ATMIA Information Alert: Card Trapping

Produced by the ATM Industry Association

Contributor:

Douglas Russell, Director, DFR Risk Management Ltd.

Copyright Information

e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com

Disclaimer

Please note this discussion paper contains confidential information and should not be left lying around or freely copied without due care for its distribution and safekeeping.

Global Sponsors

Table of Contents

1. Re-Emerging Threat of Card Trapping

ATMIA members are reminded that attacks against ATMs, while generally accepted as becoming increasingly sophisticated, can still involve relatively unsophisticated tools and methods.

Card trapping involves a criminal device positioned at the entry throat of a motorized card reader. The device, often generically referred to as a "Lebanese Loop," allows a card to be entered into the ATM card reader but prevents the card from being returned to the consumer. The perpetrator will subsequently remove the trapping device along with the trapped card.

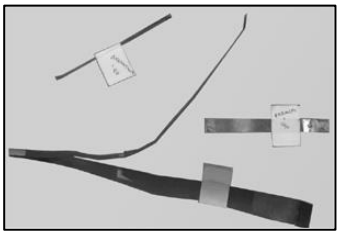
Card trapping attacks are re-emerging in many geographic regions that have ATMs fitted with motorized card readers.

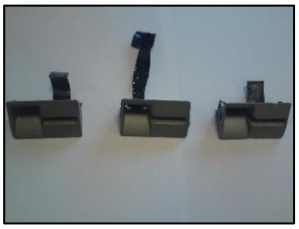
Card trapping attacks normally also involve PIN compromise, often using a spy camera disguised and attached to the ATM fascia. However, with the increasing popularity of contactless cards, financial gain can be realized without compromising the PIN.

While financial losses from card trapping are much lower than many other types of ATM fraud, ATM availability is often impacted as the card reader will usually become unavailable following a card jam. Maintenance costs might also increase if the card reader requires servicing.

ATMs in the surrounding area are often sabotaged to force consumers to use ATMs fitted with card traps. Common methods of sabotage include jamming the card reader with paper, cardboard and glue.

ATMIA believes that such attacks are increasing, as ATMs have become much better protected from ATM skimming and other more sophisticated fraud categories.





2. Best Practices for Defending Against Card Trapping

2.1. Preventing Card Trapping: General Tips

Card trapping, like most types of ATM crime, requires a combination of approaches to best address and combat the threats. These approaches are both technical and non-technical in nature and include industry solutions, inspection, staff education, environmental considerations and consumer education.

In general, we recommend:

- Selecting the most appropriate technical solutions that your ATM solution provider can offer,
- Frequent (at least daily) inspection of the ATM fascia for evidence of tampering,
- Adoption of painted defensible space around the ATM, and
- Clear and effective consumer education delivered at the ATM itself.

Technical Solutions
Daily Inspection of ATM Fascia
Defensible Space
Staff Education
Consumer Education

2.2. Industry Solutions and Options for Detection and Deterrence

ATM vendors and other solutions providers offer a range of hardware and software solutions for card trapping. The terminology used to describe the solutions does vary considerably. As this best practice guide is vendor-independent, the following is a list of examples of the types of solutions available. For specific details, ATM owners should consult directly with their advisors and suppliers about the options best suited for their specific ATM models.

- Card reader shutter/gate designed to remain closed when not in use
- Shutter/gate sensed if open when it should be closed
- Card reader design to prevent unauthorized access
- Protrusion devices to inhibit attachments to card reader entry area
- Sensors to detect the presence of suspicious/fraudulent devices
- Card entry has been manipulated; card moved in/out/in
- Card ejected if trap is detected during entry
- Physical barrier preventing criminal removal of card, once trapped
- Destruction of magnetic stripe and chip, once trapped
- Card number reported if card is known to have been trapped
- Monitoring of fascia area to sense and report unexpected or unusual objects
- Warning screen displayed when card is trapped
- Receipt printed with warning message when card is trapped
- ATM removed from service when card trap is detected/card trapped
- Option of DIP or Swipe readers rather than motorized

There is evidence that, in the UK and elsewhere in Europe, criminals have successfully removed some protrusion devices and have modified them to become traps. Given that this is difficult for a customer to spot, it is important that any devices attached to the front of a machine are designed in such a way that they cannot be removed and converted by the criminals.

2.3. Inspection

As the design of ATM models varies considerably, we recommend that, as an aid for staff inspecting the ATM, a photograph of what the actual ATM should look like be made available and used during the inspection process.

Regular inspections of ATMs by cash machine owners for evidence of tampering and unusual attachments should be conducted.

Local staff, including ATM servicers, must be trained to look for evidence of fraudulent devices and be educated on the appropriate action to be taken should they discover a card trapping device on a machine. At all times, personal safety considerations should take priority, as it is known that criminals often maintain surveillance on the ATM they are targeting.

Evidence of fraudulent devices might include:

- Retention of suspicious devices attached to, or captured by, the card reader
- Evidence of adhesive residue
- Vandalism to card reader throat, shutter/gate
- Error reports of card jams, with no card retained

2.4. Defensible Space and Environmental Consideration

The use of a painted defensible space around the ATM will help reduce interference from fraudsters. Defensible space ground markings can be effectively employed at the front of the ATM to indicate only one customer at a time may enter the space. These will usually be subject to local authority planning approval. The marked space on the ground in front of the ATM may be painted in yellow, red or white, depending on any local planning guidelines or negotiations. Ideally, the area should be large enough to prevent the possibility of "shoulder surfing" and to provide the ATM user with a comfortable space in which to conduct his transaction. It is a good method that provides added privacy at very low cost.

Ensuring the ATM is in a well-lit location and that the ATM's own fascia lighting is in good condition can also deter card trapping attacks and make the identification of fraudulent devices easier.

2.5. Staff Education

In addition to educating staff on how to inspect the ATM for evidence of tampering, staff should also be trained in how to respond when a customer reports that their card has been retained, or “swallowed,” by the ATM. Without training, staff may not associate such a report as possibly being related to card trapping.

2.6. Consumer Education

Consumer education is most effective when delivered at the ATM, both proactively and reactively.

Proactive consumer education should constantly remind consumers to report suspicions, never allow anyone to observe their PIN, and never allow anyone to help them perform a transaction. The use of graphics to show consumers what the ATM should look like and to encourage them to use their free hand to cover their other hand during PIN entry can be very effective.

Reactive education should be triggered when the ATM senses that a card trap has been inserted or a card has been jammed.

- Display a message on the ATM screen to advise the consumer what to do:
    - Contact the bank or card issuer immediately
    - Phone number to call
    - Reminder, "We will NEVER ask for the PIN"
    - Reminder, "Don't tell ANYONE the PIN"
- Print a receipt with the above information for the cardholder to take away.
- Don't use a sticker on or near the ATM with the above information – this is easily copied or altered with the attacker's phone number.
- Don't put the ATM back in service until it has been checked to make sure it is operating correctly and that no card traps are present.

When the Lebanese Loop story was first featured in the media in the early 1990s, one concern within the industry, particularly given the low-tech nature of the scam, was a desire not to describe in any detail how the fraud was committed, as there was a fear of copycat attacks. The other concern was in regard to the need to maintain consumer confidence in the ATM network.

In terms of awareness and advice to customers, card trapping and card skimming are not that different. In both cases it's a case of look out for devices attached to the ATM and protect the PIN. You want to let people know there is a problem, but you also want them to understand that the situation is being addressed by the use of Best in Practice technology, and this, too, is something that requires clear communication. It is important to communicate how the solution operates and any implications this will have for an ATM's appearance or performance.

3. Further Reading for Card Trapping

The ATM Security Association (ASA) has a full-length Best Practice Guide on card trapping, which is the source of the best practices in the previous section. The guide is available to ASA members:

ASA https://www.atmsecurityassociation.com/documents/