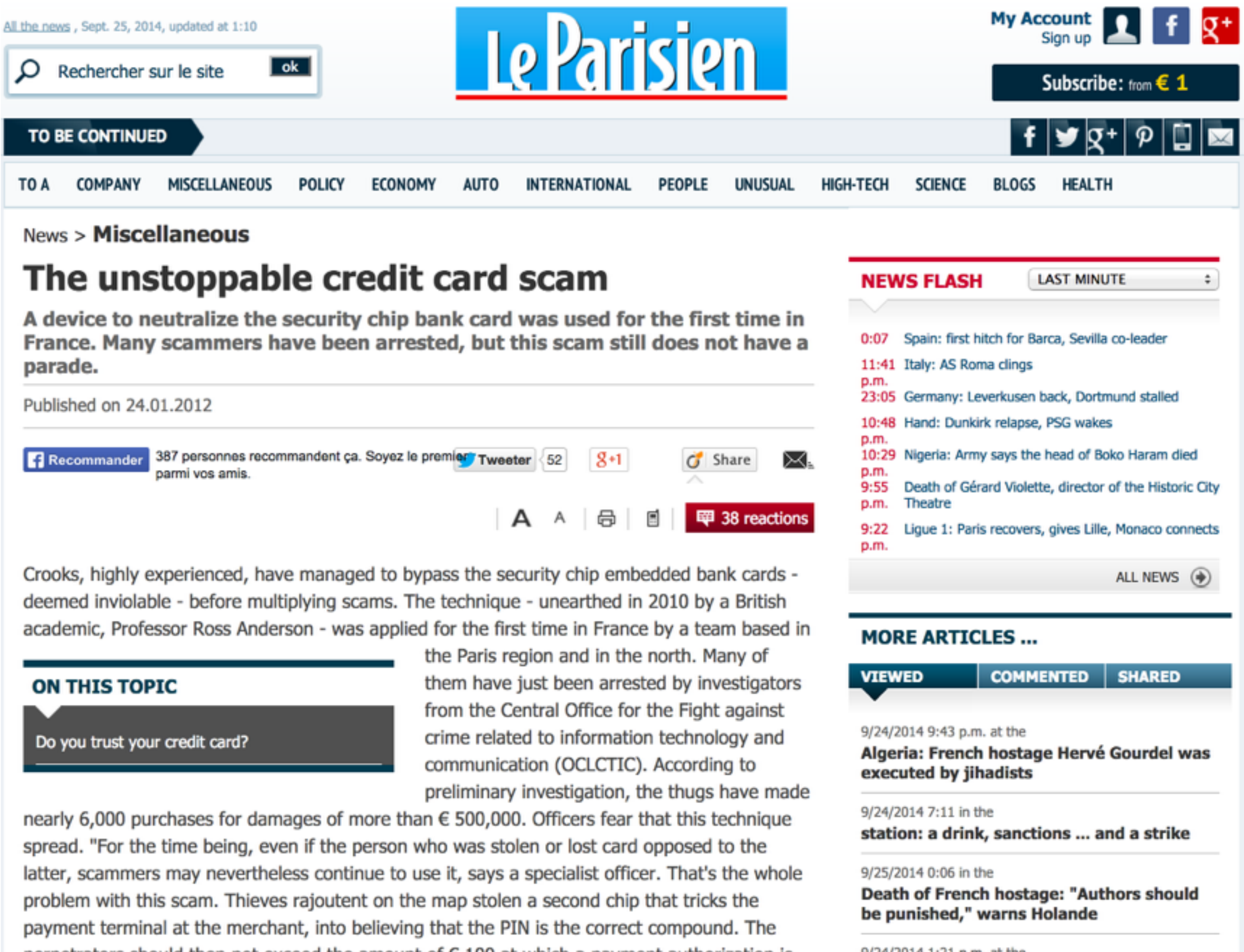
CONSULTÉS | COMMENTÉS | PARTAGÉS

le 24/09/2014 à 21h43
**Algérie : l'otage français Hervé Gourdel a été exécuté par les jihadistes**

le 24/09/2014 à 07h11
**SNCF : un apéro, des sanctions... et une grève**

le 25/09/2014 à 00h06
**Mort de l'otage français : «Les auteurs devront être châtiés», prévient Holande**

# Response from criminals



News > **Miscellaneous**

## The unstoppable credit card scam

**A device to neutralize the security chip bank card was used for the first time in France. Many scammers have been arrested, but this scam still does not have a parade.**

Published on 24.01.2012

Recommander
387 personnes recommandent ça. Soyez le premier parmi vos amis.
Tweeter
52
+1
Share
A
A
38 reactions

Crooks, highly experienced, have managed to bypass the security chip embedded bank cards - deemed inviolable - before multiplying scams. The technique - unearthed in 2010 by a British academic, Professor Ross Anderson - was applied for the first time in France by a team based in the Paris region and in the north. Many of them have just been arrested by investigators from the Central Office for the Fight against crime related to information technology and communication (OCLCTIC). According to preliminary investigation, the thugs have made nearly 6,000 purchases for damages of more than € 500,000. Officers fear that this technique spread. "For the time being, even if the person who was stolen or lost card opposed to the latter, scammers may nevertheless continue to use it, says a specialist officer. That's the whole problem with this scam. Thieves rajoutent on the map stolen a second chip that tricks the payment terminal at the merchant, into believing that the PIN is the correct compound. The perpetrators should then not exceed the amount of € 100 at which a payment authorization is

**ON THIS TOPIC**

Do you trust your credit card?

**NEWS FLASH** LAST MINUTE

| | |
|---|---|
| 0:07 | Spain: first hitch for Barca, Sevilla co-leader |
| 11:41 p.m. | Italy: AS Roma clings |
| 23:05 | Germany: Leverkusen back, Dortmund stalled |
| 10:48 p.m. | Hand: Dunkirk relapse, PSG wakes |
| 10:29 p.m. | Nigeria: Army says the head of Boko Haram died |
| 9:55 p.m. | Death of Gérard Violette, director of the Historic City Theatre |
| 9:22 p.m. | Ligue 1: Paris recovers, gives Lille, Monaco connects |

ALL NEWS

**MORE ARTICLES ...**

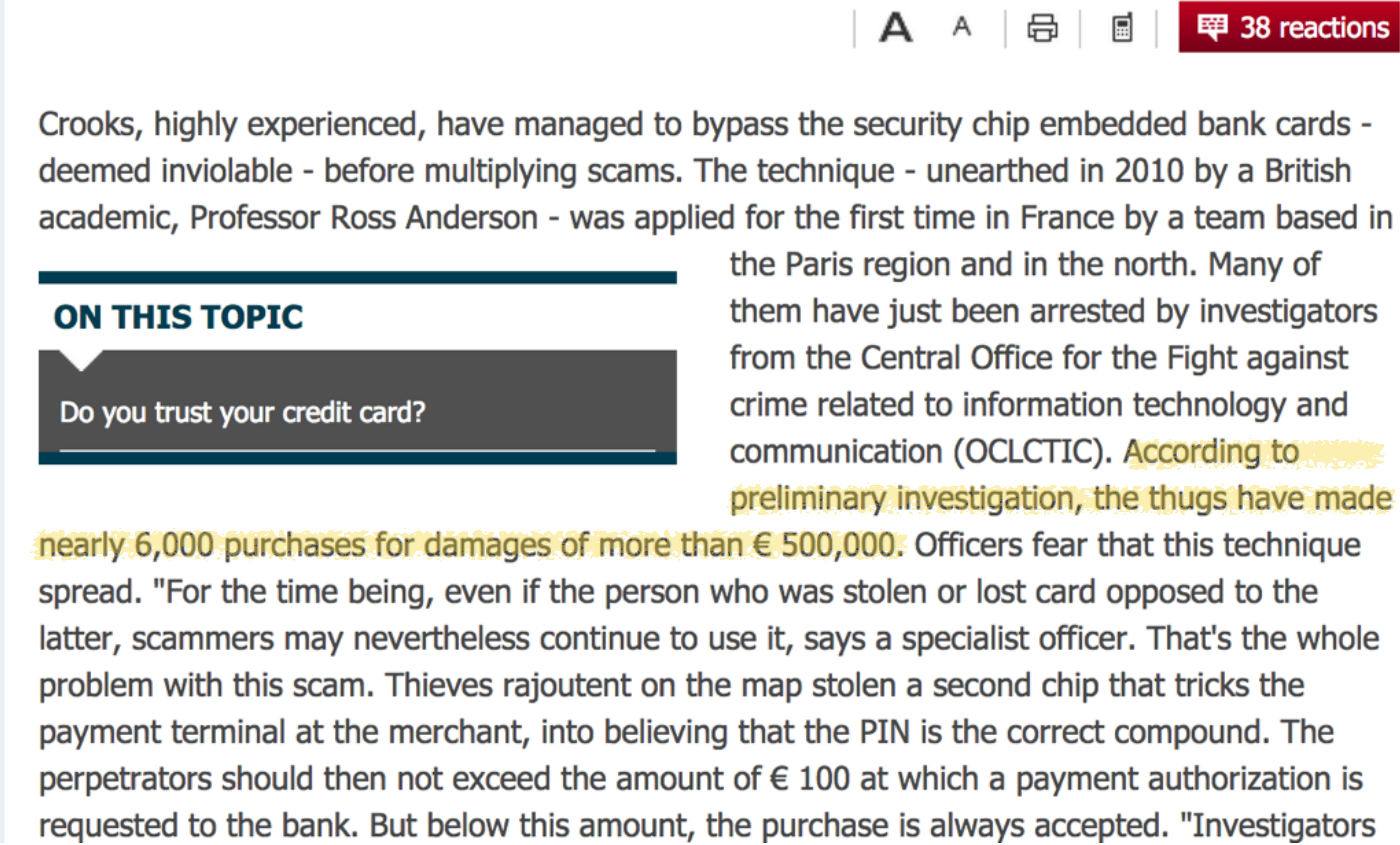
VIEWED | COMMENTED | SHARED

9/24/2014 9:43 p.m. at the
**Algeria: French hostage Hervé Gourdel was executed by jihadists**

9/24/2014 7:11 in the
**station: a drink, sanctions ... and a strike**

9/25/2014 0:06 in the
**Death of French hostage: "Authors should be punished," warns Holande**

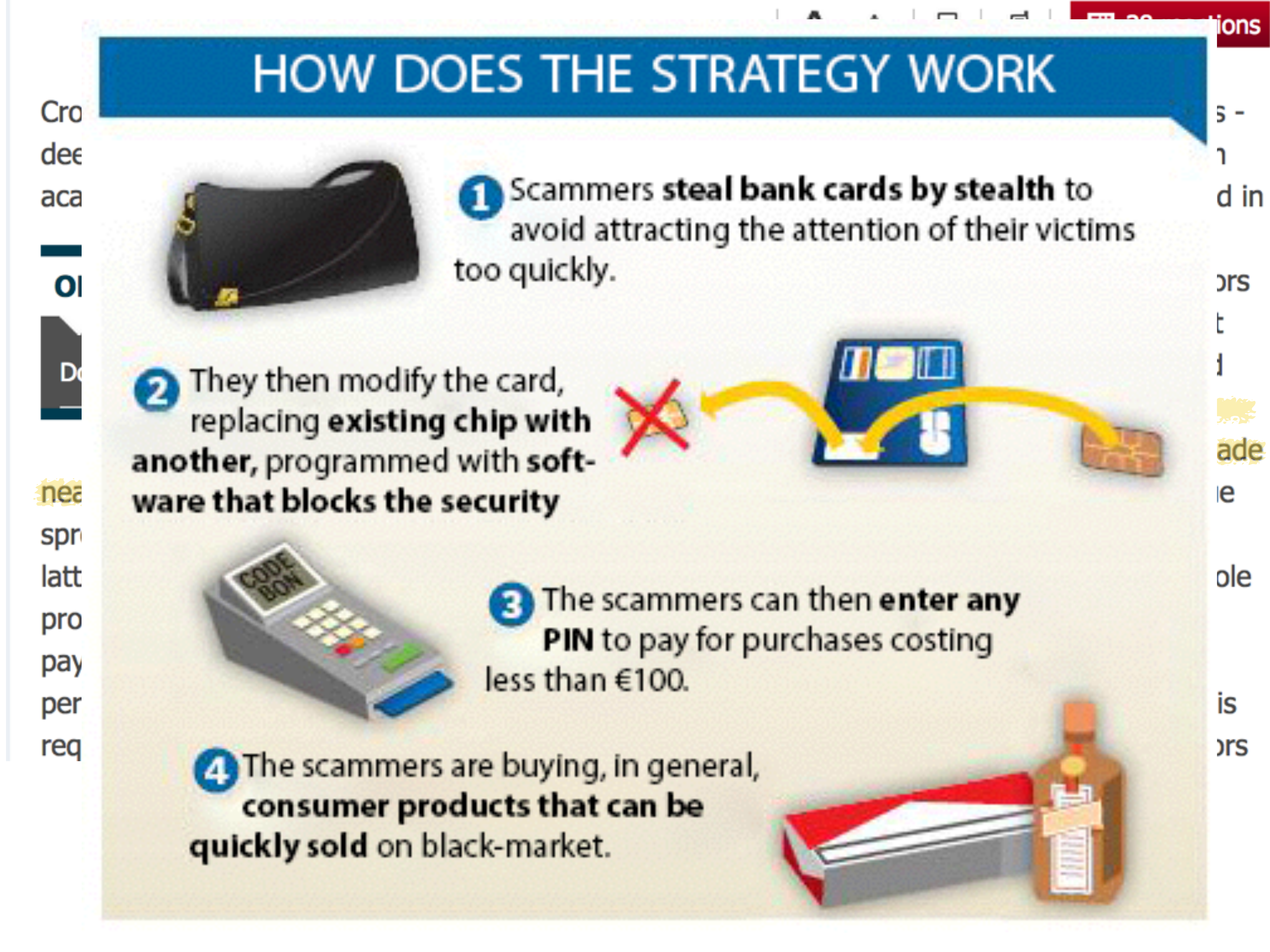
9/24/2014 1:21 p.m. at the



Crooks, highly experienced, have managed to bypass the security chip embedded bank cards - deemed inviolable - before multiplying scams. The technique - unearthed in 2010 by a British academic, Professor Ross Anderson - was applied for the first time in France by a team based in the Paris region and in the north. Many of them have just been arrested by investigators from the Central Office for the Fight against crime related to information technology and communication (OCLCTIC). According to preliminary investigation, the thugs have made nearly 6,000 purchases for damages of more than € 500,000. Officers fear that this technique spread. "For the time being, even if the person who was stolen or lost card opposed to the latter, scammers may nevertheless continue to use it, says a specialist officer. That's the whole problem with this scam. Thieves rajoutent on the map stolen a second chip that tricks the payment terminal at the merchant, into believing that the PIN is the correct compound. The perpetrators should then not exceed the amount of € 100 at which a payment authorization is requested to the bank. But below this amount, the purchase is always accepted. "Investigators

**ON THIS TOPIC**

Do you trust your credit card?



# HOW DOES THE STRATEGY WORK

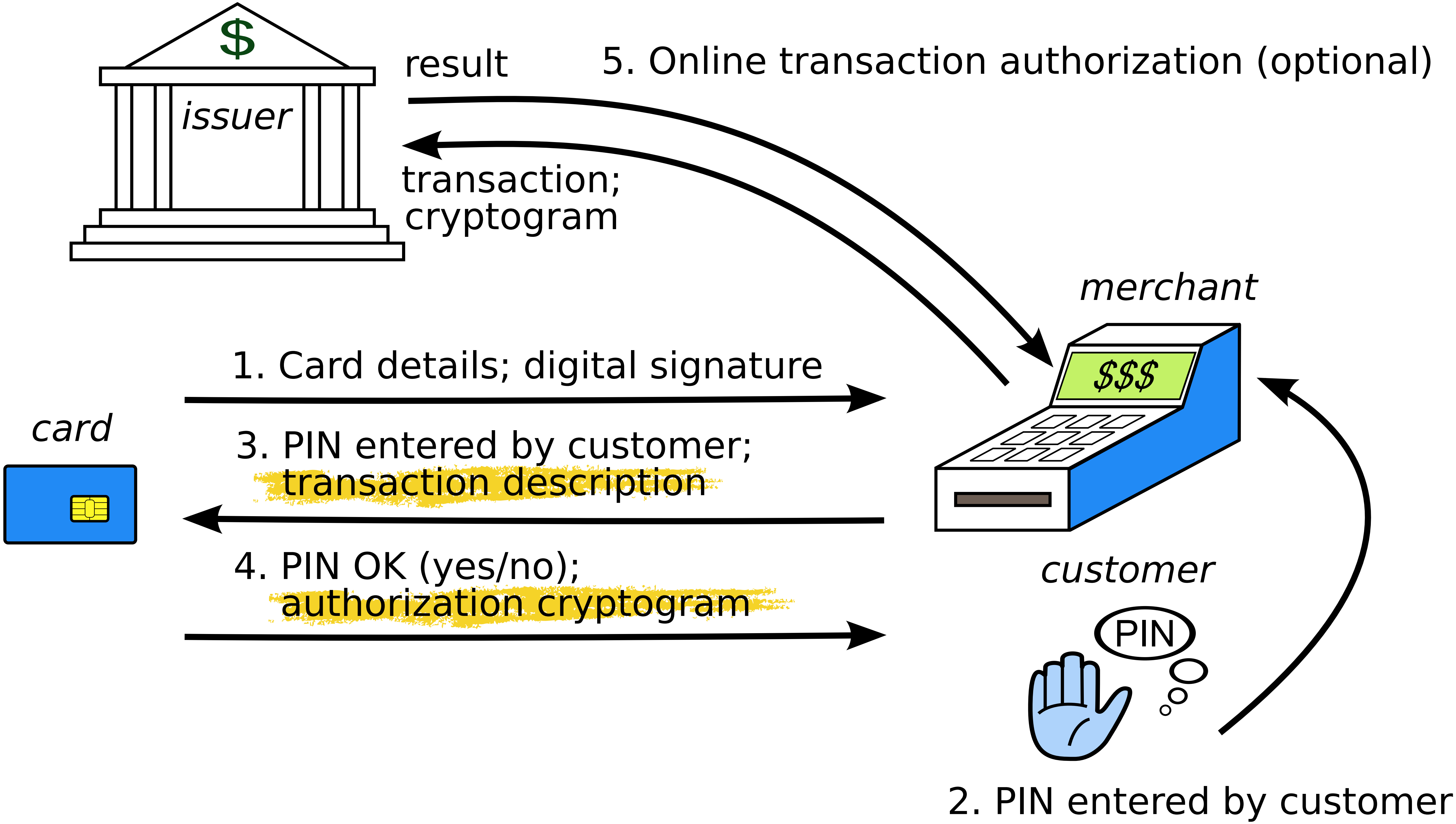
1 Scammers **steal bank cards by stealth** to avoid attracting the attention of their victims too quickly.

2 They then modify the card, replacing **existing chip with another,** programmed with **software that blocks the security**

3 The scammers can then **enter any PIN** to pay for purchases costing less than €100.

4 The scammers are buying, in general, **consumer products that can be quickly sold** on black-market.

# Unpredictable numbers are essential to prove that real card is present

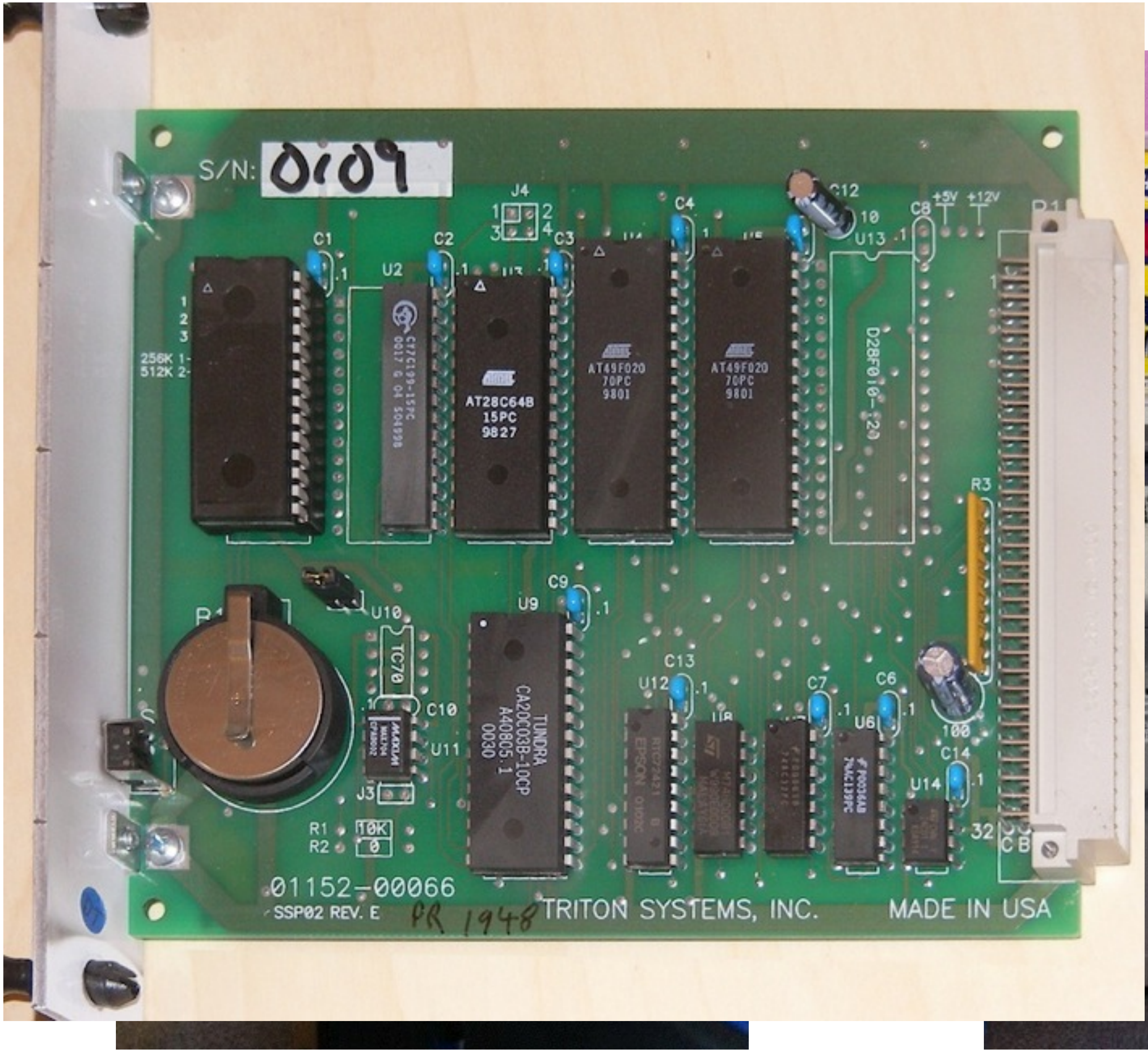

$
issuer
result
5. Online transaction authorization (optional)
transaction;
cryptogram
merchant
$$$
1. Card details; digital signature
card
3. PIN entered by customer;
transaction description
4. PIN OK (yes/no);
authorization cryptogram
customer
PIN
2. PIN entered by customer

# Random numbers?

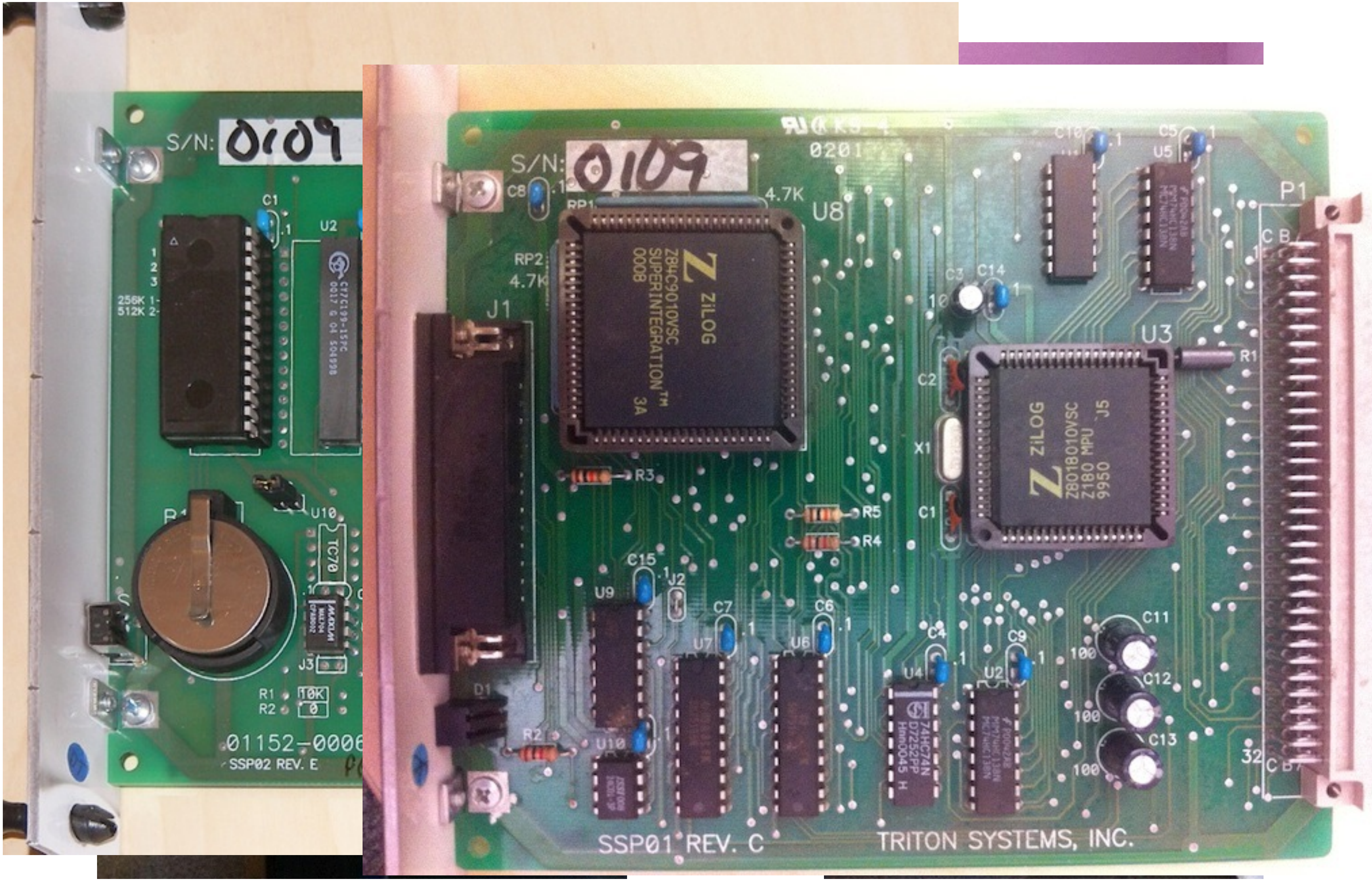
| Date | Time | UN |
|---|---|---|
| 2011-06-29 | 10:37:24 | F1246E04 |
| 2011-06-29 | 10:37:59 | F1241354 |
| 2011-06-29 | 10:38:34 | F1244328 |
| 2011-06-29 | 10:39:08 | F1247348 |

# Reverse engineering

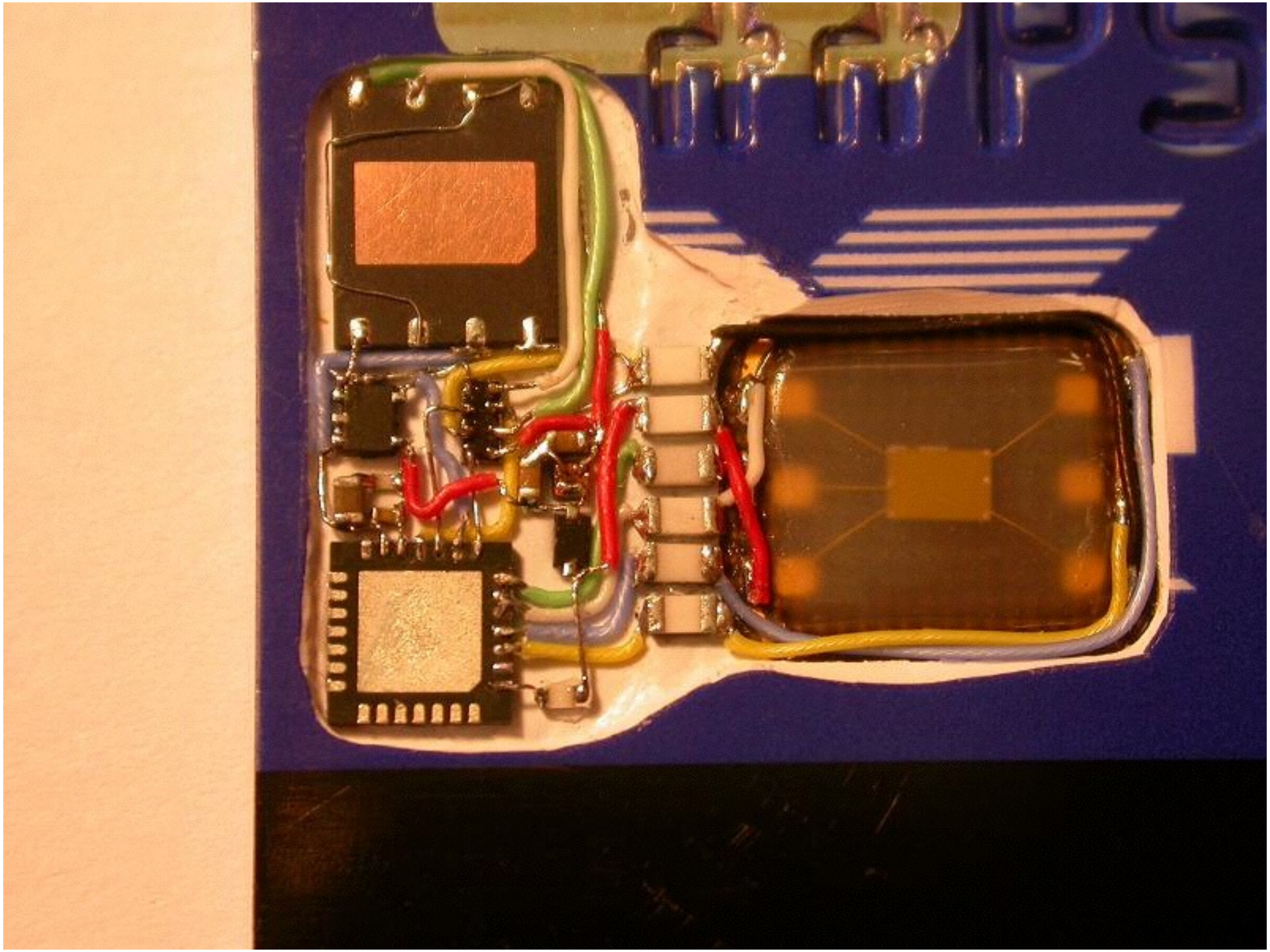
# Reverse engineering



# Reverse engineering



# Surveying the problem



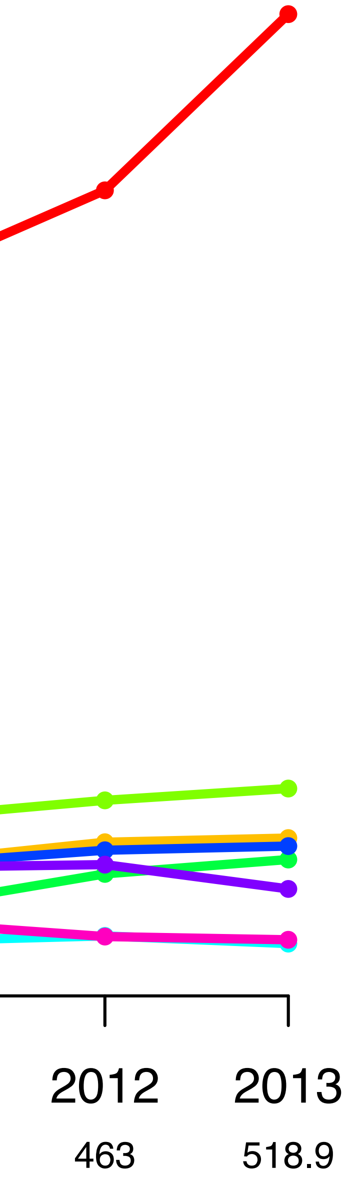
# Exploiting the vulnerability

- Pre-play card: load with cryptograms for expected UNs
- Malware attack: tamper with ATM or POS terminal to produce predictable UNs
- Tamper with ATMs or POS in supply chain
- Collusive merchant, modifies software
- Tamper with communications

# Response from industry

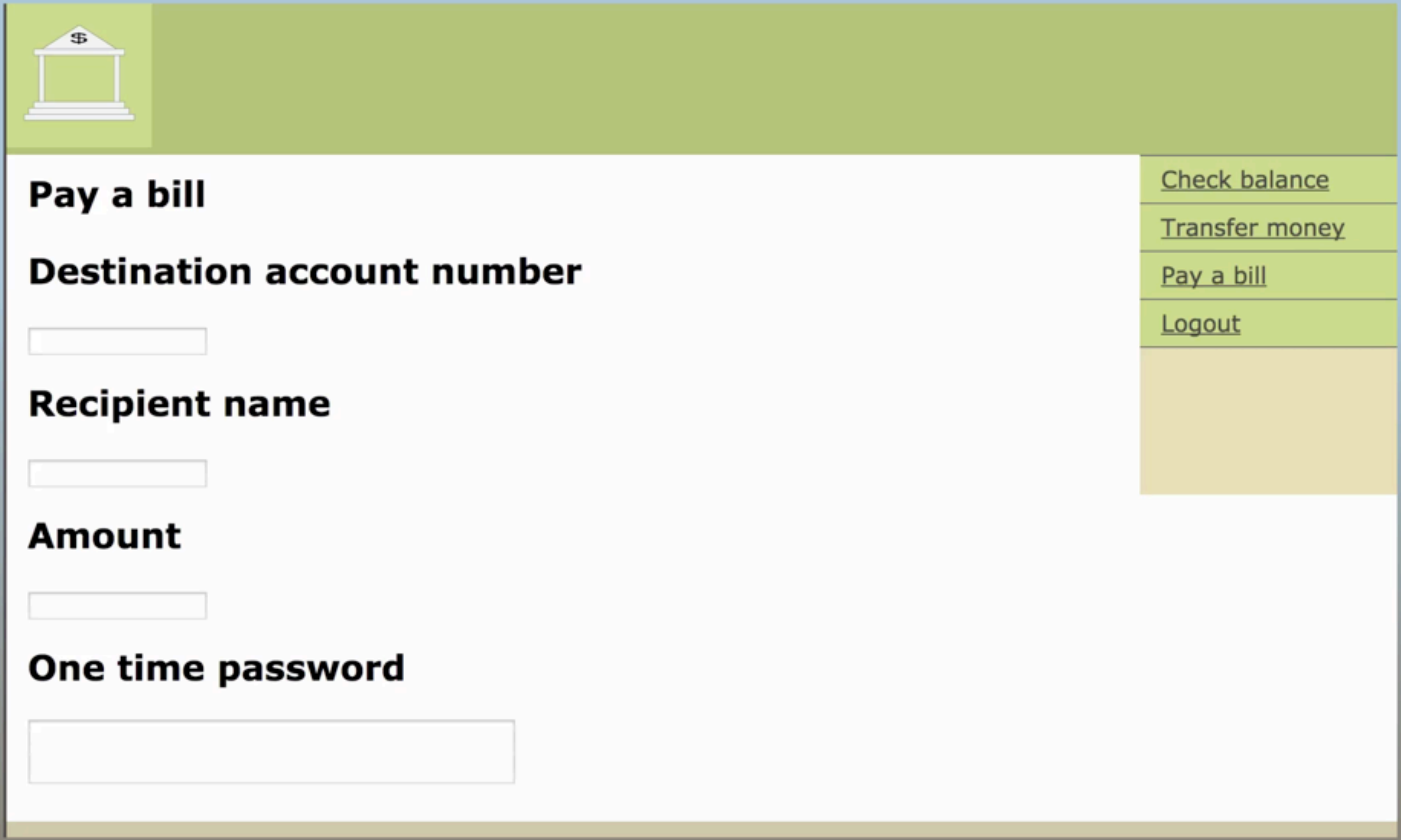
> “While Cambridge scientists have identified a theoretically potential, but technically complicated, type of card fraud, there is absolutely no evidence of this being undertaken in the real world.
>
> — UK Cards Association (September 2014)

# What about online fraud?



Card-not-present: up 22% to £301m

Online banking: up 3% to £40.9m



## Pay a bill

**Destination account number**

**Recipient name**

**Amount**

**One time password**

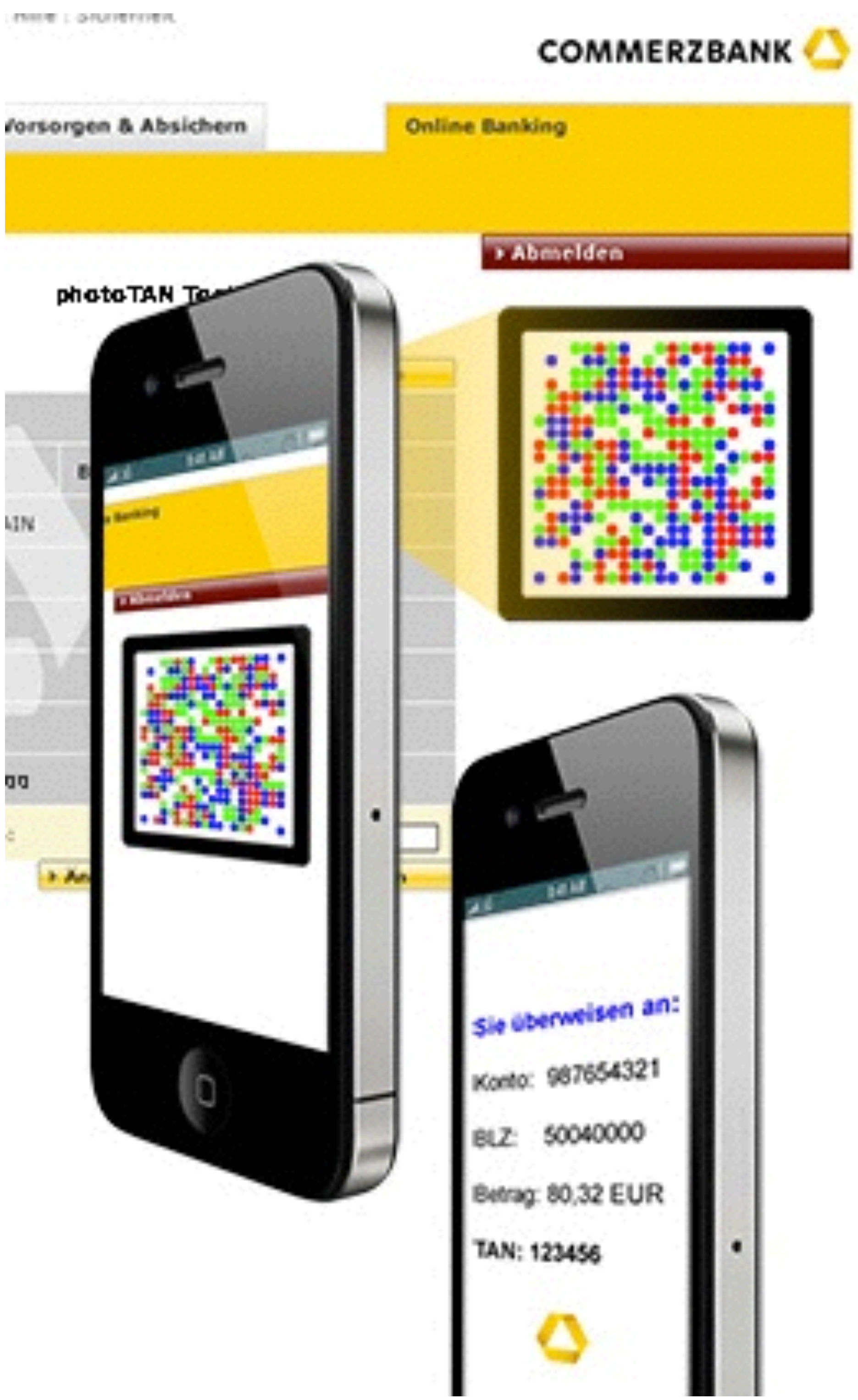
# EMV-CAP in the UK

# EMV CAP’s weakness: attacker controls user experience

- User thinks they are typing random challenge but it is really part of an account number
- User thinks it’s OK that details on device don’t match those they entered on the computer
- User thinks they are performing a POS transaction but really it’s online banking

Connect
VISA
DEBIT

# Usability is a security requirement



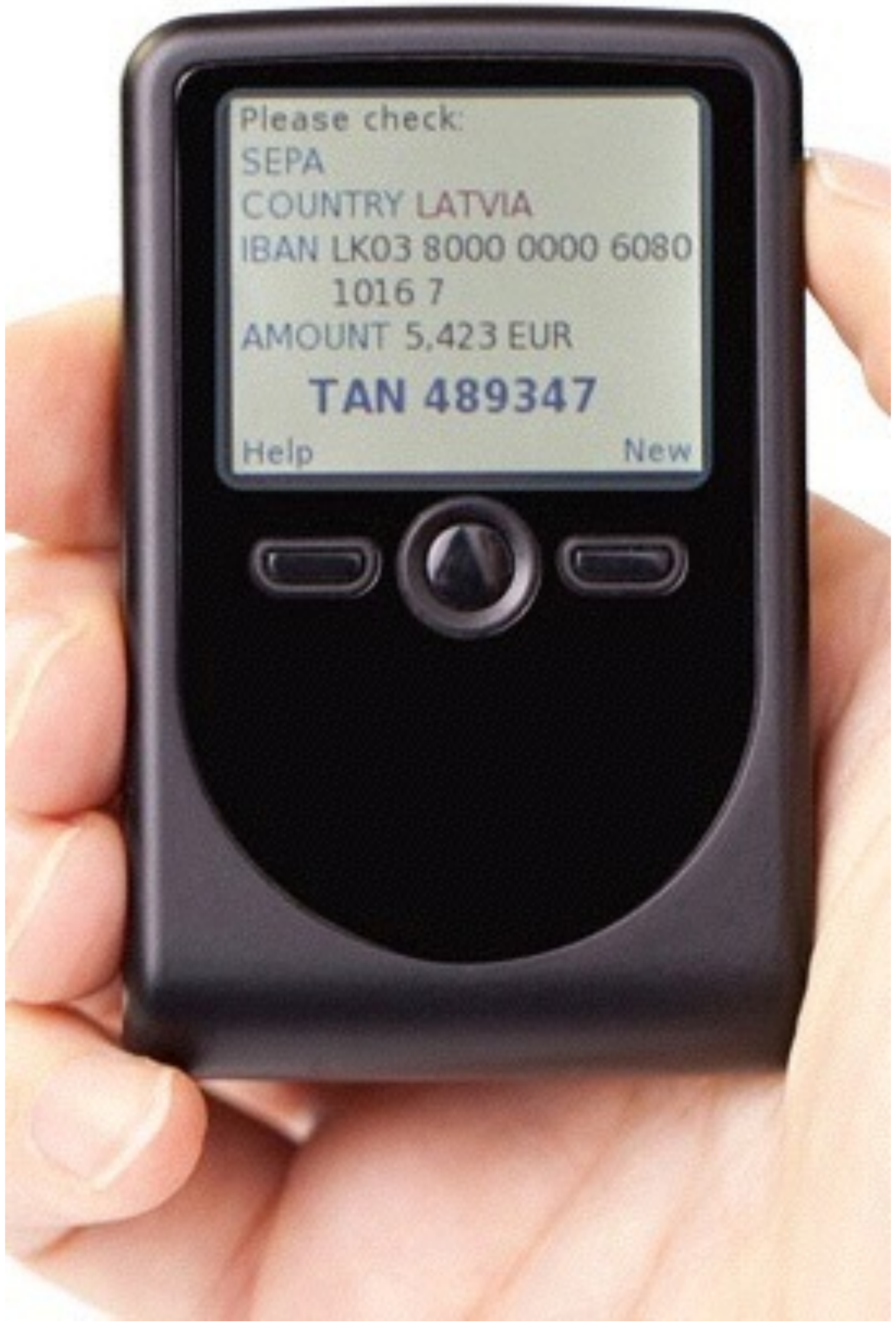
Sie überweisen an:

Konto: 987654321

BLZ: 50040000

Betrag: 80,32 EUR

TAN: 123456


Please check:
SEPA
COUNTRY LATVIA
IBAN LK03 8000 0000 6080
1016 7
AMOUNT 5,423 EUR
TAN 489347

# Research at UCL

# Research at UCL

- Simply Secure
    - Collaboration with Dropbox, Google
    - Designing and evaluating easy ways to securely communicate and authenticate
- Next generation privacy systems
    - Protecting who you are talking to, not just what you’re saying
- Measuring security
    - From a craft to a science

**Studentships available!**

# Conclusions

- Don’t underestimate criminals
- Better statistics are needed
  - Outside of UK
  - Customer losses
- Usability is a security requirement, especially when it comes to online payments