BUREAU OF STANDARDS

Effective Date: 10/1/2016 **Section No. 1**
Version: 1.0 **Procedure No. 6**

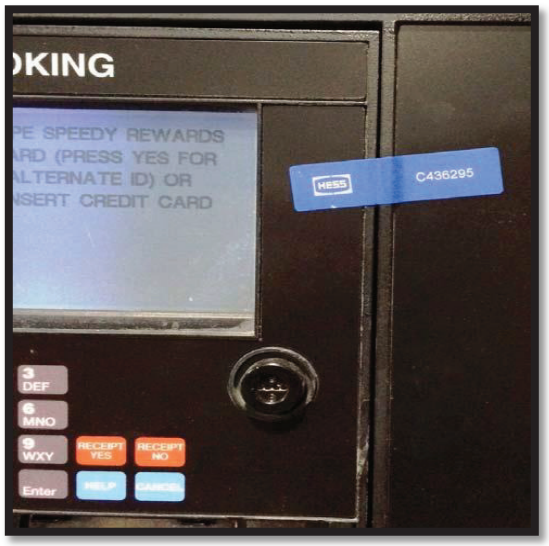
TITLE: Skimmer Detection

PURPOSE: This document details the process of detecting a credit card skimmer and the steps to take when one is found during an inspection.

A skimmer is a device used to capture & store electronic information, such as credit & debit card numbers that are contained on the magnetic strips of the cards, without the knowledge or permission of the individual.

1. As detailed in **Procedure 1.2 Approach and Contact** introduce yourself and explain the purpose of your visit.
   1.1. Obtain the card reader cabinet key
   1.2. Inquire if there are any alarms on the devices
2. Visually inspect the outside of the device
   2.1. Check for tamper evident seals as seen in Figure 1 and for any evidence of tampering.

Figure 1



2.2. Compare exterior card readers with the other pumps at the station
   2.2.1. Look for keypad overlays and hidden cameras – Figure 2

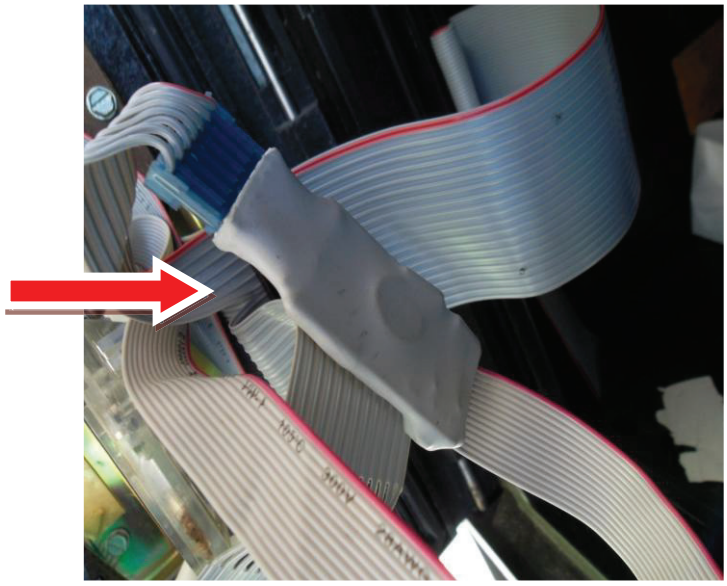
Figure 2

2.3. Check for scratches or adhesive tape residue.
2.4. Observe any differences in texture, color or material other than the original machine as seen in Figure 3.
2.4.1. Card slots are built into the device so gently tug, prod or wiggle the slot for any movement.

Figure 3

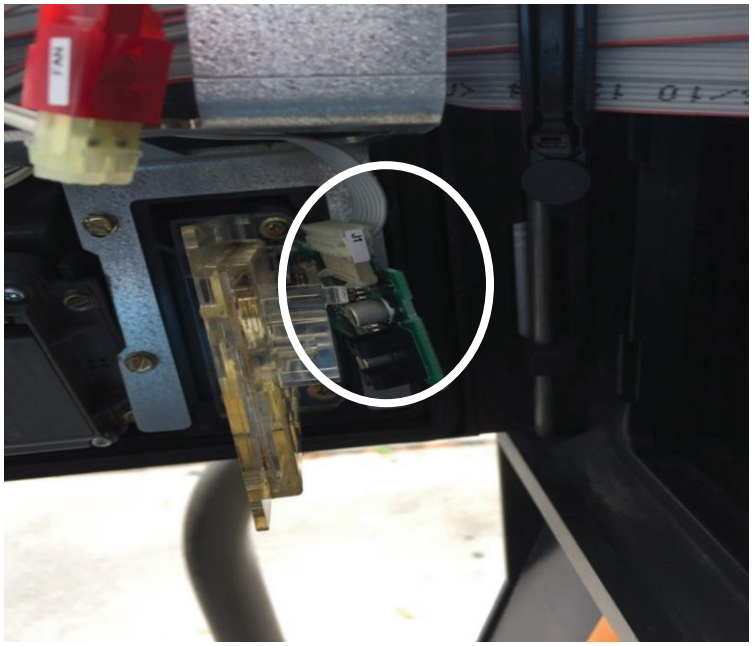
2.5. Open the device to inspect for any skimmers. Look for anything out of the ordinary. Compare all of the devices at the station and investigate any differences seen. Typical "memory stick" skimmers are generally inserted in the ribbon going from the card reader to the electronic board. The ribbon should be continuous and unbroken from the card reader to the main panel. See Figure 4.

Figure 4



2.6. Look for any holes in the ribbon as this maybe an indication that a skimmer had been previously present.
2.7. Blue tooth skimmers require detailed inspection of the card reader. They are usually attached to the main board of the card reader. See Figure 5.

Figure 5



2.8. Other types of skimmers include those embedded in the card readers and criminals replace the entire card reader as well as cameras in the brochure holder to capture the card holder's PIN. Compare and investigate any differences seen between devices.

2.9. If you are unsure that what you are seeing might be a skimmer photograph the suspect area and contact your supervisor or administrator.

3. When a skimmer is found the device is considered a crime scene.
   3.1. Secure the pump by blocking off from public use.
   3.2. Do not touch the device.
   3.3. Check all devices for additional skimmers before calling the Police.
   3.4. Call your local Police Department & Department of Agriculture Law. Inform the dispatcher of your location, pump number and how many skimming devices were found.
   3.5. Obtain a police report number to include in your inspection report.
   3.6. Write down the police officer's name that responded to the call.
   3.7. Write down the officers name that took the device off the pump
4. The report from DOCS that will be generated will have 0 days correction for a skimmer found. This will also generate a Stop Use for that dispenser but, once the skimmer is removed, the device is no longer in violation.
5. Complete the skimmer checklist in Appendix A and send to the Field Administrators, the field office Administrative Assistant II and your Supervisor within 24 hours.
6. Once a skimmer is found at a facility it must be revisited within three months for a focused inspection.

Version	Rev. Date	Change Control Comments	Approver