Weights & Measures/Enforcement Division

(WAM-ED)

Part 1: Recognizing Skimmers

Goals of This Training

- Understand what credit card skimmers are and how they work
- Are familiar with the known types of credit card skimmers and can recognize typical configurations already seen in the marketplace
- Recognize common red flags that could be a clue a device has been tampered with

How Credit Card Readers Work

- Card is swiped, and electronically read.
- Keyboard may or may not be used for security code
- Data is transferred from card reader and keypad to small board behind card reader
- Data then transferred via ribbon cable or wires to larger board which communicates with console and operates dispenser
- Data verified through cc system at console and pump authorized
- As long as signal gets successfully to console, no way to suspect that data is being stolen.

How Credit Card Skimmers Work

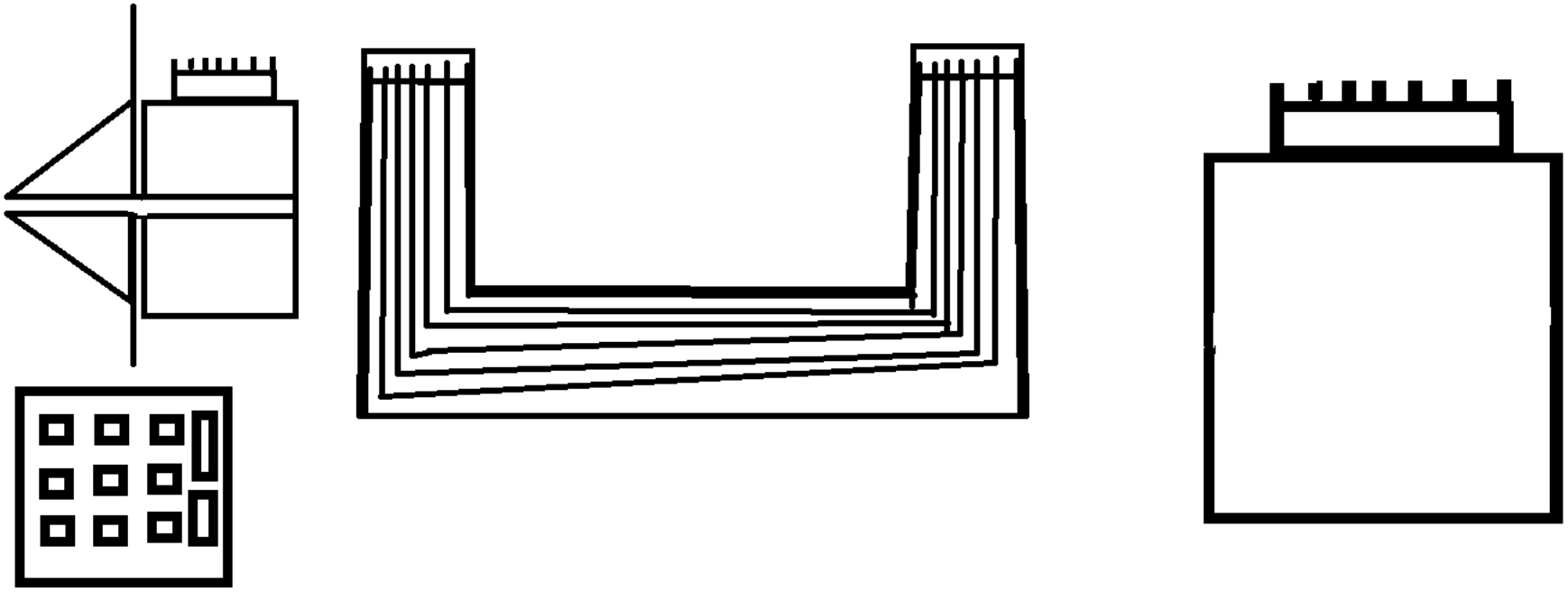
- Two Types
  - Shimmer: Fits overs the outside of a card reader and reads the credit card information even before real card reader does.
    - Used on ATMs or devices where it is hard to access interior of device
    - Reports of some being slipped into chip readers
    - Easier to install.
  - Skimmer: Reads the signal between the card reader and the main board. It copies the information but does not stop it reaching the board.
    - Most common on gas pumps with easy access to the inside
    - Rare on ATM's
    - Can't detect without opening the cabinet

How Credit Card Skimmers Work

- Both types store stolen information.
- Both types may also transmit the information via bluetooth so that the device never has to be removed.
- Once information is collected it can be:
  - Sold to someone out of state or even out of the country
  - Used for online transactions
  - Copied to fake cards using the same technology that makes hotel room keys; used to buy legitimate gift cards (name on card matches person's id but name on receipt is different)

4 Basic Components of a Credit Card System

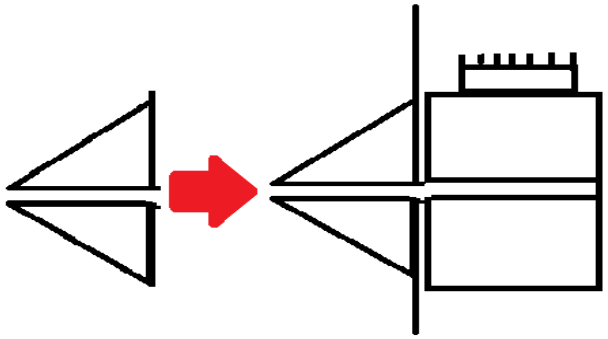
- Card reader with board and 7 pin connection
- 7 wire cable (either 4 -7 wires or a ribbon cable)
- Main board to enable dispenser
- Key pad which may be connected to card reader board or on a separate line to main board



External (Shimmers) Skimmers

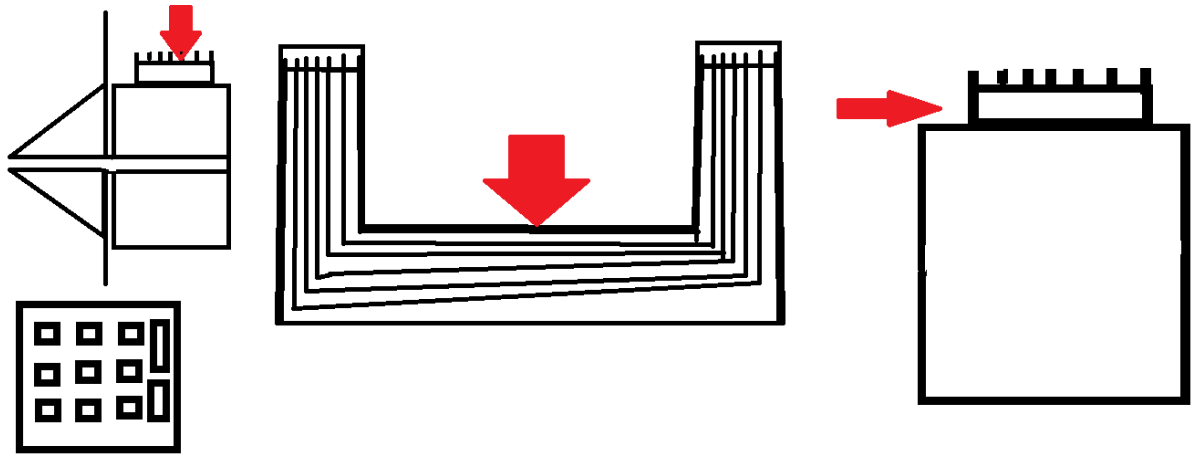
- Slide over the outside of the existing skimmer
- Are self-contained, no wires or connections to any other components
- Read the card and store the information without affecting real card reader.
- Can be quickly installed & removed without detection.

http://froggy ngs/1038/this-is-how-fast-a- an-be-installed/



Internal Skimmers

- Copy the information at one of 3 points:
  - At the card reader board (might also connect to card reader)
  - In the cable
  - At the device main board
- 10 seconds to install including opening cabinet



Internal Skimmers

- Installation requires access to inner cabinet
  - Older model dispensers have common keys which are available to virtually anyone who wants them.
  - Dispenser locks not very sturdy, designed to keep out the curious not the criminal
  - Tangle of wires inside can camouflage skimmers from the untrained eye

Transmitting the Information

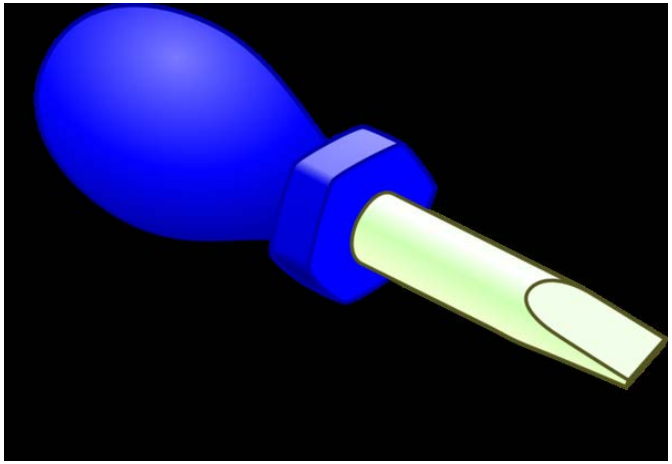
- Both types can be set up to transmit via bluetooth
- Means nobody has to risk trying to remove the devices to retrieve the information
  - When they return, they look like they are buying gas while they are really downloading the stolen information

How to Detect External Skimmers

- Look for card readers that protrude more than the rest or look slightly different
- “Wiggle” card readers. Loose external readers may actually pull right off.

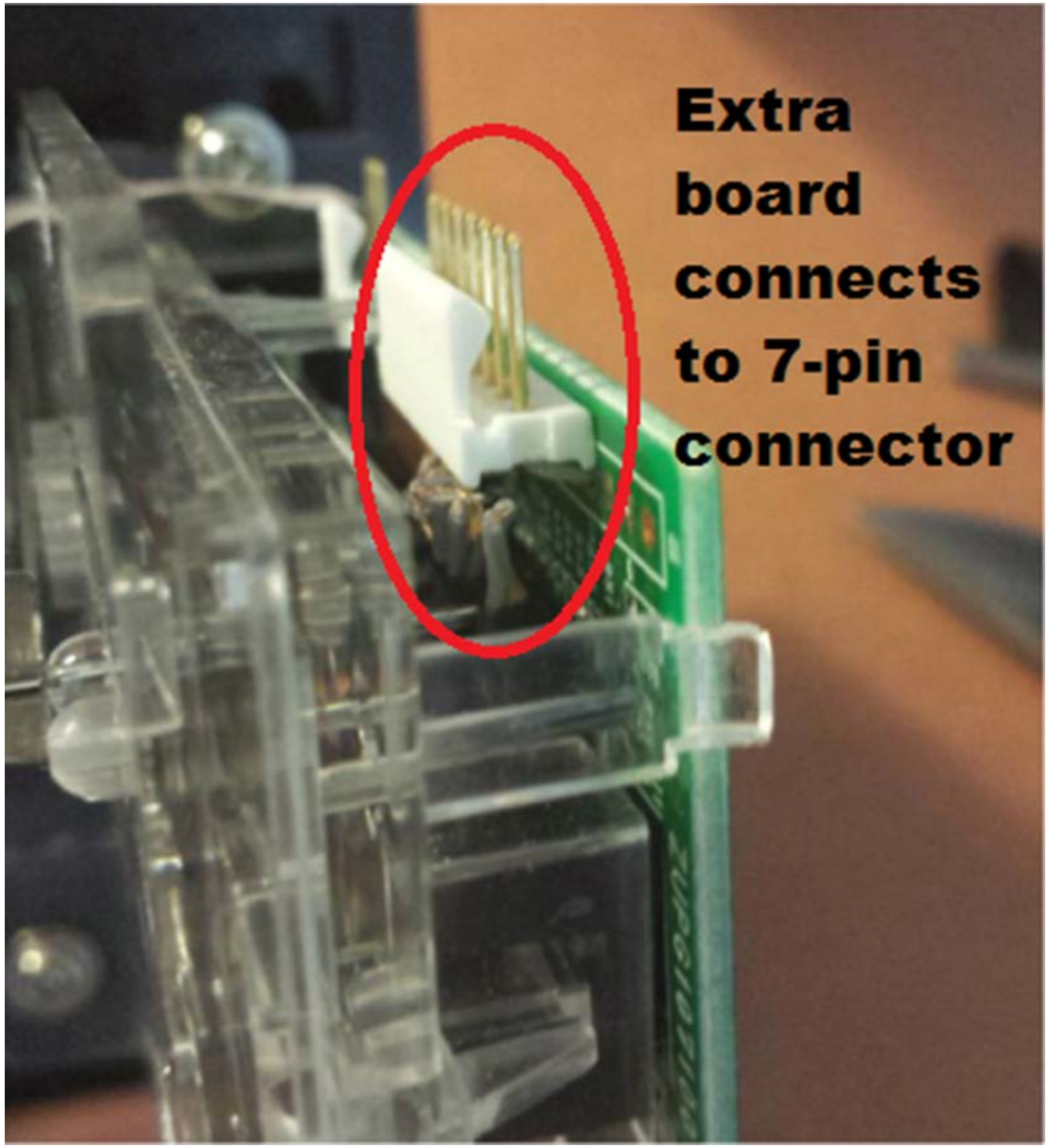
How to Detect Tampering

- Look for evidence of illicit entry into cabinet
  - Cabinet bent or scratched as if it had been pried open
  - Security tape missing or broken
  - Tool marks or damage to lock

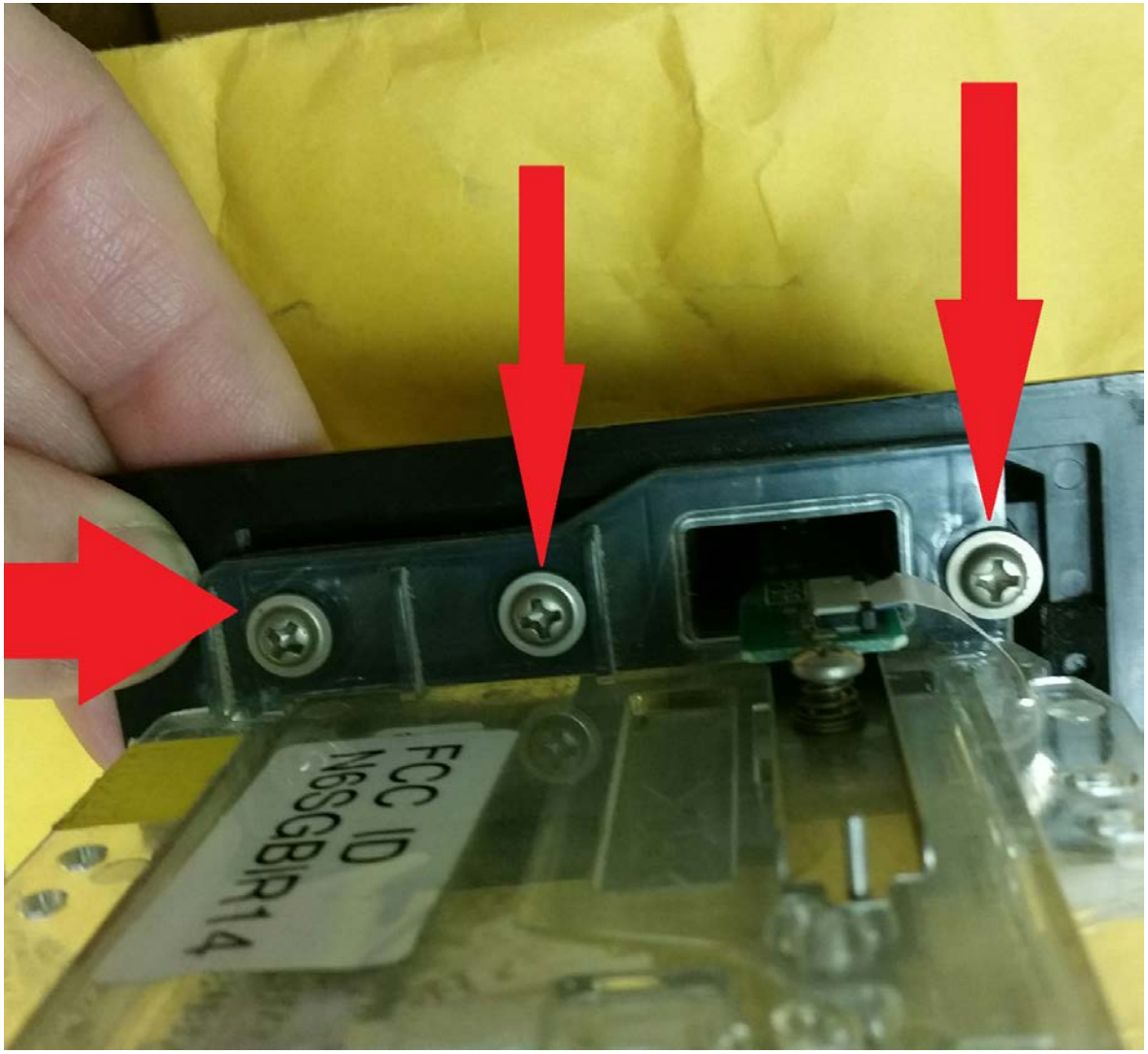


Detect Internal Skimmers at the Boards

- Check the board behind the credit card reader to see that there is nothing attached to the underside of the 7 pin connector or between the 7 pin connector and the ribbon tape.
- Look for loose or missing screws that show board has been replaced
- Do the same thing at the board which controls the pump's operation.


Extra
board
connects
to 7-pin
connector

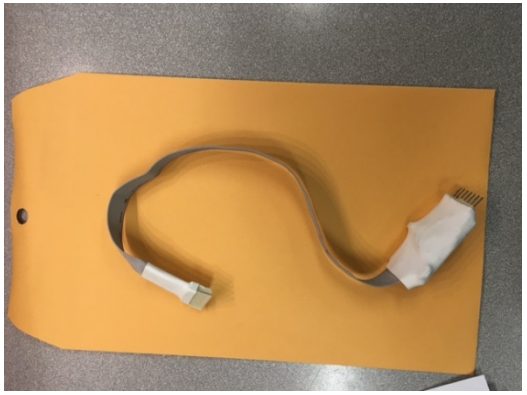
Premade to Replace Existing Board

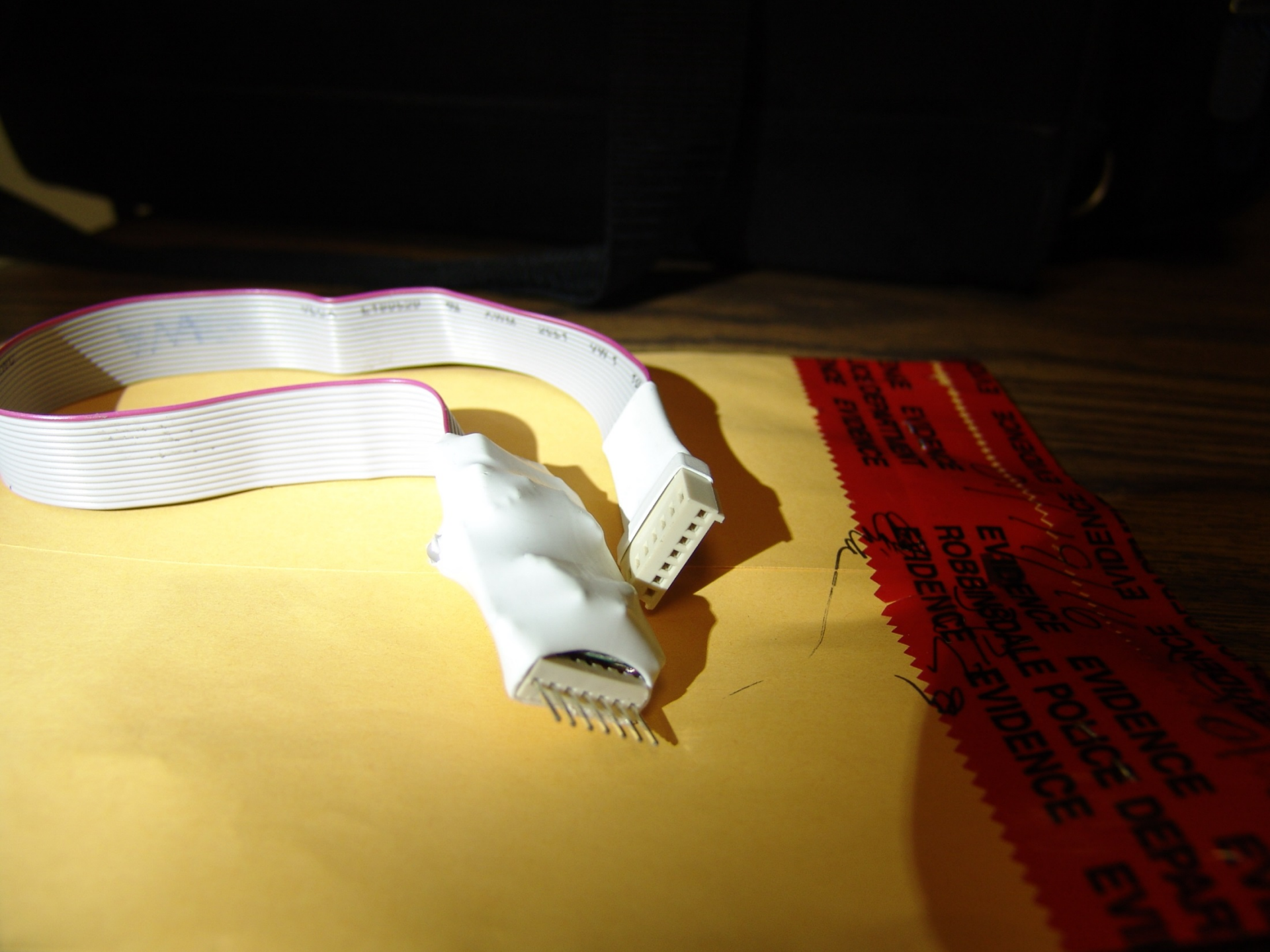


One of these things is not like the others…

Detect Internal Skimmers Between the Boards

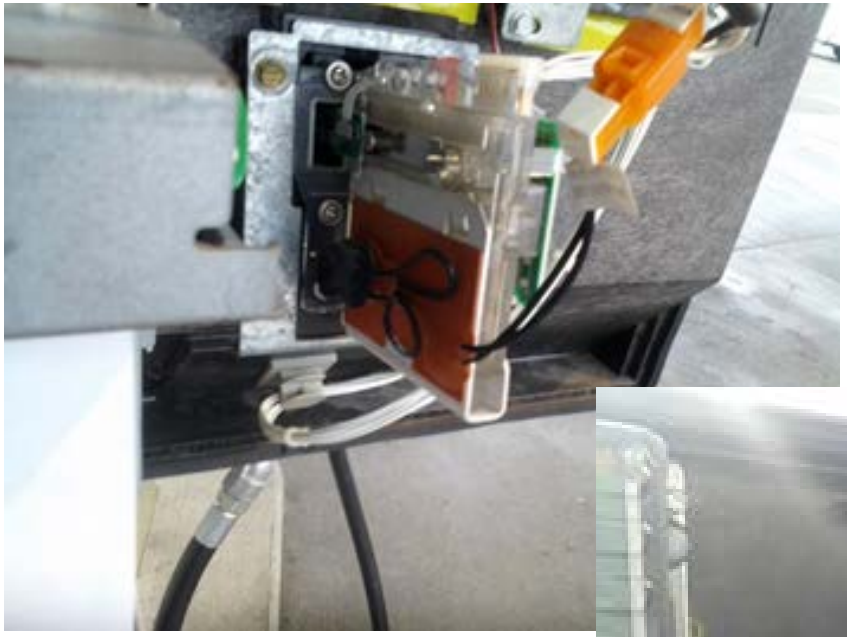
- Check the connection from the board on the card reader all the way to the board that controls the operation of the pump.
  - Ribbon (or wires) should be unbroken from one connection to the other
    - If the ribbon or wires are different
  - No objects along the ribbon
  - Only one ribbon coming from the board




EVIDENCE
EVIDENCE
EVIDENCE
EVIDENCE

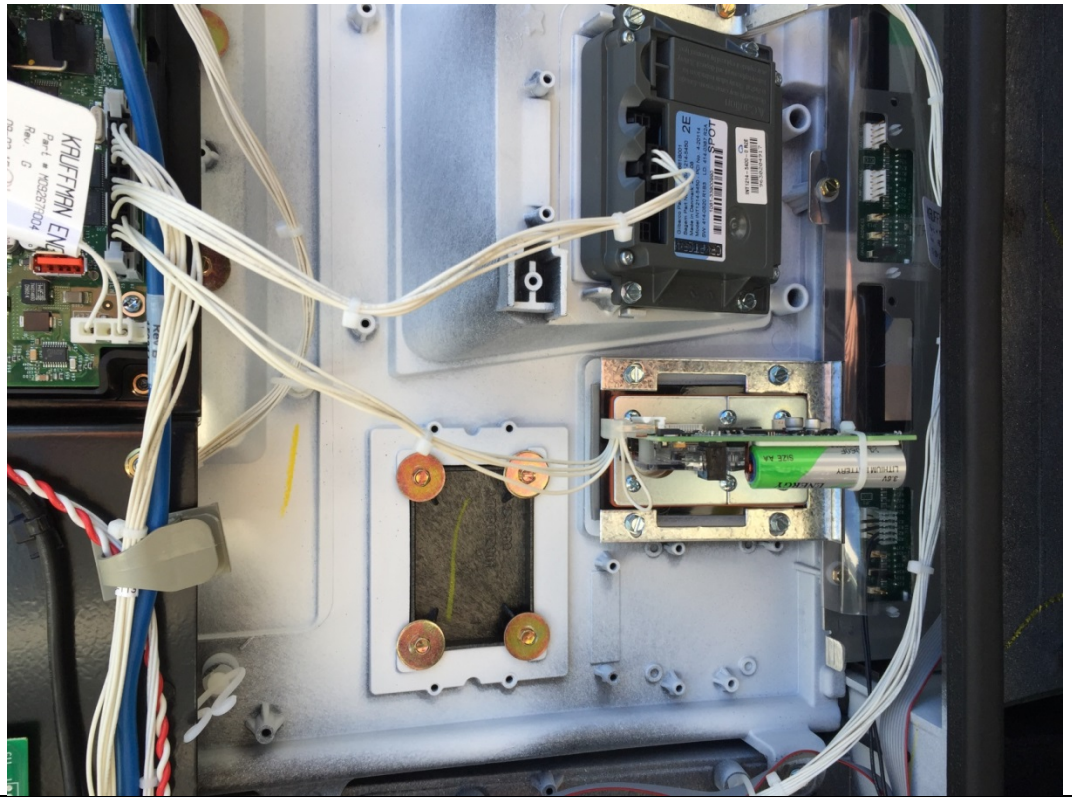
Suspicious Looking Devices

- Heaters –
  - Only 2 wires to supply power
  - Don’t connect to 7-pin data connection



Suspicious Looking Devices

- Extra battery in case of power outage
  - Batteries are rechargeable and really big!

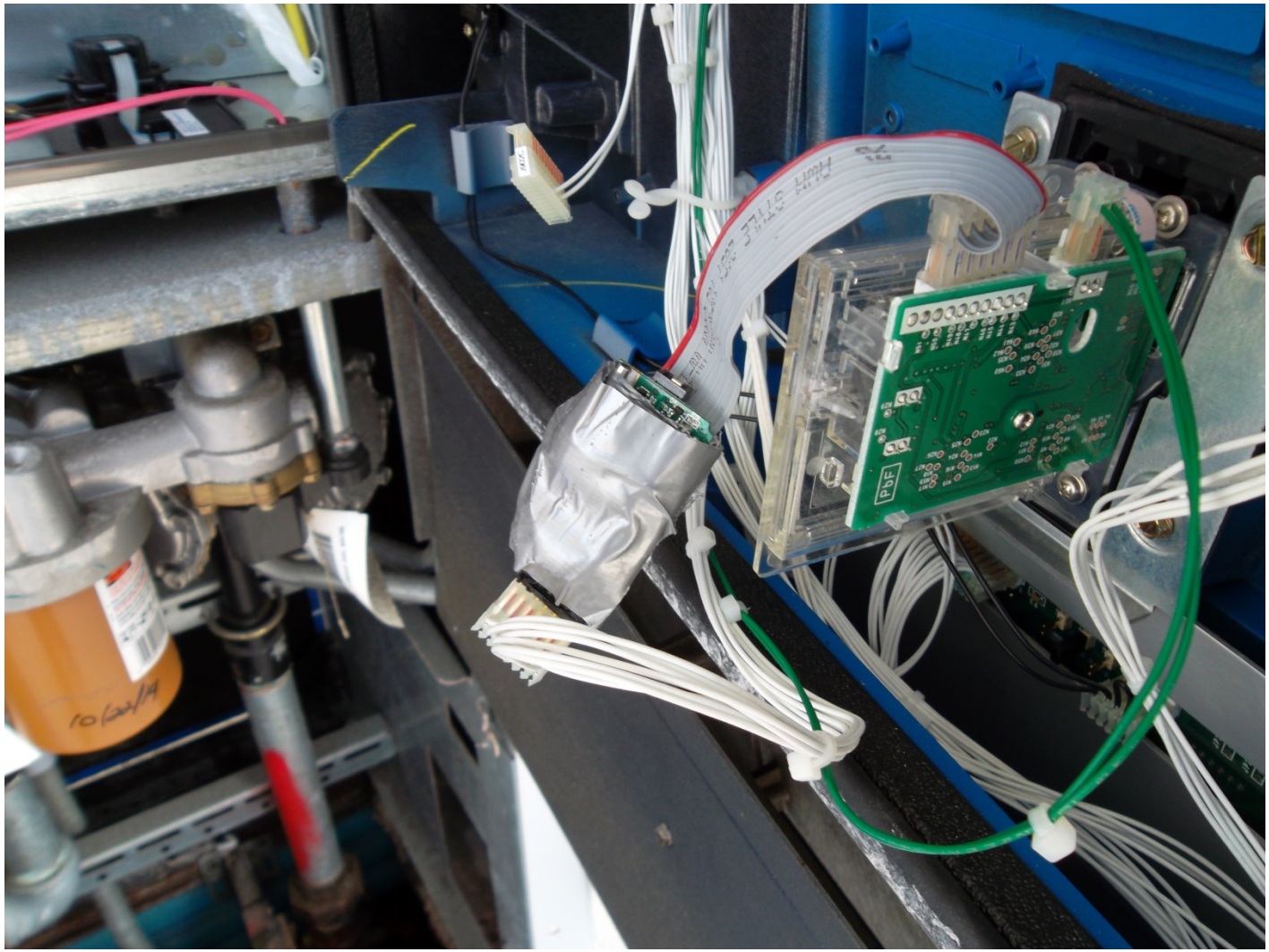


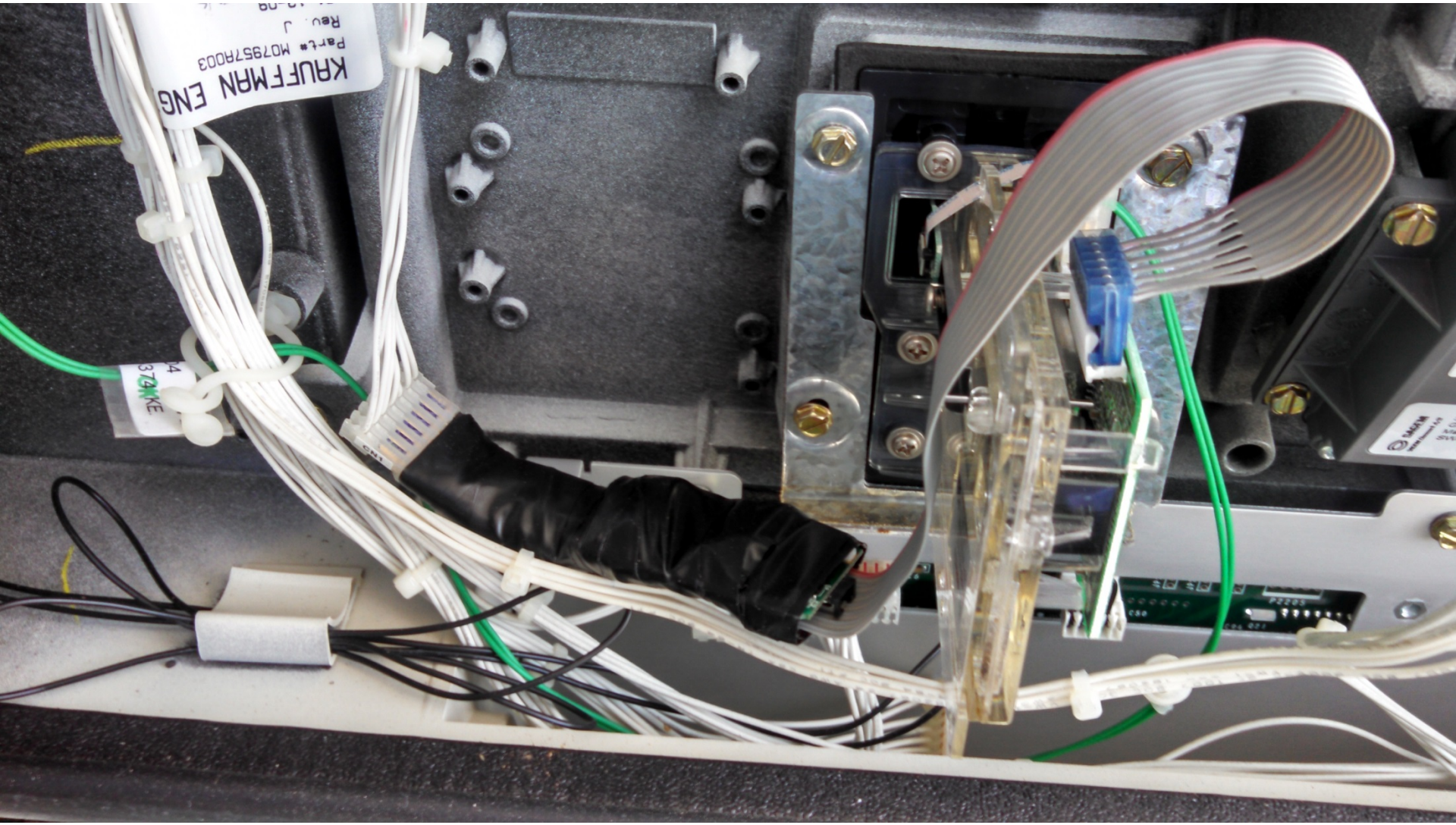
When in doubt

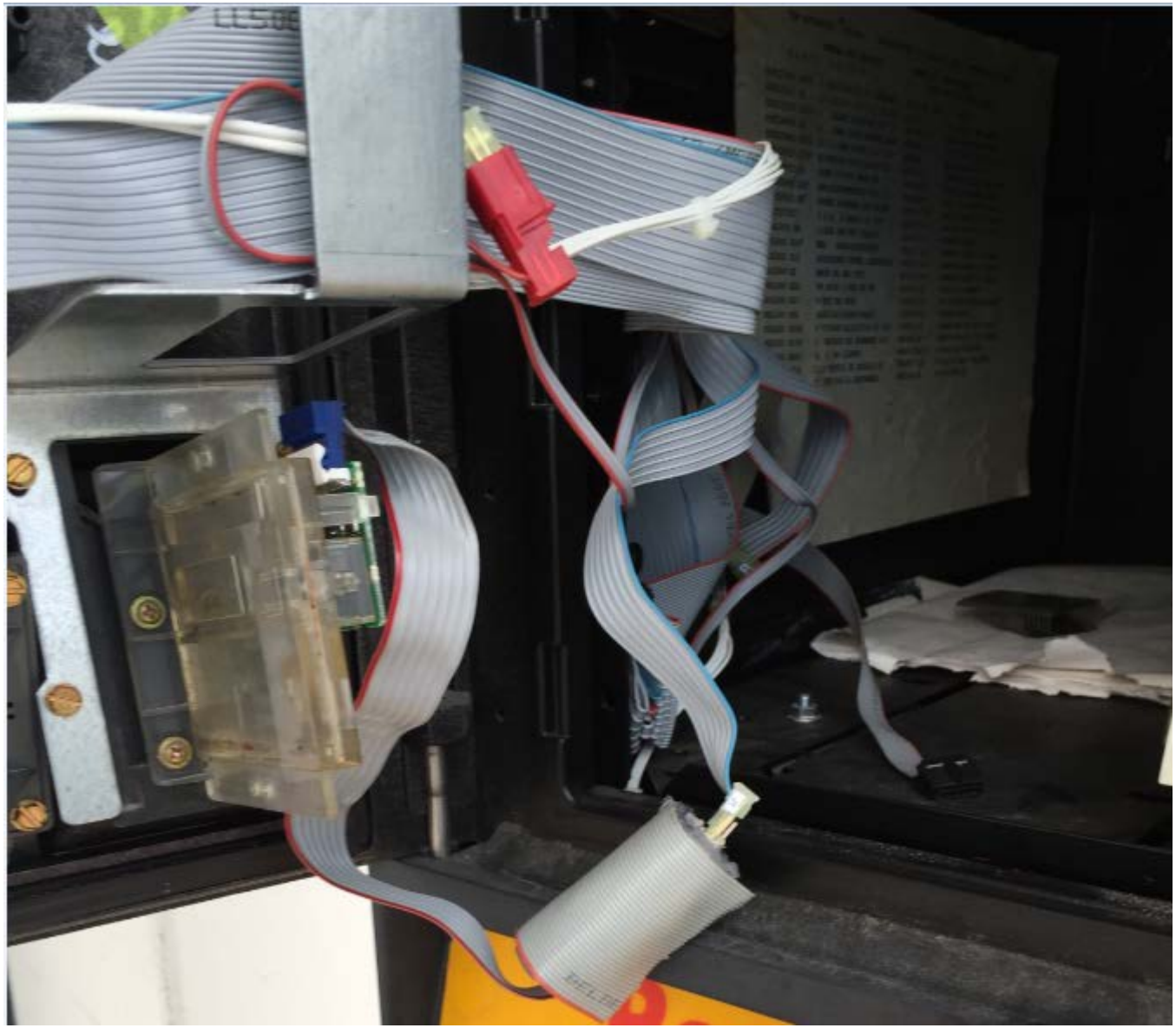
- Take a picture
- Work with service company
- Better a false alarm than a missed skimmer

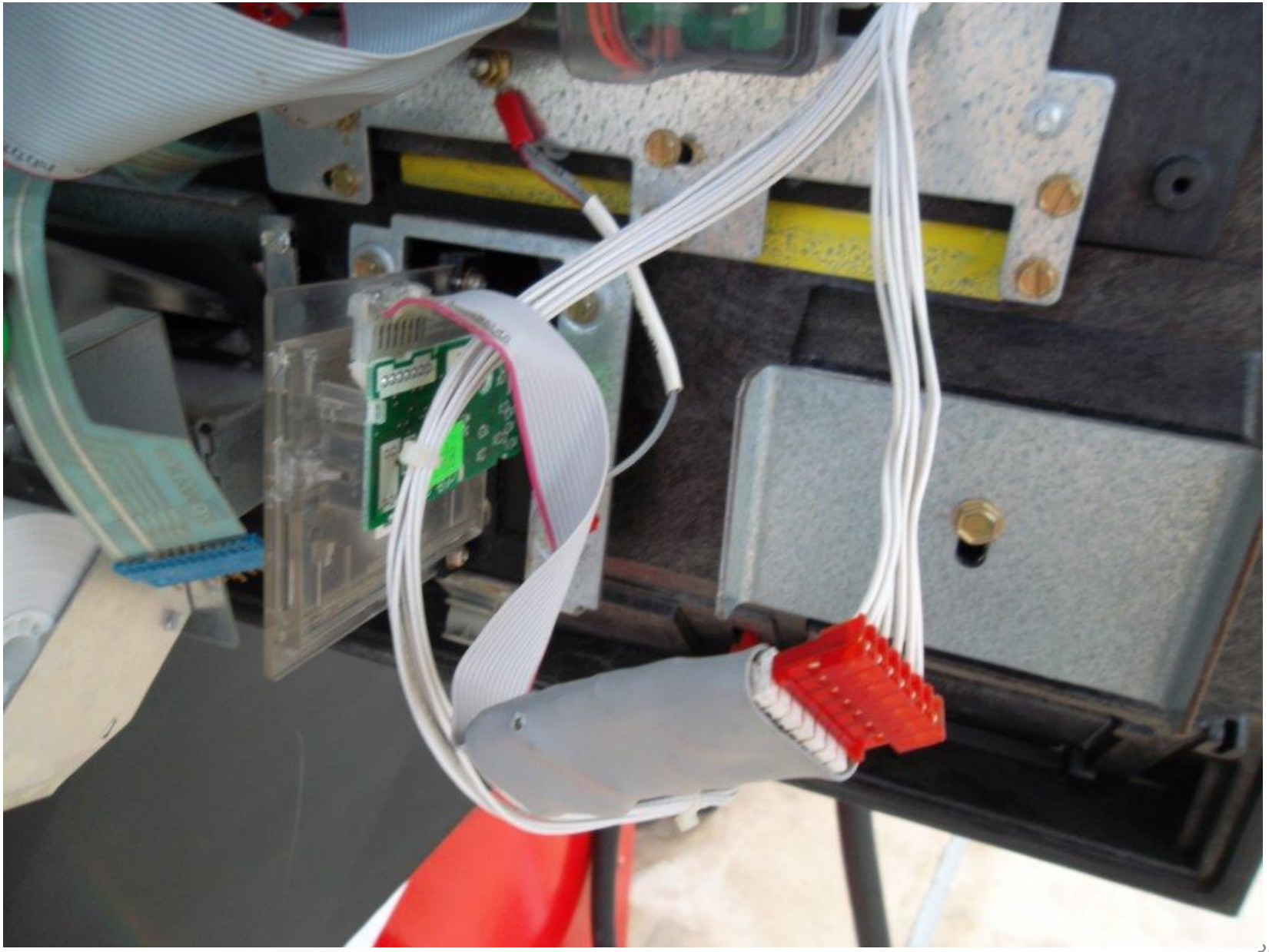
Skimmer or not skimmer?

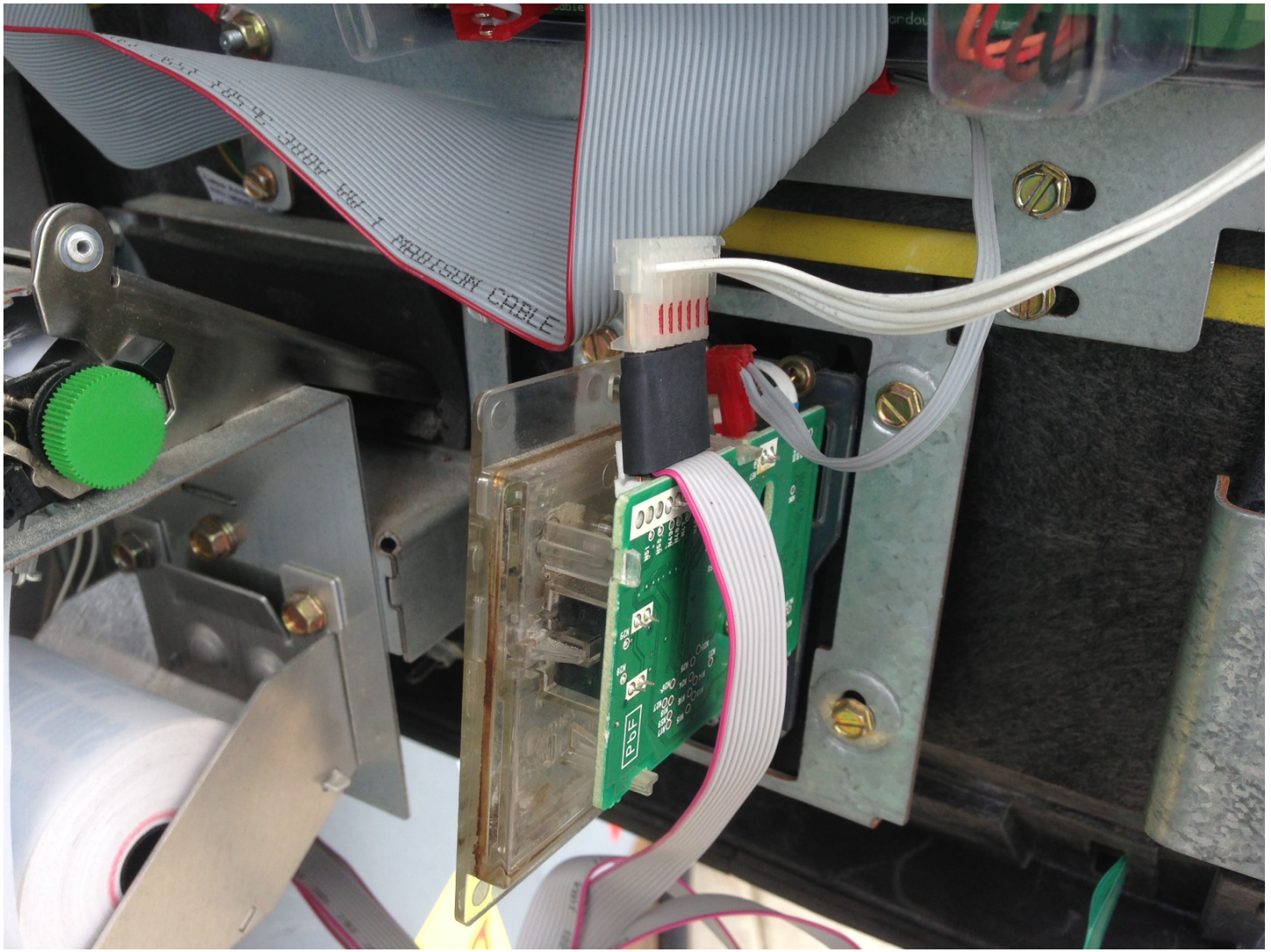
LET'S TEST OURSELVES

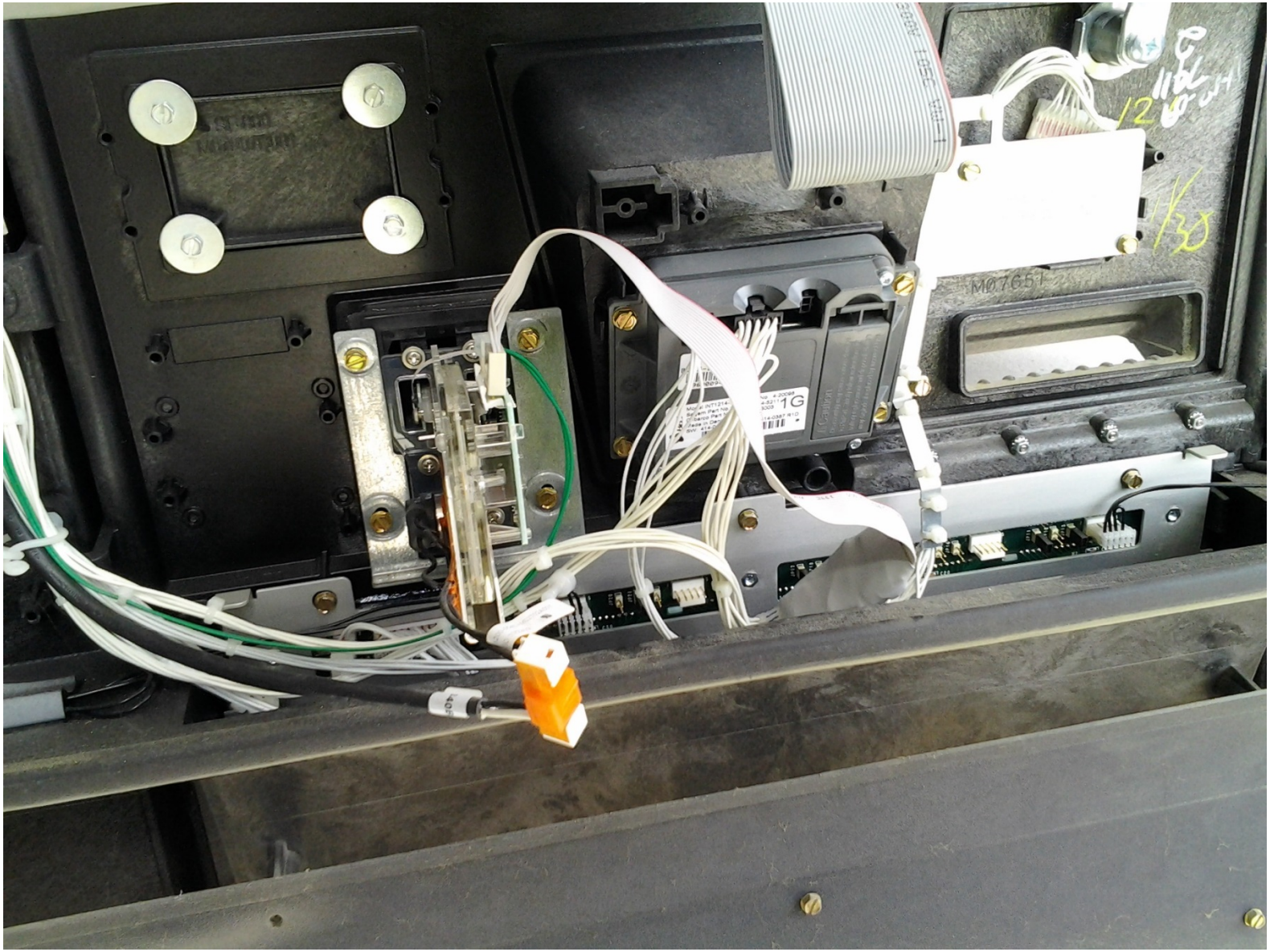


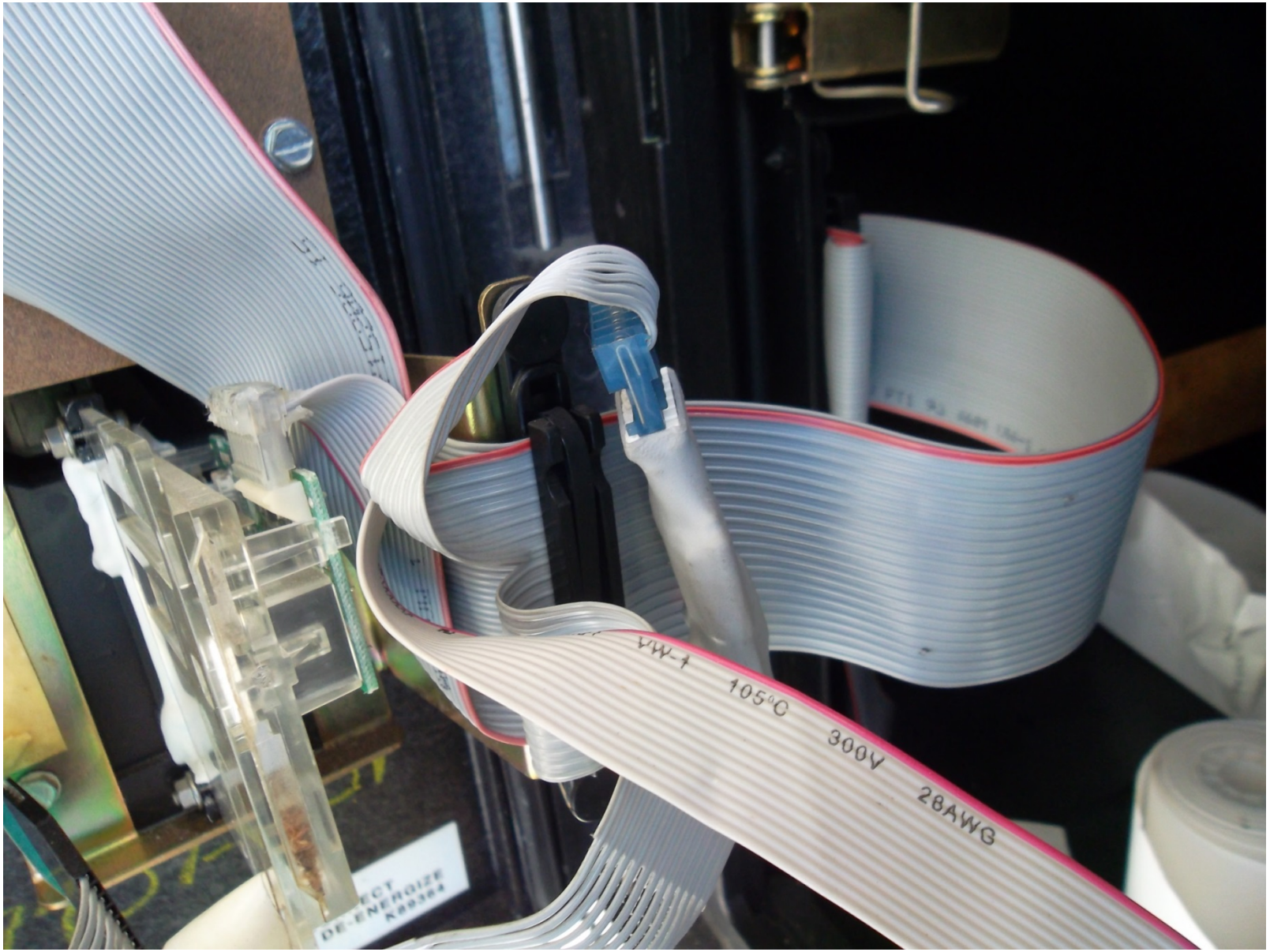

KRUEGER ENG
Part# M079578003



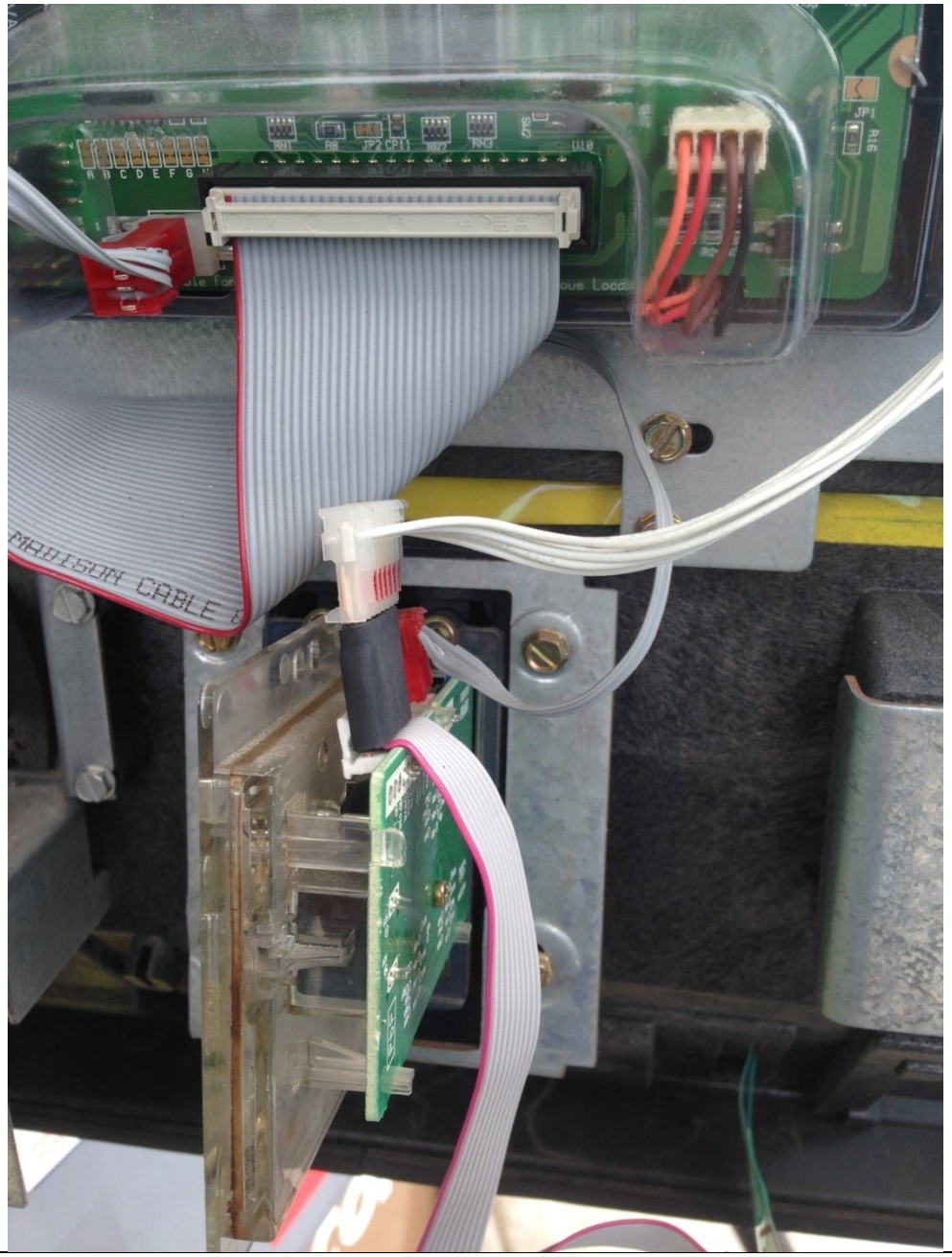



MADISON CABLE




VW-1
105°C
300V
28AWG


105°C
300V


MADISON CABLE

Questions?