



**Credit Card Skimmers:
Protect Your Customers
Protect Your Business**

Julie Quinn, Weights & Measures Director
September, 2016

Goals of This Training

Part 1:

- Understand what credit card skimmers are and how they work
- Understand how ‘Chip’ technology can protect your business as well as your customers
- Know how to deter installation of skimmers
- Know how to recognize skimmers
- Know how to respond if you discover a skimming device

Part 2:

- Know how to look for/recognize internal skimmers

Disclaimer

- Credit card fraud is constantly evolving
- Information presented today is intended to assist station owners and operators but is not guaranteed to cover all new developments
- Ultimately owners and operators bear the responsibility for protecting customer credit card data and should seek ongoing assistance from
 - Local Weights & Measures jurisdictions
 - Local law enforcement
 - Service companies
 - Credit card companies
 - Industry organizations



Shimmers and Skimmers

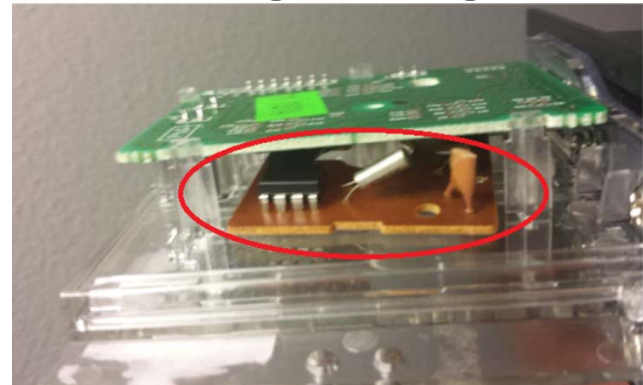
- **Shimmer:** Fits overs the outside of a card reader and reads the credit card information even *before* real card reader does.
 - Often used on ATMs or devices where it is hard to access interior of device
 - Relatively easy to detect if you are looking
- **Skimmer:** Reads the signal between the card reader and the main board *after* the card reader has already read the credit card.
 - Most common on gas pumps with easy access to the inside
 - Rare on ATM's
 - Can't detect without opening the cabinet and checking from card reader to motherboard

Shimmers and Skimmers

Shimmers: Installed easily and quickly anywhere



Skimmers: Needs internal access; requires training to recognize



Shimmers

- Look for them everywhere
 - ATMs
 - Cash Registers
 - Vending Machines
 - Car Washes
 - Fuel dispensers
- Take only seconds to install

Watch how fast a credit card skimmer can be installed at a busy cash register

How Shimmers & Skimmers Work

- Both types capture credit card and PIN info
 - cameras aimed on key pads
 - magnetic overlays on the keypad
 - Wired connections from keypad to skimmer
- Both types transfer info to ‘the bad guys’
 - Blue tooth; or
 - When device is removed from credit card reader
- Info is used or sold to others to use
 - Black net
 - Online transactions
 - Copied to fake cards using same technology used to make hotel keys



Who is Installing These Devices?



- Organized Crime
 - Hires people to travel to various states and install
 - May hire contractors or employees
 - Sells info on ‘Black Net’, info might be used right away, or not for months, or even a year
- Tech-savvy individuals with access
 - Skimmers easy to make from readily available materials
 - Make fake cards that match their own credentials, then buy gift cards that can’t be traced. (Clue: Customer info on card won’t match info on receipt)

Why You Should Care

- Customers harmed financially
- Credit card fees raised to cover theft loss
- Business reputation damaged
- Potential financial liability to your business



Chip Technology = Financial Protection

9 U.S. payment card networks have shifted liability for fraud to merchants who have not activated Europay Mastercard Visa (EMV) chip technology by October 1, 2015.

- Accel
- American Express
- China UnionPay
- Discover
- MasterCard
- NYCE Payments Network
- SHAZAM Network
- STAR Network
- Visa



Gas Pumps and ATM's have until October 1, 2017

Credit: <http://www.creditcards.com/credit-card-news/understanding-EMV-fraud-liability-shift-1271.php>

When is Merchant Liabile?

- Counterfeit Card
 - Mag stripe data stolen from chip card at mag stripe terminal and fraud occurs
 - Chip card used at a mag stripe terminal
- Lost or Stolen Card
 - Chip card used at mag stripe terminal
 - Chip & PIN card used at chip & signature terminal

Sources: <http://www.creditcards.com/credit-card-news/understanding-EMV-fraud-liability-shift-1271.php>

<http://www.entrustdatacard.com>

How EMV Chip Tech Protects

- ***Encrypted*** live communication between credit card company and card at retail location protects against fake cards
 - Random code exchanged to verify legitimacy of card
 - No ability for counterfeiters to generate correct random codes
- PIN and/or signature protects against lost or stolen card
 - Name on card should match name on signature box
- Card is still vulnerable if used online or swiped at a reader which doesn't have chip technology
- Everybody safer when everybody has EMV chip

Deter Use of Fraudulent Cards

- Limit small purchases with credit cards
 - Criminals often test a card with a purchase of a few dollars before using it for a bigger purchase
 - Some banks and credit cards are already setting \$5 minimums
- Check the name on the credit card against the name that appears on the cash register and signature box .
 - Refuse the transaction if they do not match.
- Get chip technology installed and activated

Deter Skimmer Installation

- Upgrade your dispensers
- Add or change locks on dispensers
- Install security cameras and alarms
- Create a clear line of sight
- Use tamper tape
- Develop and advertise daily inspection program
- Encourage local law enforcement to create community program

Upgrade Dispensers

- Older models are vulnerable
 - Universal keys work across models
 - Locks easily jimmied
- New models have security options
 - Alarms if opened
 - Automatic shutdown if credit card compartment opened, requiring technician to reactivate
 - Become inoperable if components disconnected even momentarily


Add or Change locks

- Customize keys
- Only necessary on compartment which accesses card reader and key pad
 - Often not the same compartment as the printer paper
- Hasp and padlock can do the job
- Control who has access to the keys
 - Keep a log



Install Cameras and Alarms

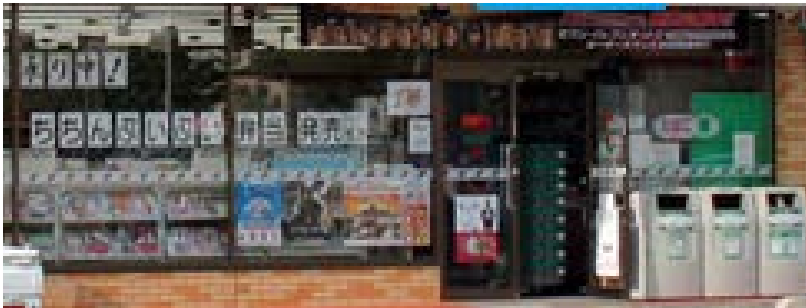
- Make sure external cameras capture all dispensers
 - Some criminals like the far pumps because of less risk when installing
 - Some criminals willing to take a risk for bigger payoff at busier pumps
- Consider installing after-market security
 - internal motion-activated cameras
 - Tie alarms to building security for after-hour protection
- Advertise that alarms and cameras are in use



Warning!
Alarm Will Sound
if Dispenser is
Opened.

Create a Clear Line of Sight

Safer for everyone if cash register can see what is happening at the dispensers.



Tamper Tape Recommendations

- Personalized, not generic
- Serial number and/or bar code
- Void if tampered with
- Place it strategically
- Checked daily (or even every shift)
 - Don't have it be the same person every time
 - Keep a log
 - Consequences if checks are not done
- Checked after contractors/inspectors to make sure tape is replaced

Where to use Tamper Tape

- Over opening to card reader boards
 - not on hinge side!
 - Might not be the same as printer paper access
- Over outside of card reader
- Over key pad
- Over key holes



Issues with these seals?

Tamper-evident seals



Daily Inspection Program

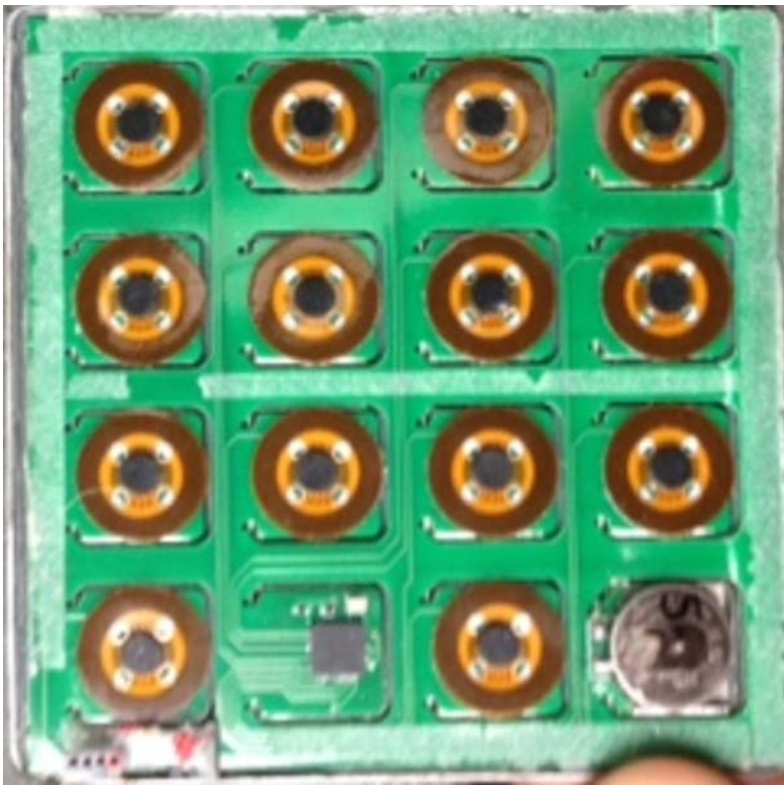
- Build a detection system
 - All employees trained to look for external indicators & shimmers
 - Broken or missing tamper tape
 - Tool marks/bent or damaged cabinets
 - Jammed card readers (sign of a shimmer)
 - Management trained to recognize internal skimmers
 - Tamper tape serial numbers and locations tracked
 - Daily inspections
 - Every shift?
 - Last thing at night/first thing in the morning?
 - Ability to detect if daily inspection not done
 - Consequences if daily inspection not done
- Weekends and evenings are especially important
 - Staffing low
 - Less chance of detection

Look for External Shimmers

- 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.



Look for Key Pad Overlays



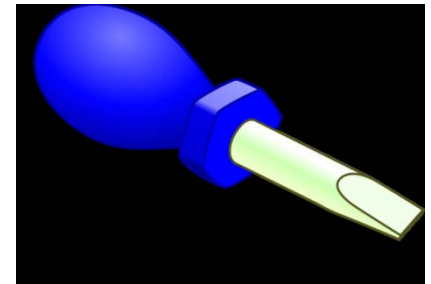
Look For Cameras

- ‘Pin-hole’ cameras located above or to side of keypad
- Camera located at a distance



Look for 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
- Clerks should call Management
 - Someone w/authority should be on hand
 - Only trained personnel should open cabinets



Community Enforcement Program

SkimStop Program

Developed by Eagan MN Police /available to other PDs

Aaron Machtemes

(651) 675-5728

amachtemes@cityofeagan.com

http://www.cityofeagan.com/images/police/CrimePrevention/PDF/Program_for_gas_stations_SkimStop_updated_final.pdf



- Meet with local police to determine no current skimmers
- Place tamper tape on devices
- Check pumps every 24 hours for tampering
- 24 hour logs available upon request to document daily inspections
- Eagan Police check annually
- Skim Stop Stickers issued to let consumers know station is participating in the program

When a Skimmer is Found

- Make sure it really is a skimmer
 - May need W&M or service company confirmation
 - Take photos and send for confirmation
- Contact authorities
 - Local law enforcement
 - Weights & Measures
- Secure dispenser from further use
 - Block with truck/cones/bag-on-handle or power down unit
 - Don't touch other than to re-close cabinet until police arrive
- Preserve evidence
 - Touch as little as possible
 - Wear gloves
 - Secure all video footage and logs
- Be aware that an employee or a contractor may be involved. Follow law enforcement instructions on whether you discuss what you find with station personnel.



Safety First!!!

Never allow anyone to remove internal skimmer unless dispenser is completely powered down from the external switch.

- Electrocution danger
 - 120 power to components
- Explosion danger
 - Spark generated ignites vapors
- Equipment damage
 - Through design or through power surge



Law Enforcement/W&M Roles

- Law Enforcement
 - Maintains chain of custody of evidence
 - Conducts investigations
- Weights & Measures
 - Can look for skimmers & shimmers as part of inspections
 - Can coordinate between law enforcement agencies
 - Report to legislature & Governor
 - Can assist in identifying skimmers, and help educate owners and employees

Nebraska

Contact either local law enforcement
or

Nebraska Department of Agriculture
Food Safety & Consumer Protection

402-471-3422



South Dakota

- Contact law enforcement first
- Contact SD Department of Public Safety
Weights & Measures Division second

605.773.3697

Lori Jacobson, Director

Brenda Sharkey, Assistant Director



Iowa

- Contact local law enforcement first
- Then contact Iowa Department of Agriculture Weights and Measures Bureau

Randy Watts , Bureau Chief
515-725-1492



Iowa
The Hawkeye State

Minnesota

- Twin Cities Metro Area
 - Contact MN Dept. of Commerce W&M first
 - Contact law enforcement
 - after hours and on weekends
 - follow-up w/ W&M later
- Greater MN
 - Contact law enforcement first
 - Call W&M with law enforcement contact later



651-539-1555

Julie Quinn, Director

Benj FitzPatrick, Deputy Director

Greg VanderPlaats, Assistant Director

Questions on 1st half?

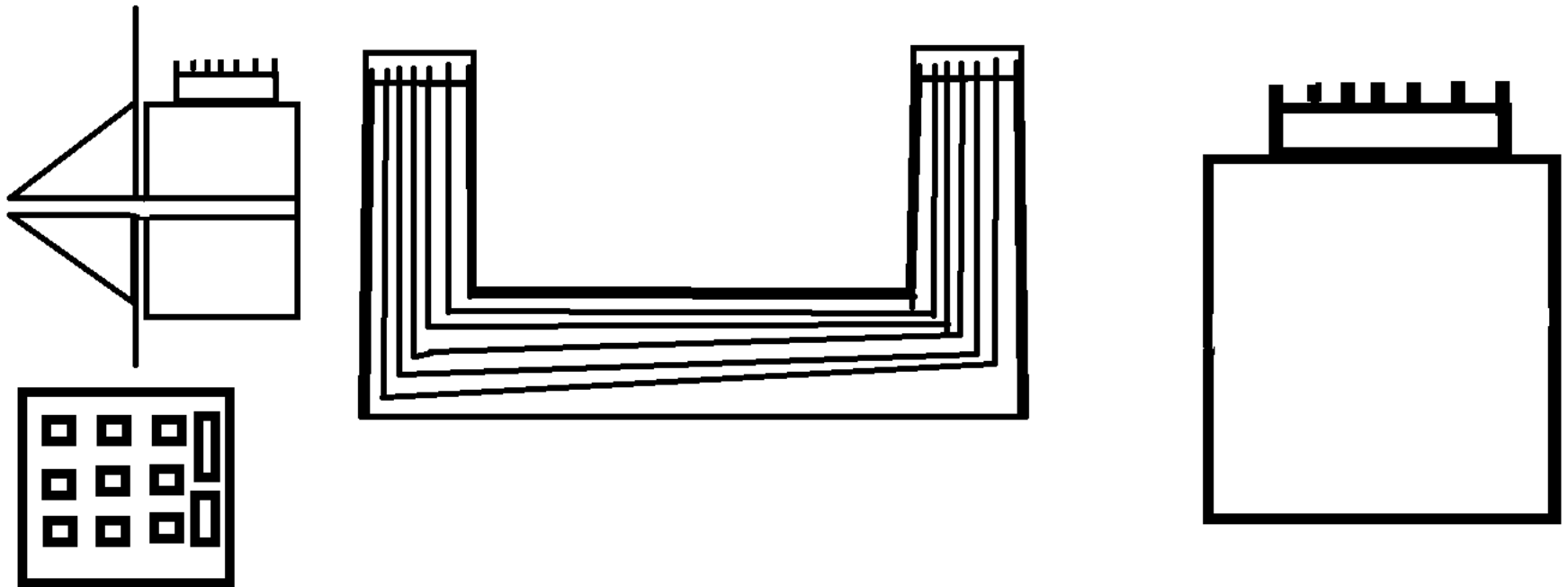


TIME FOR A QUICK BREAK.



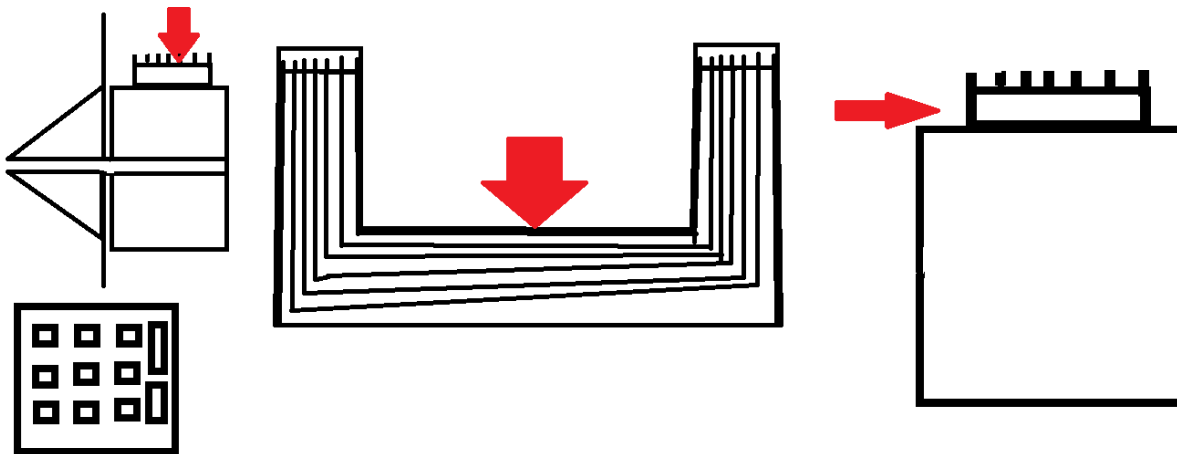
4 Basic Components of a Credit Card System

- 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



Internal Skimmers

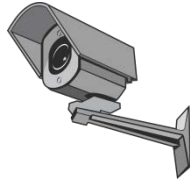
- Copy the information at one of 3 points:
 - At the card reader board (might also connect to card reader)
 - In the cable
 - At the device main board
- 10 seconds to install including opening cabinet



Key Pad Information

Key pad information
obtained by:

- Camera



- Magnetic key pad overlay



- Wired from back of keyboard up to skimmer



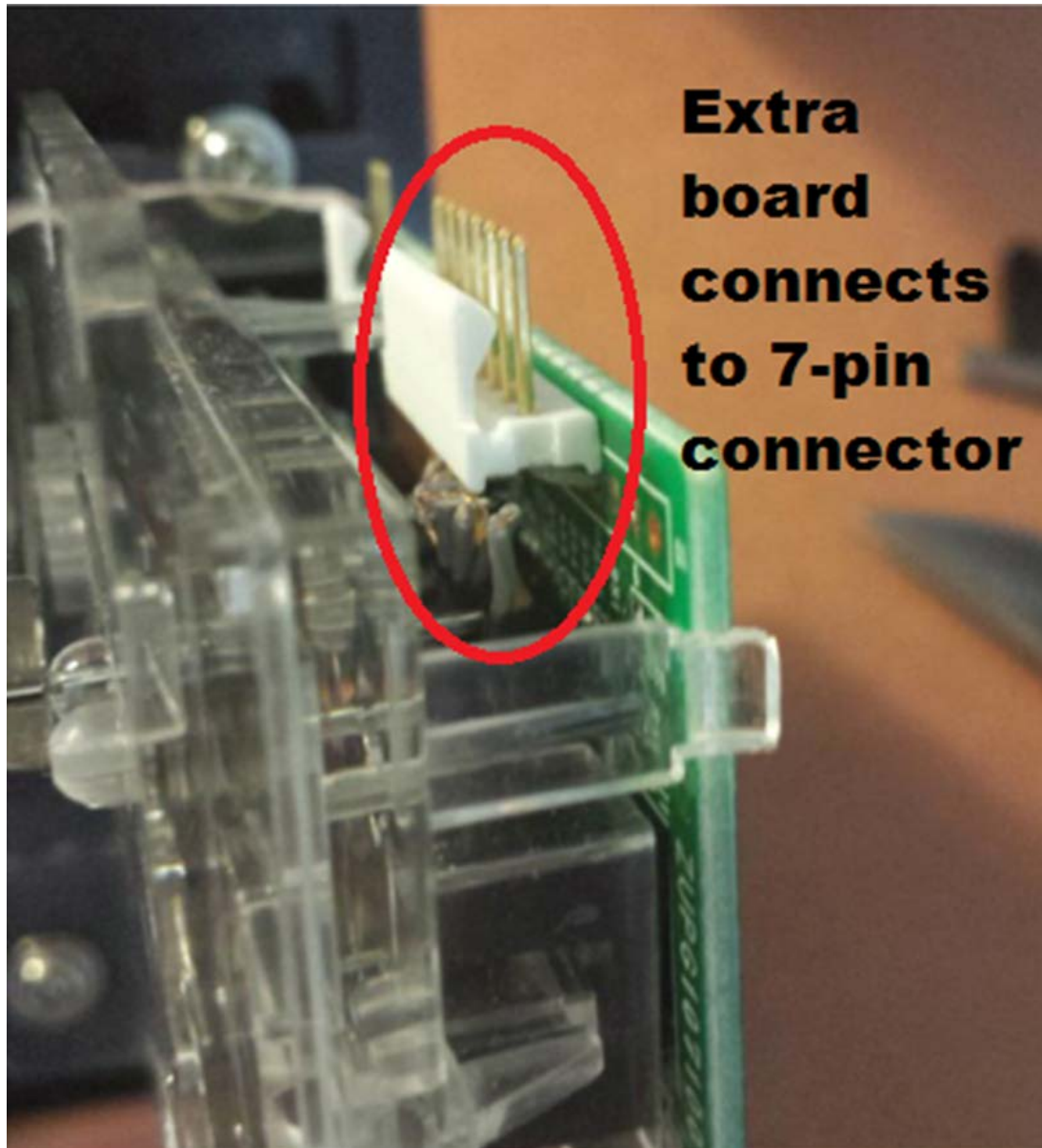
Easy as 1-2-3

1. Check card reader board
2. Check connection between boards
3. Check mother board

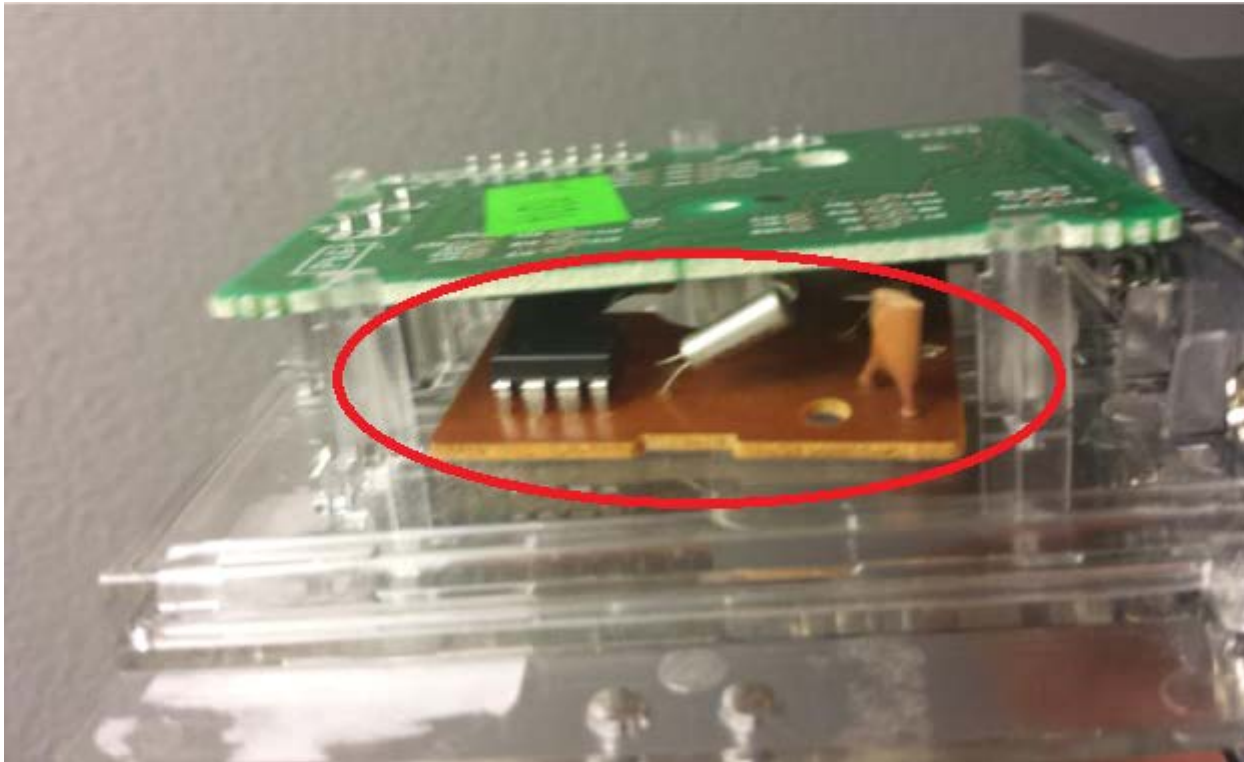


1. Check Credit Card Board

- 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



**Extra
board
connects
to 7-pin
connector**



Premade to Replace Existing Board

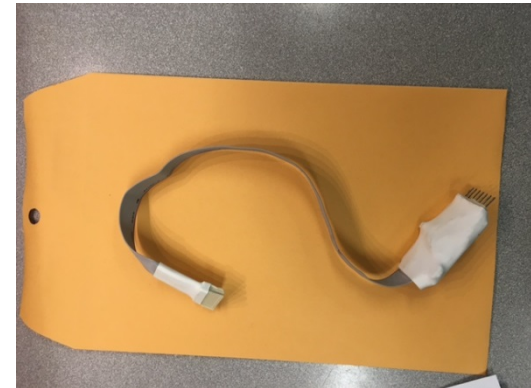


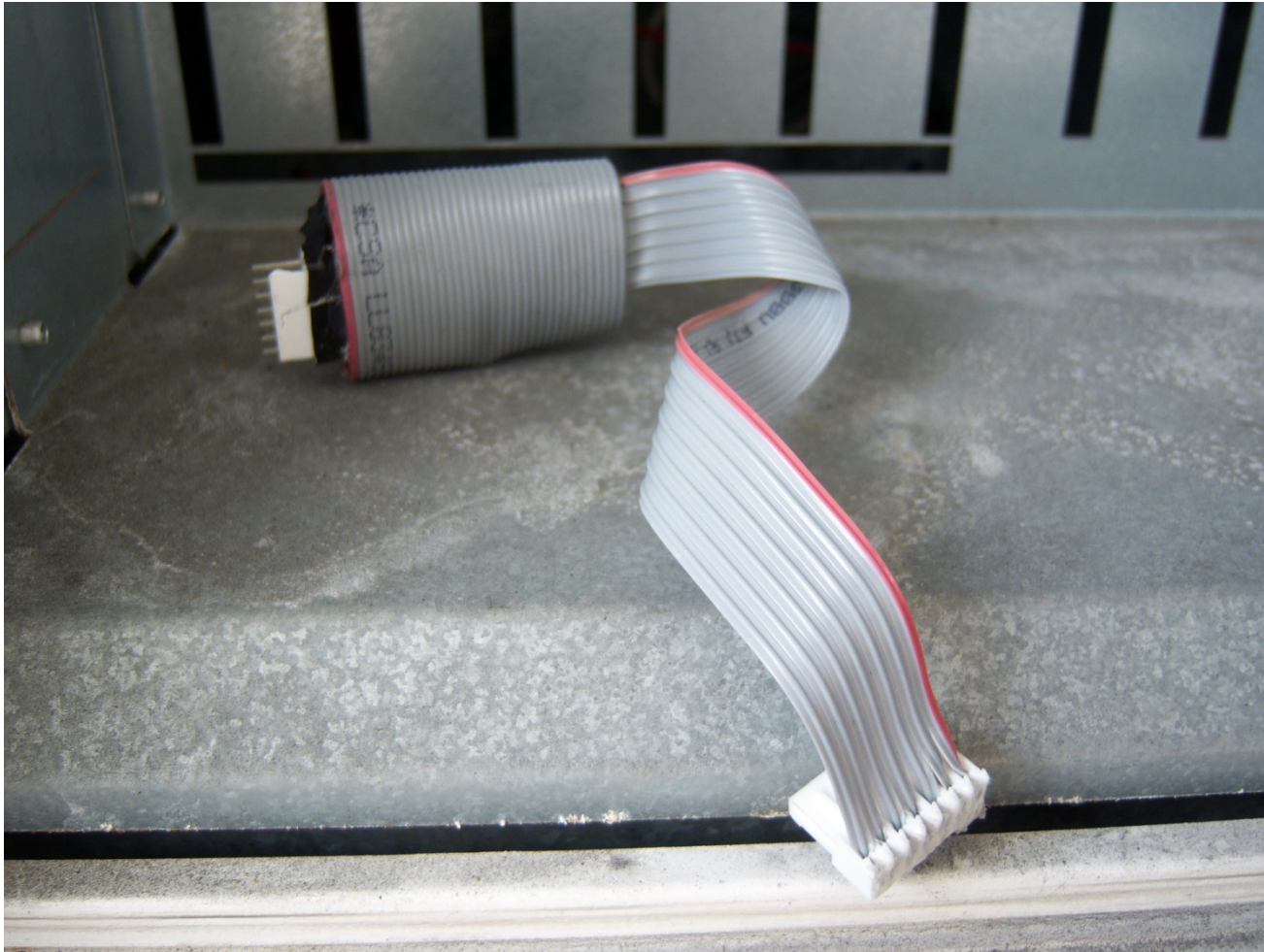
One of these things is not like the others...



2. Check Connections 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
 - Red flag if the ribbon or wires are different
 - No objects along the ribbon
 - Only one ribbon coming from the board

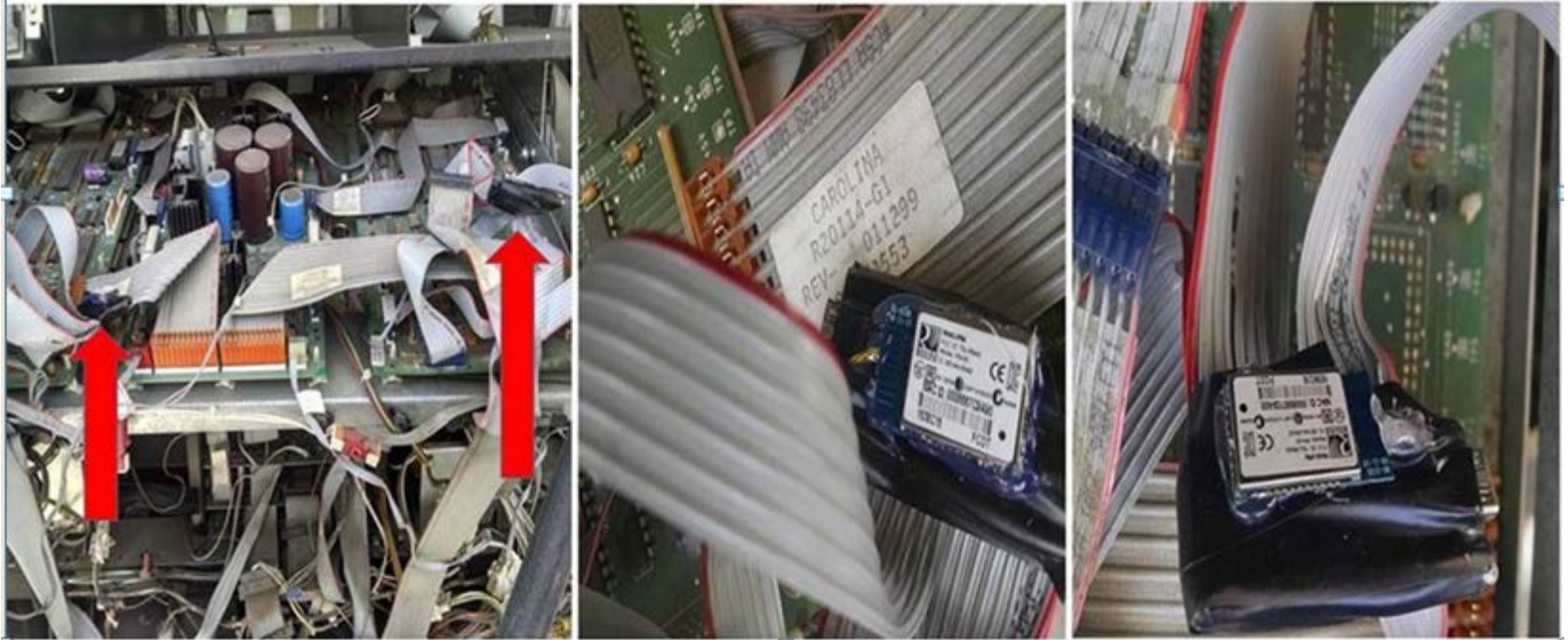






3. Check the Motherboard

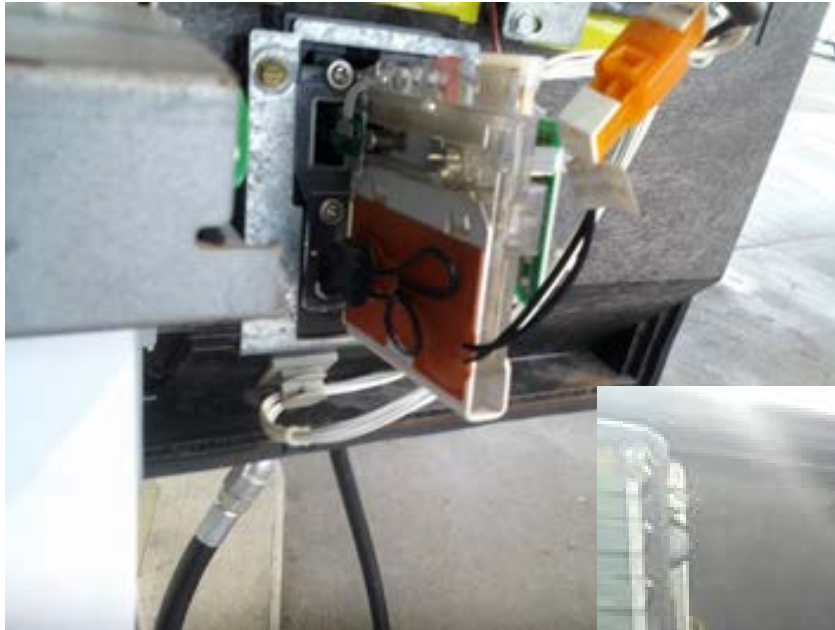
- May be behind shielding
 - Missing screws or clips may be clue
- Contact W&M if suspicious
 - Skimmer at mother board could mean technician involvement
 - Devices at mother board look the same as devices at card reader



Suspicious But Innocent Devices

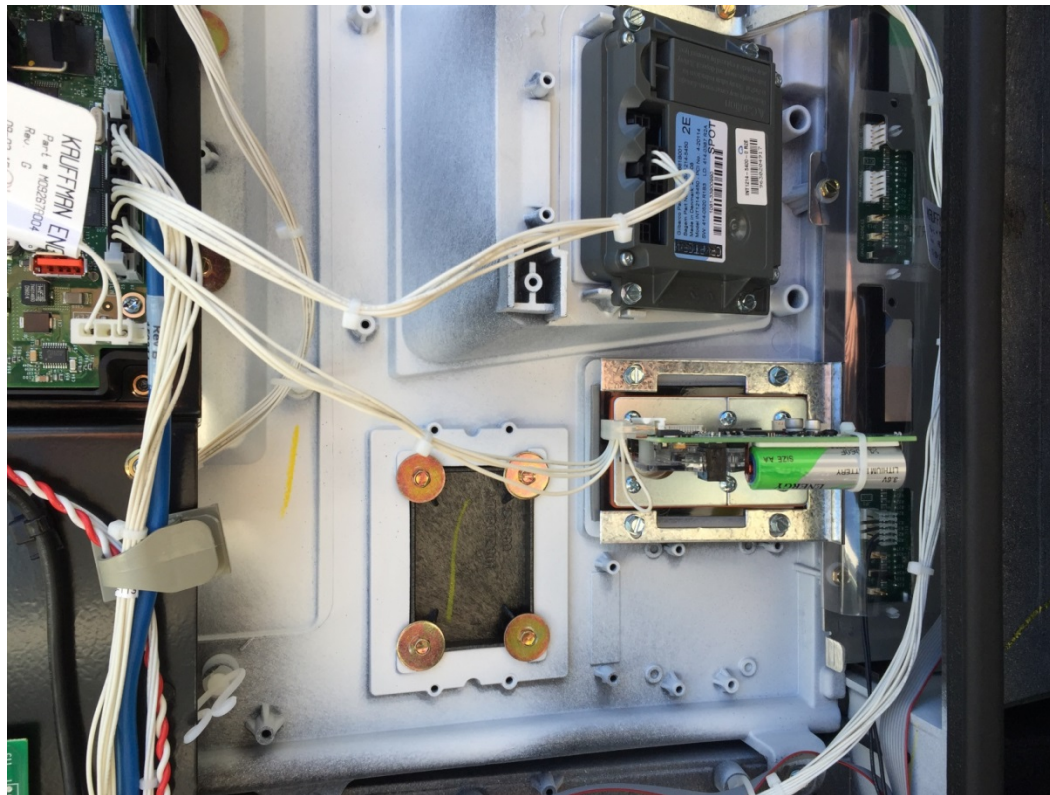
- Heaters –
 - Only 2 wires to supply power
 - Don't connect to 7-pin data connection





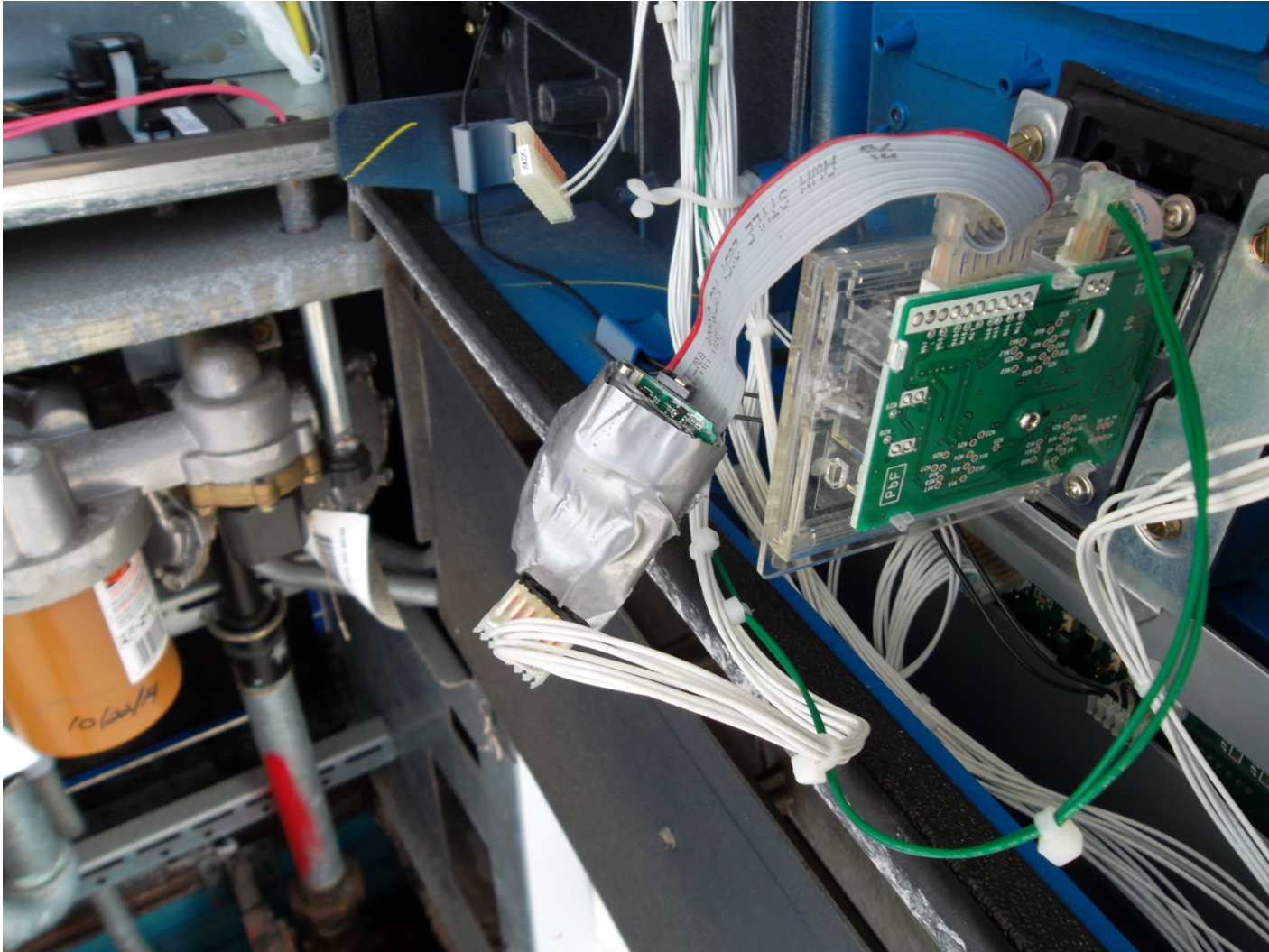
Suspicious But Innocent Devices

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

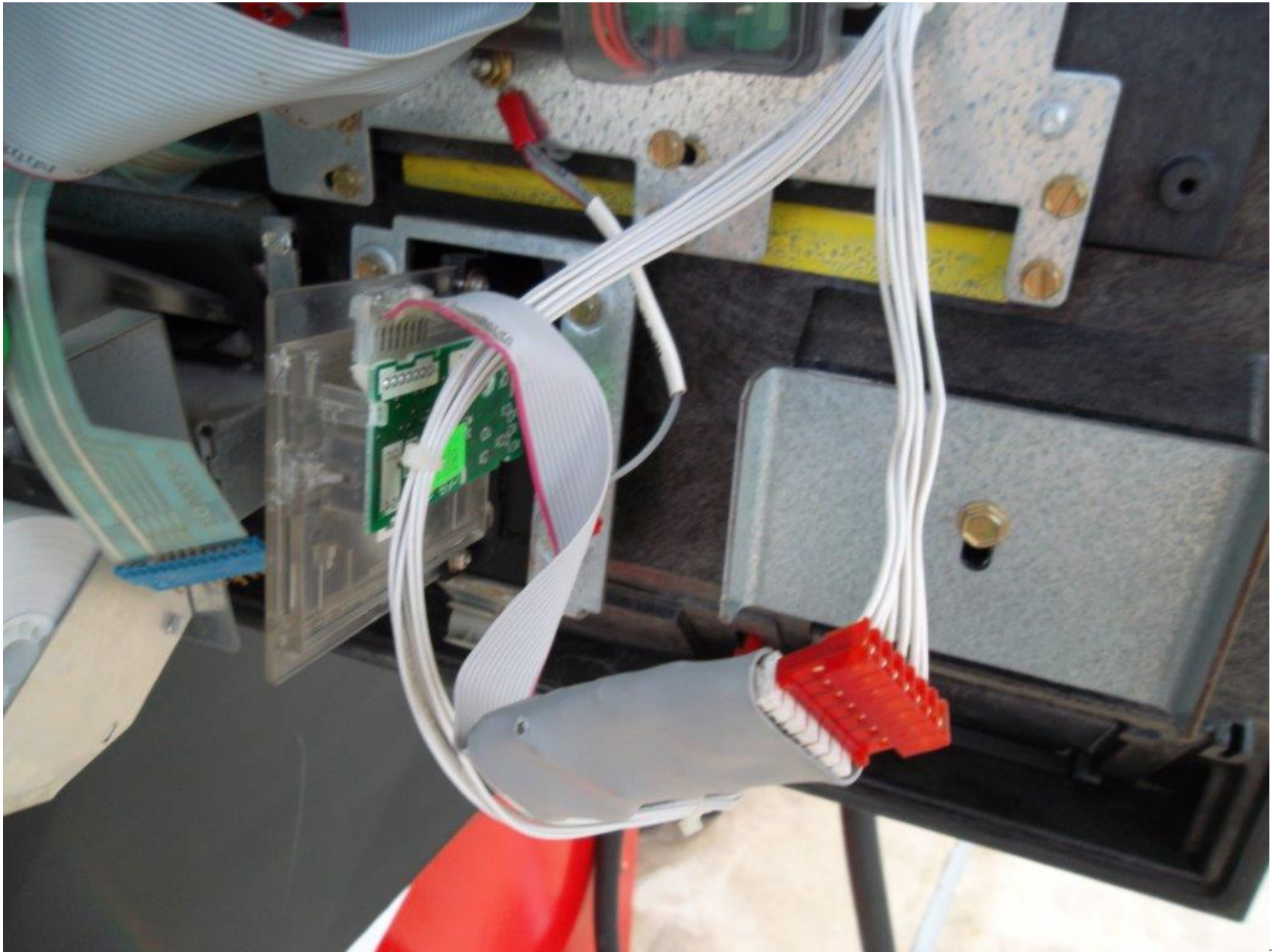


Skimmer or not skimmer?

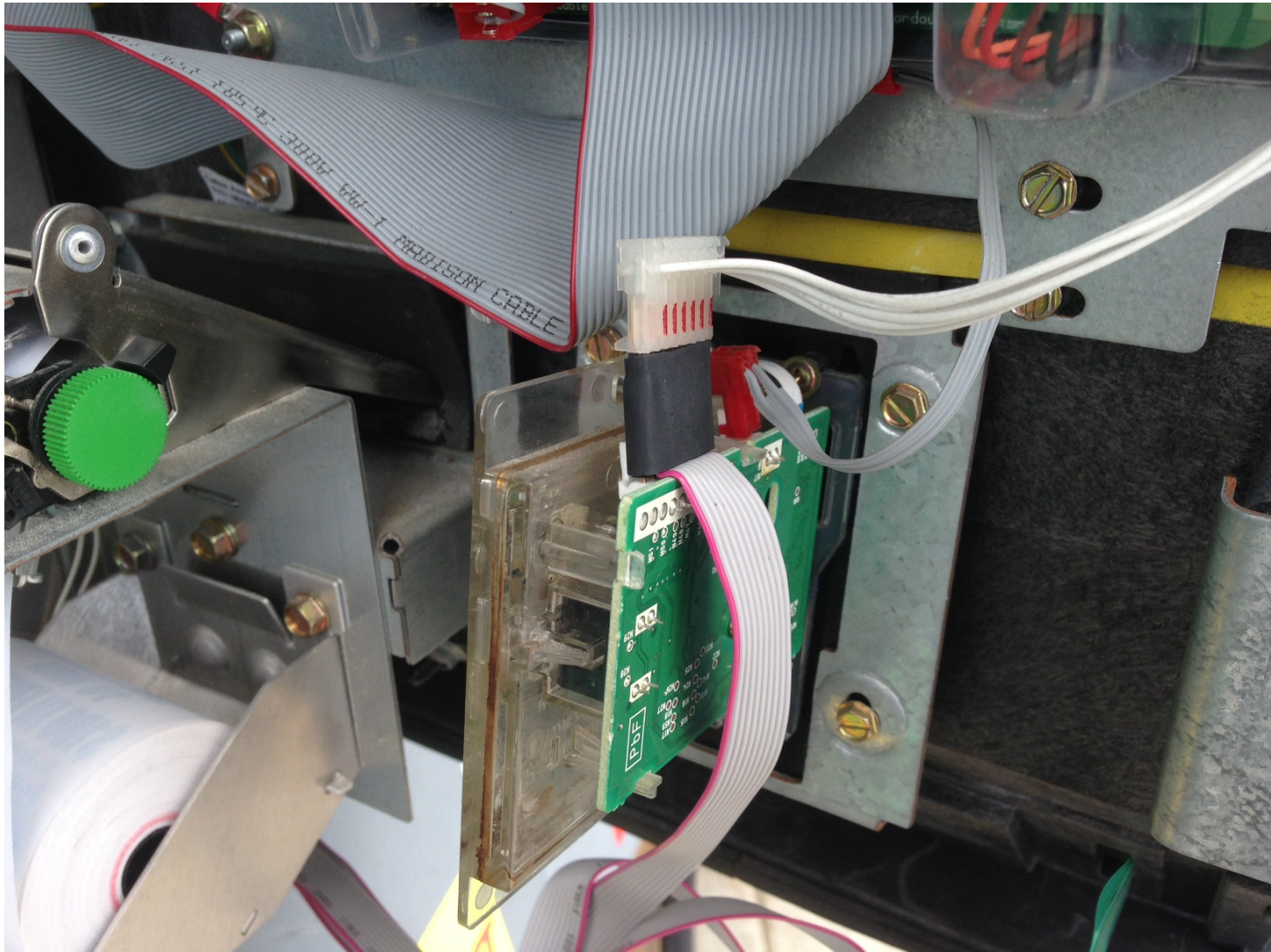
LET'S TEST OURSELVES

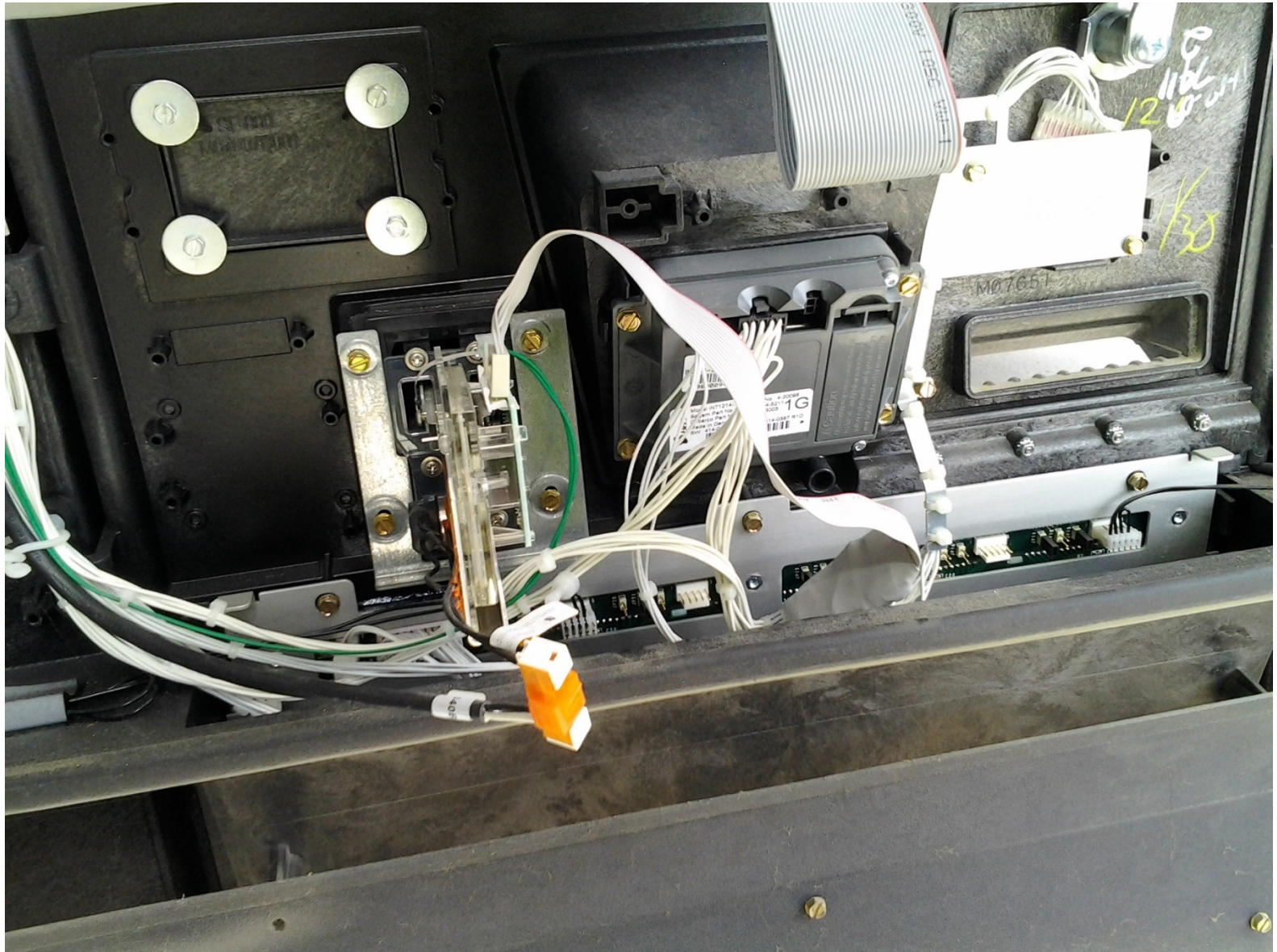


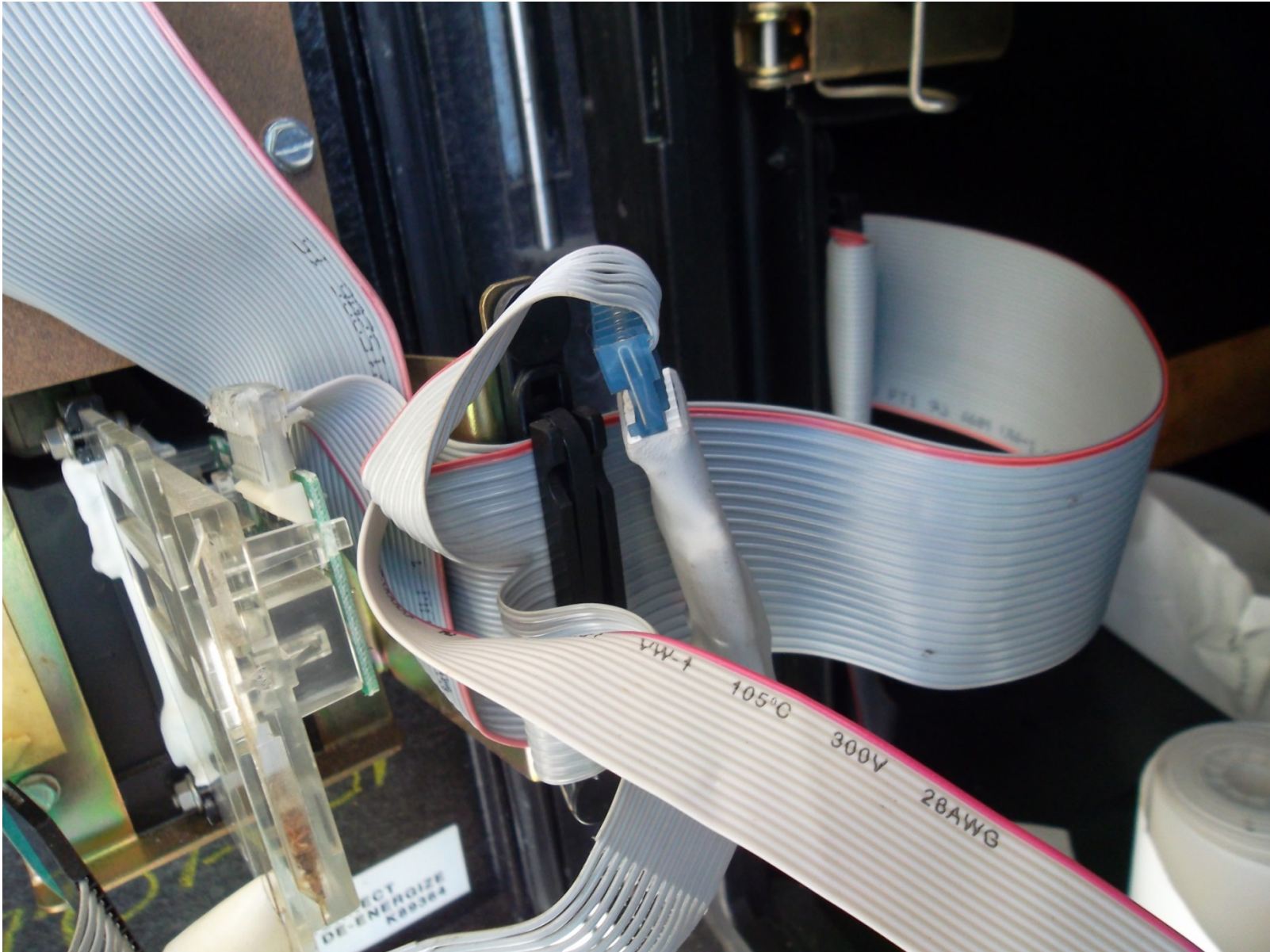








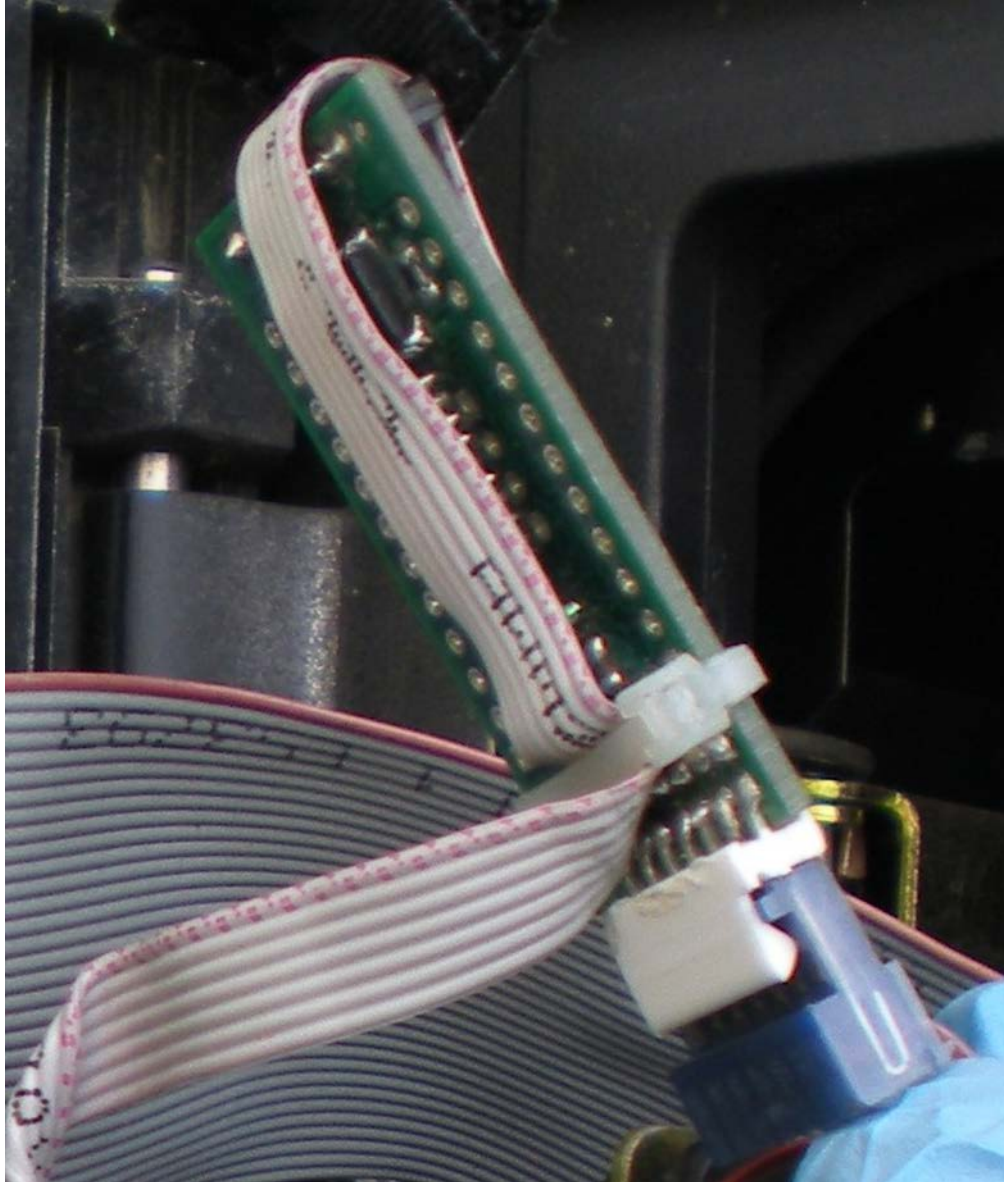












Questions?