ATM Skimming

Presented by Chenguang Wang, Jiachen Hou, Yuguang Huang

ATM Skimming

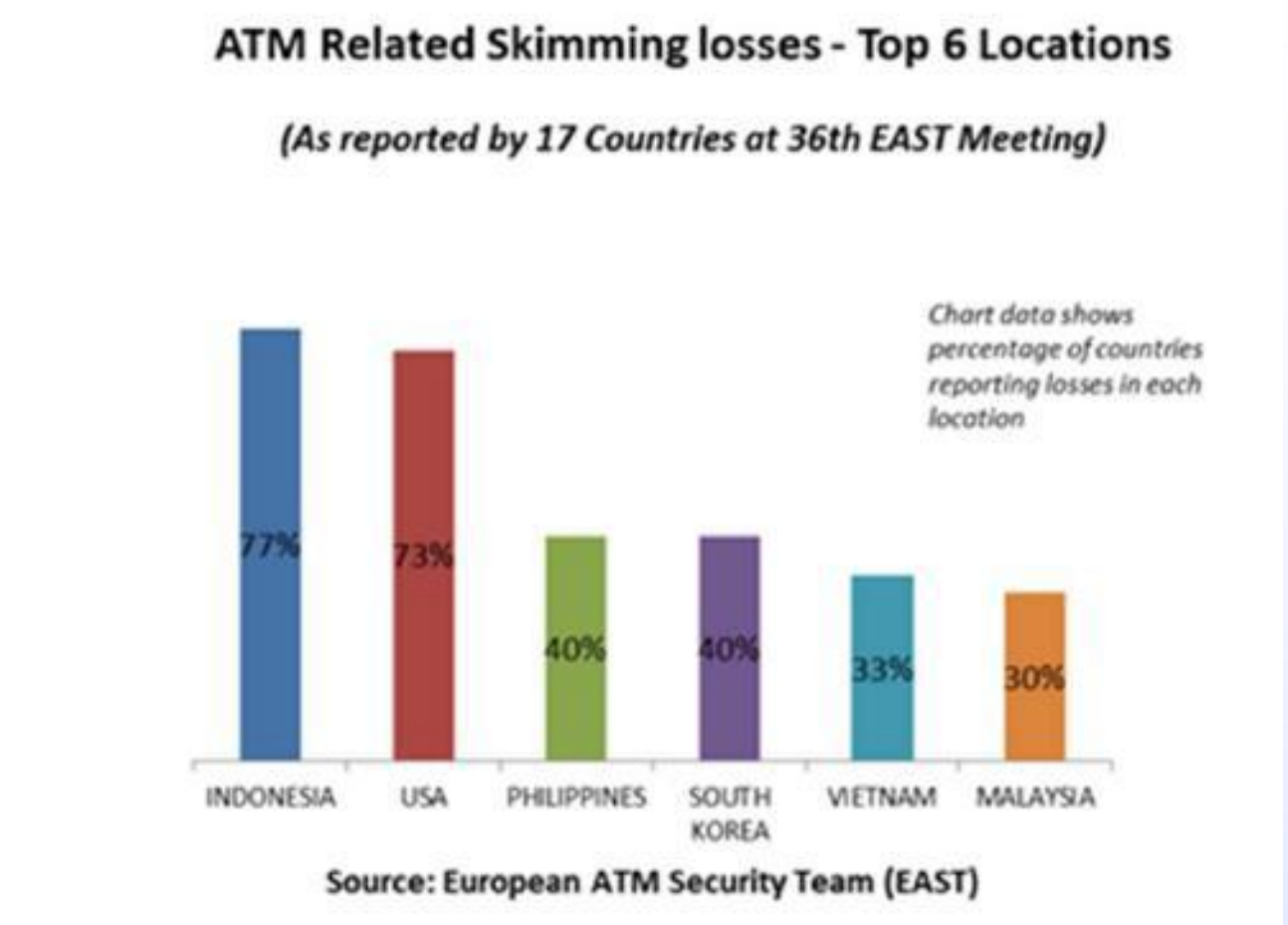
- What is skimming?
- How does it work?
- Several kinds of skimming
- How to prevent?

What is skimming

- Data theft tool
- Hidden inside in cash machine
- Record credit/debit card information
- Capture PIN pad

What is skimming

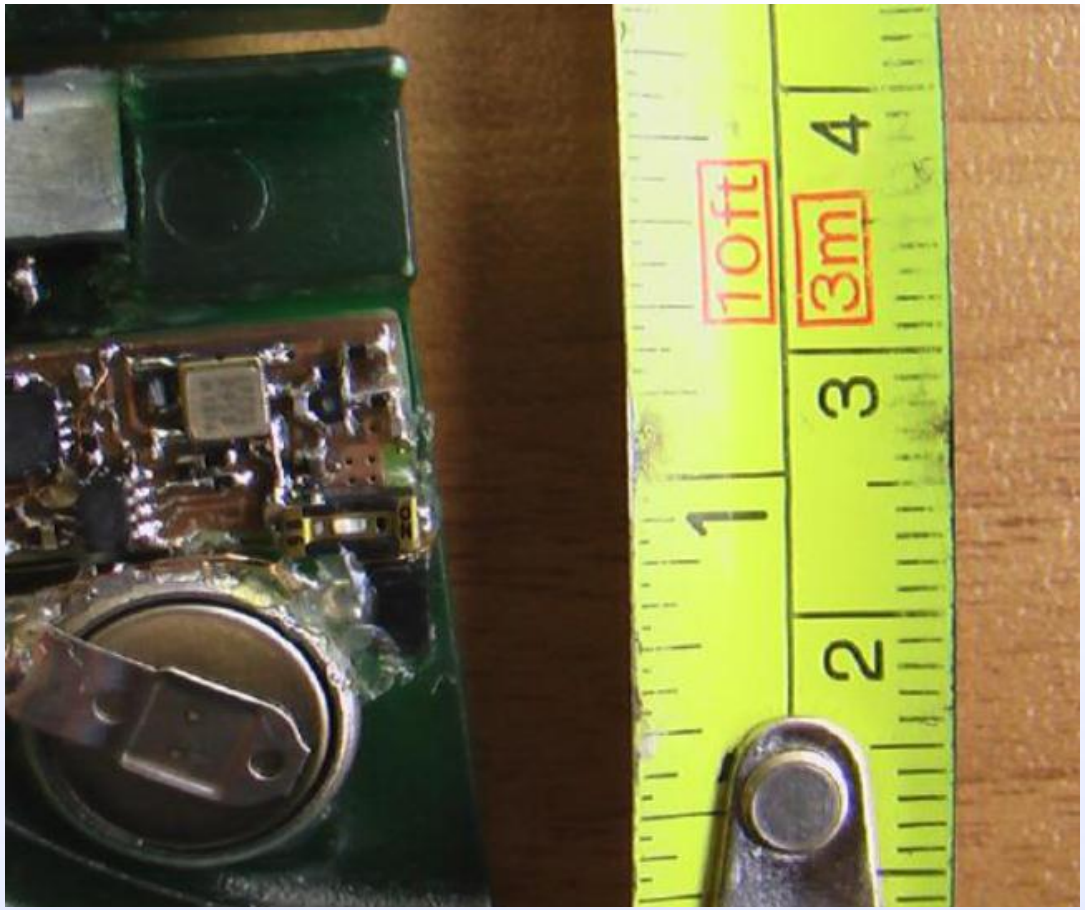
Criminal Trend



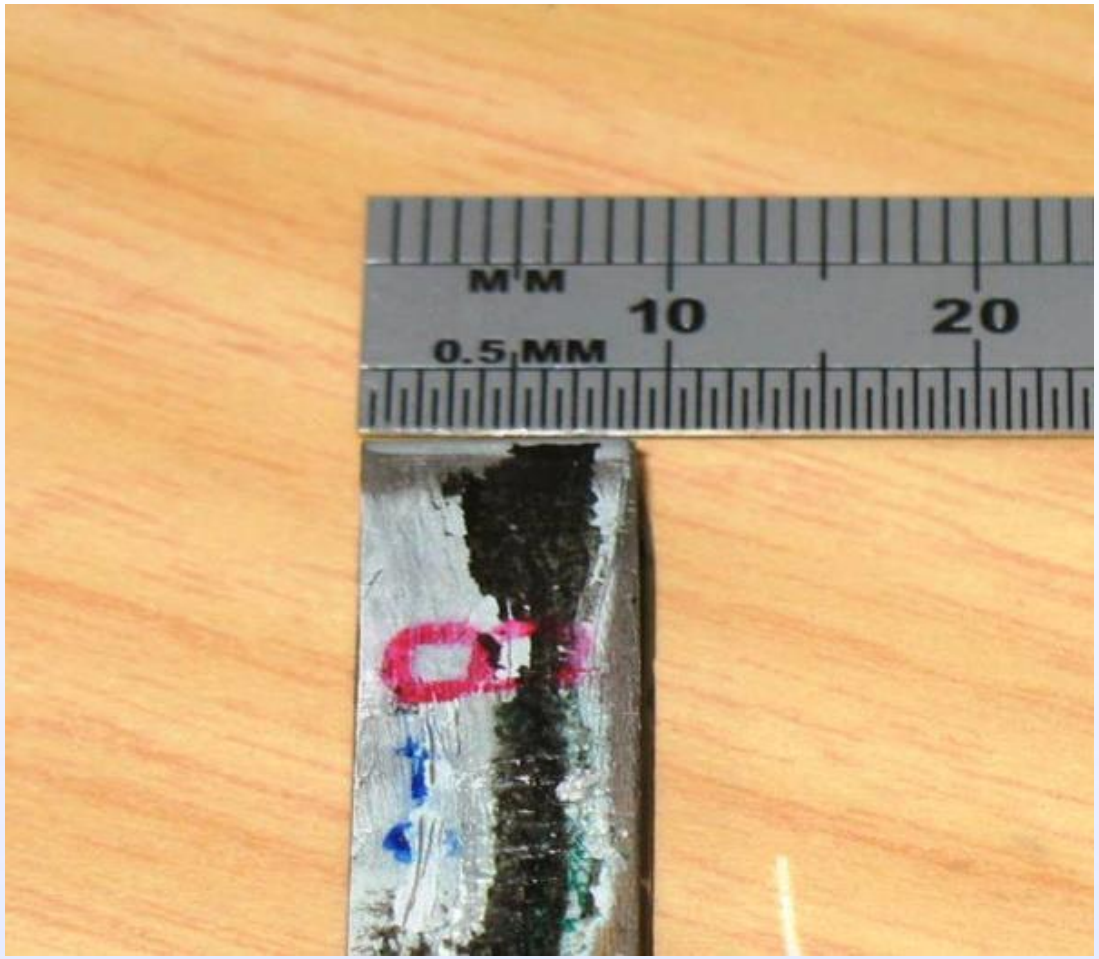
“Traditional” Skimming Attack

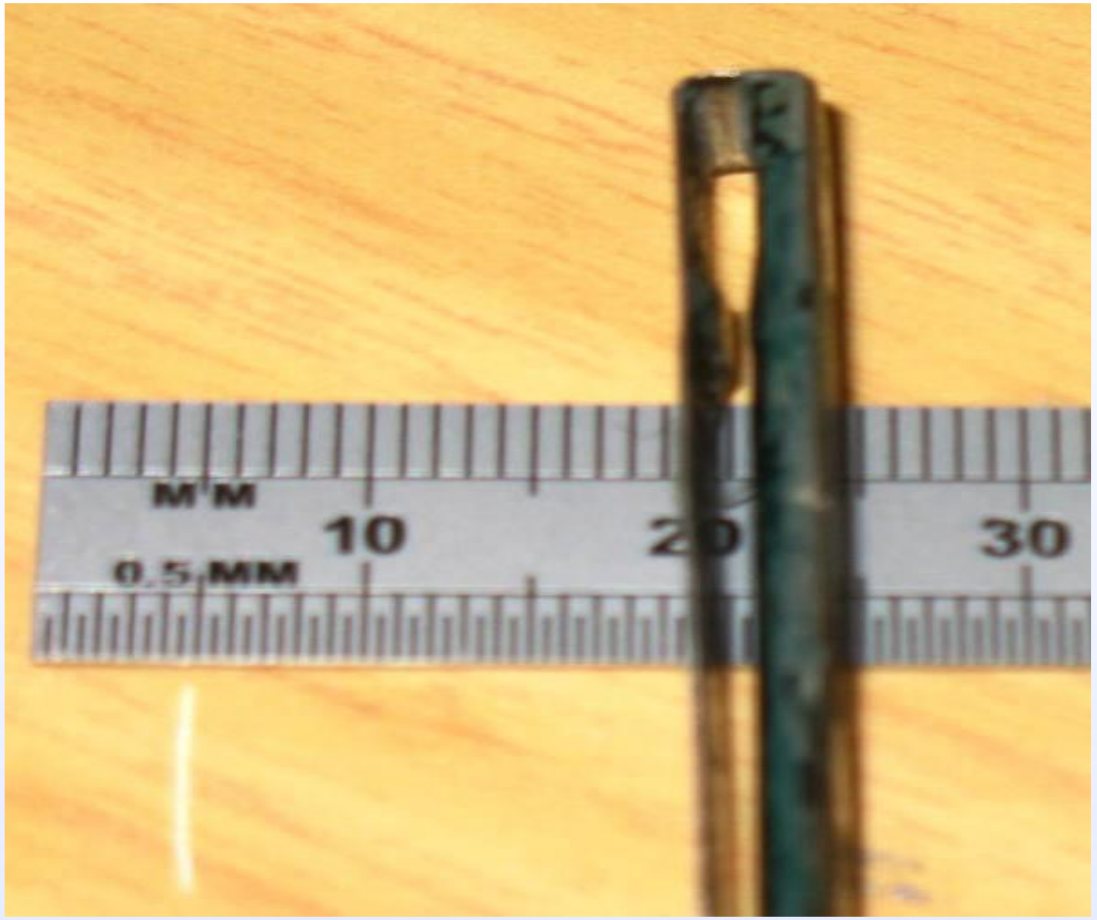
- Skimmer added to fake panel over card slot.
- Skimming pin pad is designed to mimic the pin pad's design and fit over it like a glove
- Camera hidden in fake panel above PIN Pad.

Camera hidden in fake panel above PIN Pad


10ft
3m

It becomes smaller and smaller





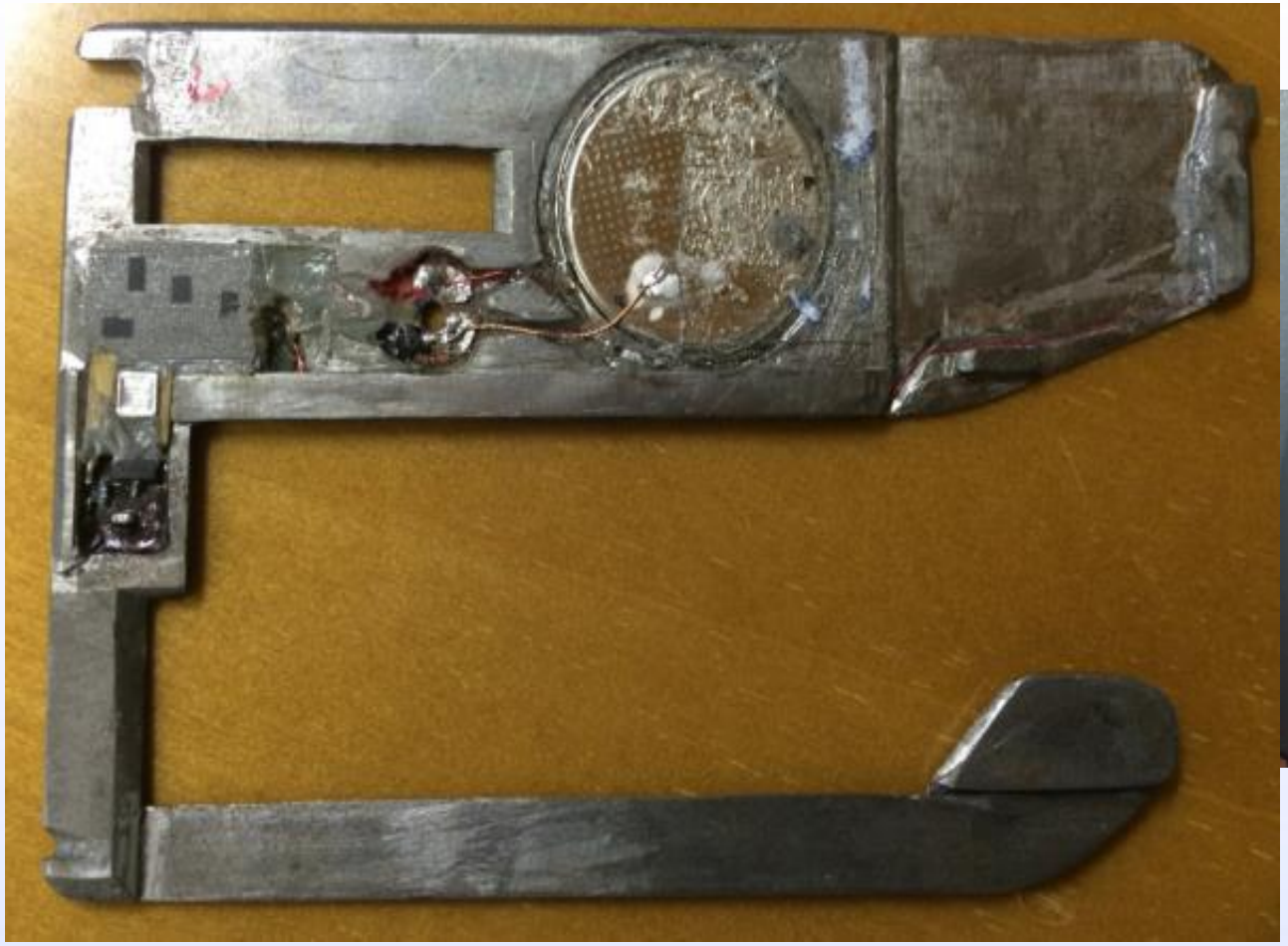
Options of retrieving the captured details

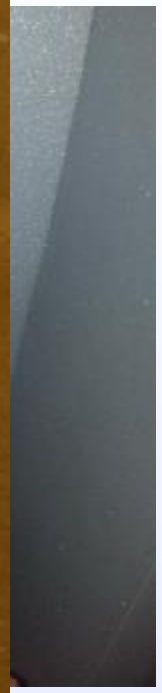
- Control the device remotely through mobile network
- Come physically to remove the device and download the details onto his computer

“Deep” Insert Skimming

- Sits further into the card reader then typical insert skimmers
- Defeat jamming technology
- Devices often transmit card data in real time, not on the board storage

“Deep” Insert Skimming





Software Skimming: Offline Malware Attack

- Insert to Card Reader
- Connector turned through 90 deg.
- Connects to Card Reader USB Connections
- Malware harvests Card and PIN Data
- Allows injection of malware ‘from the street’
- Exploits non-PCI EPP firmware

2. After inserting the fraud device into the reader, turn this handle clock-wise over 90 degree

3. By turning the handle clock-wise over 90 degree, the USB connector is rotated to a more vertical position

1. Direction of inserting the fraud device into the reader

Network Sniffing

- Sniffing device connects inline with network cable
- Device is able to intercept and read all network traffic, including card data
- A separate device is used to capture the PIN
- PIN capture device transmits the PIN to the sniffer

Stereo Skimming

- Record the data used on the magnetic stripe using audio technology.
- Stereo skimming uses 2 separate skimmers wired in differential mode to eliminate the effects of electromagnetic jamming
- Stereo skimming is very hard to defend against using only electromagnetic jamming

PIN capture: Keyboard Overlays

- Fake keyboard placed on top of the ATM's keyboard
- Looks exactly like the real thing so impossible to detect unless you are an expert
- Captures your PIN in real time

PIN capture: Keyboard Overlays

Safeguarding Against Skimming Attacks

Three effective strategies to combat skimming

Migrate from magnetic stripe

- Reduce the counterfeit card risk
- Migrate to EMV chip

Protect the installed base

- While mag stripe is still used, we need effective, active, defended, prevention and detection tools

Identify anomalous behaviour

- If the worst happens and cards are skimmed, we must limit the opportunity for the data to be used

Use of Contactless Card Readers as prevention from skimming risks

Magnetic Stripe Vulnerabilities

- Markets that use magnetic stripe are more vulnerable to counterfeit
- EMV chip cards reduce the risk
- Card skimming still occurs in EMV markets, because the data can be used in non-EMV markets

Contactless Security Benefits

- Eliminates the risk for card data to be skimmed by eliminating the DIP or swipe of the stripe
- Excellent migration properties
- Just one solution reduce the risk

Contactless EMV live today

In November 2014,
ANZ announced a world-first
ATM EMV transaction: 'Tap & PIN'

- ***Faster*** Transaction
- ***Secure*** Contactless Transaction
- Seen as a good way to ***avoid skimming***
- Mobile phone and ATM can communicate in a **secure way**

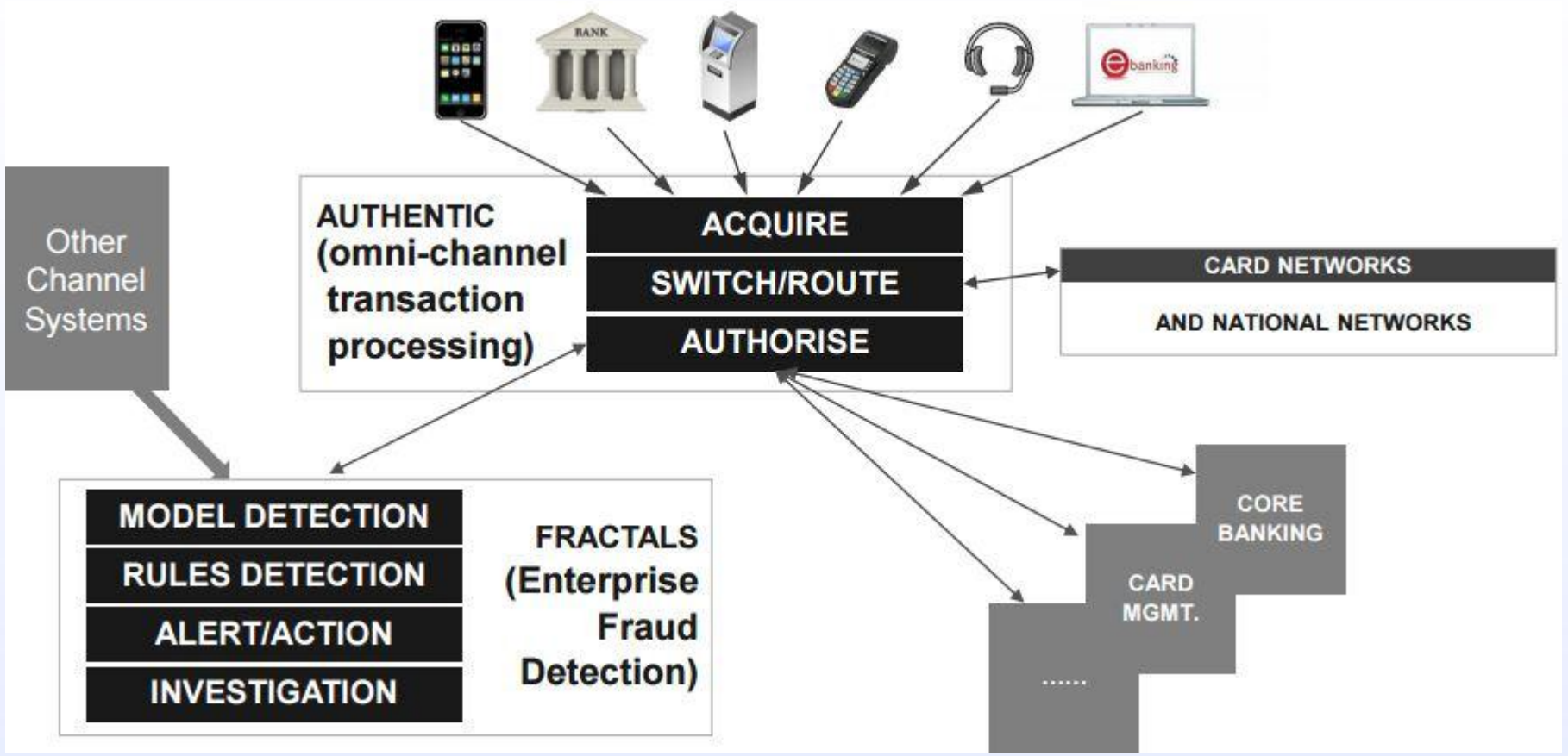
ANZ claims 'world's safest ATM' source .. source Australian Banking and Finance
ANZ to roll out tap and PIN ATM in 2015 .. source ZDnet

Active Anti-Card Skimming

- Prevents skimming through object detection and electromagnetic disruption
- Built in self defence using multiple anti-tamper sensors
- Integration into ATM Software to provide flexible response to attack
- Peripheral defences to prevent side channel attacks

QUICK FACTS	Optimum protection for NCR ATMS	Upgrade kit availability	Available for Motorized and DIP Card readers
	Comprehensive levels of anti-tamper defences	Supported through NCR normal support channels	Downloadable software for ease of flexible response

Transaction Processing and Fraud Detection



here are a few steps we can all take to minimize the success of skimmer gangs.

- Cover the PIN pad while you enter your PIN.
- Keep your wits about you when you’ re at the ATM, and avoid dodgy-looking and standalone cash machines in low-lit areas, if possible.
- Stick to ATMs that are physically installed in a bank. Stand-alone ATMs are usually easier for thieves to hack into.
- Be especially vigilant when withdrawing cash on the weekends; thieves tend to install skimming devices on a weekend — when they know the bank won’ t be open again for more than 24 hours.
- Keep a close eye on your bank statements, and dispute any unauthorized charges or withdrawals immediately.

Q1: WHAT IS ATM SKIMMING?

- A: Skimming is the theft of credit/debit card information by a device placed in, on, or around an ATM.

Q2: How many types of hardware skimming?

- Camera, pin pad overlay, card skimmer

Q3: What is the main point to avoid card skimming?

- Migrate to EMV chip card
- Do not cash out on the unknown or unfamiliar ATM machines