Transaction Reversal Fraud

ATMs have experienced cash losses and physical damage because of Transaction Reversal Fraud (TRF). This is a scheme where the perpetrator forcibly removes cash from the dispenser prior to the transaction being fully completed and then through the process manipulates the machine to reverse the transaction (i.e. not debit the account).

Here is how it works:

1. A card and PIN are correctly entered into the ATM, and a cash withdrawal is requested.
2. While the transaction is being authorized the ATM will pre-position the bills behind the dispenser shutter, ready to dispense.
3. The card is ejected waiting for the user to take before dispensing the cash.
4. Rather than take the card as per a normal transaction, the criminal leaves the card in the slot.
5. The machine will try to re-capture the card.
6. The criminal will hold onto the card preventing it from being captured. The criminal may use a screwdriver or other tool to hold the card in the reader.
7. This results in the ATM reporting a card jam.
8. Because no cash has been dispensed, the software will reverse the transaction.
9. The criminal will force open the cash dispenser and remove the cash before the ATM is able to put it into the dispenser reject bin.
10. The criminal leaves with the cash along with the debit/credit card and no account has been debited. The machine will be out of balance and likely show signs of damage.

** This crime depends on precise timing. In some variations - during the process, the criminal may insert a gift card while simultaneously removing the debit/credit card. This gift card has been captured in some instances. Finding non-financial cards in the card capture bin may be an indicator. See images that follow.*

** This crime is only applicable to ATMs with motorized card readers, and with applications configured for card before cash.*