EVRY TRANSACTION REVERSAL FRAUD SOLUTION for NCR 58xx

July 2017
BN054

Table of Contents

1 Transaction Reversal Fraud (TRF)

TRF involves the creation of an error that makes it appear as though the cash had not been dispensed. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction message.

Several cases of TRF fraud have been reported on NCR 58xx ATMs in Norway in Summer 2017. The perpetrators have managed to steal large amounts of money.

The fraudsters refrain from taking the card, and wait for the ATM to retract it. The cash exit shutter is forced open and the cash – now in the pre-present position – is stolen. They then physically prevent the card from being retracted. After the timeout they pull the card out. The Acquirer host issues a reversal message to the Issuer.

The transaction is reversed and the money is stolen. The operation can be repeated so the fraudsters can potentially empty the ATM.

2 Countermeasures

We have been in dialogue with NCR. They do not currently have any configuration options to prevent the notes from being moved to a pre-present position. NCR recommend the following countermeasures:

Change the flow from:

- Insert the card
- Enter PIN
- Select withdrawal amount
- Authorisation
- Dispense cash (note bundle is moved to the pre-present position just behind the shutter)
- Return card
- Present cash
- Send transaction
- Print receipt

To:

- Insert the card
- Enter PIN
- Select withdrawal amount
- Authorisation
- Return card
- Dispense cash (note bundle is moved to the pre-present position just behind the shutter)
- Present cash
- Send transaction
- Print receipt

NCR do offer protection devices which can be fitted at the ATM however these have the potential to be circumvented.

3 New NCR devices

We have the following statement from NCR re new devices:

With S1 dispenser ATM's, in general, NCR would advise to use EPS2. With the S2 dispenser there is the option to turn on Fraud status monitoring. There are also sometimes specific updates to combat specific issues, and I should also point out that often TRF issues are actually in fact resolved at the host level, not the ATM.

EPS

Enhanced Present Sequence, or EPS, is a firmware solution for the currency dispenser which helps to prevent Transaction Reversal Fraud (TRF).

TRF is a fraud where a criminal will attempt to induce a condition on the ATM such that the ATM software will interpret the manipulation as a fault condition, and return status information to the host such that the card holder account is not debited, but the card holder has managed to get the cash. In scenarios where a pre-paid card is used, then the card is not debited with the amount requested. Pre-paid card TRF has advantages for the criminal in that the account holder is anonymous.

EPS is a suite of dispenser anti-fraud countermeasures that have evolved over time, however, the basic function of EPS is to recognize that certain error conditions are more indicative for fraud, and in that circumstance, EPS will change the responding Transaction Code (T-Code) to a value of '3'. Most host systems will recognize a T-Code 3 as an 'unknown dispense' and will not reverse the transaction. This behavior deters the attack since the criminal account is always debited.

4 Result

In this way TRF can be prevented, and the customer will always be charged because they have access to the notes.

Actions to prevent TRF can either be implemented at the ATM with new protection devices or atg the processor, we recommend at the processor as a preference.