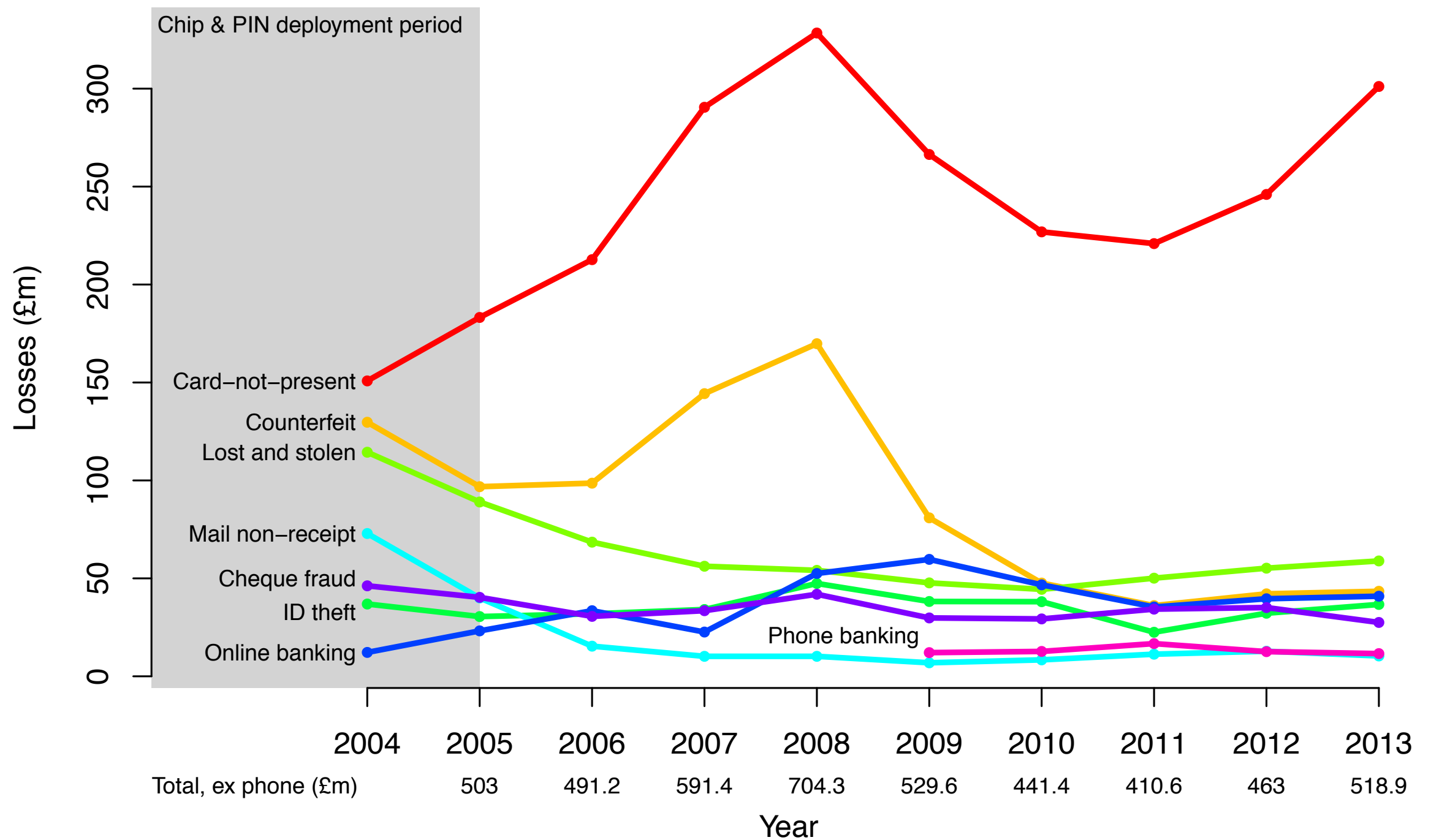


Payment Security: Attacks & Defences

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

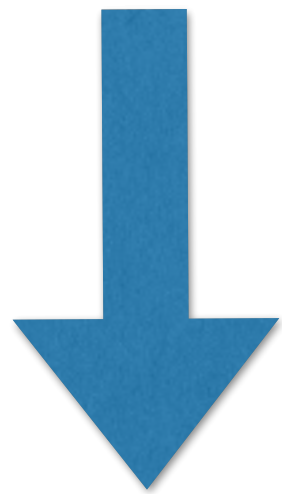
2012 2013
463 518.9

...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

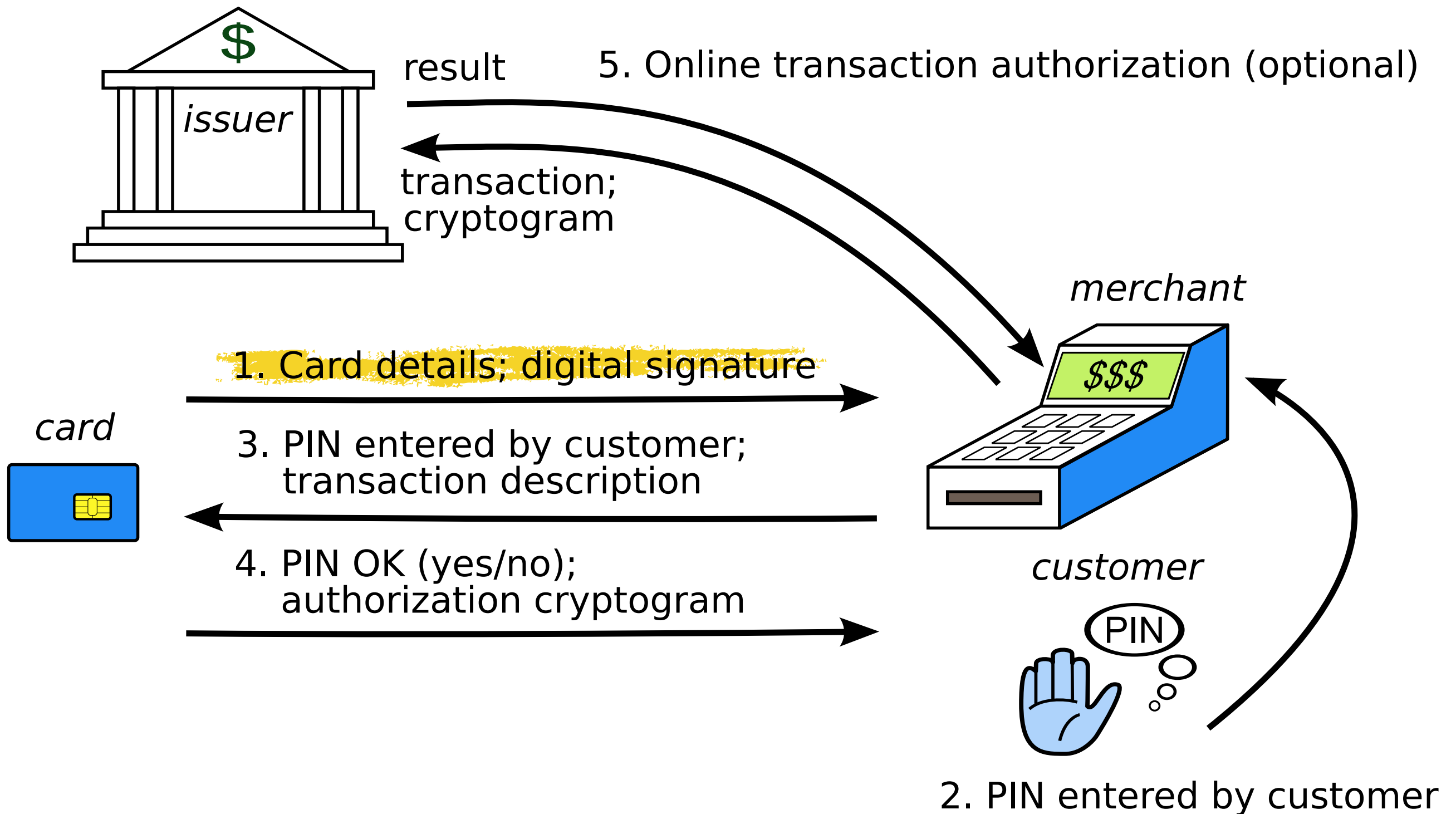
UK retail face-to-face: up 11% to £60.8m

UK cash machine: up 10% to £31.9m

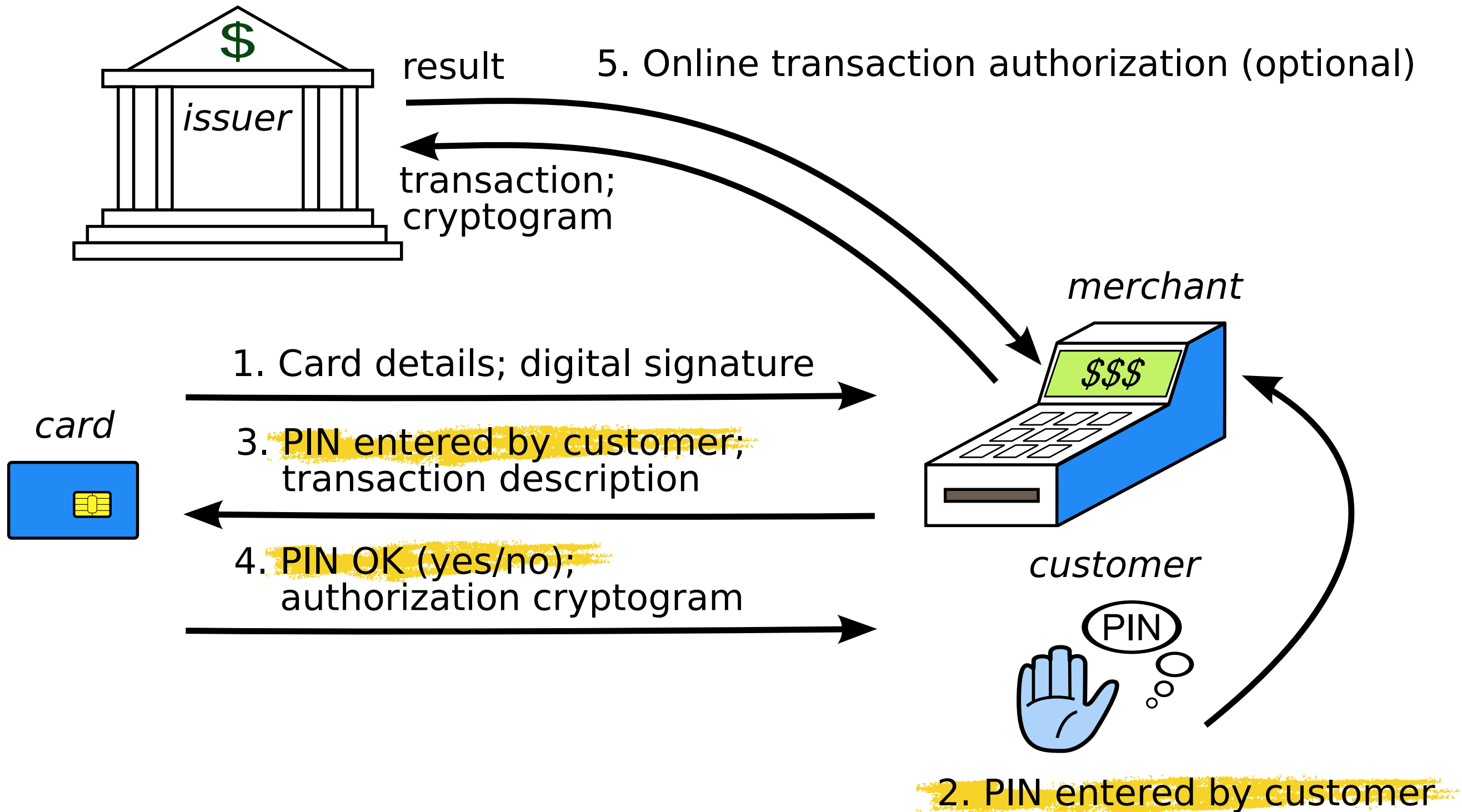
Chip and PIN transactions have three main stages

- **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

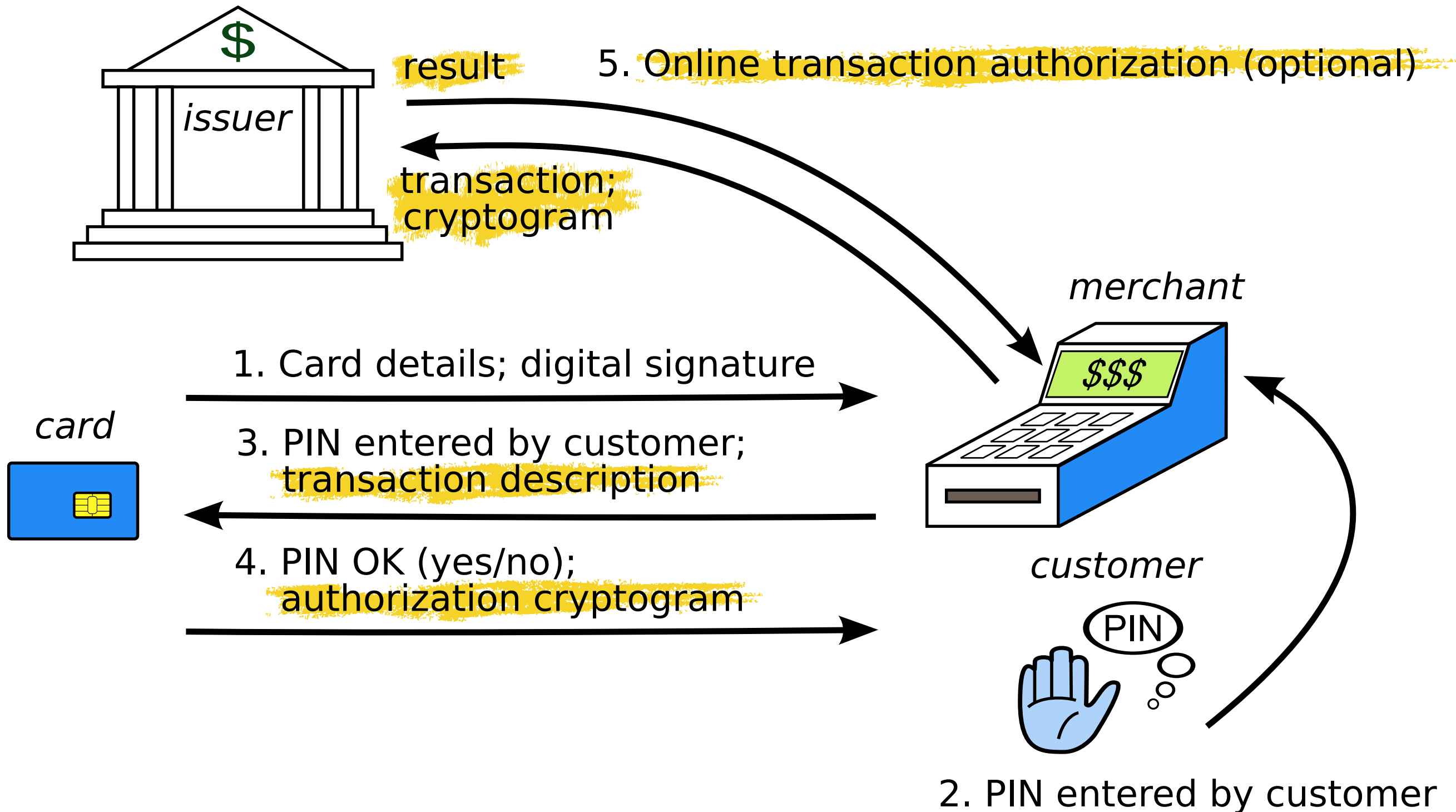
Card authentication



Cardholder verification



Transaction authorisation



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

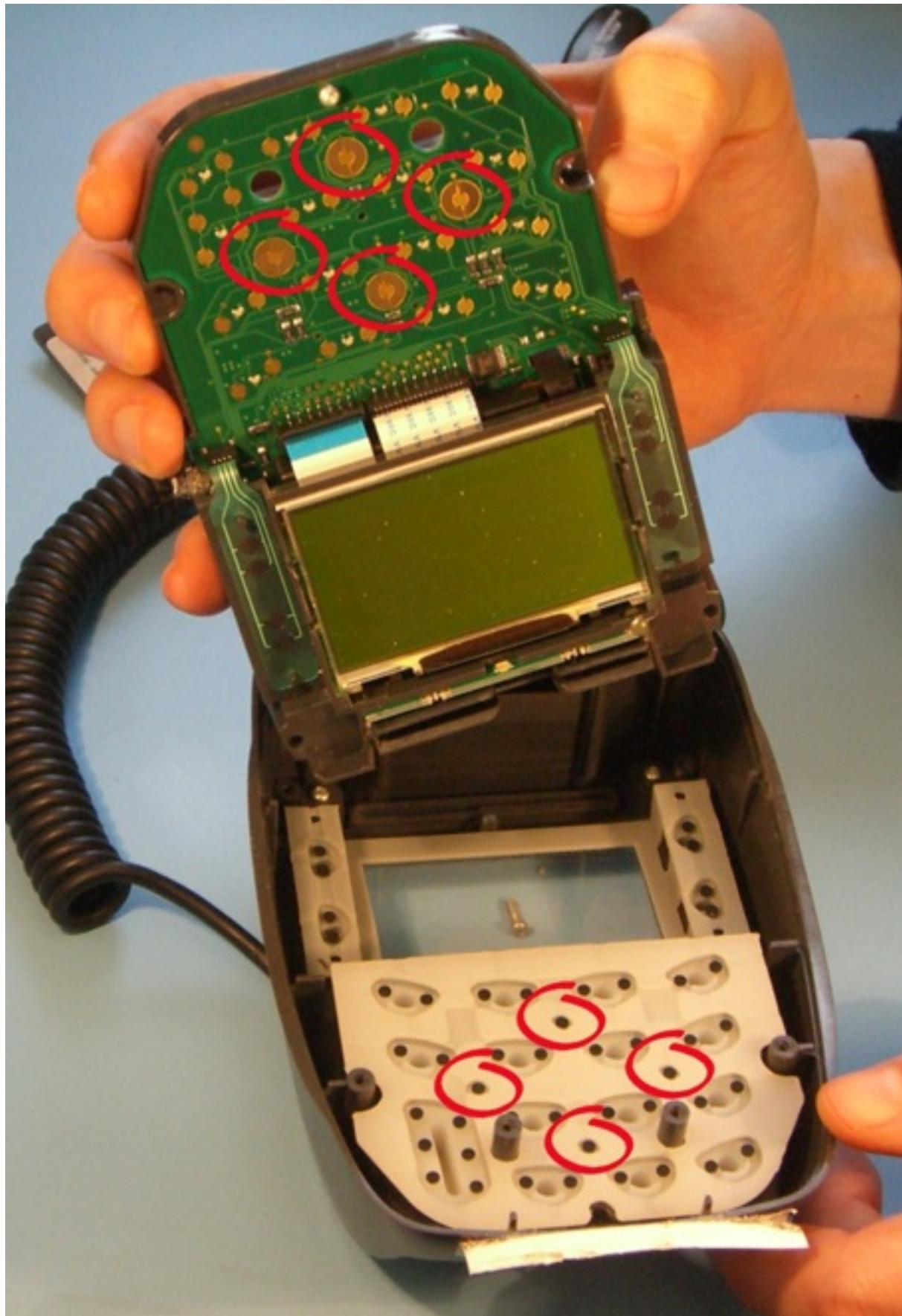
Lost and Stolen

Sensitive data is sent unencrypted between the card and the terminal

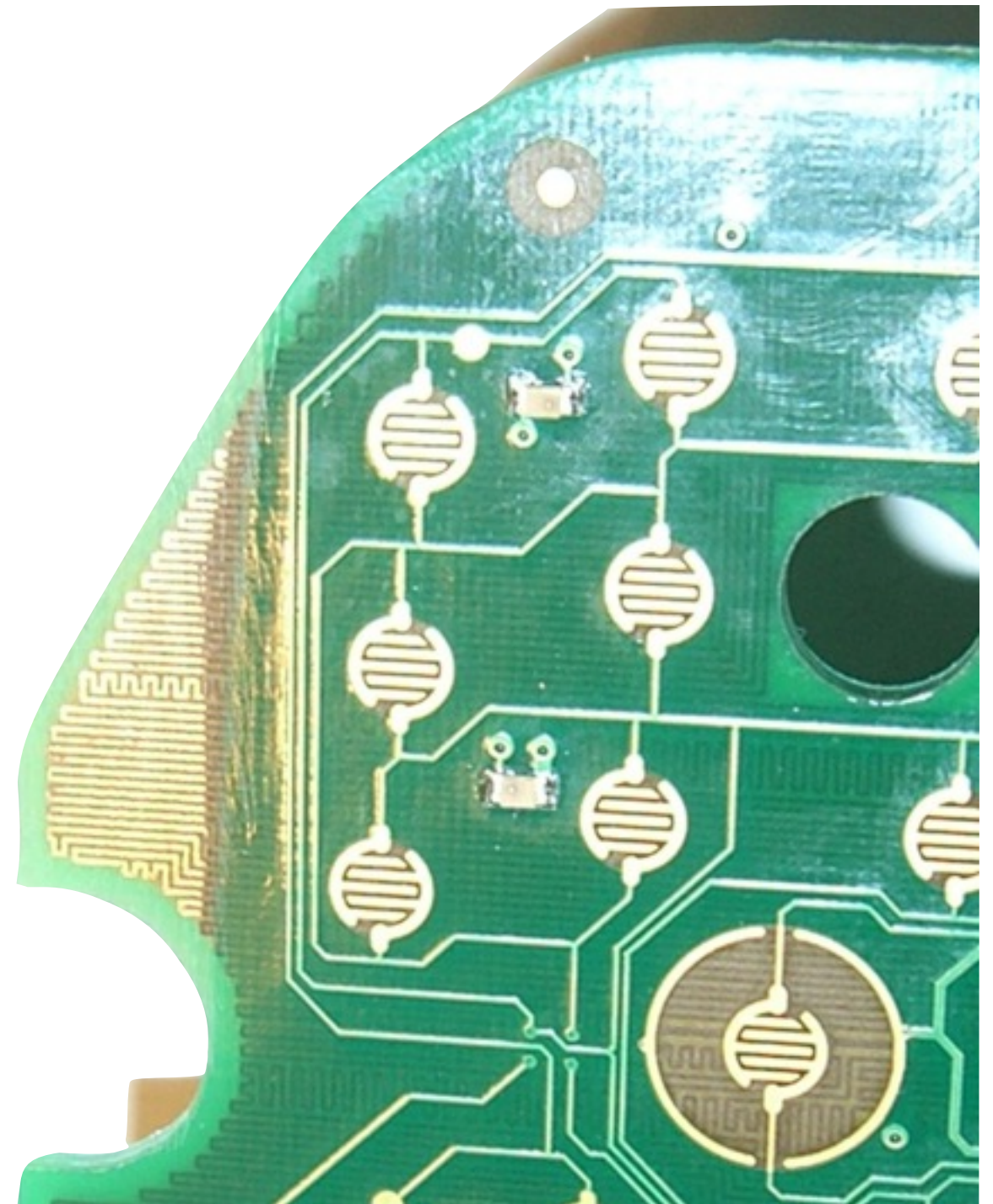
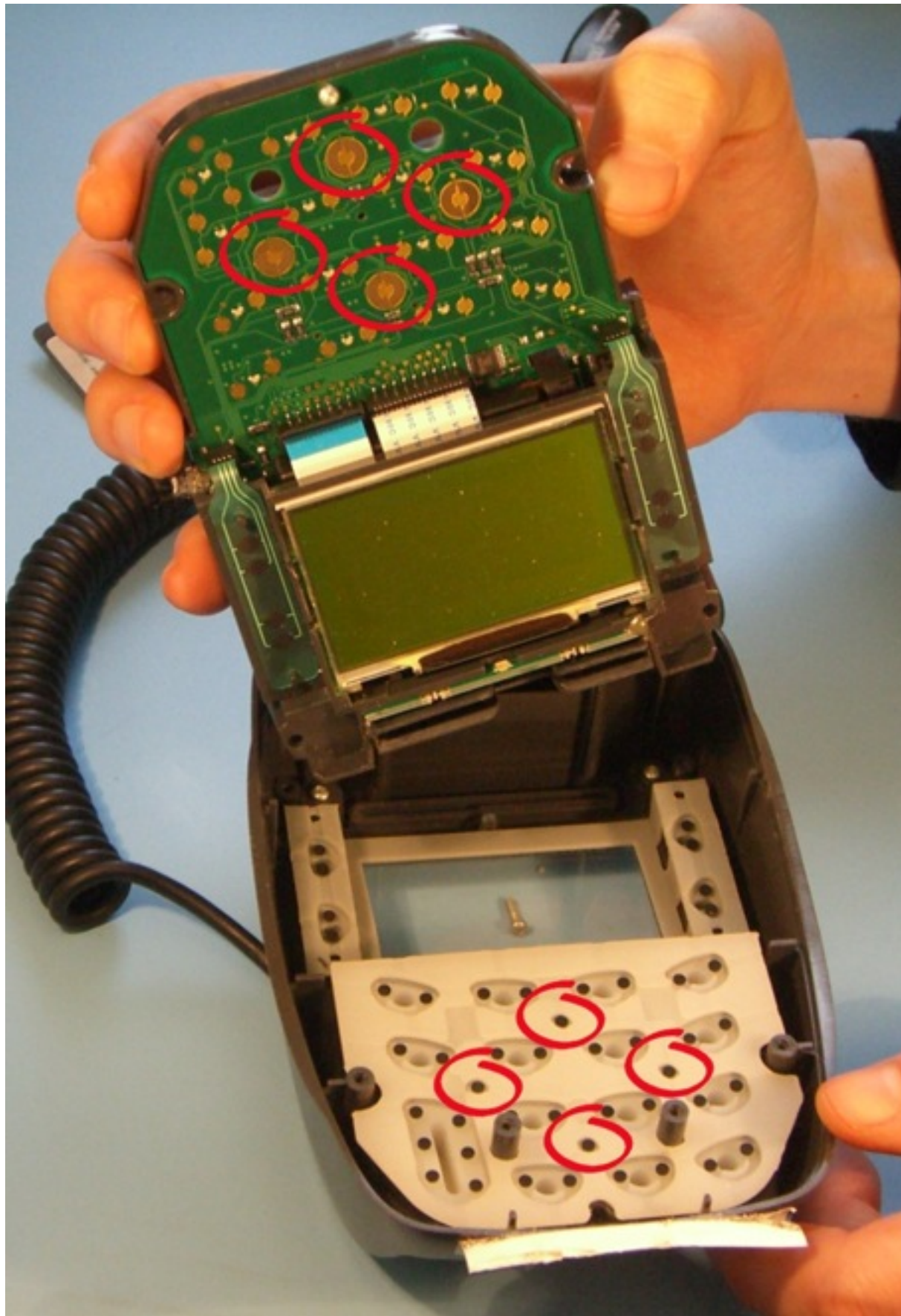
- Card number, expiry date, cardholder name ...
- Copy of magnetic stripe including CVV (for some cards)
- PIN to be checked by card

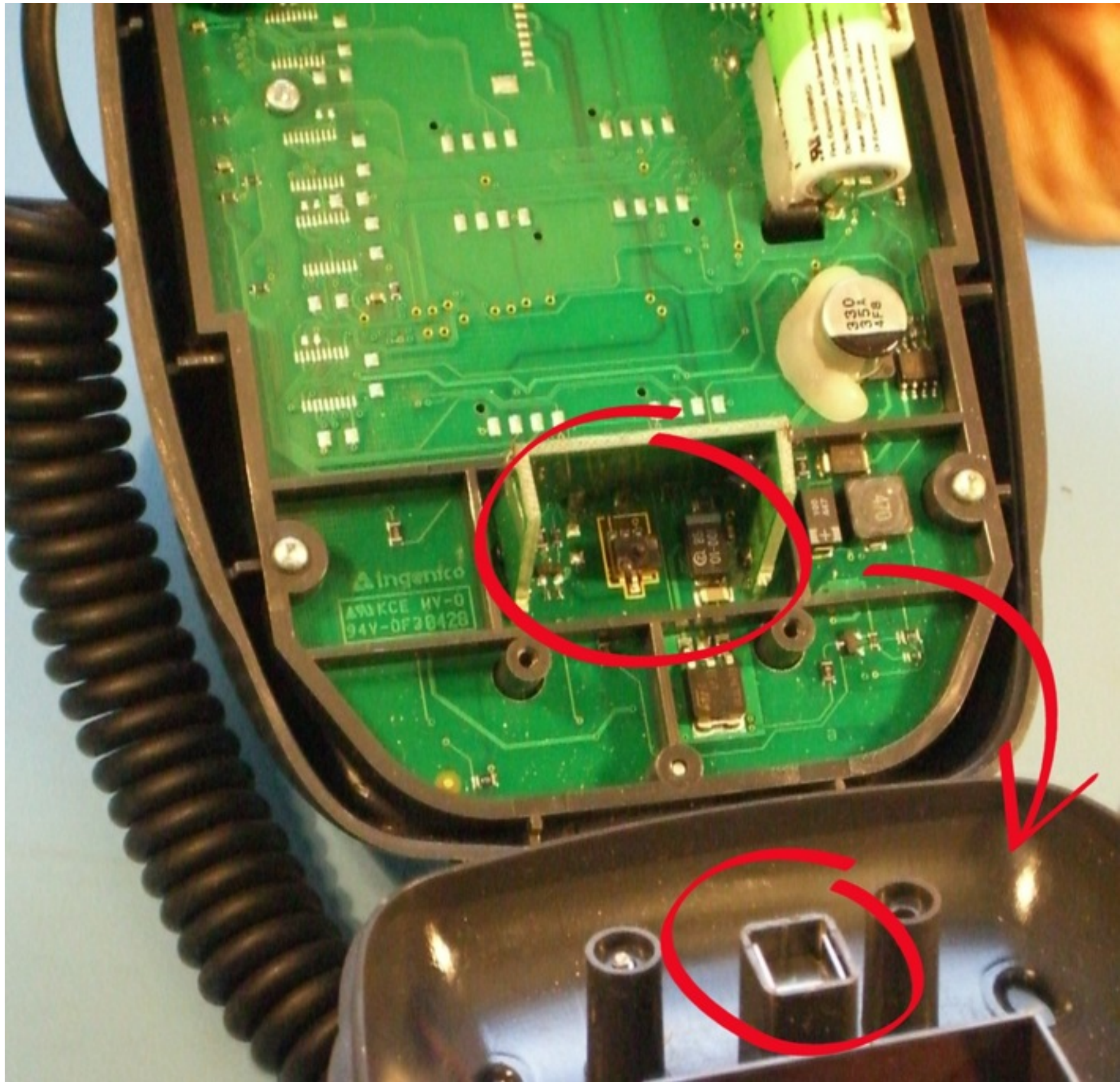
Chip and PIN terminals are supposed to protect this information against being recorded: **tamper resistance**

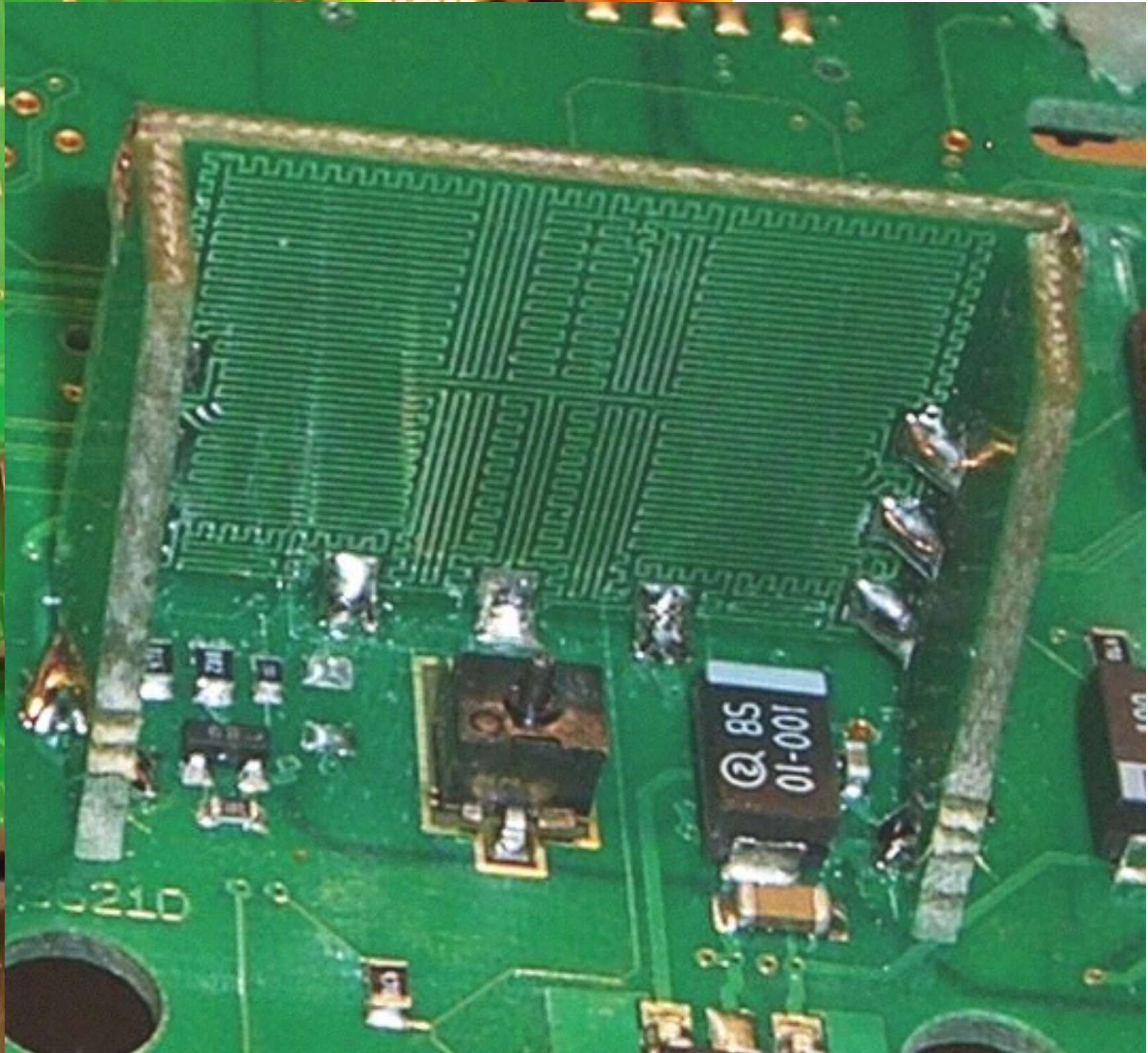
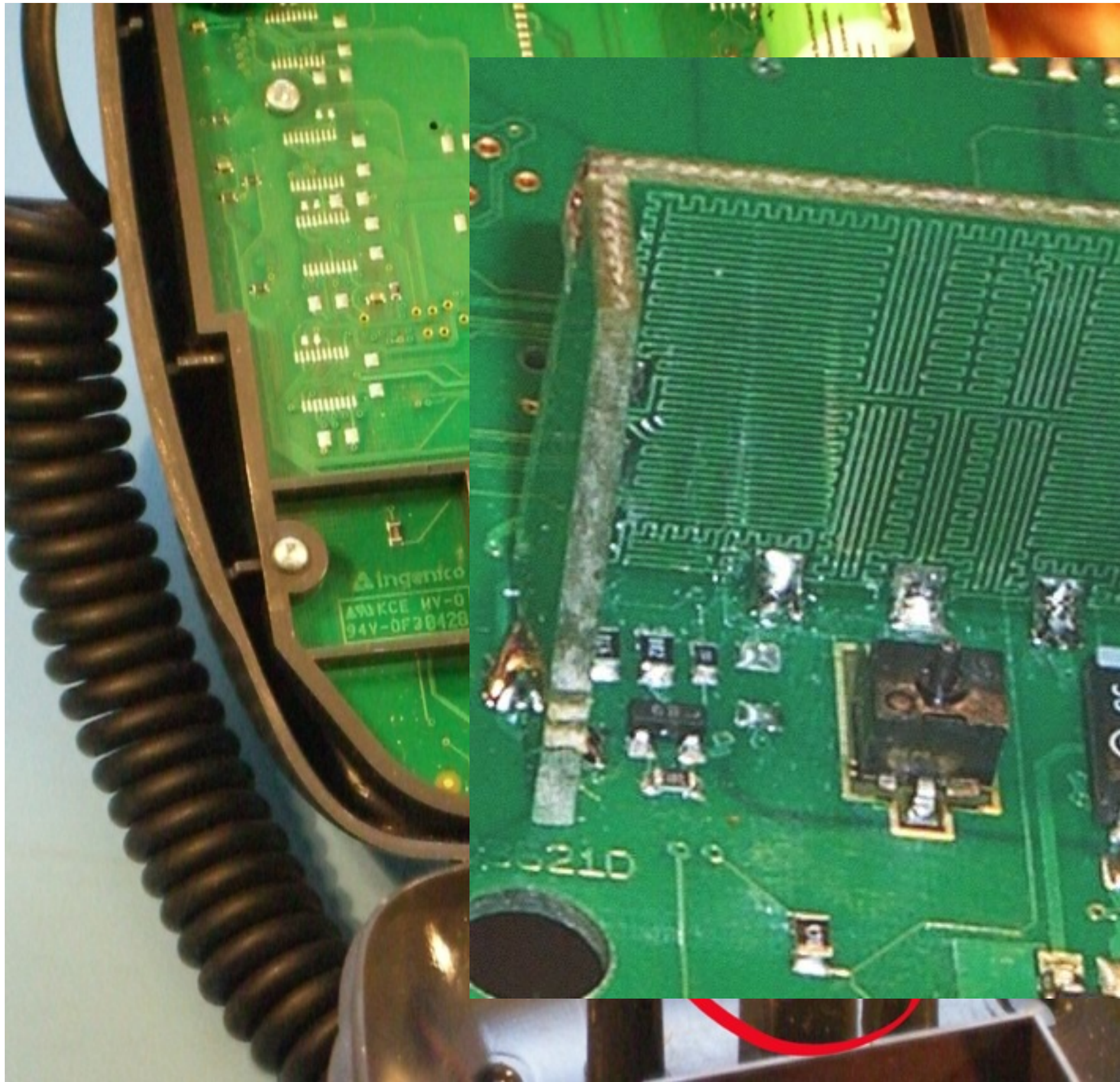
Tamper switches

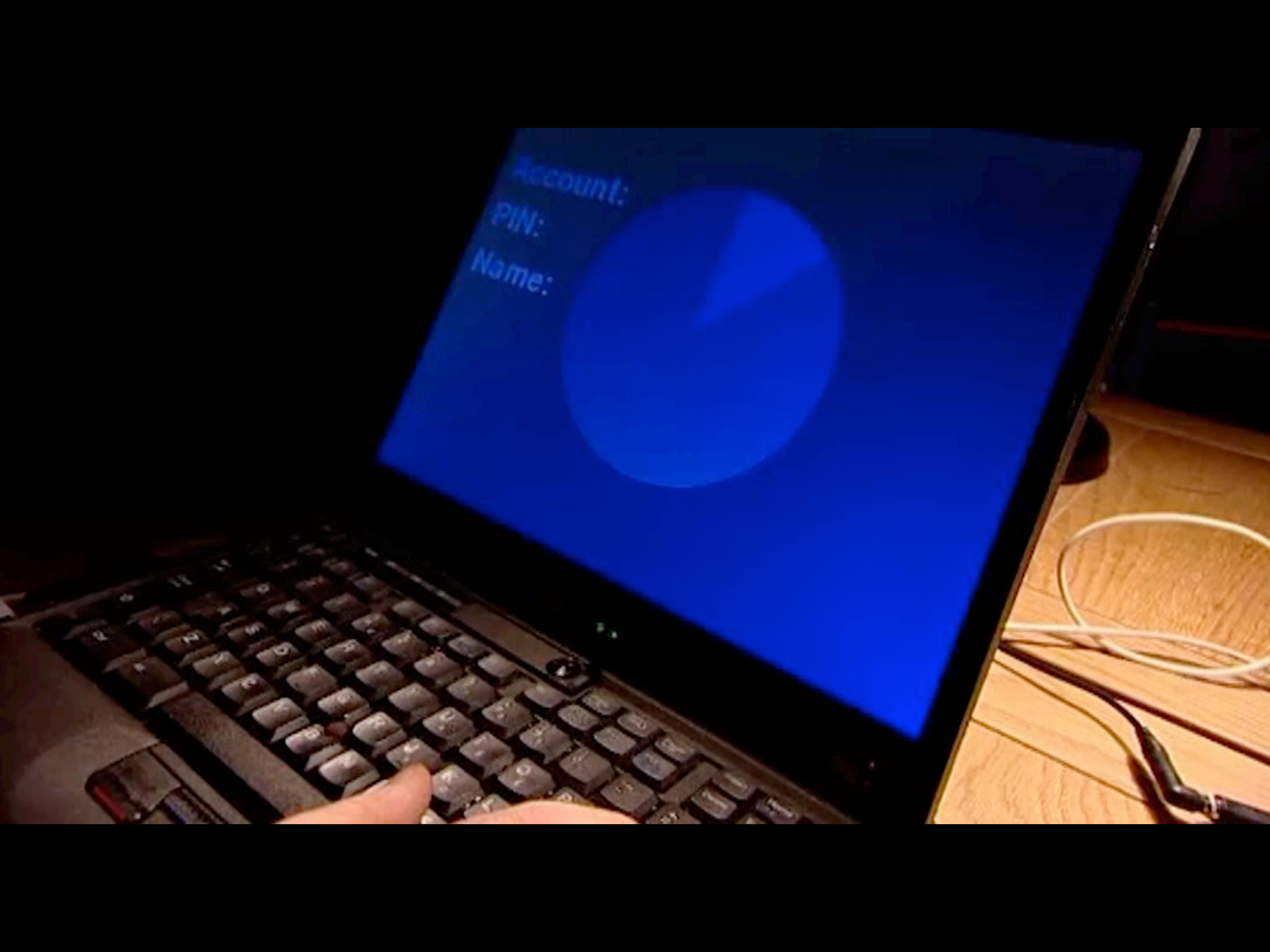


Tamper mesh









Account:
PIN:
Name:






ingenico

9, quai de Dion Bouton 92816 Puteaux FRANCE



PN: 

Rev : 56

Electrical Specification: 6.5 to 15VDC 0.5 A

SN: 

IFM-UCC2-IFM-3-AB Made in EU/Fabriqu  en UE

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

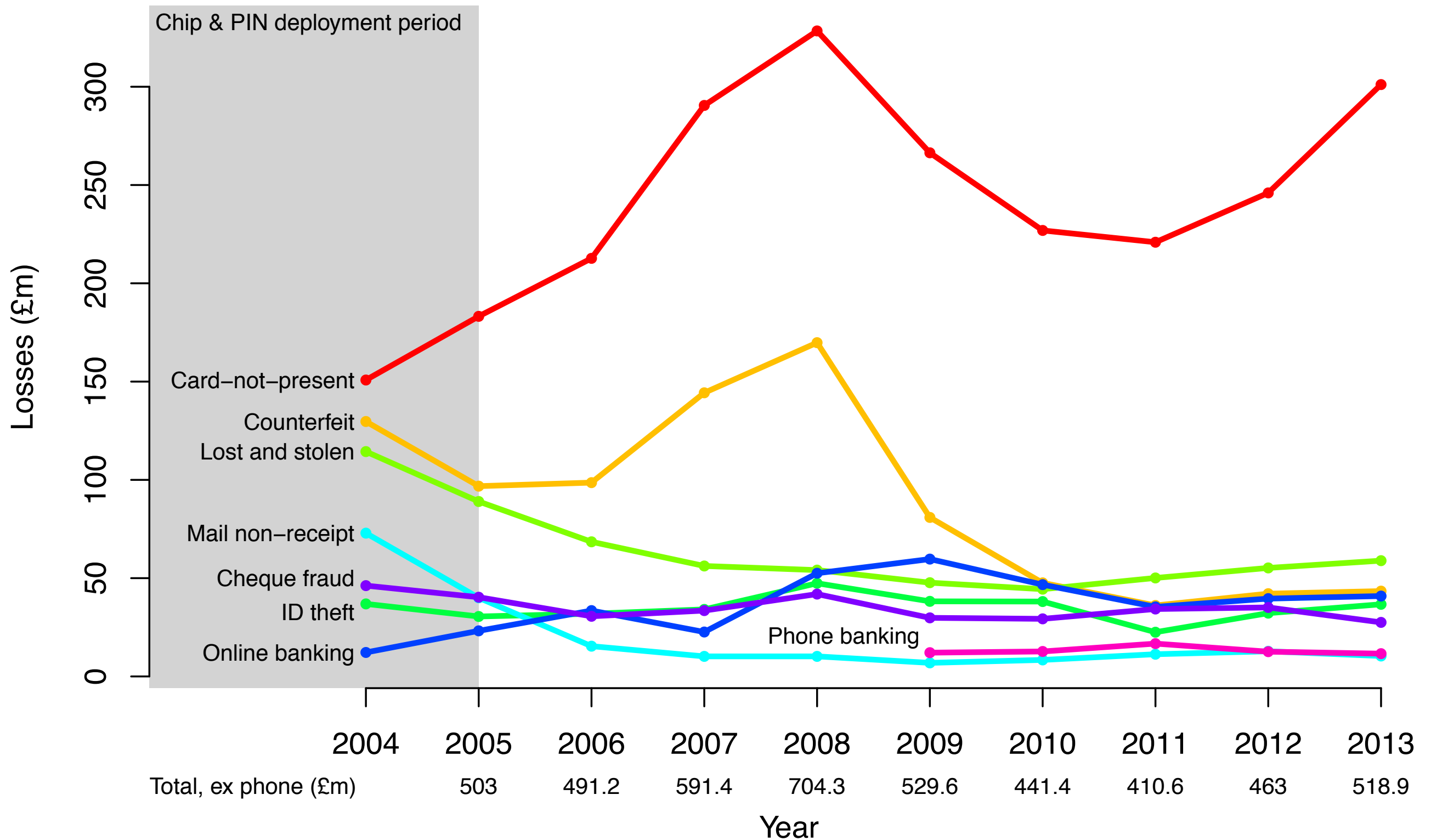
Criminal gets all that is needed to make a magnetic stripe card

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

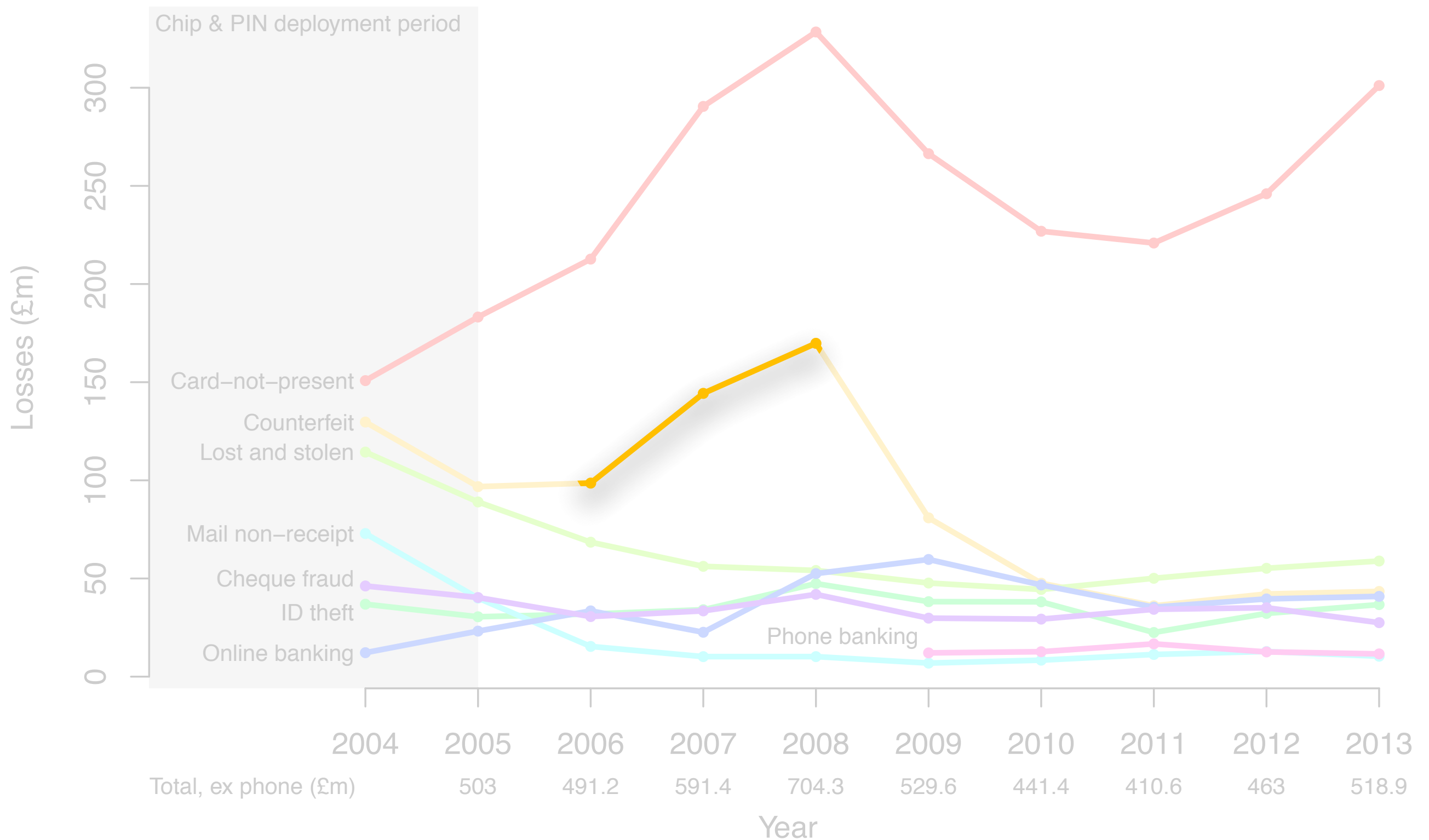


CASH

Chip and PIN led to increase in counterfeit fraud



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

011900

£5.00

VISA

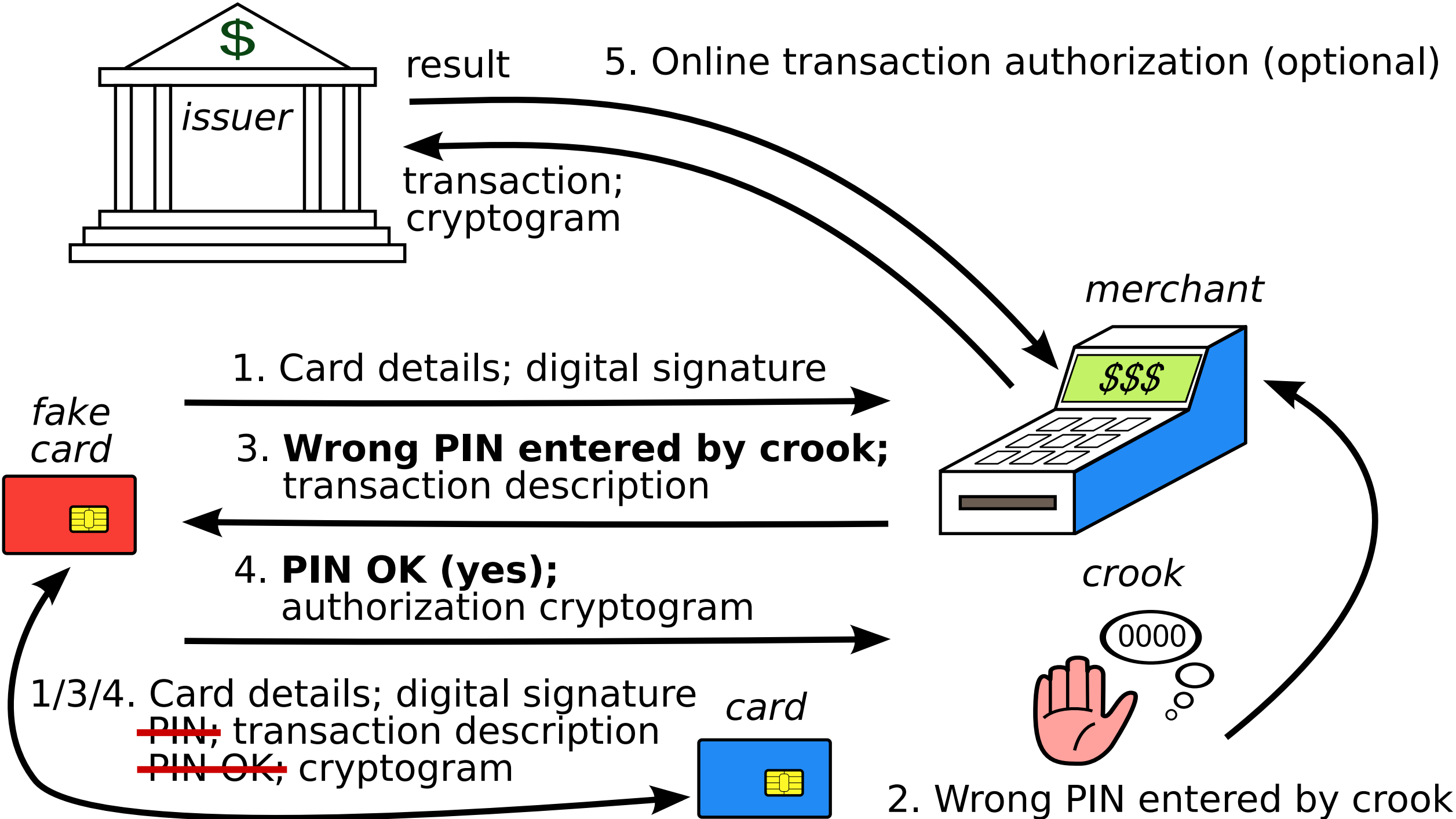
Enter PIN

* _

ENT = OK

CNL = NO

The no-PIN attack



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

Toute l'actualité, 25 septembre 2014, mis à jour à 01h10

Le Parisien

Mon compte Inscrivez-vous



Rechercher sur le site OK

Abonnez-vous : à partir de 1€

À SUIVRE

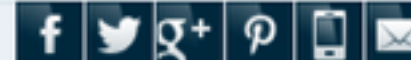
Question du jour

Otage français exécuté

Jihadistes présumés

iPhone 6

Caen-PSG



À LA UNE

SOCIÉTÉ

FAITS DIVERS

POLITIQUE

ECONOMIE

AUTO

INTERNATIONAL

PEOPLE

INSOLITE

HIGH-TECH

SCIENCES

BLOGS

SANTÉ

Actualité > **Faits divers**

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

Recommander

387 personnes recommandent ça. Soyez le premier parmi vos amis.

Tweeter 52

+1

Share



A

A



38 réactions

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

SUR LE MÊME SUJET

Avez-vous confiance en votre carte bancaire?

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 €.

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 Hollande

Response from criminals

All the news , Sept. 25, 2014, updated at 1:10



My Account Sign up  

Rechercher sur le site

Subscribe: from € 1

TO BE CONTINUED






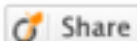

TO A COMPANY MISCELLANEOUS POLICY ECONOMY AUTO INTERNATIONAL PEOPLE UNUSUAL HIGH-TECH SCIENCE BLOGS HEALTH

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

ON THIS TOPIC

Do you trust your credit card?

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

NEWS FLASH

LAST MINUTE

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

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 Hollande**

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

ON THIS TOPIC

Do you trust your credit card?

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

COMMENT FONCTIONNE LE STRATAGÈME



1 Les escrocs dérobent des cartes bancaires au cours de vols par ruse pour ne pas attirer trop vite l'attention de leurs victimes.

2 Ils modifient ensuite la carte en remplaçant la puce existante par une autre, programmée avec un logiciel qui bloque le système de sécurité.

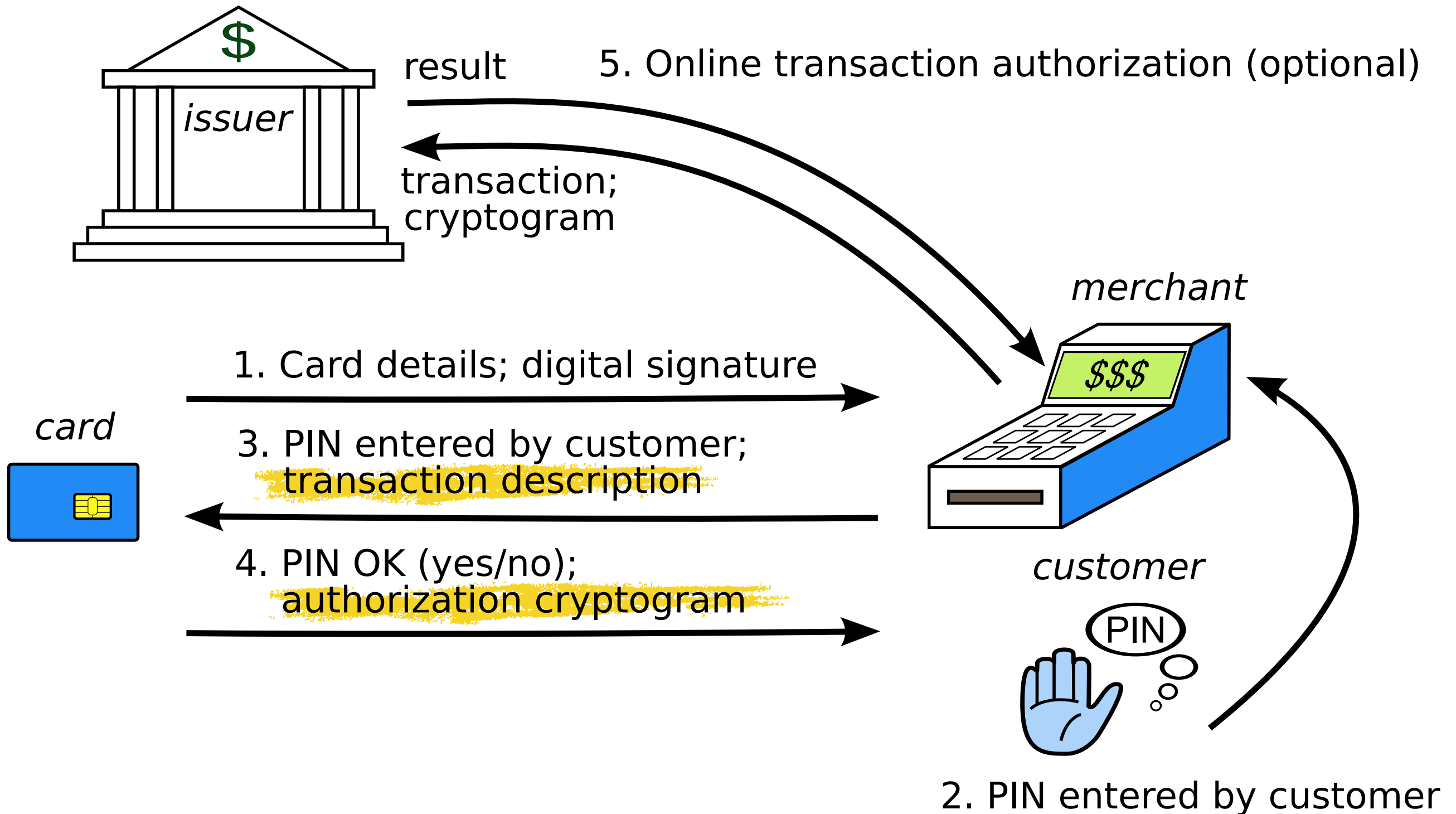


3 Les escrocs peuvent alors composer n'importe quel code confidentiel pour payer leurs achats, d'un montant inférieur à 100 €.

4 Les malfrats achètent, en général, des produits de consommation courante qui sont écoulés dans des réseaux clandestins.



Unpredictable numbers are essential to prove that real card is present



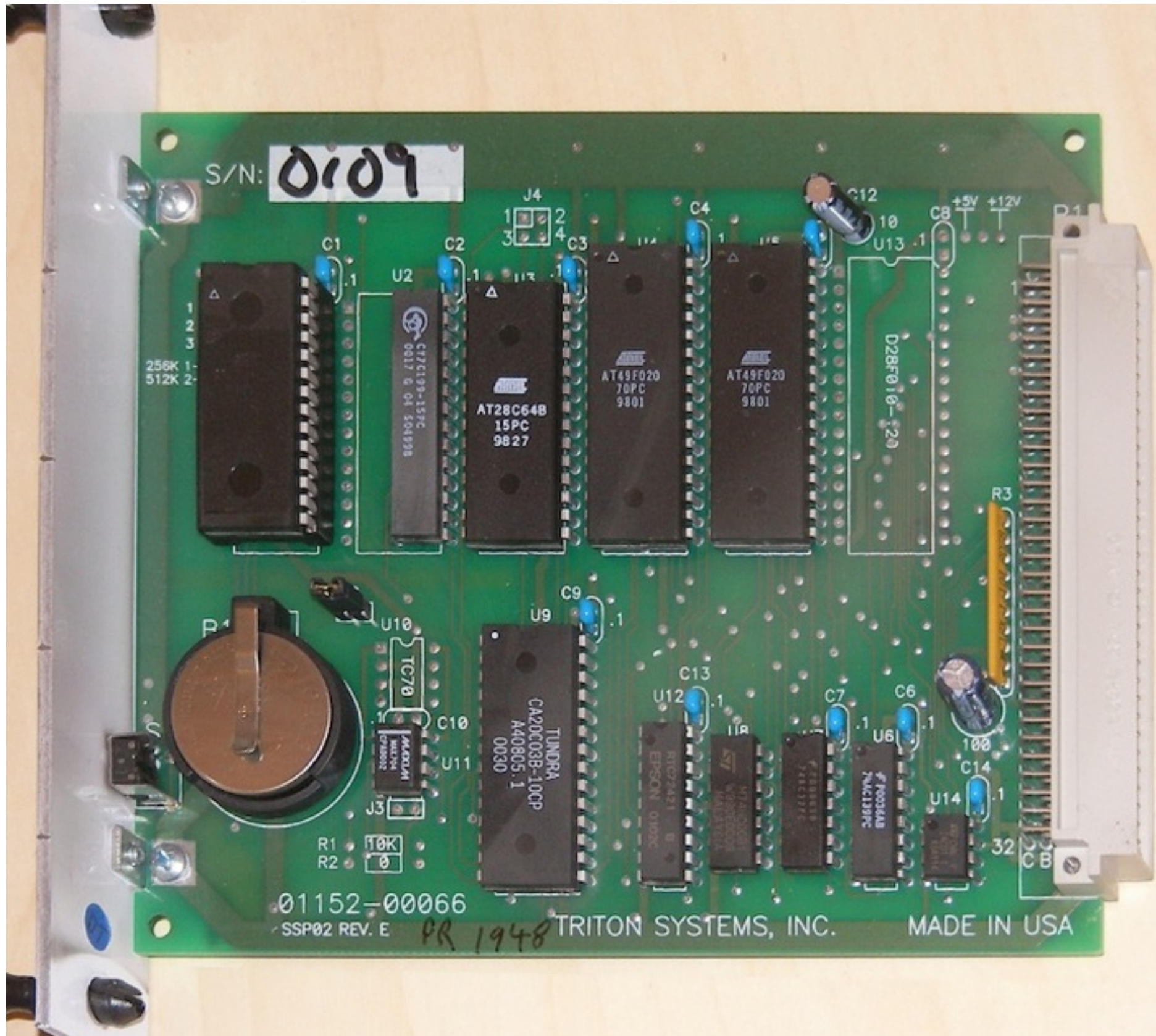
Random numbers?

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

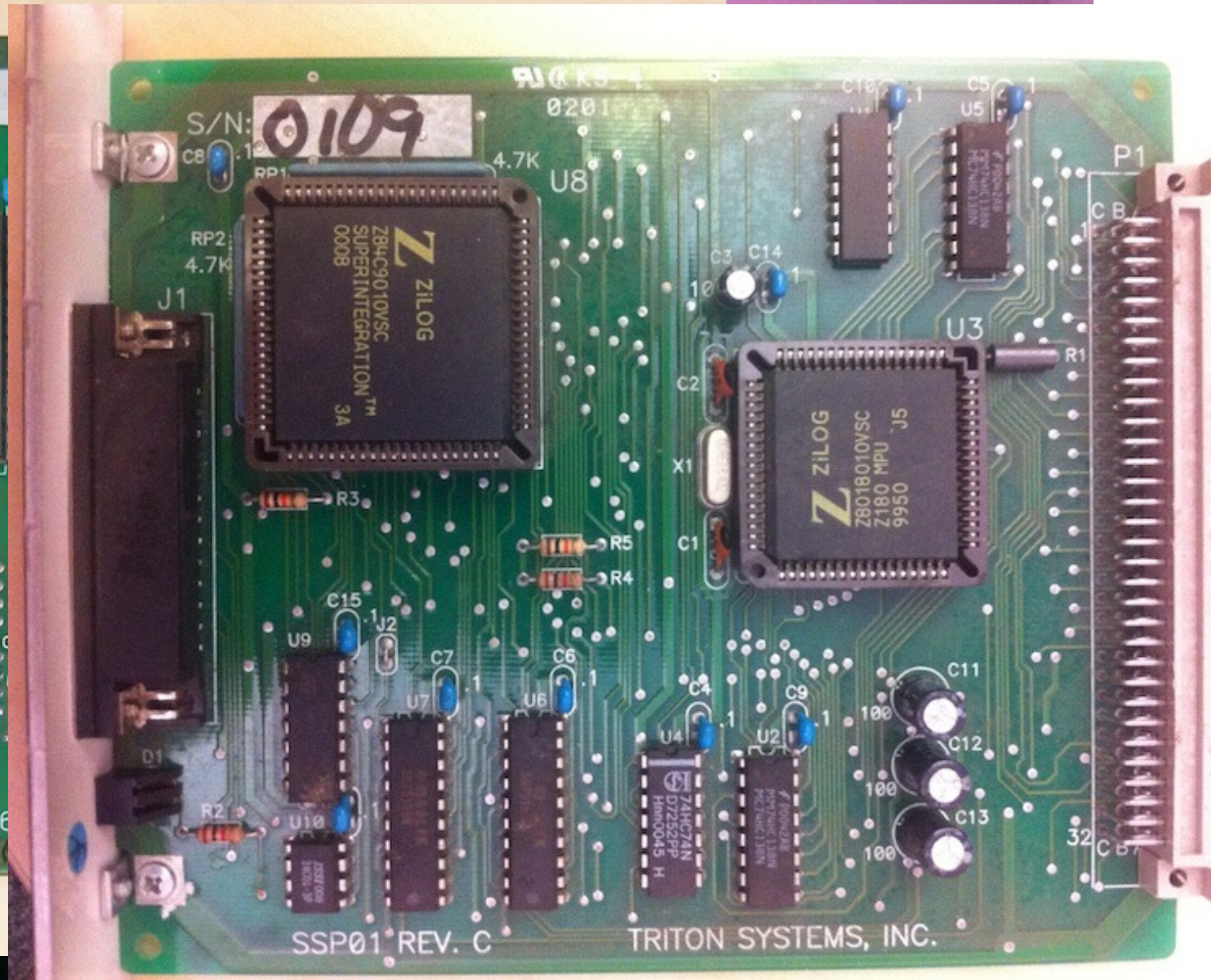
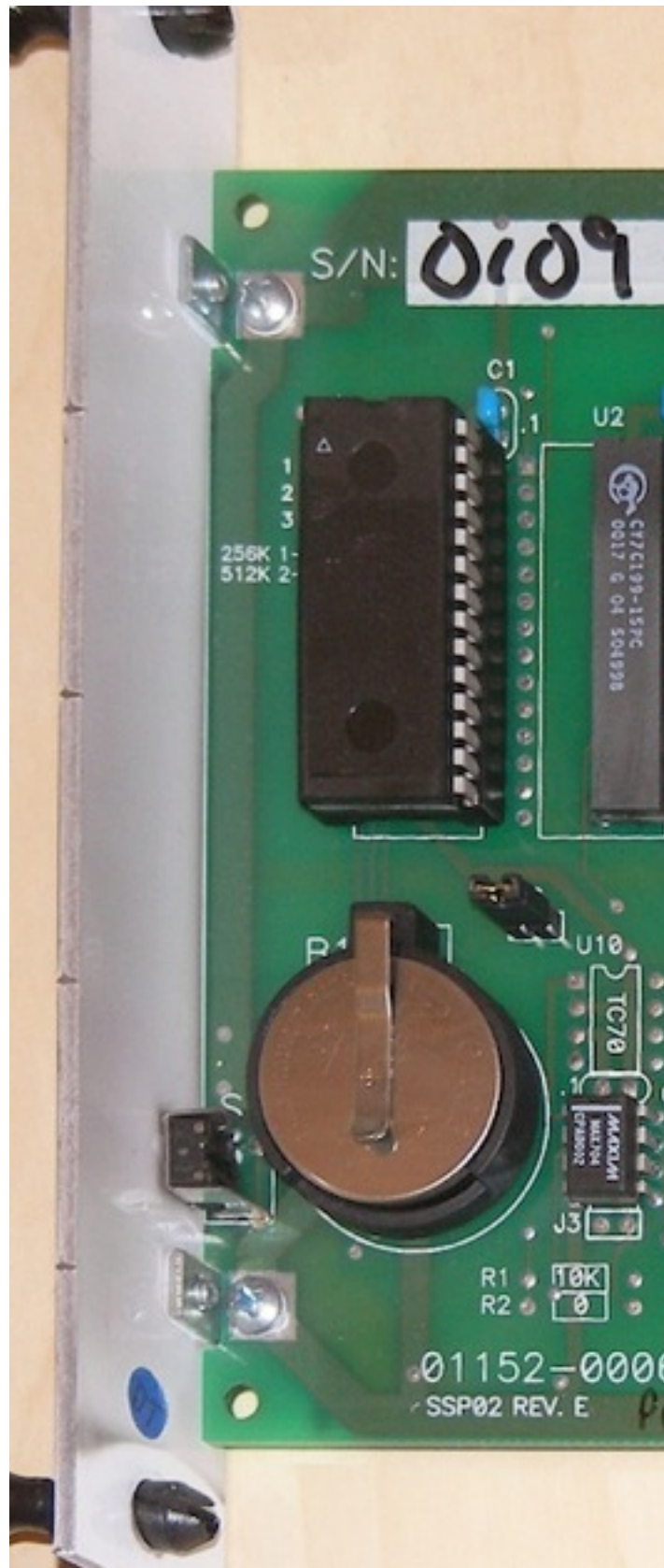
Reverse engineering



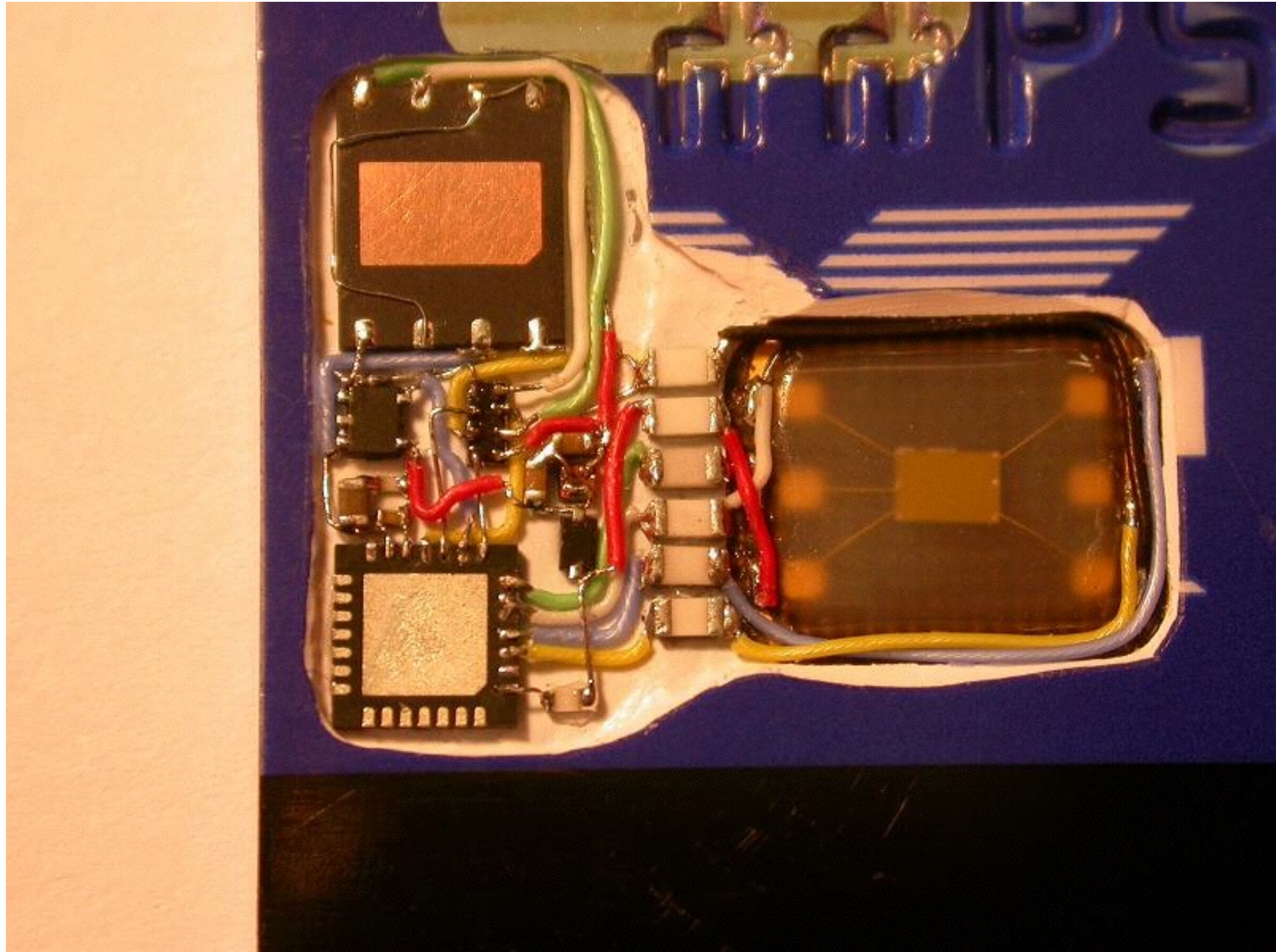
Reverse engineering



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

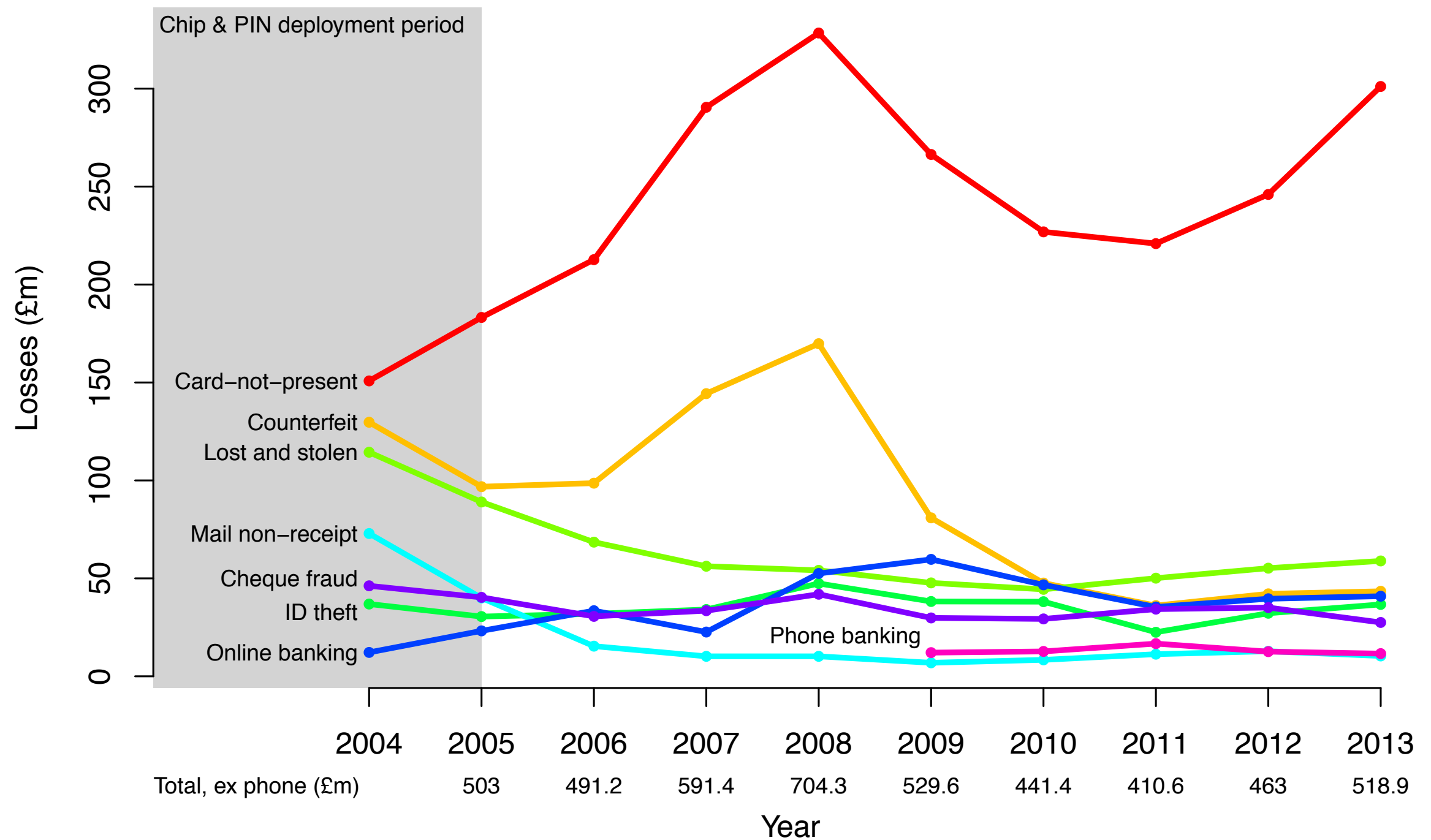
Response from industry



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?



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

[Check balance](#)

[Transfer money](#)

[Pay a bill](#)

[Logout](#)

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
CREDIT

5
11/11
2111



Usability is a security requirement



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