CALIFORNIA FUELS + CONVENIENCE ALLIANCE

PROTECT OUR COMMUNITY FROM SKIMMING

WHAT IS *SKIMMING?* WHAT *DEVICES* ARE TYPICALLY USED TO SKIM?

Card Skimming occurs when devices illegally installed on ATMs, point-of-sale (POS) terminals, or fuel pumps capture data or record cardholders' PINs, posing significant risks to businesses' financial integrity and reputation.

Impact on Business:

- Unauthorized Purchases: Skimmed card data is used to make unauthorized purchases online or over the phone, leading to financial losses for businesses.
- Data Selling: Skimmers sell stolen data to other scammers, contributing to a thriving black market economy.
- Identity Theft: Stolen card information is used for identity theft, potentially damaging the reputation of businesses whose systems were compromised.
- Counterfeit Cards: Criminals use captured data to create counterfeit cards, leading to fraudulent transactions that may be attributed to the affected businesses.

How Does it Work?

- Installation: Skimmers are discreetly installed on ATMs, gas pumps, point-of-sale terminals, or other payment devices. They are often designed to blend in with the legitimate card reader.
- Data Capture: When a card is swiped or inserted into a compromised device, the skimmer reads and stores the card's magnetic stripe data, including the card number and expiration date.
- Data Theft: Skimmers retrieve the stolen information either remotely or by physically retrieving the device. They then use the stolen data to make unauthorized purchases or sell it on the black market.

WHAT ARE SOME WAYS TO *DETECT/PREVENT* SKIMMING?

Protocol for your employee(s) to follow in order to identify potential skimming devices:

1. **Inspect the Card Reader:**
   Have your employee look for any unusual attachments or protrusions on the card reader → Check for loose or mismatched parts, such as a different-colored card reader or keypad, which could indicate tampering.
   - Skimmers may be disguised as additional card slots, overlays, or bulky attachments.
2. **Check for Tamper-Evident Seals:**
   Many legitimate card readers have tamper-evident seals or stickers. If these seals are broken or appear to have been tampered with, it could signal the presence of a skimmer.
3. **Wiggle the Card Reader:**
   Attempt to wiggle the card reader gently. Legitimate card readers are securely attached and should not move or feel loose. If the reader feels loose or comes off easily, it could be a sign of tampering.
4. **Inspect the Keypad and Surroundings:**
   Have your employee look for hidden cameras positioned near the keypad or above the card reader. Skimmers often use cameras to capture PIN numbers entered by unsuspecting victims.
5. **Compare with Other Gas Pumps and Machines**
   Have your employee(s) compare card readers and keypads with neighboring devices (i.e. card readers at other pumps) to identify discrepancies that may signal skimming devices → Do the card slot and keypad at your pump look about the same as the others? If not, or if anything looks like it's bulging or out of place, that might be a sign of a skimmer.
6. **If you believe you located a card skimming device:**
   - Turn off access to the gas pump, or to the point-of-sale device or ATM.
   - Ascertain if video surveillance of the area is available.

OVERLAY SKIMMING DEVICES

CARD READER

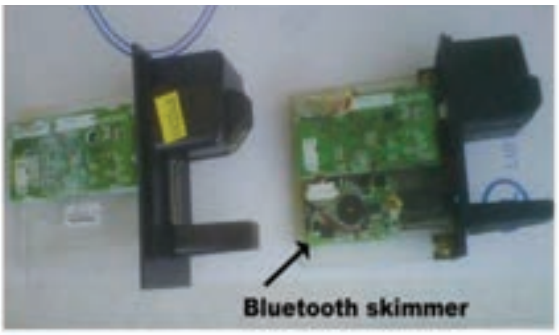
POINT OF SALE (POS)

PIN PAD

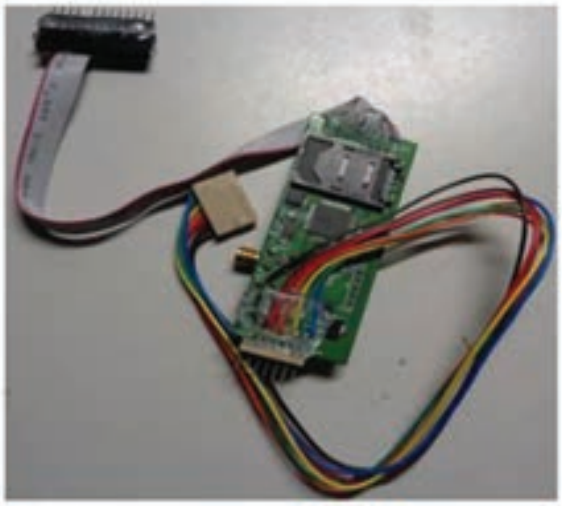
WHAT SHOULD YOU DO ONCE YOU *FIND A SKIMMER?*

- **Contact the County Agriculture Sealers of Weights and Measures Office or the CA Division of Measurement Standards (DMS) and local law enforcement to report the device**
  - It is imperative that the local County Office of Weights and Measures or DMS gets contacted as well as local law enforcement in order to ensure reporting in a timely fashion.
- **Contact the County Agriculture Sealers of Weights and Measures Office or the CA Division of Measurement Standards (DMS):**
  - Research contact information: Visit the official website of your local County Office of Weights and Measures or the state's Department of Agriculture or similar regulatory agency. Look for the section related to measurement standards or consumer protection. You should find contact details for the County Officials or Division of Measurement Standards there. County links; County Agricultural Commissioner and Sealer of Weights and Measures Contact Information (ca.gov). DMS complaint- CDFA - DMS - How To File a Complaint (ca.gov).
  - Make the call or send an email: Use the provided contact information to reach out to the DMS. If there's a phone number listed, call them directly. If only an email address is provided, compose a message detailing your concerns about the skimming device. Provide as much detail as possible, including the location where the device was found, any observations you made, and why you suspect it may not be compliant with standards.
  - Inquire about the process: Ask the DMS representative about the process for reporting issues related to skimming devices. They may have specific procedures in place for handling such reports. Also, inquire about any specific information they may need from you to assist with their investigation.
- **Contact local law enforcement:**
  - Dial the non-emergency number: Look up the non-emergency contact number for your local police department or sheriff's office. This information is often available online or in the local directory.
  - Explain the situation: When you reach law enforcement, express your concerns about the skimming device and its potential impact on the community. Provide details about where the device was found and why you suspect it may be illegal.
  - Follow their instructions: Law enforcement may dispatch an officer to investigate the situation further. Follow any instructions they provide, and provide additional information or assistance as needed.

INSERT-TYPE SKIMMER



NO SKIMMER ON LEFT; SKIMMER ON RIGHT



GLOBAL SYSTEM MOBILE-BASED SKIMMER

TYPICAL SKIMMER