NCR SECURITY ADVISORY

DATE: March 5, 2021 **REV:** 1

Transaction Reversal Fraud (TRF)

Summary

Transaction Reversal Fraud (TRF) is a category of fraud where a criminal is able to remove some or all of the notes of a dispensed bunch, while the ATM host reverses the transaction such that no funds are debited from the account used to request the cash dispense. This reversal may be deliberately caused by a transaction fault caused by the criminal, or it may occur as a result as a reversal policy choice at the ATM host.
This paper describes considerations to be taken when implementing a host reversal policy, and some specific mitigations that can be taken against specific versions of TRF.

Transaction Reversal Description

Transaction Reversal may occur after a dispense operation when the result dispense operation is something other than a 'good' status. In that scenario, the ATM will send a message to the host indicating the status, and the host will either reverse the transaction or not, depending on the host policy for that dispense response status. If the host policy is to reverse, then the account which was used to request the dispense will be recredited with the amount of the dispense request. An example of a situation where the host would be expected to reverse would be in the case where the cash jams in the dispenser before it is presented to the cardholder and before the shutter unlocks. In this case, the cardholder would have no access to the cash, and therefore the transaction can be reversed as not to inconvenience the cardholder.

© 2021 NCR Corporation. All rights reserved.

NCR SECURITY ADVISORY

Dispense Response status codes – NDC

Table 1 below lists the possible dispense operation status codes in response to a Transaction Reply command message.

Table 9-48
Cash Handler Status

Field	Number of Characters	Content
g1/e1	1	Device Identifier Graphic 'E'.

Field	Number of Characters	Content
g2/e2	Var (23)	Transaction/Device Status (T-code plus T-data). Gives details of a dispense operation in response to a Transaction Reply Command message. Character 1 (T-code) can be:

Sol/Unsol	Code	Description
U	'0'	Successful operation and no cassette accessed, but an exception has occurred as detailed in subsequent fields.
S	'1'	Short dispense. For a spray dispenser, this can also indicate that an extra note has been dispensed.
S	'2'	No notes dispensed.
S	'3'	Notes dispensed unknown. The cardholder may have had access to any presented notes, so it should be assumed some may have been dispensed. Intervention may be required to reconcile the cash amount totals. The following counts contain requested dispense values.
S	'4'	No notes dispensed or card not ejected. This status is returned on a card before cash transaction if the stack operation fails and the notes are purged prior to card eject.
S/U	'5'	Some notes have been retracted when the notes were not taken following a Present time-out. The number of notes retracted is unknown.

Table 1 – extract from AANDC Reference Manual B006-6180-T000

© 2021 NCR Corporation. All rights reserved.

Using Table 1 above, this paper will now discuss typical reversal policies that could be applied.

TCode1 = 5 (response message E5)

Some notes have been retracted when the notes were not taken following a present timeout. The number of notes retracted is unknown.

This response would be received in the situation where the cardholder requested funds; the dispenser presented the cash; the cardholder does not take the notes; the transaction times out and the dispenser retracts the notes and deposits them in the retract bin. However, exactly the same response would be received if the cardholder carefully removes some of the presented notes and allows only the remainder to be retracted. The currency dispenser has no mechanism to count the retracted notes and so cannot be sure if all the cash is retracted or not. In this scenario, this transaction should not be reversed, because the cardholder had access to the cash.

Some financial institutions may wish to 'fine tune' their reversal policy in the event of a cash retract. For example, if the card bin can be recognized as an 'on us' transaction, the host may reverse on the basis that the cardholder is a known customer. In the case that such a policy is be implemented, mitigation should also be applied i.e. by manual balancing of the ATM to check that all funds are accounted for. In the case that the card is a foreign card (off us), or a pre paid card, than E5 transaction responses should never be reversed.

TCode1 = 3 (response message E3)

Notes dispensed unknown. The cardholder may have had access to presented notes, so it should be assumed that some have been dispensed. Manual intervention is required to reconcile cash totals.

This response may be generated if there is a fault in the cash dispense operation after the shutter has been unlocked. It may also be generated if a criminal deliberately causes a fault with the cash dispenser.

The policy considerations to an E3 response are similar to an E5. E3 responses should not routinely be reversed given that the cash whereabouts is unknown. It is far rarer for a financial institution to reverse on an E3, even where the cardholder account can be identified.

© 2021 NCR Corporation. All rights reserved.

Reversal Policy Guidelines

The examples given above illustrate some of the considerations that should be taken into account when applying a host reversal policy, but clearly those examples are not exhaustive. Criminals will attempt to exploit the specific interactions between specific versions of device hardware, firmware, platform software, application software, host message software and transaction timing in order to cause a reversal. Some further general points to consider are as follows.

Account number – TRF is a form of crime that requires a valid account number. This means that there would be a direct link to the criminal if the criminals own account was used. Typically, the criminal will use an untraceable account number for the fraud, either by using a skimmed or stolen card, or by using a prepaid card. For EMV based regions, skimmed cards are not feasible because the ATM will enforce that the chip is used. Since EMV chips cannot be copied, TRF in EMV regions is limited to stolen or prepaid cards. As soon as a stolen card is recognized as being used for TRF, it must be immediately blocked.

Pre-present operations – cash dispensers will often 'pre-present' the notes, meaning the notes are picked from the cassettes, stacked, and moved to a position directly behind the shutter, waiting for the final 'present' command that will open the shutter and move the notes to the cardholder. Pre-present is done to shorten transaction time. Most reversal policies will be based on cardholder access to cash or not, but be aware that there is a big difference between notes in the cassettes in the safe and a bunch of notes directly behind the shutter. Care should be taken not to reverse transactions with pre-presented bunches if the dispenser cannot safely retract the bunch into the reject bin.

Shutter manipulation – extra care must be taken before reversing any transaction that reports any kind of shutter fault. For example, a 'shutter jammed closed' fault may be deliberately caused by a criminal holding the shutter closed. This may lead to scenarios where the shutter has been unlocked by the ATM, and the criminal can exploit the time between the fault being reported (E2 - no notes dispensed) and the cash being retracted into the reject bin.

© 2021 NCR Corporation. All rights reserved.

Timing – TRF is a crime which happens in real time, and the criminal will try to exploit the message flow timing. Dispenser manipulation can happen outwith the normal command/response sequence of a transaction, so reversal decisions must also take account of unsolicited messages sent from the dispenser. For example, unexpected cash or carriage movement, or shutter movement after a fault are all indicators of possible TRF.

'3rd party' module faults – criminals can also be successful with TRF by causing faults on modules other than the cash dispenser. The example here is card reader faults where a card before cash transaction is interfered with to cause a reversal, but a pre-present operation on the dispenser provides an opportunity to steal the cash before it can be retracted.

Testing – it's not possible to give specific guidance for the above situations due to the variation in hardware and software combinations that may be deployed for any given ATM. However, it is possible for individual ATM deployers to test for TRF scenarios under lab conditions by performing a range of potential manipulation using the deployers production hardware and software, and then testing that the host reversal policy operates as expected. Under lab conditions it is also possible to simulate TRF without necessarily causing damage to hardware. For example, many TRF methods require the breaking open of the shutter. Under lab conditions, this can be simulated by operating the shutter by hand, either by opening the ATM fascia, or by removing the shutter assembly from the ATM. Other simulation can be made easier by having the dispenser racked out during the test so that various sensors and cash can be accessed. Testing is the most effective tool for determining that a reversal policy is operating as expected, because it tests the specific combinations of hardware and software in use.

Specific examples of TRF

Card Reader manipulation

Card reader manipulation TRF is an example of '3rd party' module fault TRF. This method applies to ATMs with motorized card readers, and a 'card before cash' application flow. In this method, the criminal will cause a fault at the card reader after the ATM has received the

© 2021 NCR Corporation. All rights reserved.

authorization to dispense. The card reader fault will cause the transaction to reverse (because no cash has been presented), but the criminal has the opportunity to force the shutter open to remove the pre-presented cash. Card reader manipulation TRF may be prevented by configuring the ATM application such that it does not pick notes until after the card is successfully returned to the cardholder.

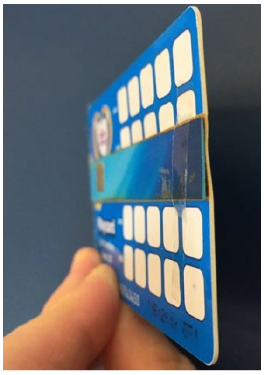
There are four known variations of this method:

- The 'Swallow'. When the card is ejected, the criminal does not take the card, and will wait for the transaction to time out. The ATM will then capture (swallow) the card and reverse the transaction. At this point, the shutter will be forced, and the cash removed.
- The 'Jam'. When the card is ejected, the criminal does not take the card, and will wait for the transaction to time out. But instead of letting the card be captured, the criminal will hold on to the card such that it appears to be jammed. The ATM will then timeout and reverse the transaction. At this point, the shutter will be forced, and the cash removed.
- The 'Swap'. When the card is ejected, the criminal does not take the card, and will force a second sacrificial card into the card slot, while removing the original card. The ATM cannot recognize the swap, and will capture the sacrificial card. The ATM will then reverse the transaction. At this point, the shutter will be forced, and the cash removed. In this method, the sacrificial card will not be a bank card, but can be any magnetic card, e.g. loyalty cards, hotel key cards, lottery cards etc. The reason for this method is so not to lose an EMV card corresponding to the account used for TRF. The TRF card will typically be a stolen card.
- The 'Chip on a Strip'. This is a more sophisticated version of 'the swap'. In this method, the TRF EMV card is located into a sacrificial magnetic carrier card. The TRF EMV card is cut into a strip such that is can be carried by the magnetic card. (See pictures below). When the strip and carrier is ejected, the criminal will carefully remove the strip, leaving the carrier to be captured. The transaction then reverses, the shutter is forced, and cash removed.

© 2021 NCR Corporation. All rights reserved.

NCR SECURITY ADVISORY





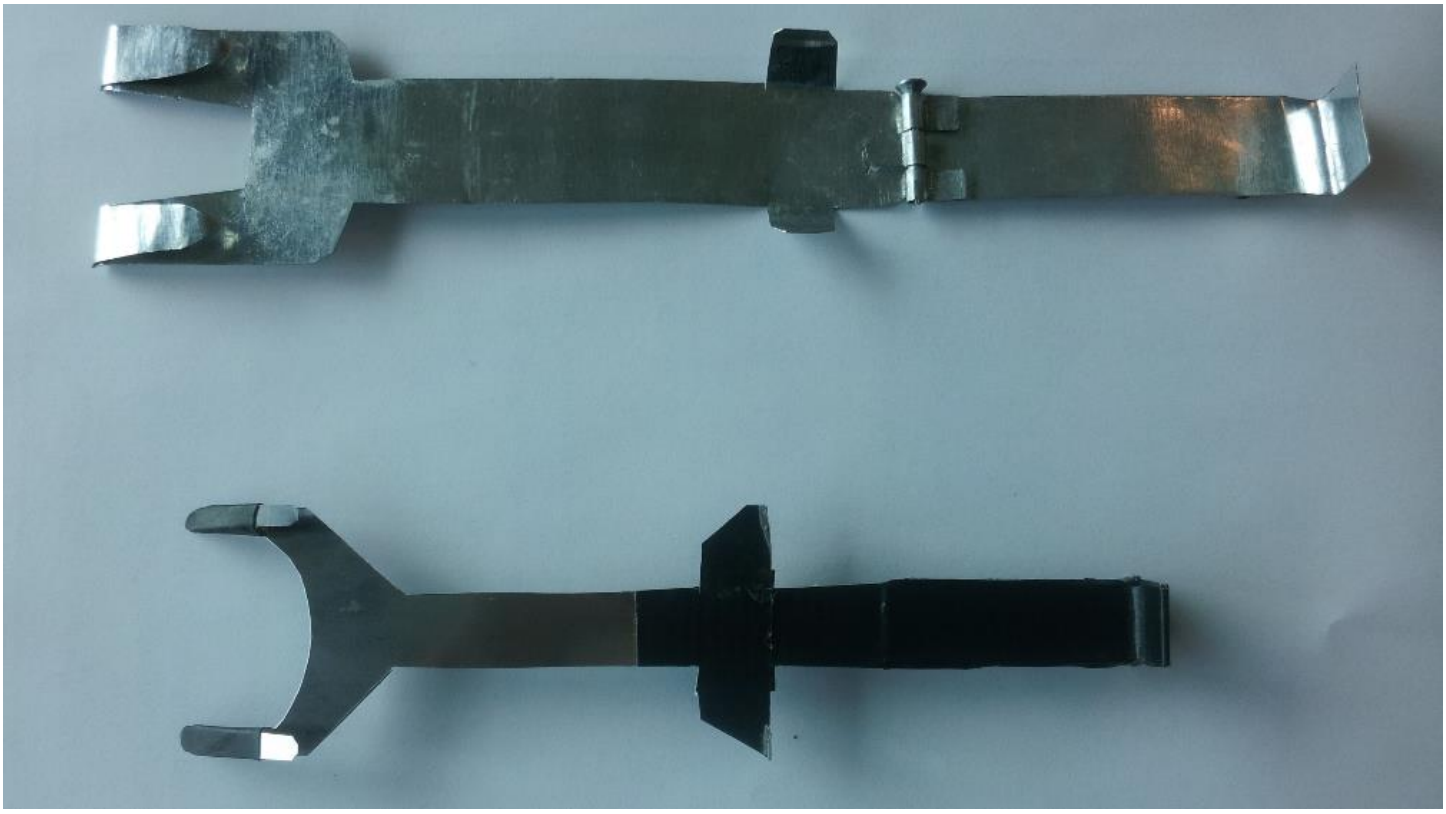
‘Chip on a strip’ carrier cards and example TRF EMV strip.

Cash Claw TRF

In this method, a device is inserted into the belt driven transport of a dispenser such as the NCR S1. The purpose of the device is to trap cash before it can be presented to the cardholder, and also to prevent the cash from being into the reject bin. The criminal will begin by preforming a legitimate transaction, typically for a low value amount. When the cash is presented through the open shutter, the criminal will use that opportunity to insert the trapping device. Once the device is fitted, the cash will be taken, the shutter will close leaving the device inside the dispenser. A second transaction will then be requested, this time for the maximum amount allowed. The cash will be trapped by the device and cause a jam. The transaction will reverse and the ATM will go out of service. The criminal can now break open the shutter and remove both the device and the cash. No funds will have been debited from the account. Cash claw TRF can be identified by the pattern of events; low value transaction followed by high value transaction with the same card, a cash jam at a specific point in the transport, and a shutter break. Cash Claw TRF can be prevented by recognition of the pattern to prevent reversal of the high value transaction. Alternatively, upgrade hardware is available to prevent successful placement of the claw. Cash Claw TRF is not feasible on the NCR S2 dispenser.

© 2021 NCR Corporation. All rights reserved.

NCR SECURITY ADVISORY



Examples of cash claws.

Please contact your NCR Account Manager if you have any questions or need additional information.

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 please contact Owen Wild

© 2021 NCR Corporation. All rights reserved.

NCR SECURITY ADVISORY

Please refer any media inquiries or questions to Aaron Gould

© 2021 NCR Corporation. All rights reserved.