Identifying, Preventing, and Mitigating Skimming Attacks

April 13, 2016

Sylvia Auyeung – Director, Merchant Risk, Visa Inc.
Lester Chan – Director, Merchant Security, Visa Inc.
Charlie Harrow – Solutions Manager, NCR Corp.

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

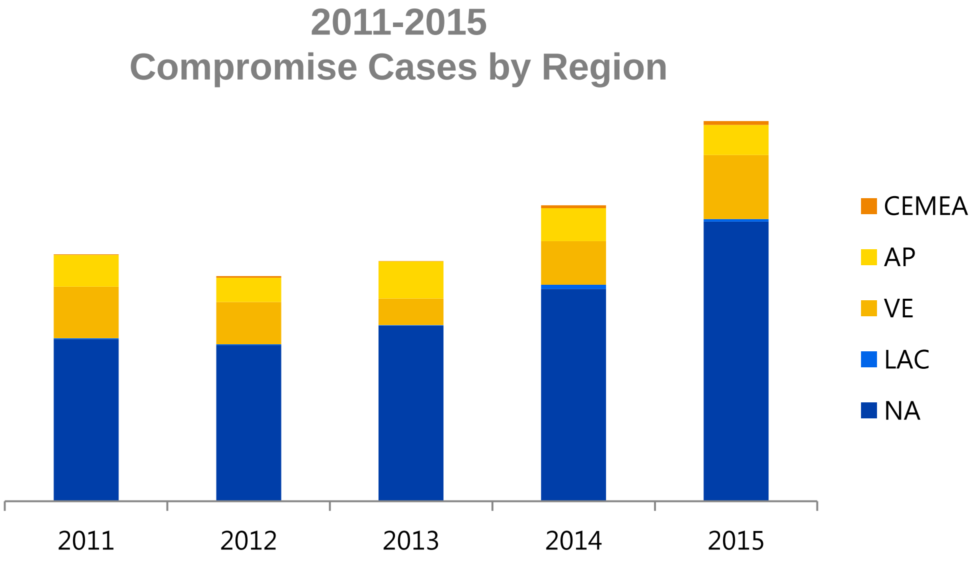
Agenda

- Global Data Compromise Landscape
- Liability Shift and Increase in Skimming Attacks
- Card Skimming – Criminal Trends
- Safeguarding Against Skimming Attacks
- How to Report a Skimming Device
- Key Takeaways
- Resources

Global Data Compromise Landscape

Sylvia Auyeung – Director, Merchant Risk, Visa Inc.

Global Data Compromises



- Global data compromise events are slightly higher in 2015 over those managed in 2014
- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- VE and AP represent the next largest contributors to known breach events, together comprising a quarter of the total
- Breaches in VE and AP are primarily CNP

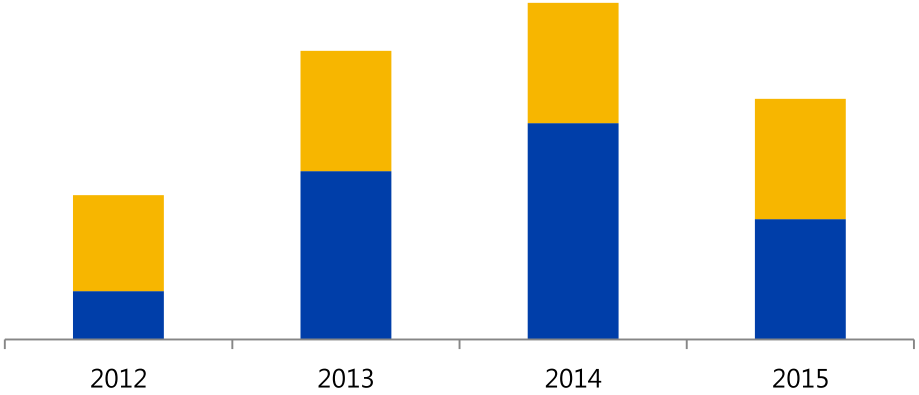
Global Data Compromises

Breach trends by merchant level

Entity Type		2012	2013	2014	2015
		%	%	%	%
	Level 1	<1%	1%	1%	<1%
	Level 2	<1%	1%	1%	<1%
	Level 3	1%	4%	4%	5%
	Level 4	95%	92%	93%	92%
Agent		<1%	1%	1%	2%
Other		2%	<1%	0%	0%
Total		**100%**	**100%**	**100%**	**100%**

- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- At-risk accounts in 2015 were largely attributed to L4 merchants
- Level 4 merchants outnumber L1s in the US

Large breach events (levels 1 & 2)



- Fewer level 1 and 2 breaches in 2015
- Threat actors are targeting smaller interconnected merchants in large numbers
- Restaurants and “other retail” make up the biggest portion of total known breaches
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs

EMV Liability Shift and Increase in Skimming Attacks

Lester Chan – Director, Merchant Security, Visa Inc.

EMV Liability Shift and Counterfeit Fraud

Understanding how the liability shift affects fraud

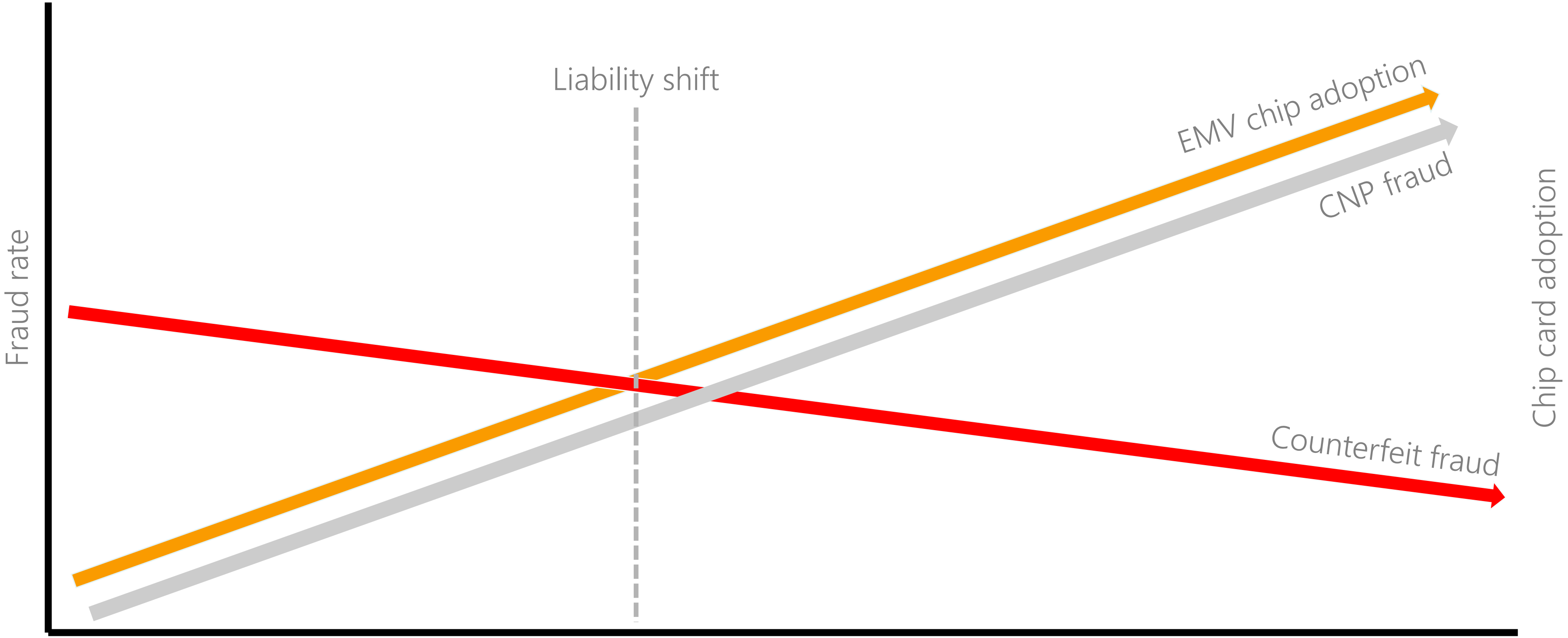
Oct. 2015 U.S. EMV liability shift
(excludes AFD & ATM)

Criminals continue to attack the Payment System to steal and monetize cardholder data

Oct. 2017 U.S. AFD & ATM liability shift

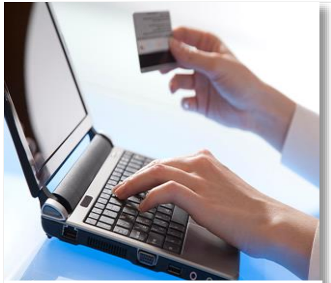
EMV Chip Adoption & Fraud

Fraud will likely migrate to other channels



Fraud Migration to Other Channels

Fraud migrating to e-commerce, automated fuel dispensers, and ATMs



- Fraud and attacks will continue in CNP/e-commerce channels
- Insecure websites and mis-configured security settings
- Internet facing websites getting exploited

- Scan for vulnerabilities
- Be aware of OWASP Top 10
- Work with a qualified integrator/reseller

- AFD EMV liability shift in October 2017
- Stations in remote locations often targeted
- Skimmers and overlays are getting more sophisticated

- Regularly check pumps for devices
- Review POS for overlays
- Know who to contact if known or suspected attack

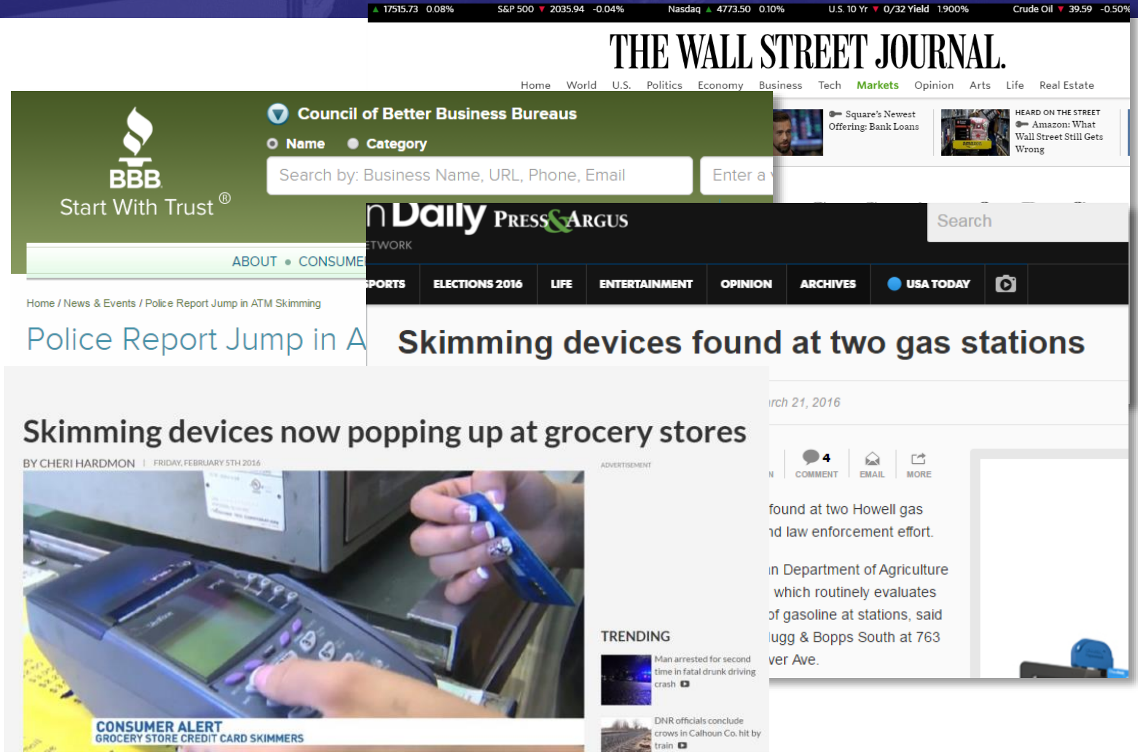
- ATM EMV liability shift in October 2017
- Overlays and cameras are getting more sophisticated
- Remote locations at higher risk

- Regularly check ATMs
- Ensure software is kept up to date
- Know who to contact if known or suspected attack

Rise in Skimming Attacks

Criminals are targeting mag stripe data

- Criminals are shifting their attacks to skimming
- Increase skimming attacks in the news
- Criminals are targeting:
  - Self-checkout terminals at stores
  - Automated fuel dispensers
  - White-label ATMs
- Increasing in sophistication of attacks and technology



▲ 17515.73 0.08% S&P 500 ▼ 2035.94 -0.04% Nasdaq ▲ 4773.50 0.10% U.S. 10 Yr ▼ 0/32 Yield 1.900% Crude Oil ▼ 39.59 -0.50%

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

Square's Newest Offering: Bank Loans

HEARD ON THE STREET
Amazon: What Wall Street Still Gets Wrong

BBB Start With Trust ®

Council of Better Business Bureaus

○ Name ● Category

Search by: Business Name, URL, Phone, Email

Enter a

Home / News & Events / Police Report Jump in ATM Skimming

Police Report Jump in A

n Daily Press & Argus

ETWORK

Search

PORTS ELECTIONS 2016 LIFE ENTERTAINMENT OPINION ARCHIVES USA TODAY

Skimming devices found at two gas stations

rch 21, 2016

found at two Howell gas
nd law enforcement effort.

n Department of Agriculture
which routinely evaluates
of gasoline at stations, said
ugg & Bopps South at 763
ver Ave.

Skimming devices now popping up at grocery stores

BY CHERI HARDMON | FRIDAY, FEBRUARY 5TH 2016

ADVERTISEMENT

CONSUMER ALERT
GROCERY STORE CREDIT CARD SKIMMERS

TRENDING

Man arrested for second time in fatal drunk driving crash

DNR officials conclude crows in Calhoun Co. hit by train

Card Skimming – Criminal Trends

Charlie Harrow – Solutions Manager, NCR Corp.

Card Skimming: Trends

ATM Related Skimming losses - Top 6 Locations

(As reported by 17 Countries at 36th EAST Meeting)

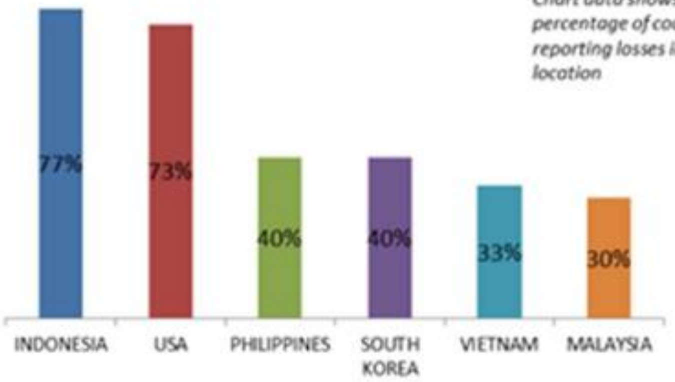


Chart data shows percentage of countries reporting losses in each location

Source: European ATM Security Team (EAST)

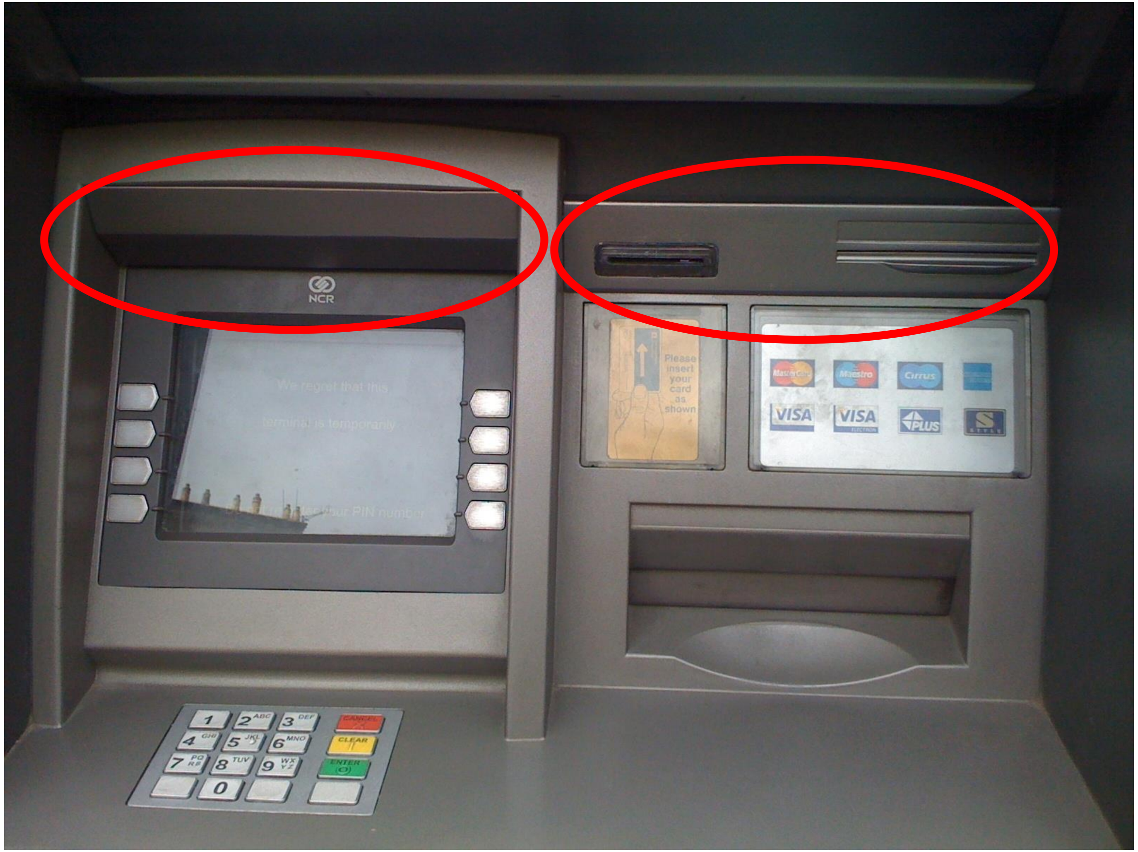
Skimming continues to be the #1 cause of fraud loss on ATMs.

- **Criminal techniques have grown increasingly sophisticated**
- **Criminal techniques have diversified to avoid anti-skimming defences**
- **An arms race has taken place**
  - **Industrialisation**
  - **Avoidance techniques**
  - **Sabotage**
  - **Side Channels**

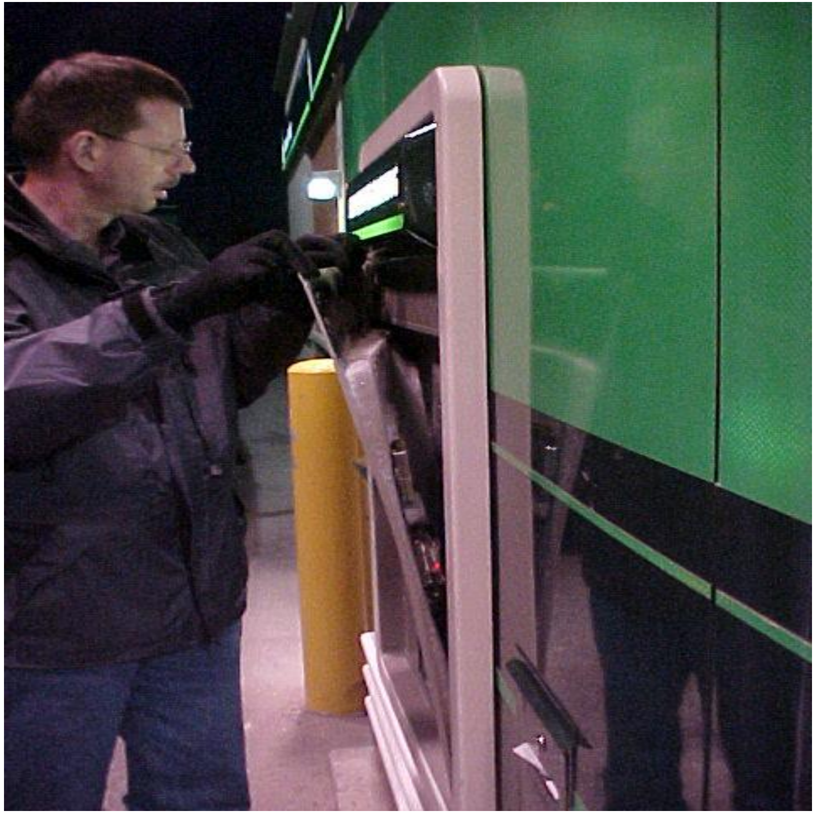
“Traditional” Skimming Attack

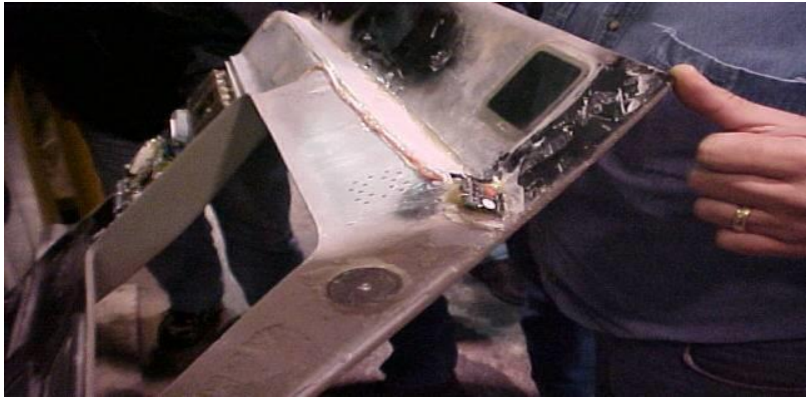
Skimmer added to fake panel over card slot.

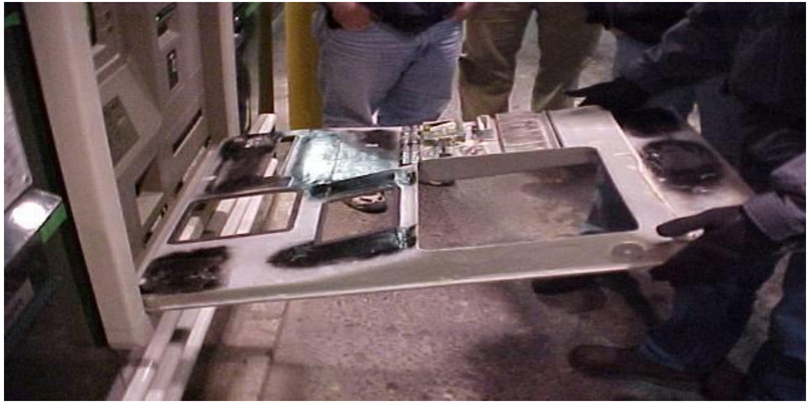
Camera concealed in fake panel above PIN Pad.



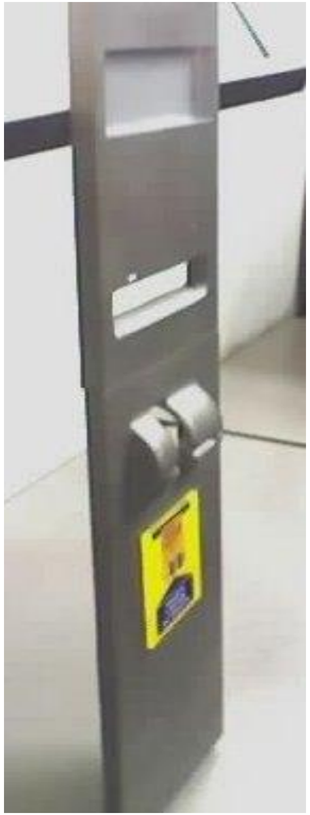
Skimming History: full fascia overlays…

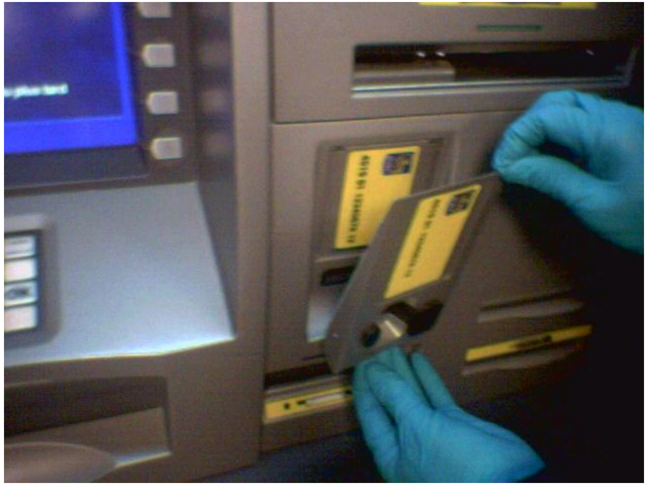


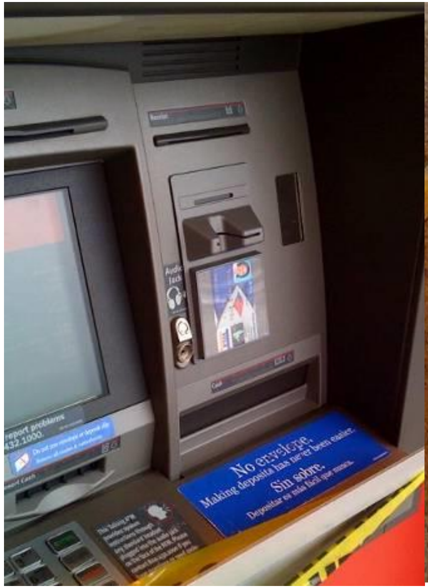


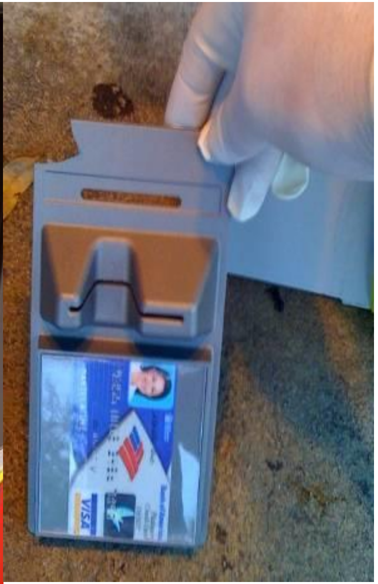


Getting smaller….





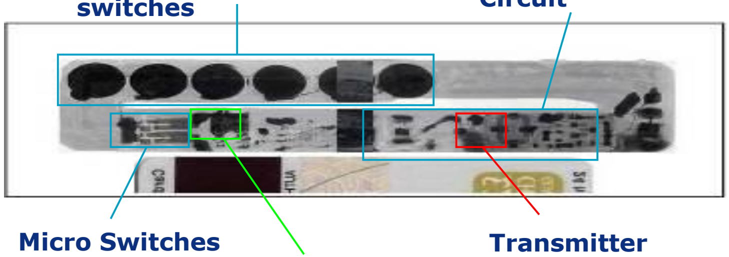

No envelope.
Making deposits has never been easier.
Sin sobre.
Depositar es más fácil que nunca.



Getting smaller….

No envelope.
Making deposits has never been easier.
Sin sobre.
Depositar es más fácil que nunca.

Smaller….



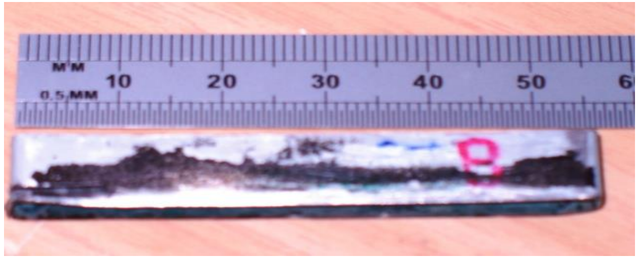
Six small batteries connected to micro switches

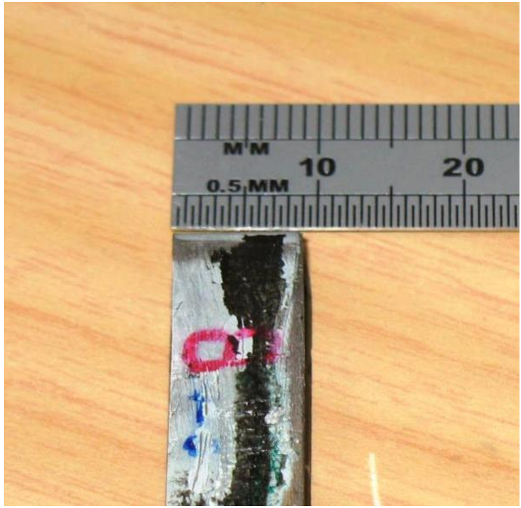
Transmitter Circuit

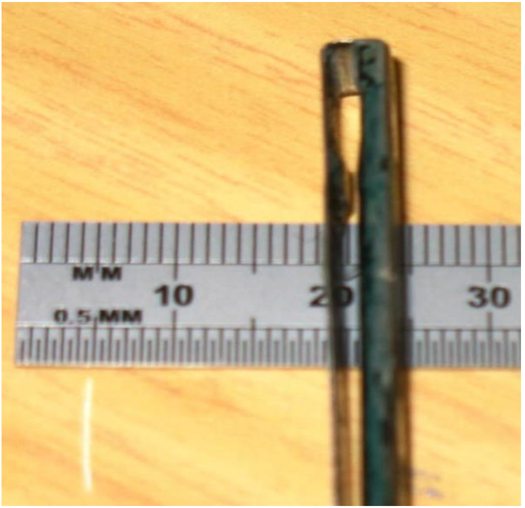
Micro Switches

Magnetic Read Head

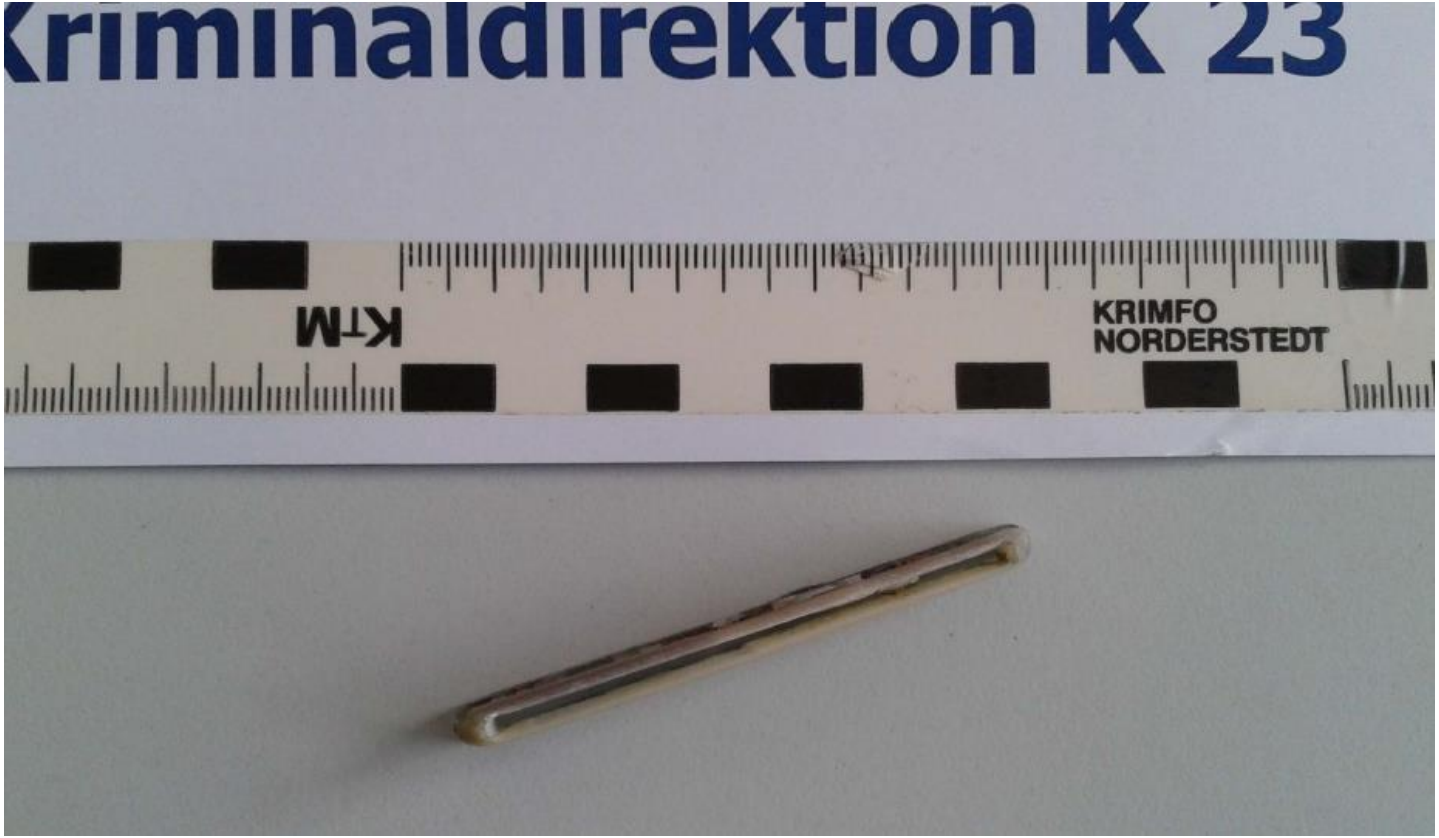
Transmitter Antenna



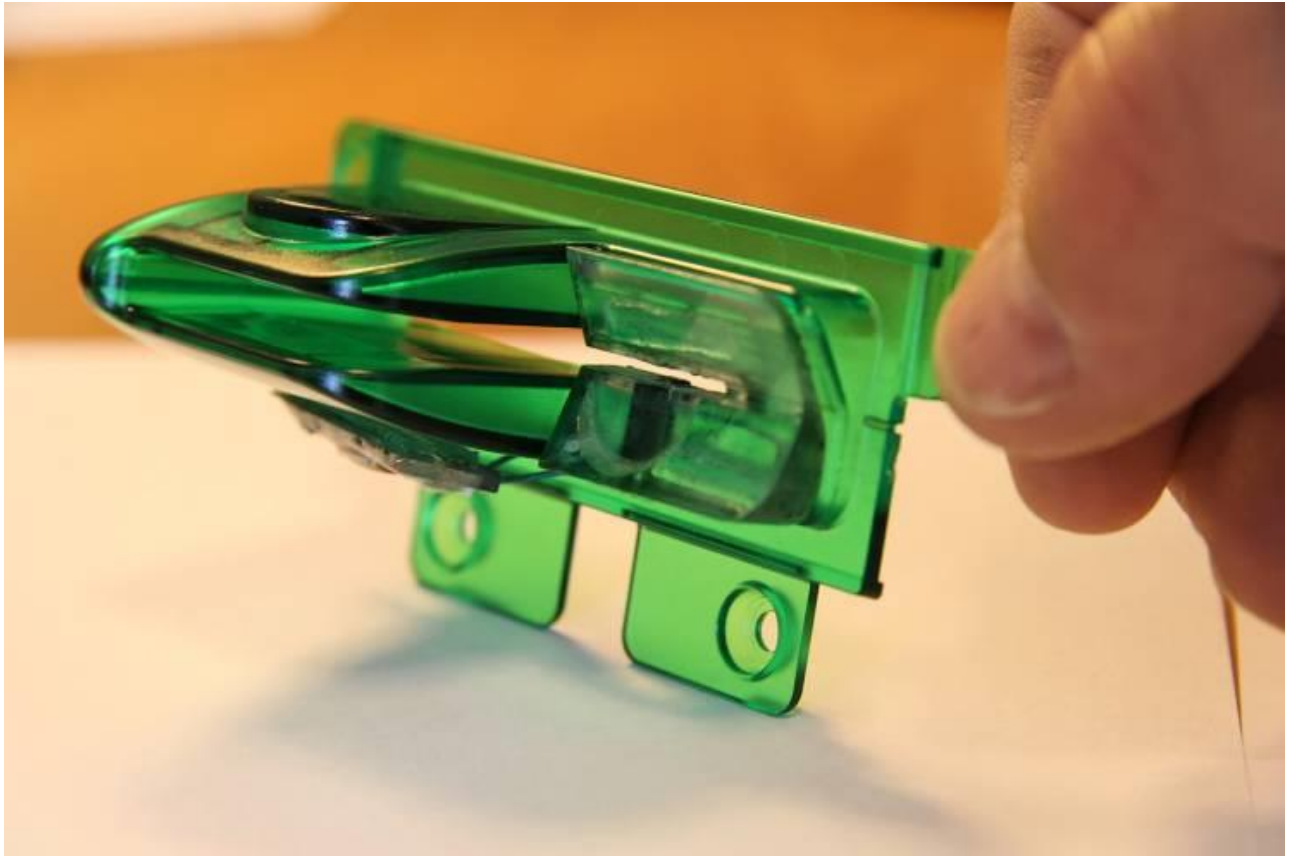




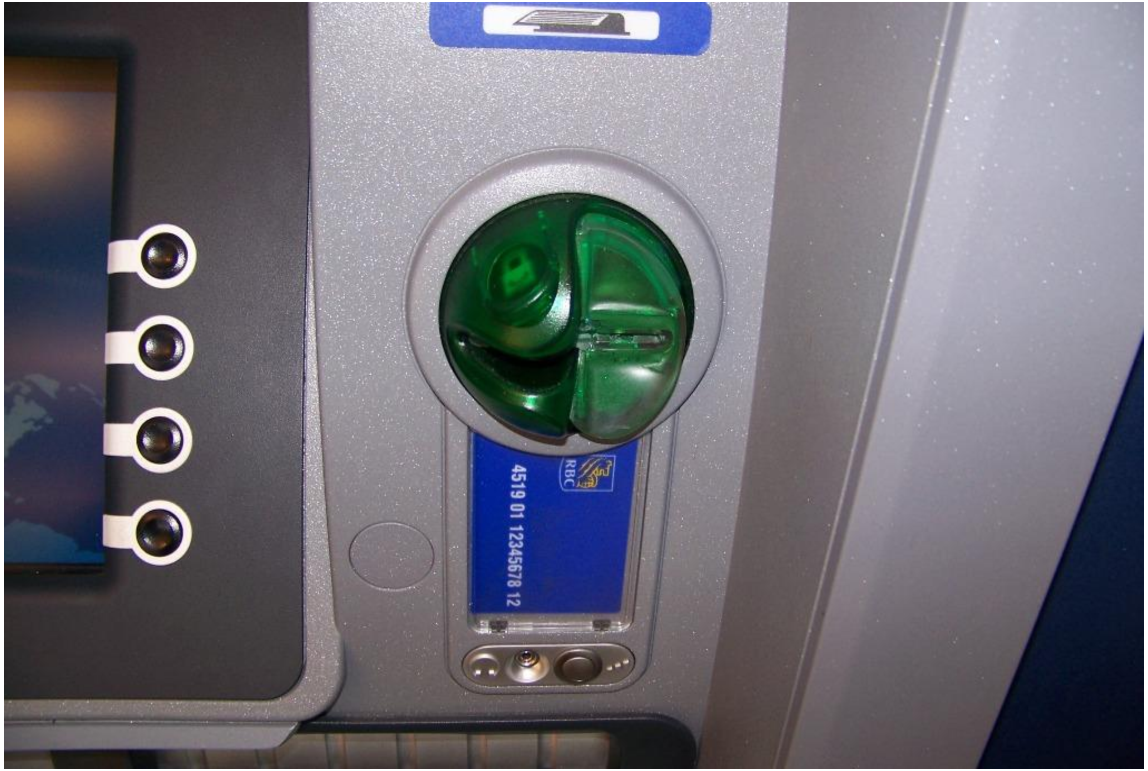
Smallest: Insert Skimmer, Germany



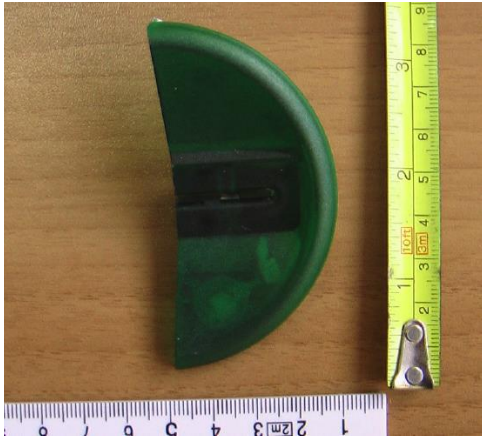
Bypassing Passive Protection

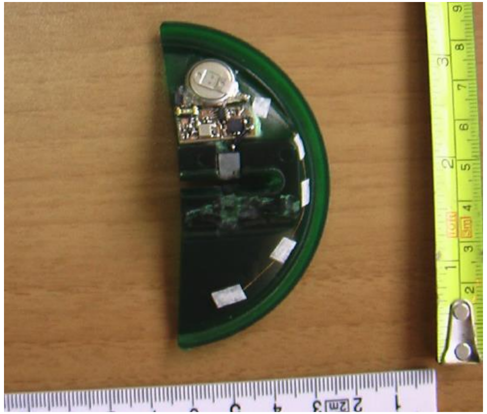


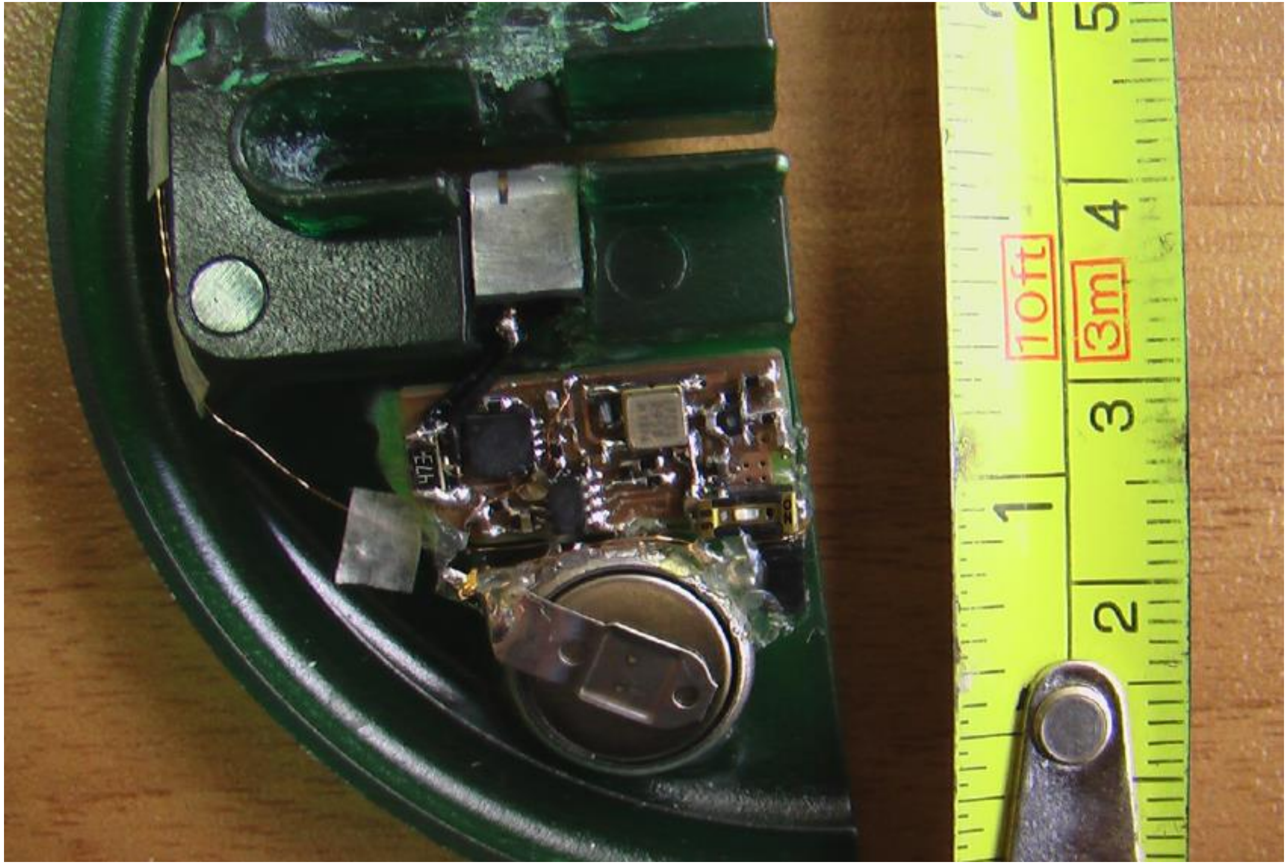
Bezel Overlay Skimmer - Canada



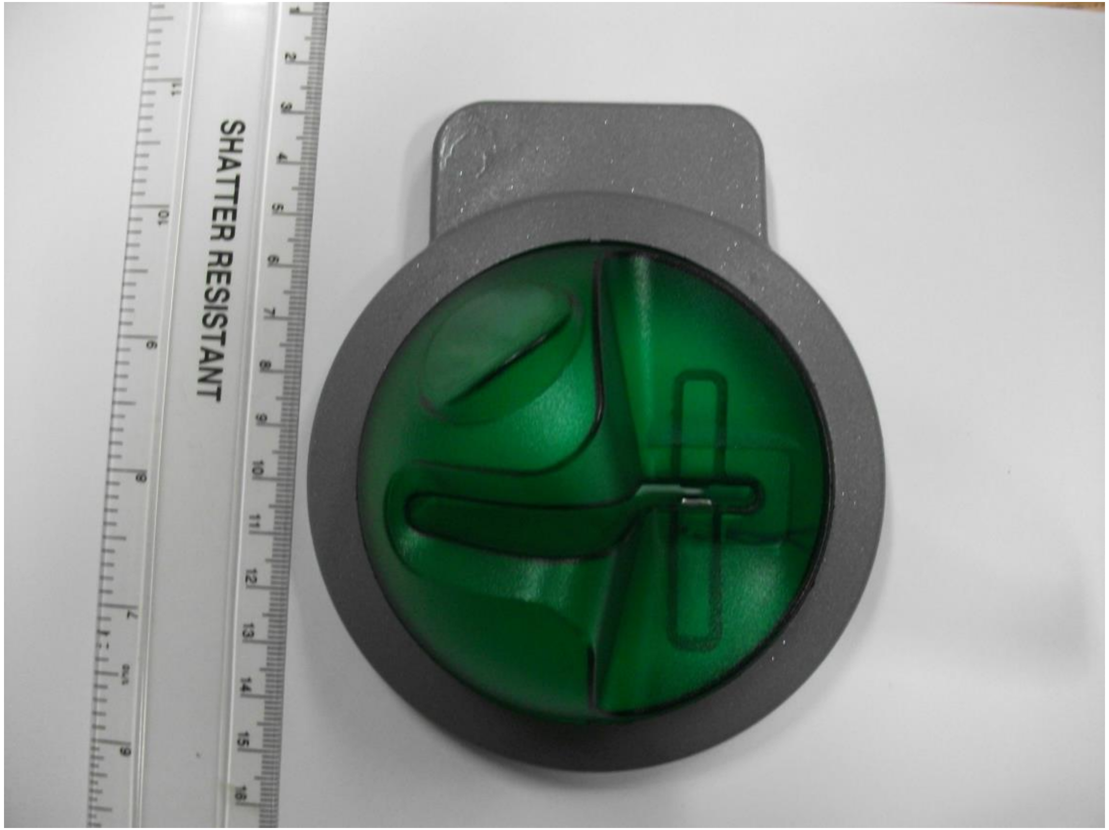
Bulgaria

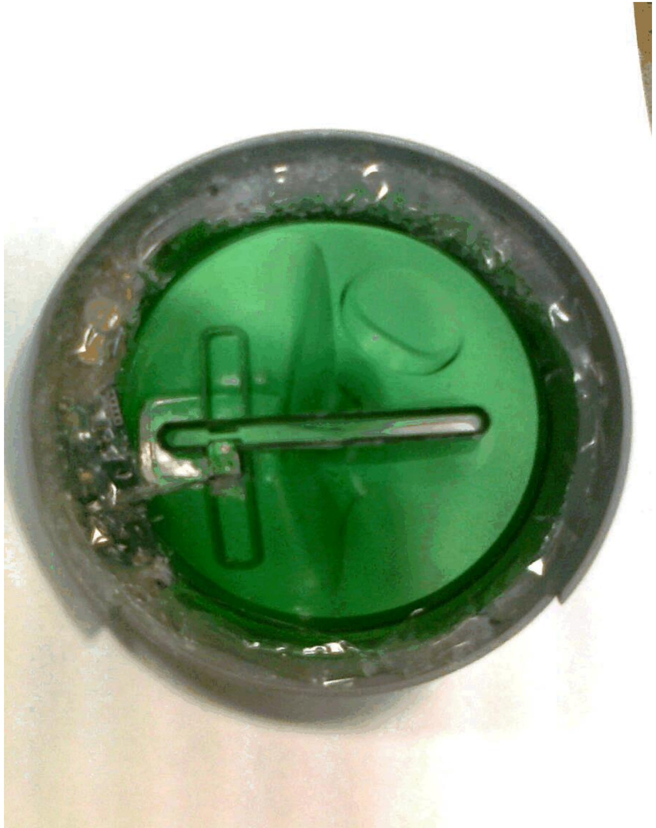




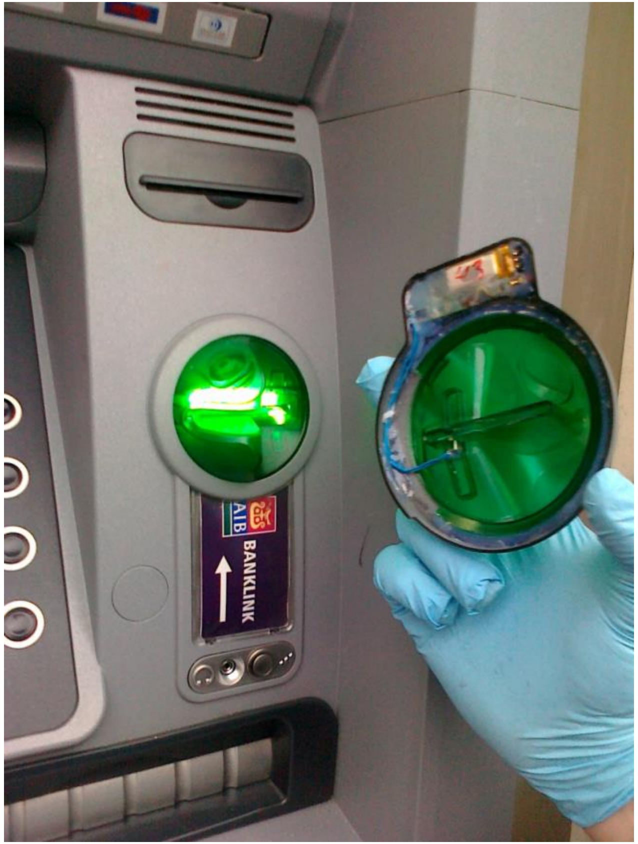


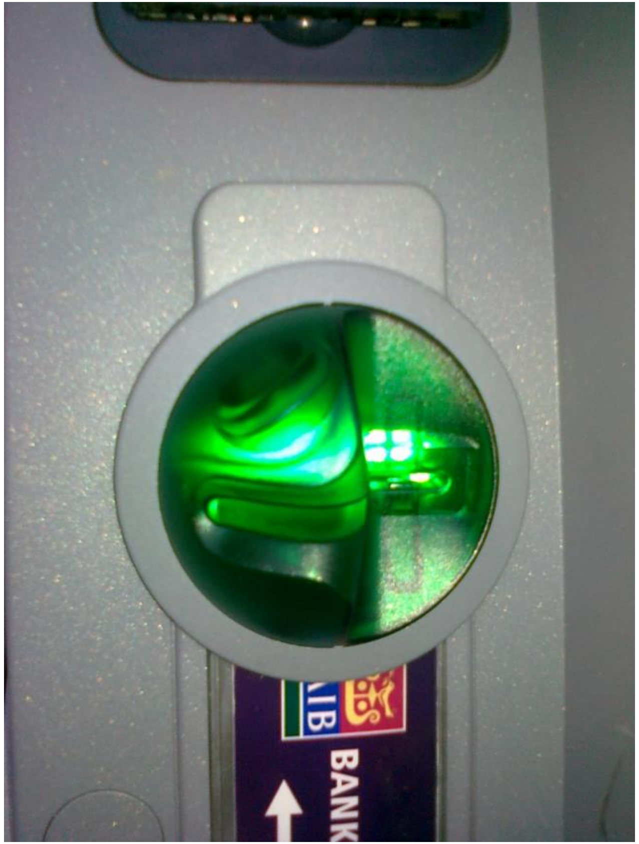
Skimming - Ireland



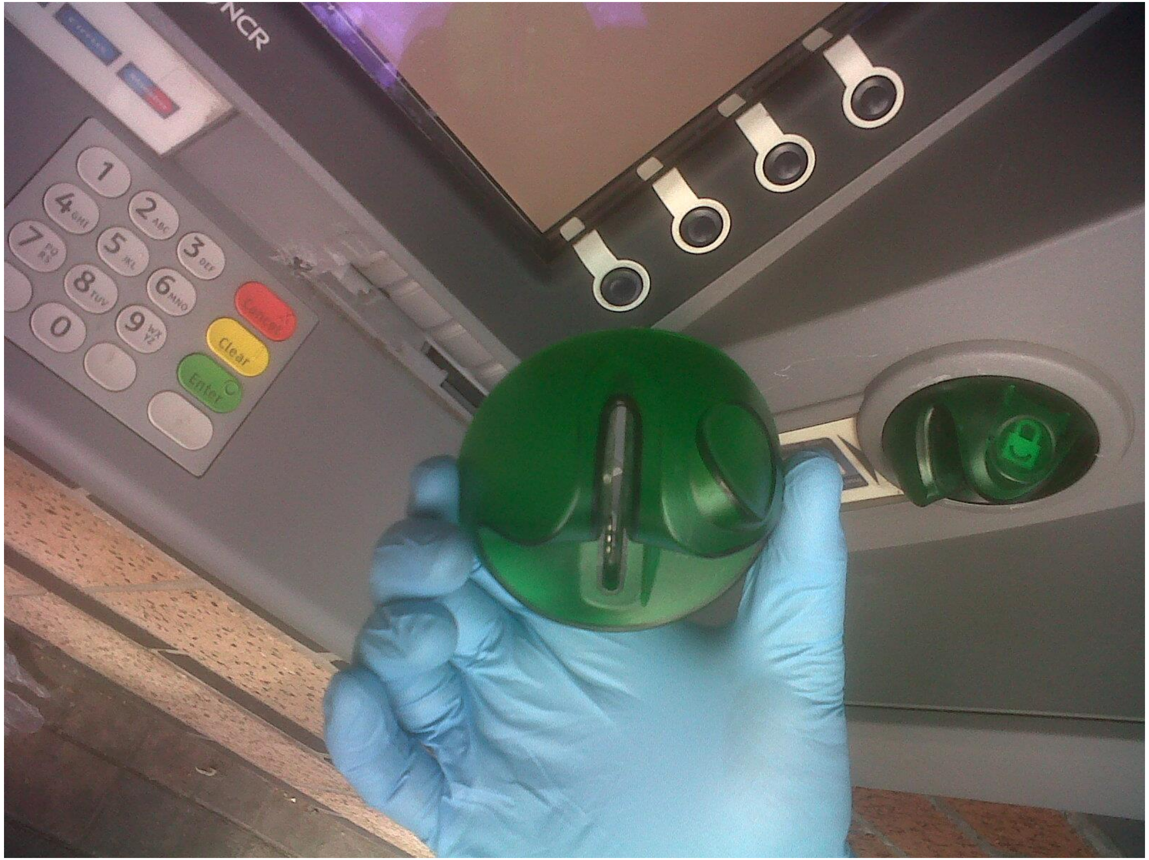


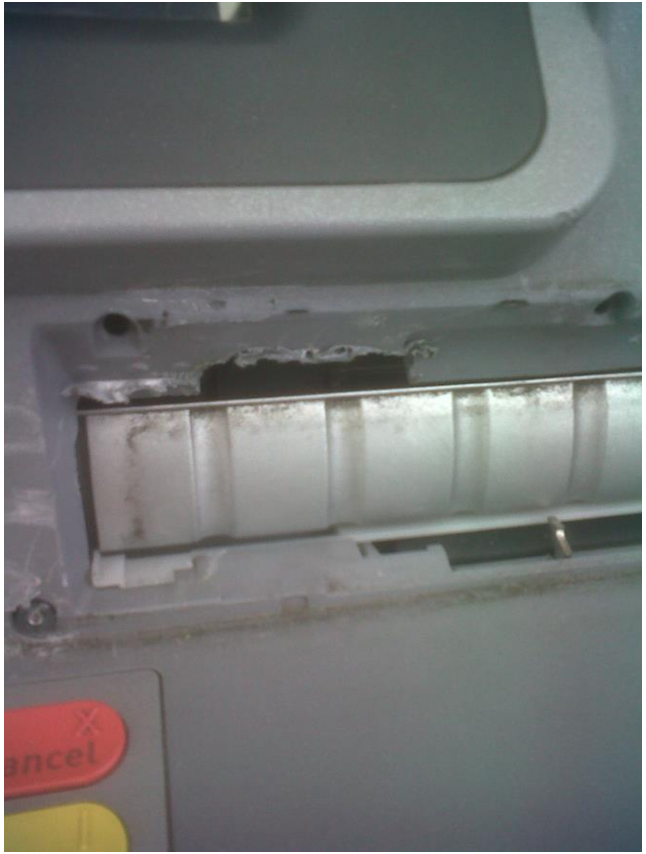
Skimming - Ireland



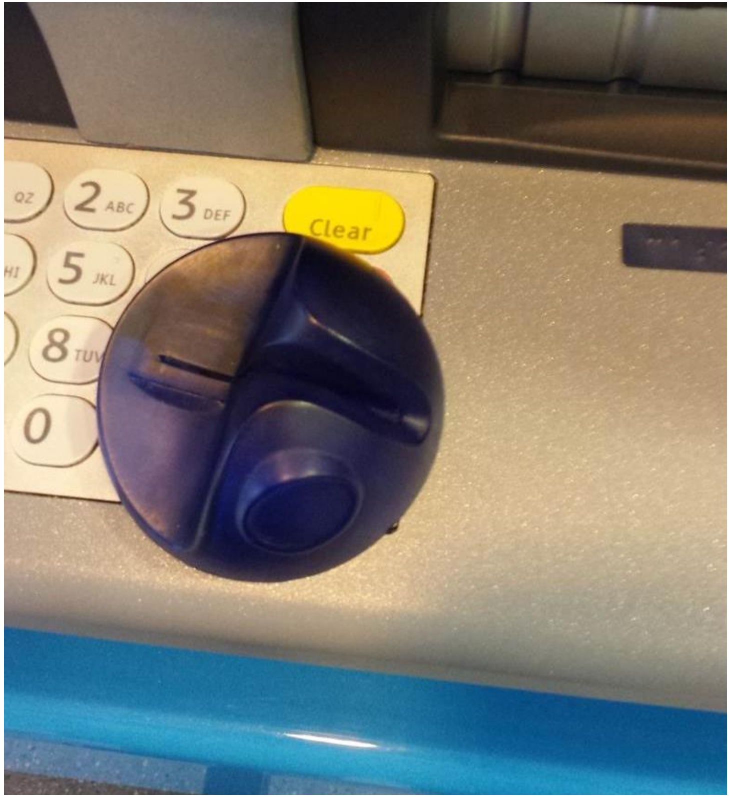


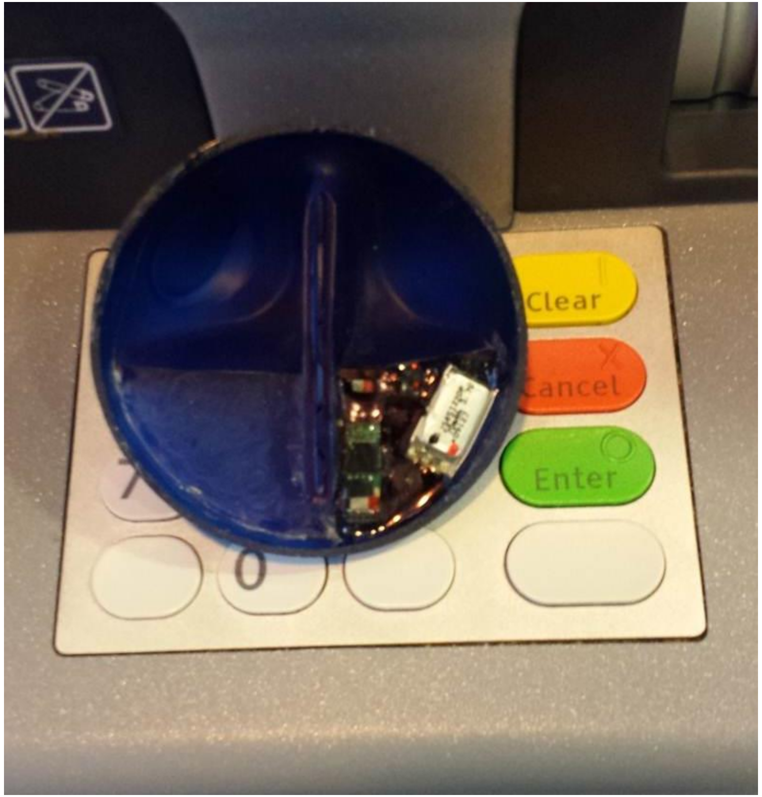
Skimming – UK


NCR
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Cancel
Clear
Enter

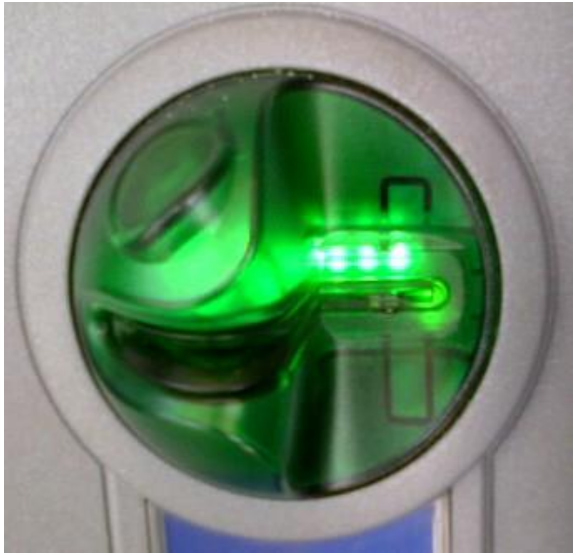

ancel

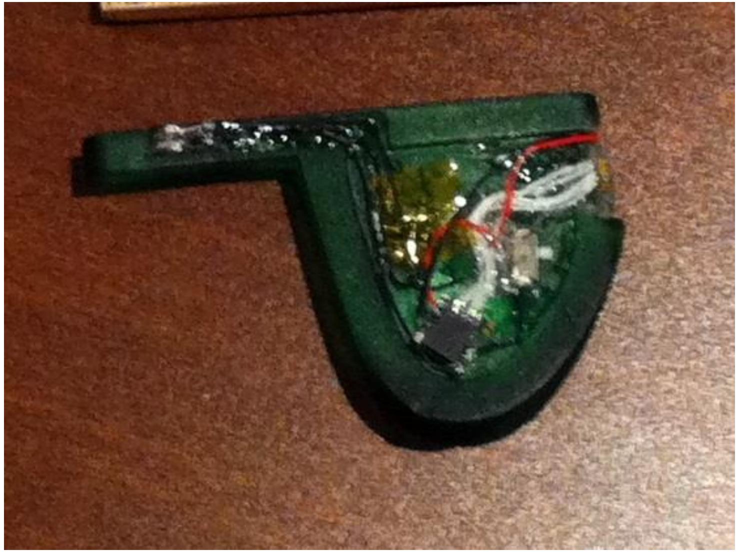
Australia

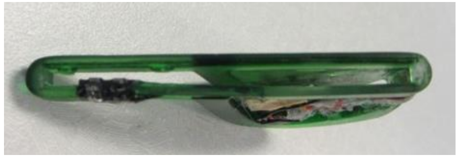


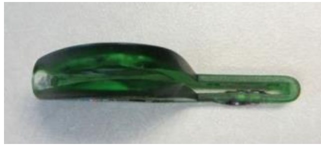


Insert Skimmers

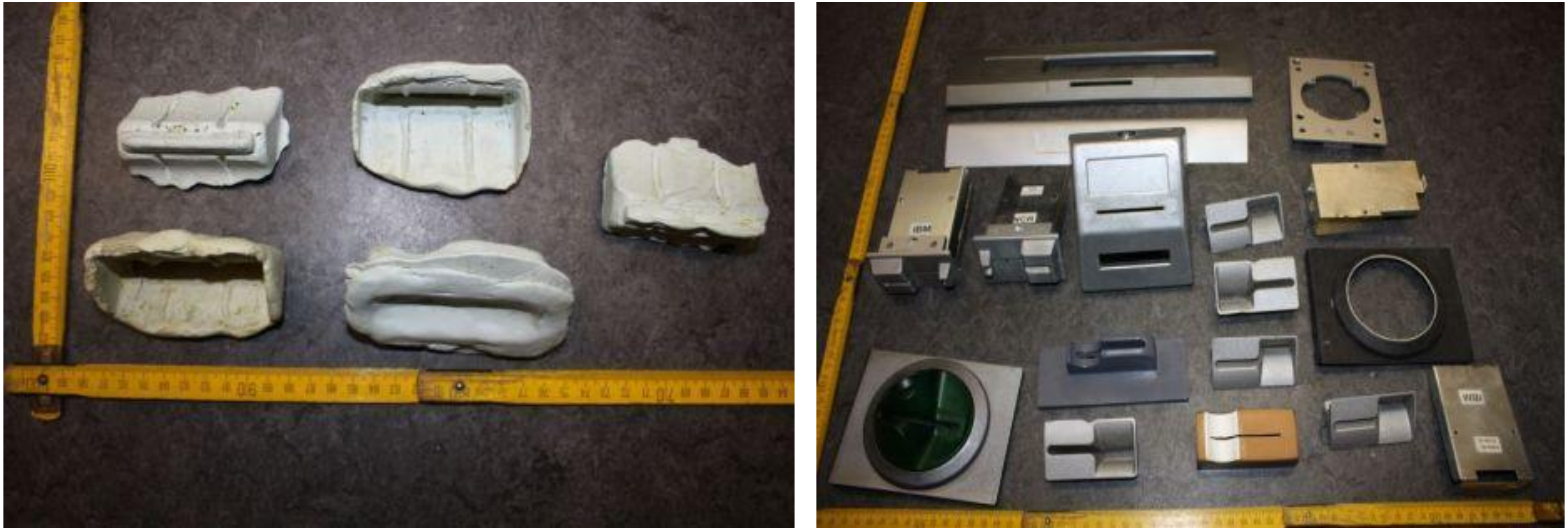






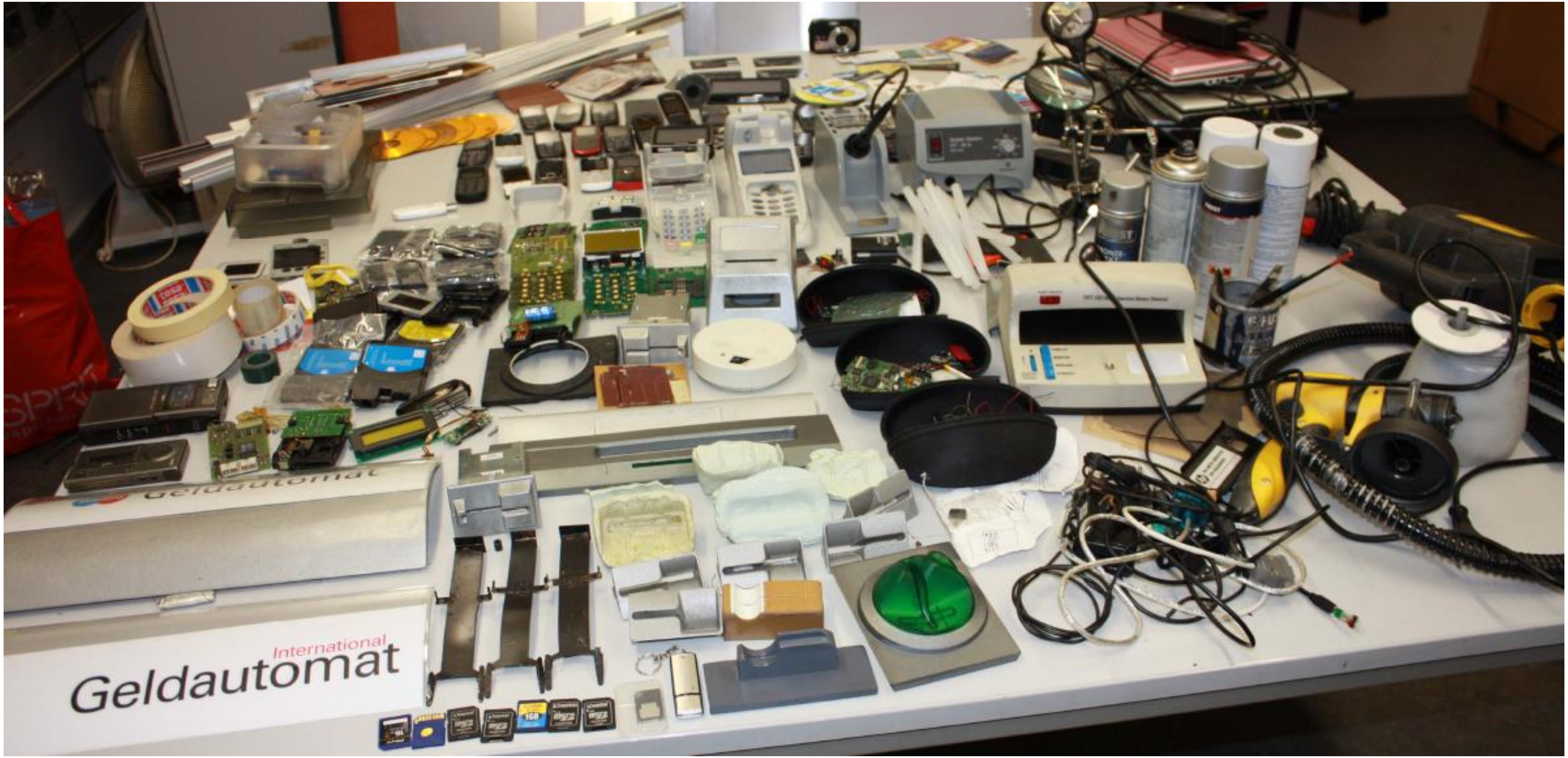


Criminal Lab Raid: Germany

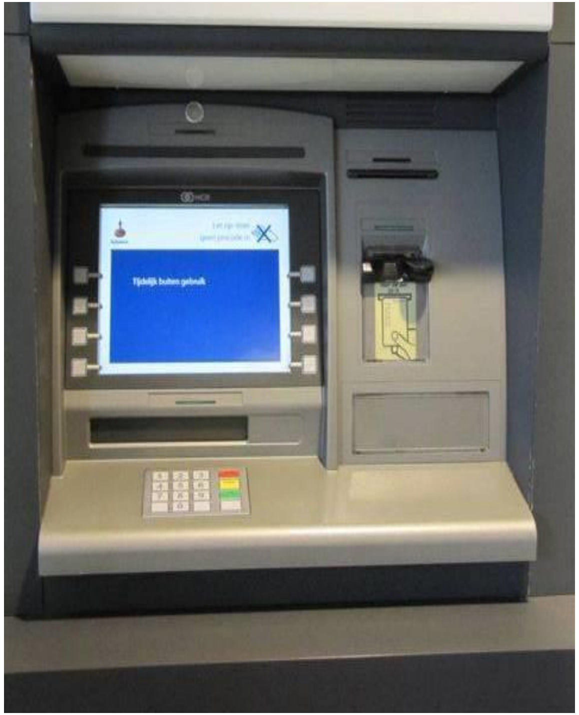


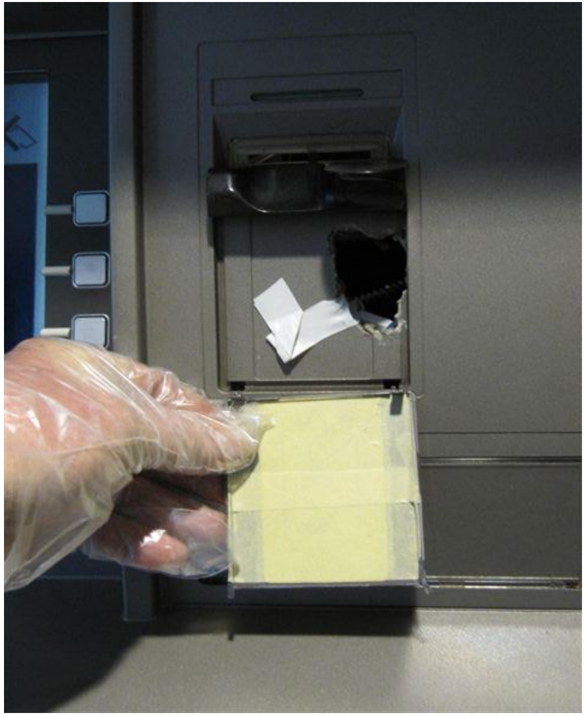
Card Reader Moulds and Surrounds

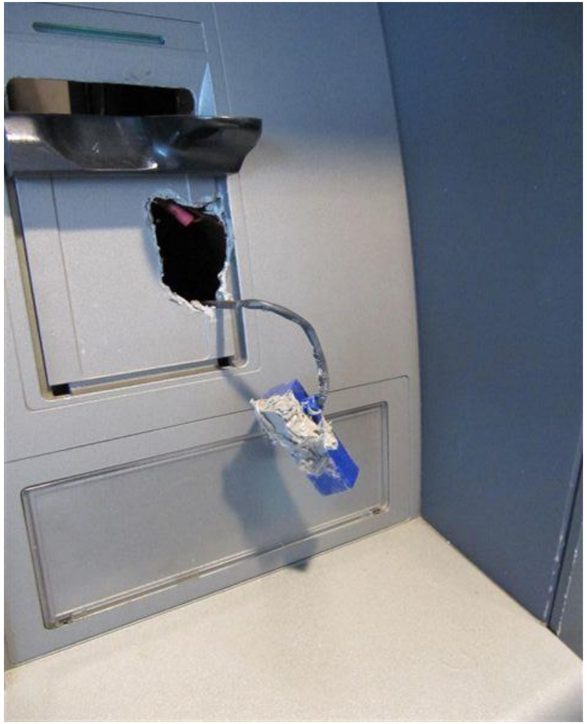
Criminal Lab Raid: Germany



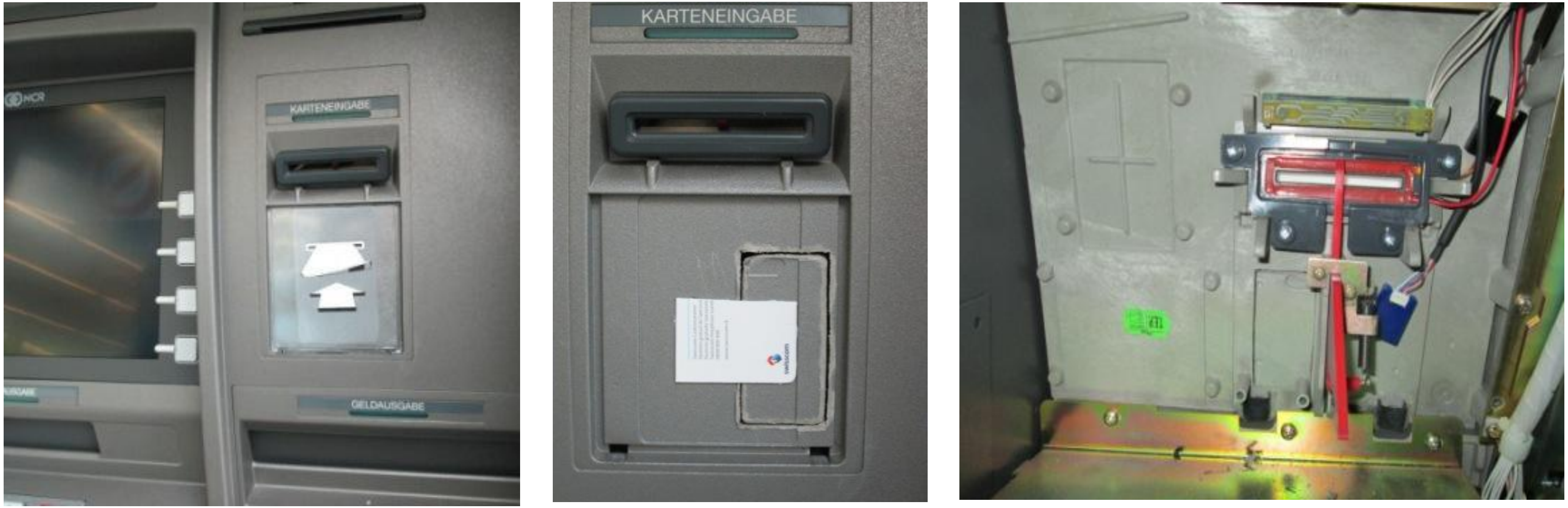
Bypassing Active Prevention





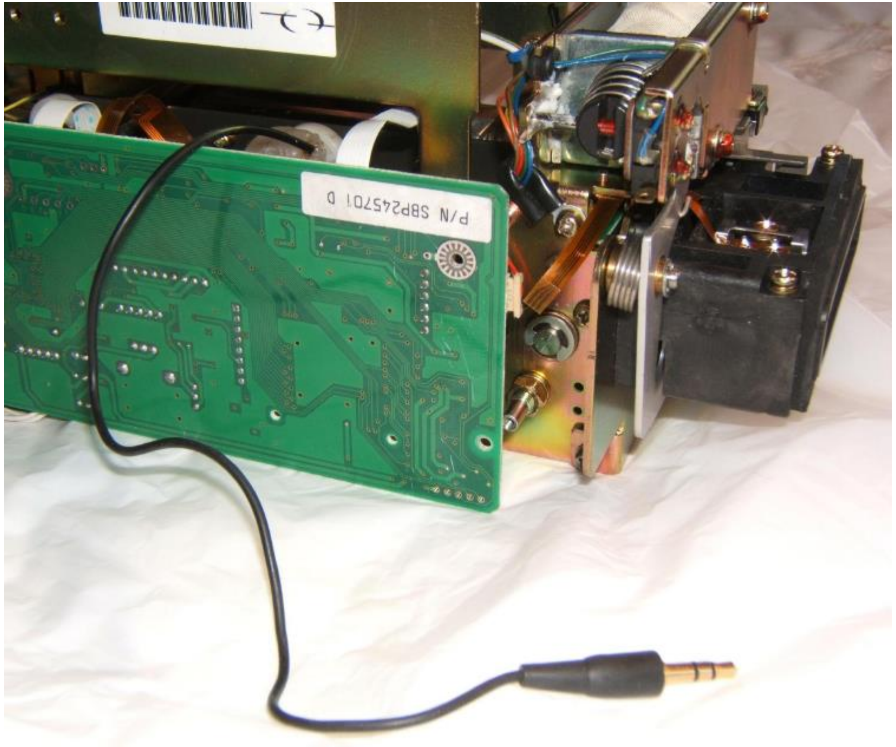


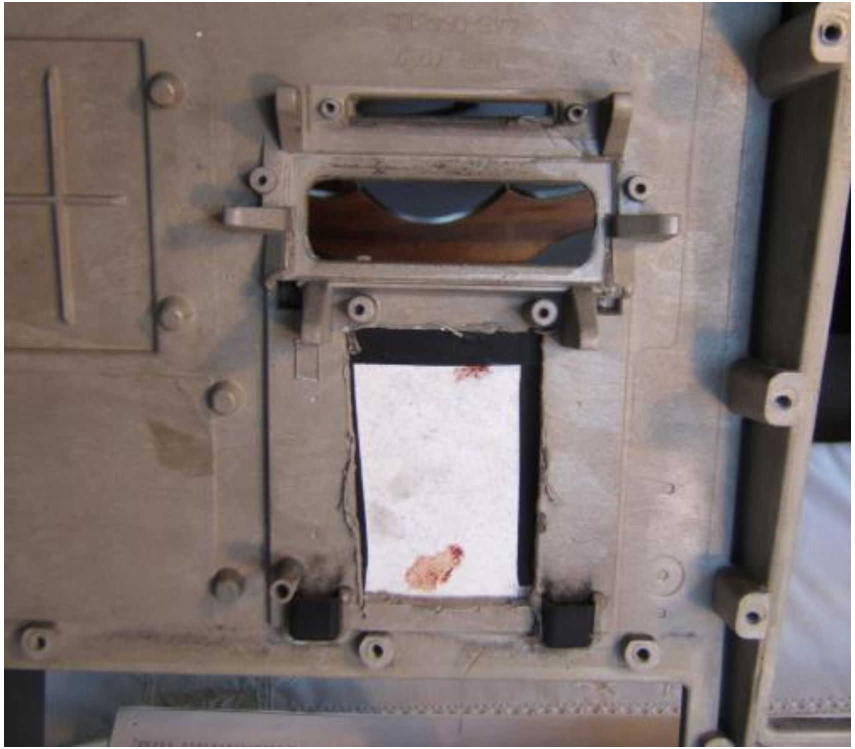
Fascia penetration



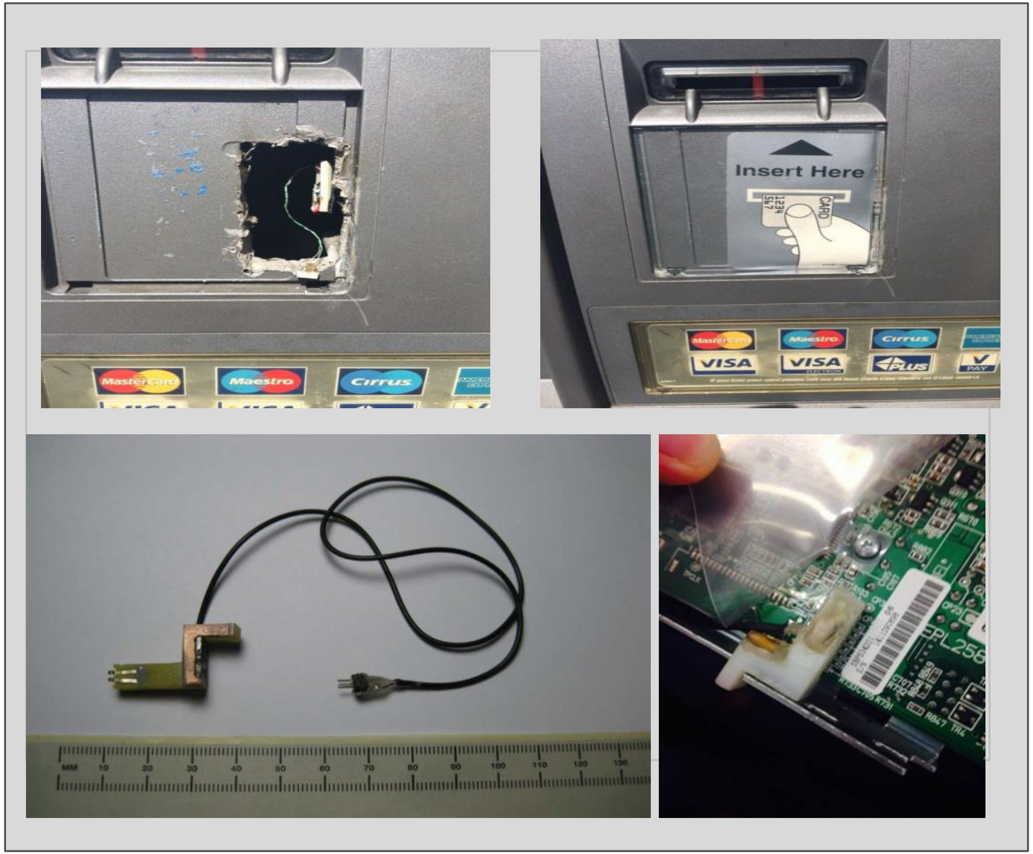
Switzerland

Ireland – Internal Attacks





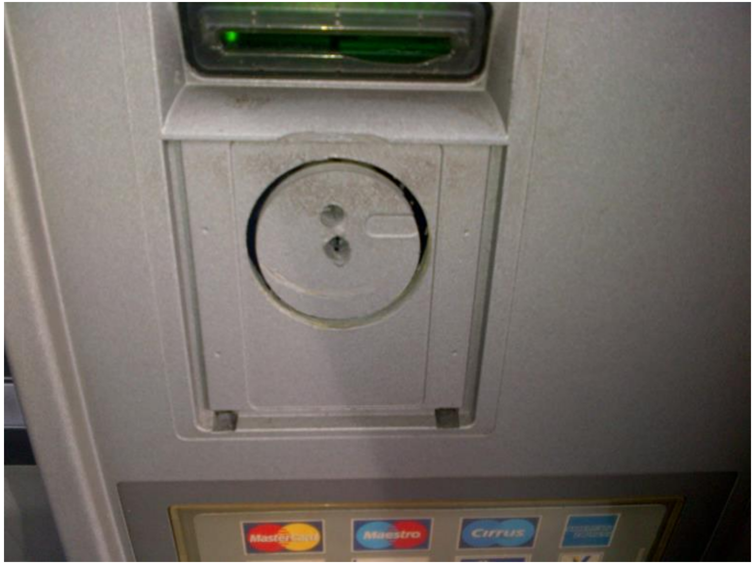
Eavesdropping attacks expanding



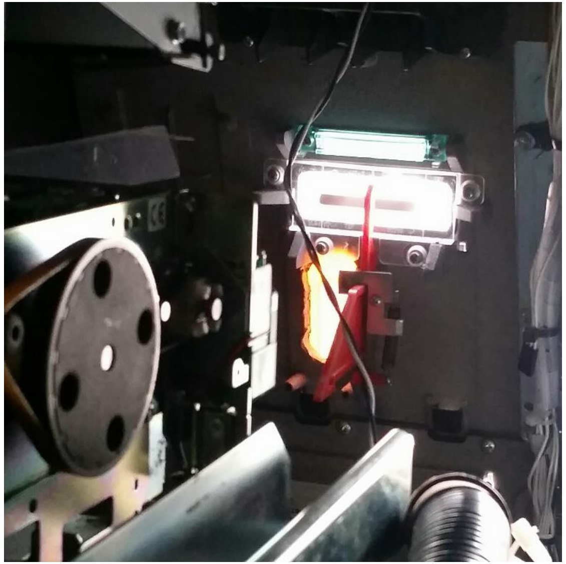
- Create hole in Fascia, typically under card orientation window
- Attach to control electronics within card reader module
- Fascia break-through “naturally” hidden
- Impact as per “traditional” skimming
- Different styles of eavesdropping device observed.

Eavesdropping - Global Expansion

- Attacks continuing globally

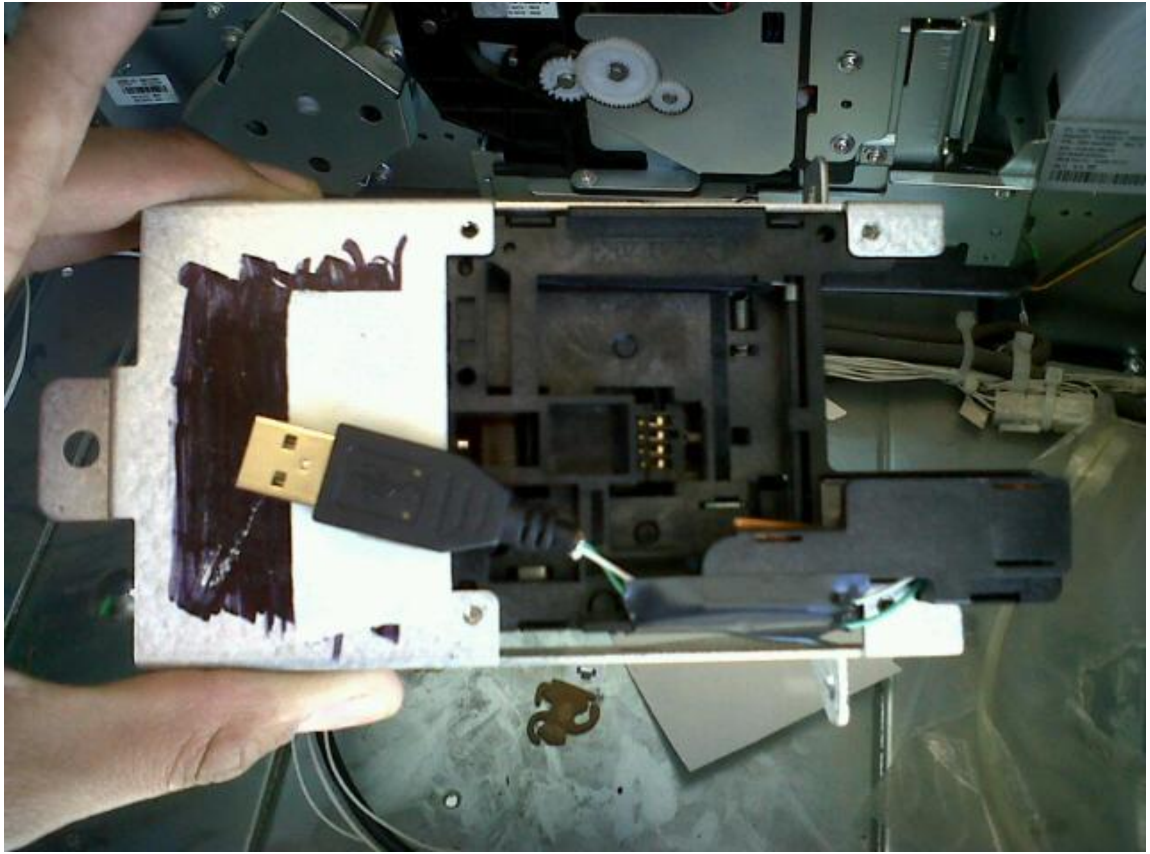


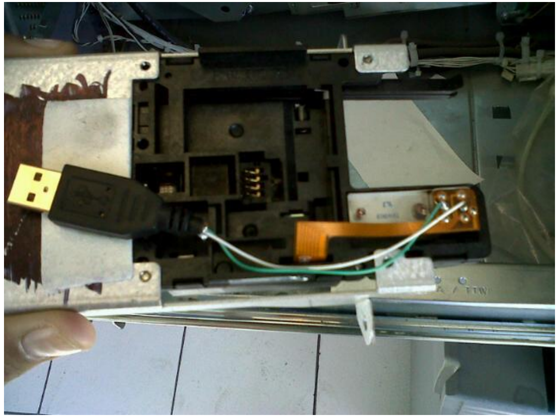
UK

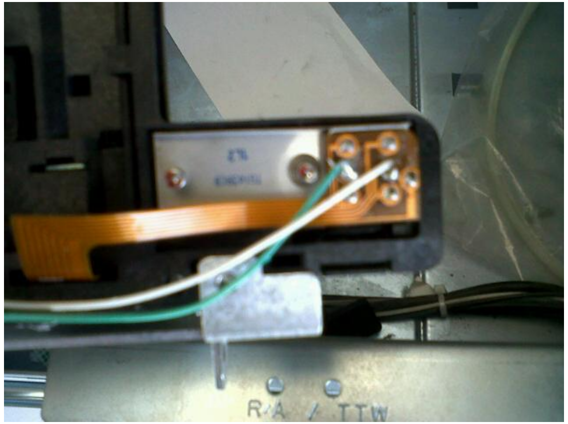


Canada

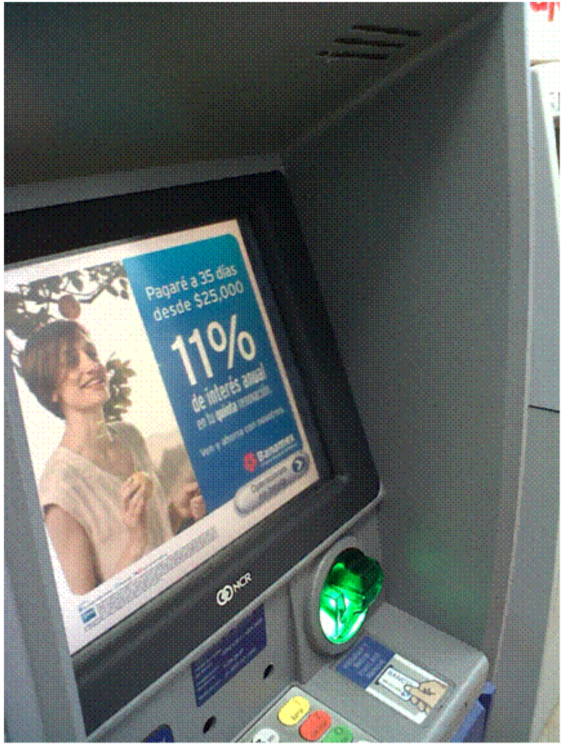
Mexico – Internal Skimming: DIP

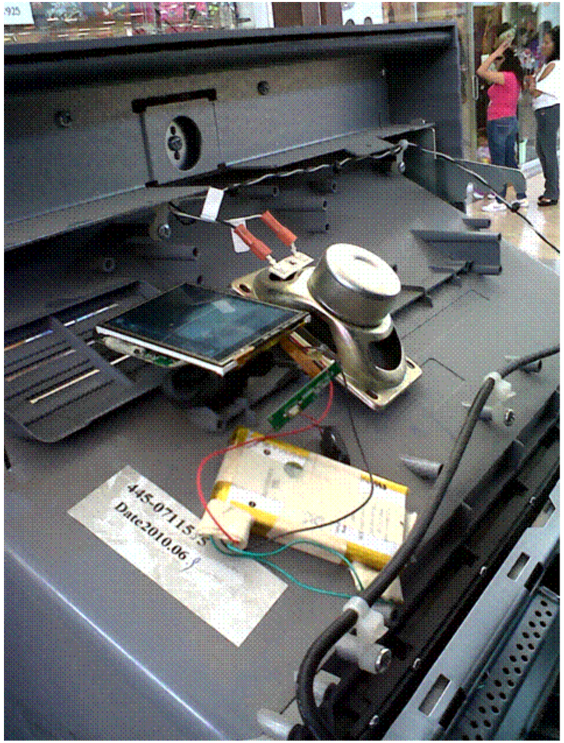


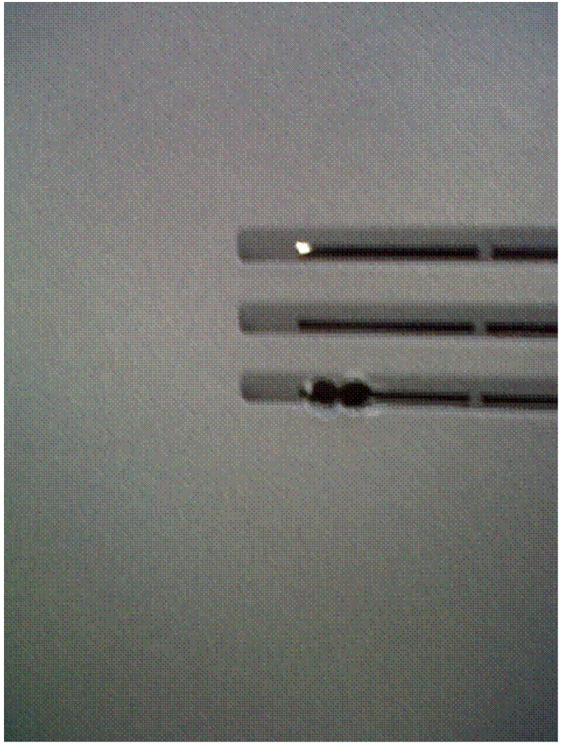




Mexico – Internal Skimming: DIP

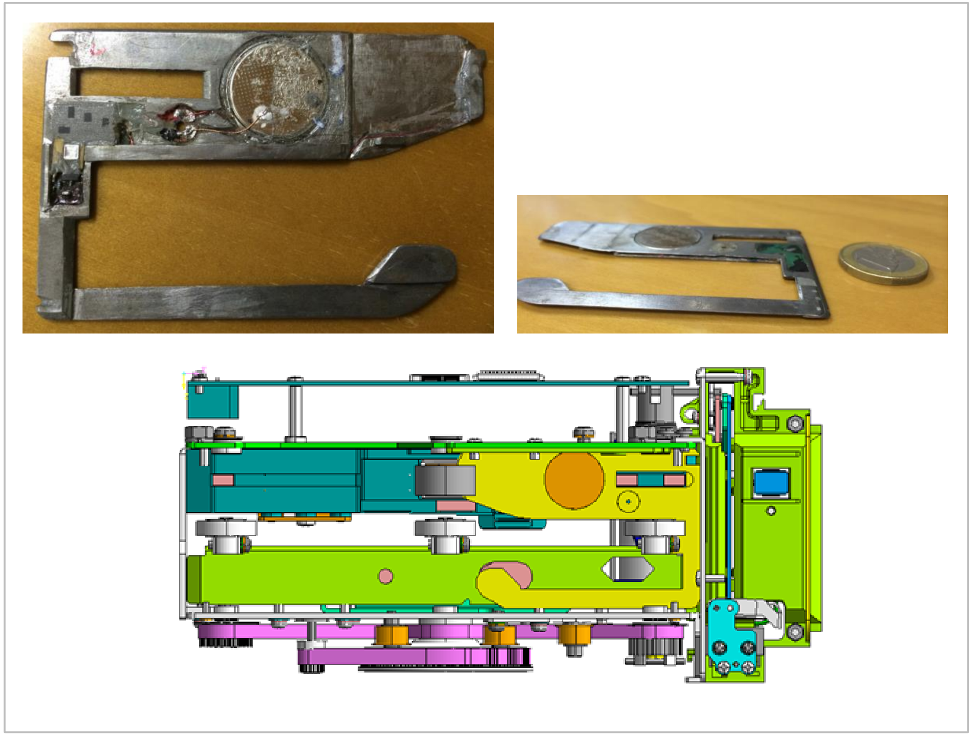






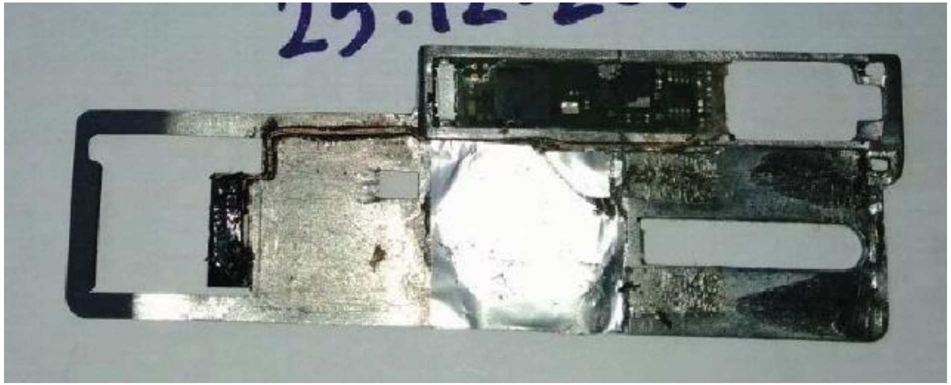
“Deep” Insert Skimming

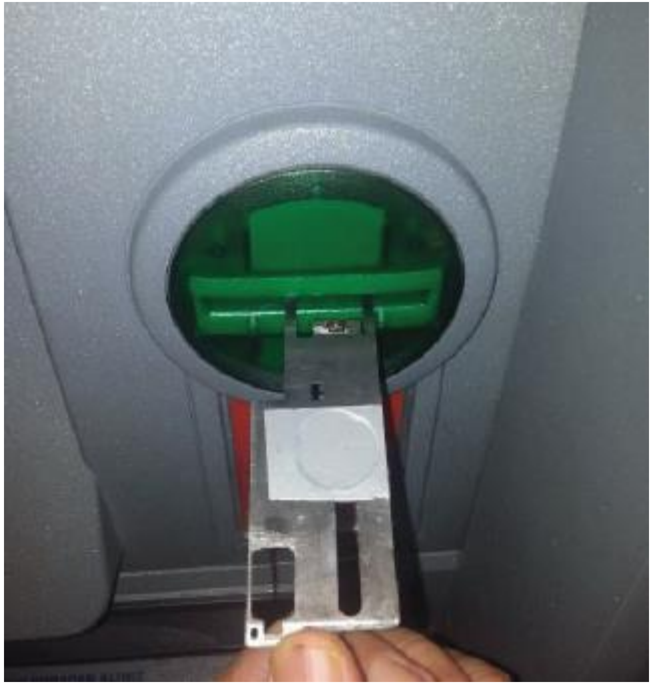
- Sits further into the card reader then typical insert skimmers
- Intent of this technique is to defeat jamming technology which focuses on the bezel
- Different styles of device observed
- Devices often transmit card data in real time, no on board storage



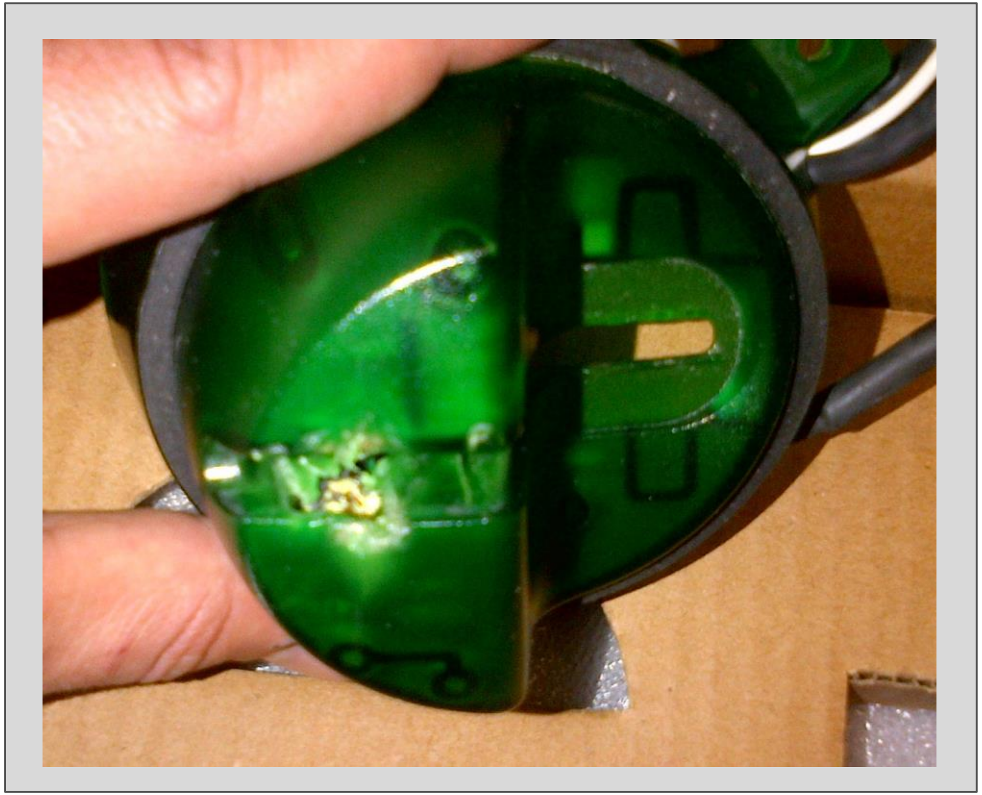
Deep Insert Skimmers - Variations

- New form factor Deep Insert Skimmers reported in Turkey and Ireland (not pictured).



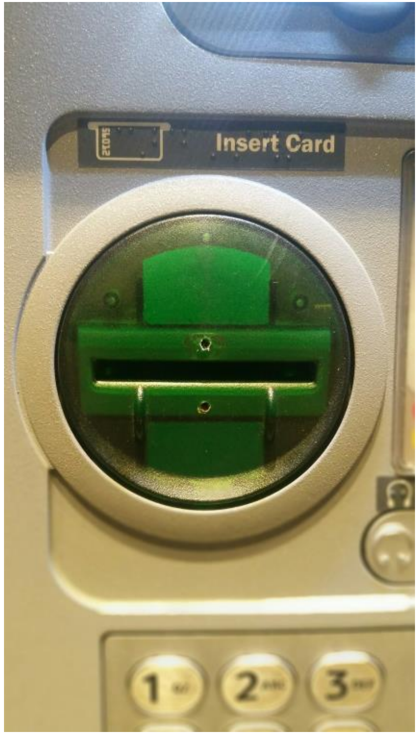


Sabotage: Attempts to Disable SPS

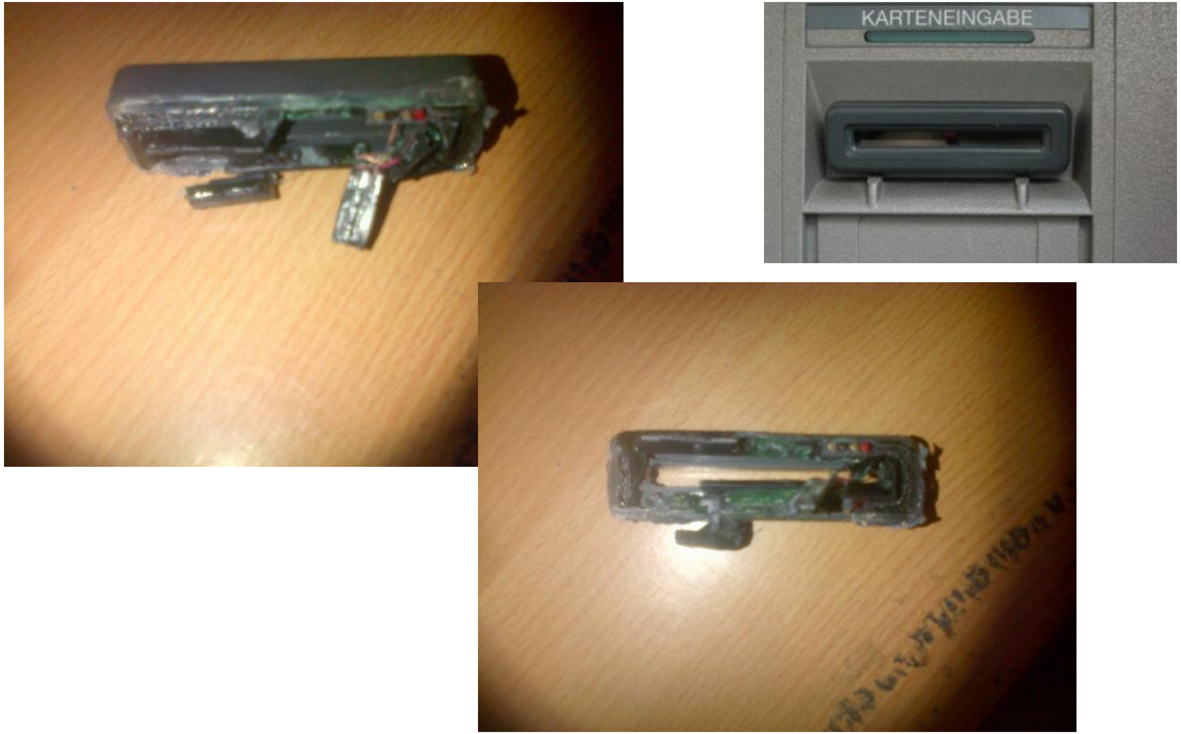


- Criminal has attempted a crude attack on the SPS bezel to damage and disable the SPS electromagnetic disruptor
- SPS anti-tamper sensors will detect and alert on a wide range of tamper conditions, including simple disabling attacks like this one.
- ATM infrastructure MUST be configured to react to SPS anti-tamper alerts.

Attacks concerning CPK



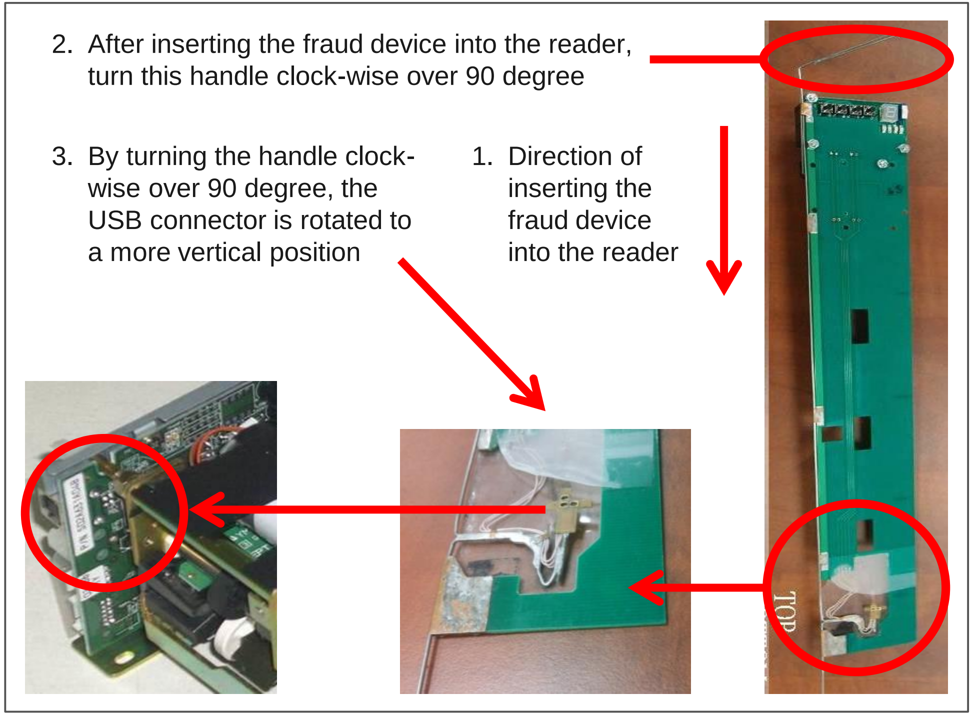
Sabotage



Cloning

Software Skimming: Offline Malware Attack

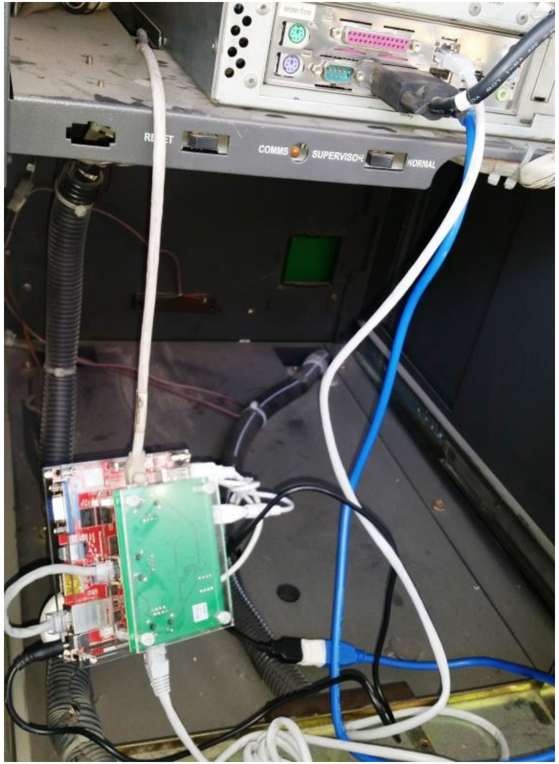
- Insert to Card Reader
- Connector turned through 90 deg.
- Connects to Card Reader USB Connections
- Malware harvests Card and PIN Data
- Allows injection of malware ‘from the street’
- Exploits non-PCI EPP firmware



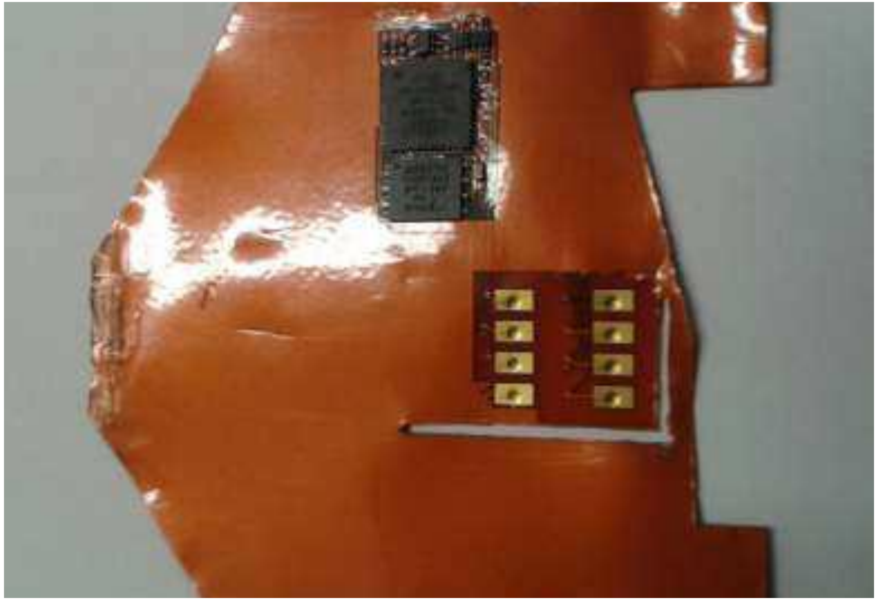
1. Direction of inserting the fraud device into the reader
2. After inserting the fraud device into the reader, turn this handle clock-wise over 90 degree
3. By turning the handle clock-wise over 90 degree, the USB connector is rotated to a more vertical position

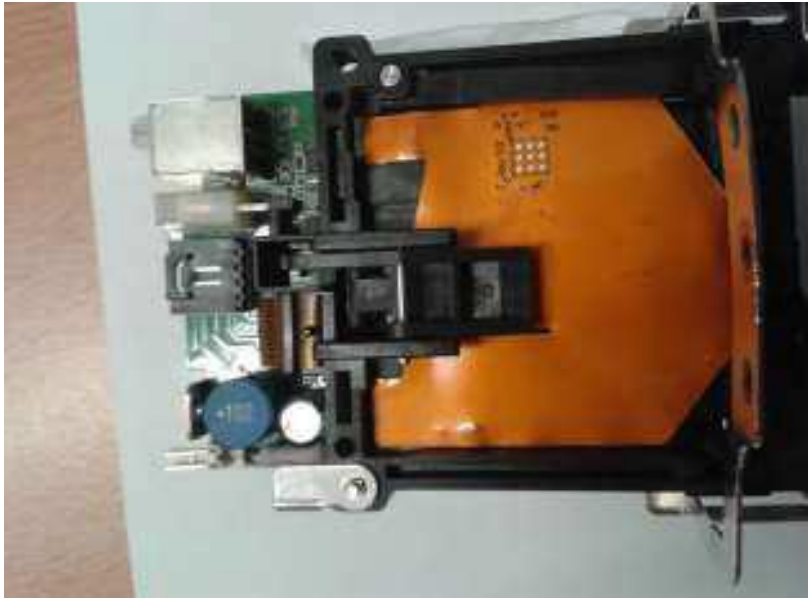
Network Sniffing: Internal and External

- 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. Both overlays and cameras have been observed
- PIN capture device transmits the PIN to the sniffer
- Encrypted communications prevents this attack



‘Shimming’ - Mexico, Greece, Portugal

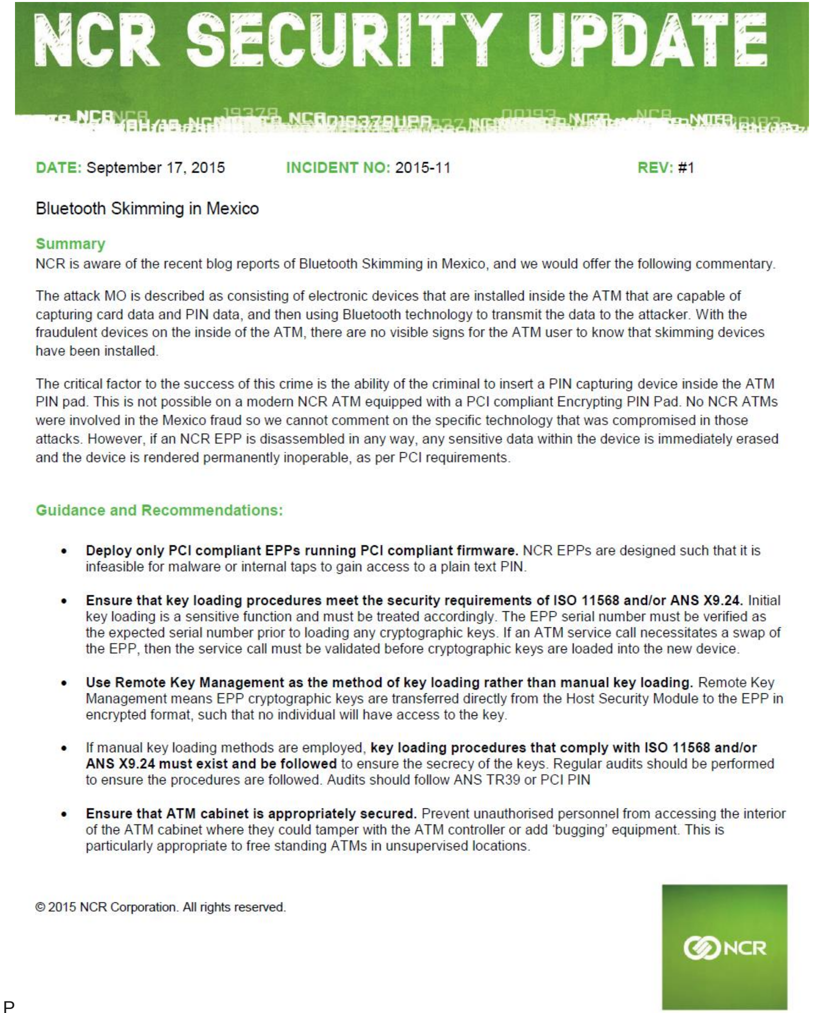




- Correct EMV implementation protects against this attack

Bluetooth Skimming

- Blog posts report internal skimming in Mexico
- Bluetooth devices transmit card and PIN data from inside the ATM.
- Bugs placed inside card reader and EPP
- High levels of corruption of service staff
- Attacks are not possible with latest EPPs
- Attacks highlight the importance of EPP Key Management



NCR SECURITY UPDATE

DATE: September 17, 2015 **INCIDENT NO:** 2015-11 **REV:** #1

Bluetooth Skimming in Mexico

Summary

NCR is aware of the recent blog reports of Bluetooth Skimming in Mexico, and we would offer the following commentary.

The attack MO is described as consisting of electronic devices that are installed inside the ATM that are capable of capturing card data and PIN data, and then using Bluetooth technology to transmit the data to the attacker. With the fraudulent devices on the inside of the ATM, there are no visible signs for the ATM user to know that skimming devices have been installed.

The critical factor to the success of this crime is the ability of the criminal to insert a PIN capturing device inside the ATM PIN pad. This is not possible on a modern NCR ATM equipped with a PCI compliant Encrypting PIN Pad. No NCR ATMs were involved in the Mexico fraud so we cannot comment on the specific technology that was compromised in those attacks. However, if an NCR EPP is disassembled in any way, any sensitive data within the device is immediately erased and the device is rendered permanently inoperable, as per PCI requirements.

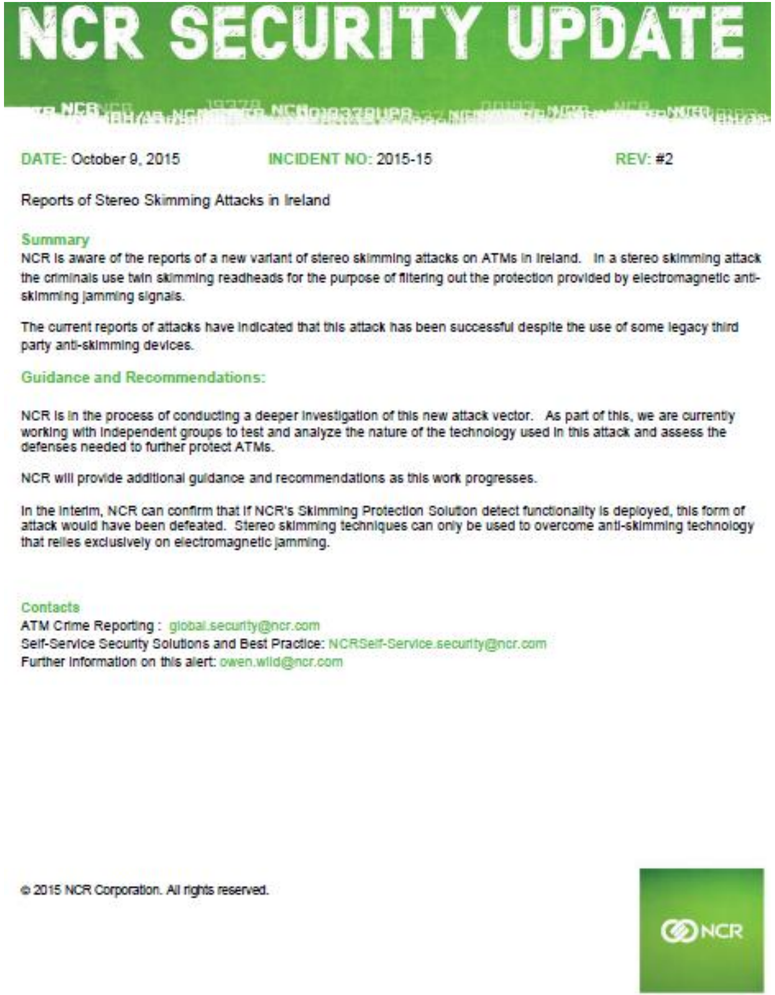
Guidance and Recommendations:

- **Deploy only PCI compliant EPPs running PCI compliant firmware.** NCR EPPs are designed such that it is infeasible for malware or internal taps to gain access to a plain text PIN.
- **Ensure that key loading procedures meet the security requirements of ISO 11568 and/or ANS X9.24.** Initial key loading is a sensitive function and must be treated accordingly. The EPP serial number must be verified as the expected serial number prior to loading any cryptographic keys. If an ATM service call necessitates a swap of the EPP, then the service call must be validated before cryptographic keys are loaded into the new device.
- **Use Remote Key Management as the method of key loading rather than manual key loading.** Remote Key Management means EPP cryptographic keys are transferred directly from the Host Security Module to the EPP in encrypted format, such that no individual will have access to the key.
- If manual key loading methods are employed, **key loading procedures that comply with ISO 11568 and/or ANS X9.24 must exist and be followed** to ensure the secrecy of the keys. Regular audits should be performed to ensure the procedures are followed. Audits should follow ANS TR39 or PCI PIN
- **Ensure that ATM cabinet is appropriately secured.** Prevent unauthorised personnel from accessing the interior of the ATM cabinet where they could tamper with the ATM controller or add 'bugging' equipment. This is particularly appropriate to free standing ATMs in unsupervised locations.

© 2015 NCR Corporation. All rights reserved.

Stereo Skimming

- Two confirmed reports of stereo skimming in Ireland
- ATMs were fitted with TMD CPK 6000 which failed to prevent the attacks.
- 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
- NCR recommend using skimmer detect functionality in parallel with electromagnetic jamming



NCR SECURITY UPDATE

DATE: October 9, 2015 INCIDENT NO: 2015-15 REV: #2

Reports of Stereo Skimming Attacks in Ireland

Summary

NCR is aware of the reports of a new variant of stereo skimming attacks on ATMs in Ireland. In a stereo skimming attack the criminals use twin skimming readheads for the purpose of filtering out the protection provided by electromagnetic anti-skimming jamming signals.

The current reports of attacks have indicated that this attack has been successful despite the use of some legacy third party anti-skimming devices.

Guidance and Recommendations:

NCR is in the process of conducting a deeper investigation of this new attack vector. As part of this, we are currently working with independent groups to test and analyze the nature of the technology used in this attack and assess the defenses needed to further protect ATMs.

NCR will provide additional guidance and recommendations as this work progresses.

In the interim, NCR can confirm that if NCR's Skimming Protection Solution detect functionality is deployed, this form of attack would have been defeated. Stereo skimming techniques can only be used to overcome anti-skimming technology that relies exclusively on electromagnetic jamming.

Contacts

ATM Crime Reporting : global.security@ncr.com
Self-Service Security Solutions and Best Practice: NCRSelf-Service.security@ncr.com
Further information on this alert: owen.wild@ncr.com

Card Skimming - Threat Summary

Skimming Category	Description	Recommended Solutions
Bezel Overlay	Manufactured overlay containing a skimmer which fits a specific ATM model	SPS with Skimmer Detect and Alert Monitoring
Bezel Insert	Manufactured insert containing a skimmer which fits a specific ATM model	SPS with Skimmer Detect and Alert Monitoring
Card Read Tap - Destructive (Eavesdropping)	Attacks that penetrate the ATM fascia or cabinet with the intention of providing direct access to the card reader	SPS with Skimmer Detect and Alert Monitoring, plus Anti-Eavesdropping Kit
Card Read Tap - Non-Destructive	Attacks that involve opening the ATM cabinet with the intention of providing direct access to the card reader	ATM location security, appropriate cabinet locks, encrypted USB
Differential Skimming (Stereo Skimming)	Using twin read heads connected in differential mode to negate the effects of a jamming signal	SPS with Skimmer Detect and Alert Monitoring
Deep Insert Skimmer	A device placed inside the card reader using the card slot as the entry point	Card reader device detection firmware, anti-insert kit
Sabotage	Any attempt to disable any anti-skimming technology	SPS with Skimmer Detect and Alert Monitoring
Shimming	Capture of chip card data with the intent to produce a cloned mag strip card	Transaction Authorisation as per EMV
Network Sniffing	Capture of card data via sniffing of network communications to the host	Communications Encryption TLS 1.2

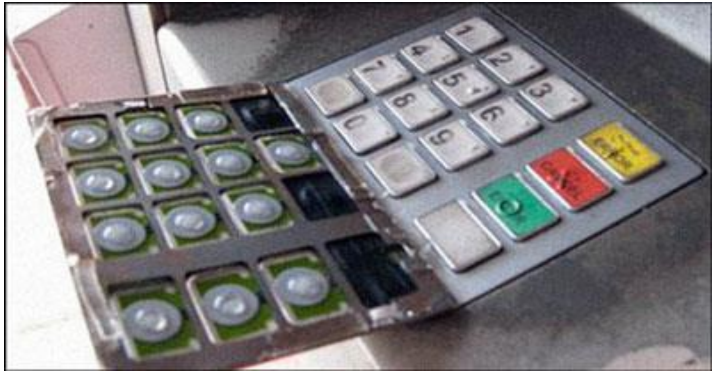
PIN capture: Keyboard Overlays

Keyboard overlays increase work function for criminal - cost/effort

Overlays have a higher probability of discovery

Typically cameras are used to capture PINs

SelfServ key design a small advantage



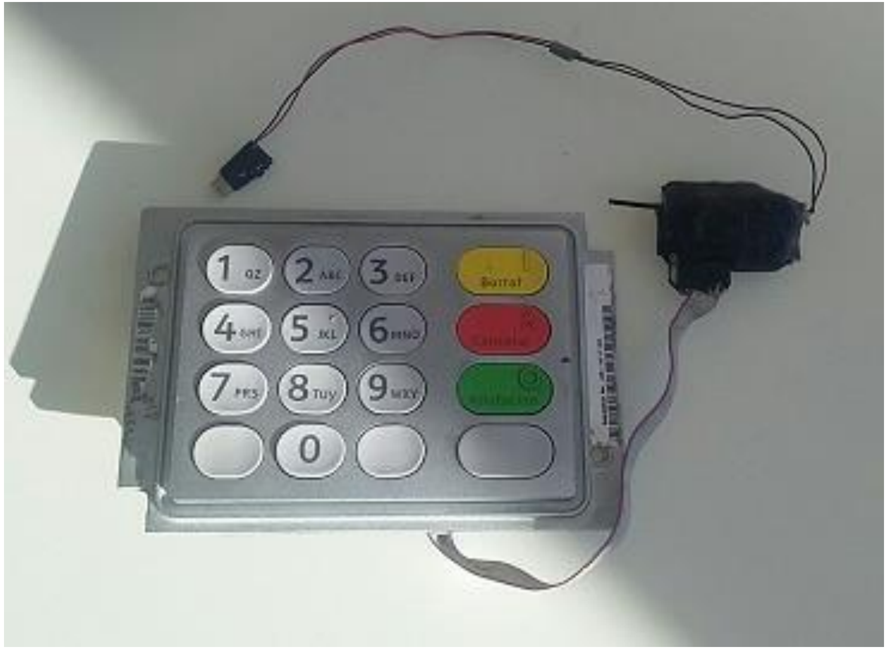
New EPP design for SelfServ

PIN Pad Overlay - Mexico

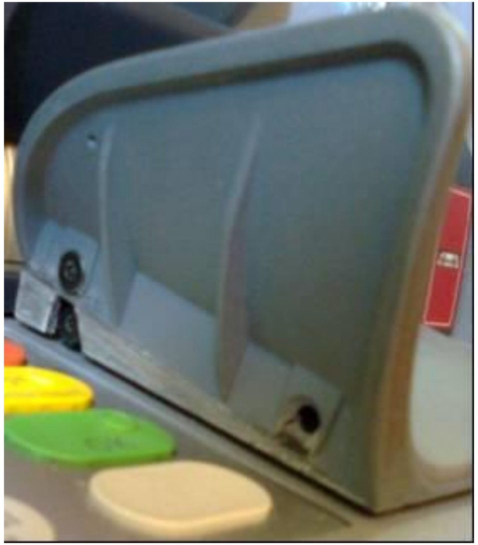
EPP overlay created by slicing the top from a genuine NCR PIN pad.

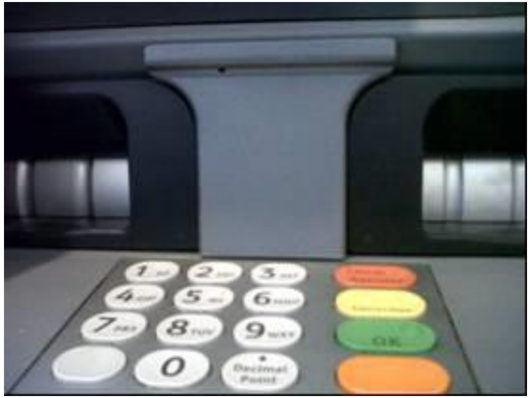
Device fitted ‘correctly’ into the ATM, with original ATM PIN pad directly below it.

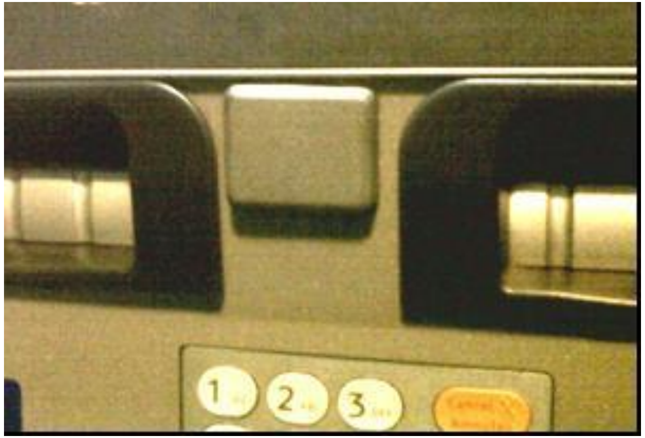
Attacker required access into top box to fit the overlay.



PIN capture: Cameras……

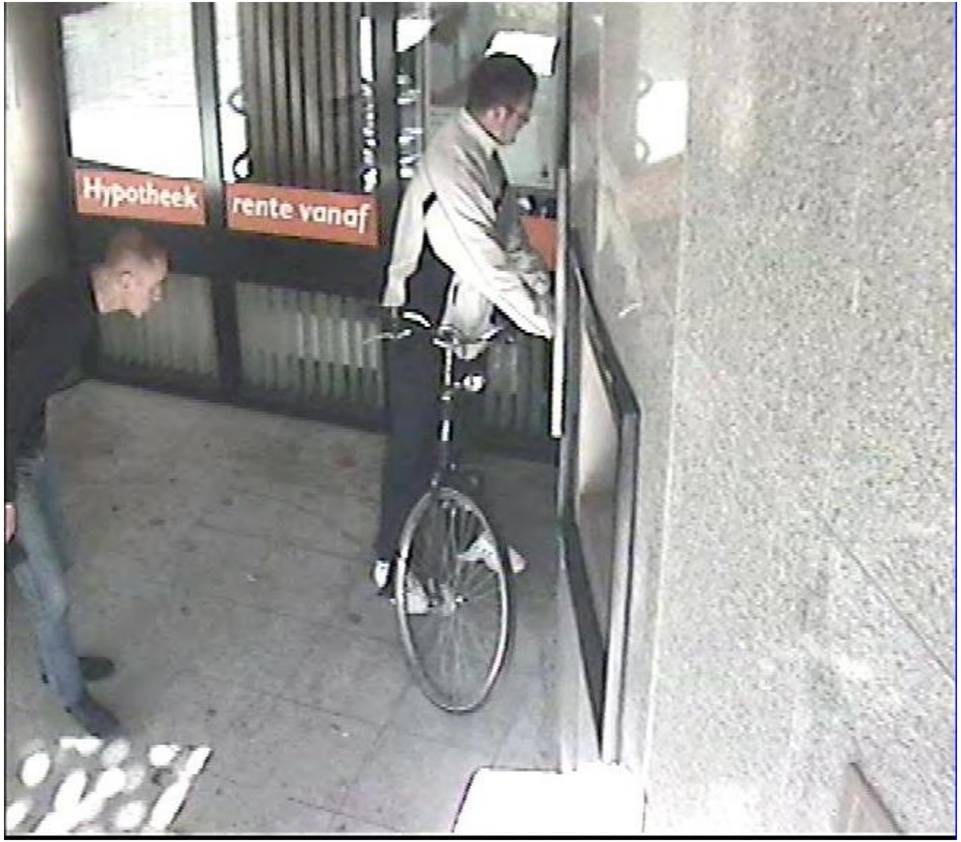






PIN capture: Shoulder Surfing

The gentleman on the left demonstrates the old fashioned way to capture a PIN…….



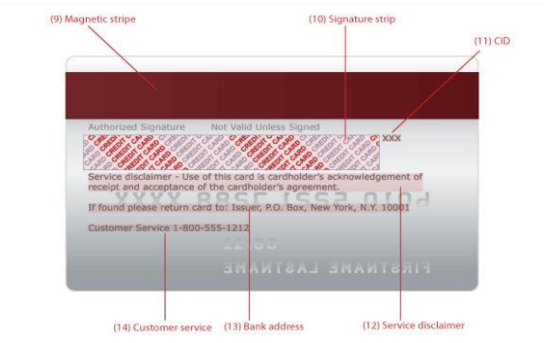
Safeguarding Against Skimming Attacks

Charlie Harrow – Solutions Manager, NCR Corp.

Three effective strategies to combat skimming

Migrate from magnetic stripe

- Reduce the counterfeit card risk
- Migrate to EMV chip


(9) Magnetic stripe
(10) Signature strip
(11) CID
Authorized Signature
Not Valid Unless Signed
XXX
Service disclaimer - Use of this card is cardholder's acknowledgement of receipt and acceptance of the cardholder's agreement.
If found please return card to: Issuer, P.O. Box, New York, N.Y. 10001
Customer Service 1-800-555-1212
(14) Customer service
(13) Bank address
(12) Service disclaimer

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

Comprehensive levels of anti-tamper defences

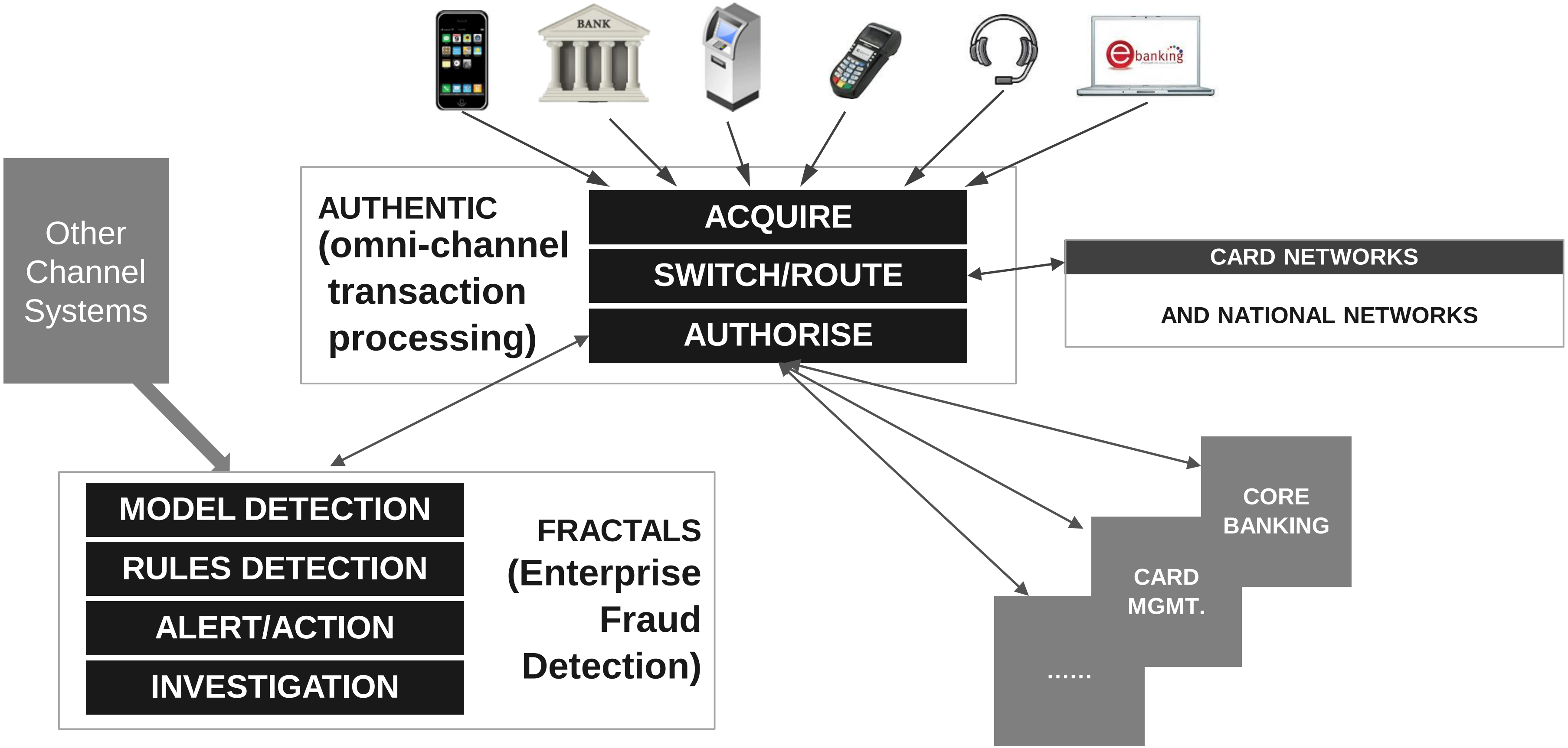
Upgrade kit availability

Supported through NCR normal support channels

Available for Motorized and DIP Card readers

Downloadable software for ease of flexible response

Transaction Processing and Fraud Detection



Other Channel Systems

AUTHENTIC (omni-channel transaction processing)

ACQUIRE

SWITCH/ROUTE

AUTHORISE

CARD NETWORKS

AND NATIONAL NETWORKS

MODEL DETECTION

RULES DETECTION

ALERT/ACTION

INVESTIGATION

FRACTALS (Enterprise Fraud Detection)

CORE BANKING

CARD MGMT.

......

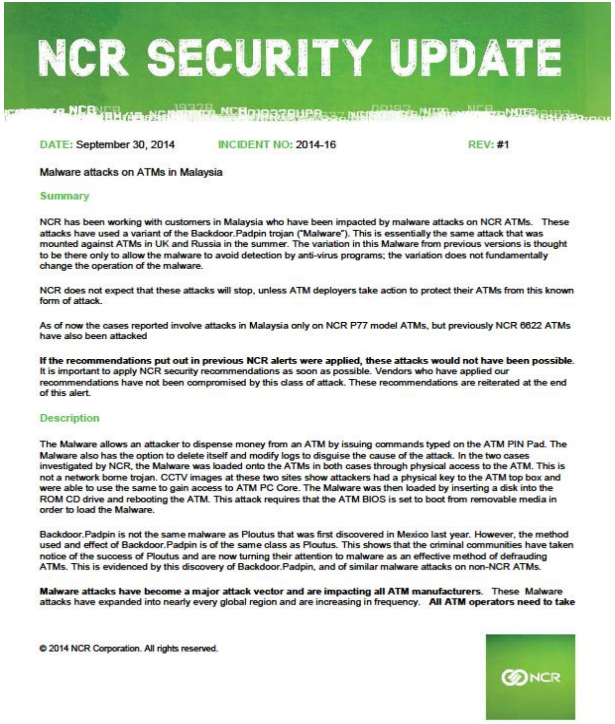
FINALLY - NCR SECURITY ALERTS

Are you enrolled?

- NCR have a proven set of solutions and practice recommendations to reduce your risk
- Get on NCR's Alert List
  - Notification of new attacks

  response.ncr.com/security-alerts

- **Lock down your BIOS**



NCR SECURITY UPDATE

DATE: September 30, 2014 INCIDENT NO: 2014-16 REV: #1

Malware attacks on ATMs in Malaysia

Summary

NCR has been working with customers in Malaysia who have been impacted by malware attacks on NCR ATMs. These attacks have used a variant of the Backdoor.Padpin trojan ("Malware"). This is essentially the same attack that was mounted against ATMs in UK and Russia in the summer. The variation in this Malware from previous versions is thought to be there only to allow the malware to avoid detection by anti-virus programs; the variation does not fundamentally change the operation of the malware.

NCR does not expect that these attacks will stop, unless ATM deployers take action to protect their ATMs from this known form of attack.

As of now the cases reported involve attacks in Malaysia only on NCR P77 model ATMs, but previously NCR 6622 ATMs have also been attacked

If the recommendations put out in previous NCR alerts were applied, these attacks would not have been possible. It is important to apply NCR security recommendations as soon as possible. Vendors who have applied our recommendations have not been compromised by this class of attack. These recommendations are reiterated at the end of this alert.

Description

The Malware allows an attacker to dispense money from an ATM by issuing commands typed on the ATM PIN Pad. The Malware also has the option to delete itself and modify logs to disguise the cause of the attack. In the two cases investigated by NCR, the Malware was loaded onto the ATMs in both cases through physical access to the ATM. This is not a network borne trojan. CCTV images at these two sites show attackers had a physical key to the ATM top box and were able to use the same to gain access to ATM PC Core. The Malware was then loaded by inserting a disk into the ROM CD drive and rebooting the ATM. This attack requires that the ATM BIOS is set to boot from removable media in order to load the Malware.

Backdoor.Padpin is not the same malware as Ploutus that was first discovered in Mexico last year. However, the method used and effect of Backdoor.Padpin is of the same class as Ploutus. This shows that the criminal communities have taken notice of the success of Ploutus and are now turning their attention to malware as an effective method of defrauding ATMs. This is evidenced by this discovery of Backdoor.Padpin, and of similar malware attacks on non-NCR ATMs.

Malware attacks have become a major attack vector and are impacting all ATM manufacturers. These Malware attacks have expanded into nearly every global region and are increasing in frequency. **All ATM operators need to take**

© 2014 NCR Corporation. All rights reserved.

How to Report a Skimming Device

Lester Chan – Director, Merchant Security, Visa Inc.

Best Practices on Handling and Reporting

What to do if a skimmer is found

Do not approach or confront anyone who looks suspicious

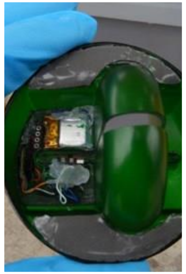
Might be installing or removing a skimming device

May be armed and dangerous

Document and take pictures of the skimming device as-is

Document before and after removal

Document date/time



Use protective gloves to remove the device

Criminals may leave DNA on device

Keep in protective bag and store securely

Review CCTV for surveillance of suspects

Contact the local authorities and the U.S. Secret Service

U.S. Secret Service is the law enforcement branch responsible for investigating these crimes

Know how to report compromises to Visa

How to Report a Compromise to Visa

Reporting requirements after a skimmer is found Issuers (ATMs)

Review Compromised Guidelines

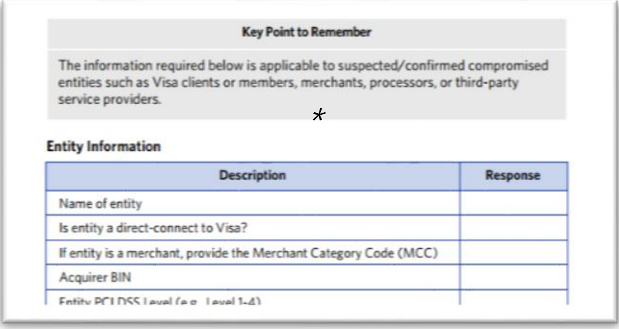
VISA

What To Do If Compromised

Visa Inc. Fraud Investigation Procedures

Version 4.0 (Global)
Effective September 2013
Visa Public

Complete Questionnaire



Key Point to Remember

The information required below is applicable to suspected/confirmed compromised entities such as Visa clients or members, merchants, processors, or third-party service providers.

*

Entity Information

Description	Response
Name of entity	
Is entity a direct-connect to Visa?	
If entity is a merchant, provide the Merchant Category Code (MCC)	
Acquirer BIN	
Entity PCI DSS Level (e.g., Level 1-4)	

Send to: USFraudControl@Visa.com

1. Send Questionnaire to Visa Cyber Investigations with incident details
2. Try to determine the potential Window of Exposure of the event
3. Pull and send in compromised accounts to Visa via CAMS*
4. Visa will distribute the at-risk accounts to the affected Issuers via CAMS

**Note – Most Issuers are set up as CAMS receivers only, send email to* VAA_VRM@Visa.com to be a submitter

How to Report a Compromise to Visa

Reporting requirements after a skimmer is found for Merchants

Review Compromised Guidelines

Complete Questionnaire

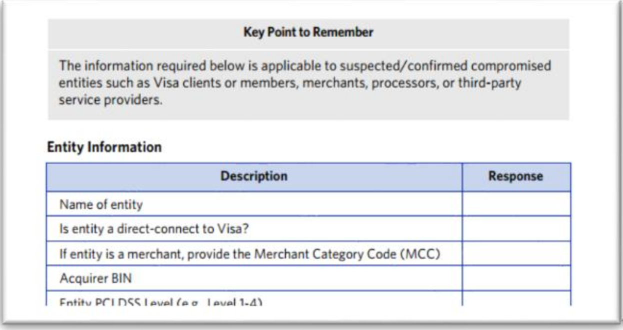
Send to acquirer

VISA

What To Do If Compromised

Visa Inc. Fraud Investigation Procedures

Version 4.0 (Global)
Effective September 2013
Visa Public



Key Point to Remember

The information required below is applicable to suspected/confirmed compromised entities such as Visa clients or members, merchants, processors, or third-party service providers.

Entity Information

Description	Response
Name of entity	
Is entity a direct-connect to Visa?	
If entity is a merchant, provide the Merchant Category Code (MCC)	
Acquirer BIN	
Entity PCI DSS Level (e.g., Level 1-4)	

1. Acquirer will forward questionnaire to Visa Cyber Investigations with incident details
2. Skimming incidents often involve the compromise of highly sensitive PIN data
3. Issuers need to be notified of the potential at-risk accounts quickly
4. Merchants should try to determine the potential Window of Exposure of the event
5. Acquirers should pull and send in the compromised accounts to Visa via CAMS
6. Visa will distribute the at-risk accounts to the affected Issuers via CAMS

Key Takeaways

- Be aware that due to EMV liability shift, fraud and compromises will likely migrate
- Recognize that criminals are targeting mag stripe data and transactions
- Skimming devices are becoming more sophisticated
- Understand how to identify different types of skimming devices
- Learn best practices for safeguarding against skimming attacks
- Conduct regular, ongoing training for current and new employees
- Know what to do if a skimmer is found and how to report a suspected compromise

Upcoming Events and Resources

Resources

- PCI Standards Council: Skimming Prevention
- NCR Security Alerts: response.ncr.com/security-alerts
- Visa’s “What To Do If Compromised” guidelines
- Visa’s “Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants” guidelines

Upcoming Webinars – Training page on www.visa.com/cisp

- Changes to PCI DSS 3.2 – May 11, 2016 - Janet Cookson, Director, Security Standards, Visa Inc.

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…

Questions?

NCR

VISA