Doc Cards 115-08 17 December 2008
(Version 1.0 Approved) FG/CS

Recommended ATM anti-skimming solutions within SEPA

(Approved by Plenary – 17 December 2008)

Circulation: Publicly available
Restricted: Yes

INTRODUCTION

The growth of skimming fraud is a major driver for the rollout of EMV across the SEPA area. This should be completed by 2010 and it has already resulted in dramatic reductions in the use of fraudulently duplicated cards in the countries where it has been introduced. However, it has also resulted in fraudulent transactions migrating to countries where EMV has not yet been implemented or is not planned, often outside the SEPA area. As many such countries have no plans to introduce EMV, cards will continue to have both mag-stripe and chip and therefore there will remain a significant risk of a fraudster skimming a magstripe in an EMV country and using the duplicate card in a non-EMV country or environment.

BACKGROUND

Card skimming involves the capture of a card's mag-stripe information (which may be debit, credit or ATM only), and matching it with the card's PIN number in order to produce a duplicate card. This may occur at ATMs, Point of Sale (POS), or indeed any other location where a customer uses their card and PIN.

The mag-stripe information is captured by fitting an additional card-reader over the ATM's card slot and the PIN is usually obtained by the use of micro cameras, although "shoulder surfing," may also be used. This information is then stored on a chip within the skimming device or more usually transmitted immediately to a lap-top PC nearby. Devices are usually attached to ATMs for short periods e.g. 20 minutes and the device is usually being observed. For this reason ATMs which are busy and which have ample adjacent parking are particularly attractive to fraudsters.

The duplicate card can then be used in a non-EMV ATM, or if the duplicate card passes visual inspection, Point of Sale (POS). Information on the chip is not captured which means that the card cannot be used in an EMV environment and this normally limits use to locations where EMV has not been introduced. Fraudulent data may be sold on and mixed with other sources of data and the actual card production may be months after the data was captured, although on other occasions duplicate cards have been used less than 24 hours after the attack.

With a duplicate card a bank account can be drained until there are no funds available, or in the case of a credit card, until the credit limit is reached. As ATM usage is subject to daily withdrawal limits, these transactions usually take place close to, or at the daily limit over a number of days. EAST (European ATM Security Team), reports that the number of cases of skimming remains high across Europe with over 4501 ATM incidents in 2007, resulting in losses of over € 438 million[1].

[1] Note: these losses include cards skimmed at point of sale as it is often impossible to identify the original point of compromise.

A number of preventative measures can be taken by ATM operators to stop or reduce skimming, but in most European countries the decision to install anti-skimming solutions is up to the individual ATM operator. These are often financial institutions that issue cards and therefore have a vested interest in protecting their own account holders when they use their own machines. However, others do not issue cards or do not issue enough cards to make the investment in preventative measures worthwhile. This means that in most countries the use of anti-skimming solutions varies depending on the individual ATM operator's perception of risk and their business case for fitting such solutions.

RECOMMENDATIONS

It is hereby proposed that the following recommendations be approved by the EPC. ATM Operators and Schemes remain responsible for their own business decisions as to which, if any, solution is appropriate for their particular circumstances and there is no obligation on ATM Operators or Schemes to follow these recommendations. These recommendations should not been seen as a complete or permanent solution to the problem of skimming and the EPC Cards Working Group will monitor their effectiveness. Further recommendations may follow in due course.

Recommendation # 1: Minimum requirements for anti skimming solutions with independent testing.

All ATM suppliers and a number of third party vendors are able to provide anti-skimming solutions and the European ATM Security Team (EAST) has established and maintains a database of anti-skimming solutions and their functionality. However, there is currently no certification or independent evaluation of these solutions and some solutions are more effective than others. This can make the selection of solutions difficult and criminals have also successfully by-passed a number of anti-skimming measures. The Cards Working Group therefore recommends setting minimum standards for anti skimming solutions and that the consideration should be given to a system of independent testing and evaluation.

Anti-skimming solutions can use a number of different approaches which must include some of the following.

- The design of the entrance of the card reader should prevent the attachment of skimming devices and /or make such devices obvious.
- Identifying, jamming, or disturbing skimming devices when they are attached to the ATM.

Wherever possible these solutions should be able to detect a skimming attack and any tampering with the device should result in the closure of the machine or the issuance of an alert.

Furthermore it is recommended that the ATM monitoring system should be able to detect remotely whether electronic anti-skimming solutions are operational.

Recommendation # 2: ATM Operators should also consider the range of additional measures which might be employed depending on their own circumstances and business cases.

- Privacy Shields to hide the customer's hand (giving due consideration to access by those with impairment to the use of their hands)
- Displaying warnings on and near to the machine warning customers to "protect and shield their PIN".

- Display warnings about skimming devices on or near the machine along with details of a customer helpline to report incidents.
- General advice on ATM security to be published for customer education
- Consideration should be given to preventing cards with ATM functionality from being used for access control e.g., to bank branches, bank lobbies etc.
- Regular (and obvious), visual inspection of machines with local staff trained as to what they should look for and what action they should take should they discover a skimming device on the machine.
- ATM screens can be used to display how the unaltered ATM and card reader should appear.
- Access and maintenance visits to the machine should be carefully controlled with audit trails of who has accessed the interior of the machine.

Recommendation #3: Where a new ATM is to be installed into a high risk location and/or a through the wall location then an anti-skimming device should be fitted as a standard feature. This may be supplied by the ATM manufacturer or a third party supplier.

Not all ATMs or locations are equally vulnerable and therefore consideration needs to be given as to how high risk locations should be defined. Examples of high risk locations might include ATMs which are “through the wall”, unattended, with 24 hour access and/or not in clear sight of staff. The nature of skimming attacks continues to evolve so any definition of a high risk locations should to be regularly reviewed.

Recommendation #4: Where an existing machine has been subject to a previous attack, an anti-skimming solution should be retrofitted.

As above, not all ATMs or locations are equally vulnerable and therefore special consideration , according to recommendation 2 , needs to be given for those ATMs having been subject to previous attacks

Recommendation #5: ATM Operators, card issuers and card schemes should continue to develop systems and procedures to identity skimming attacks and fraudulent transactions. Co-operation and information sharing should continue to develop and improve to ensure that losses are kept to a minimum.