Video Highlights Technology to Provide Information on Suspicious Prepaid Money Cards

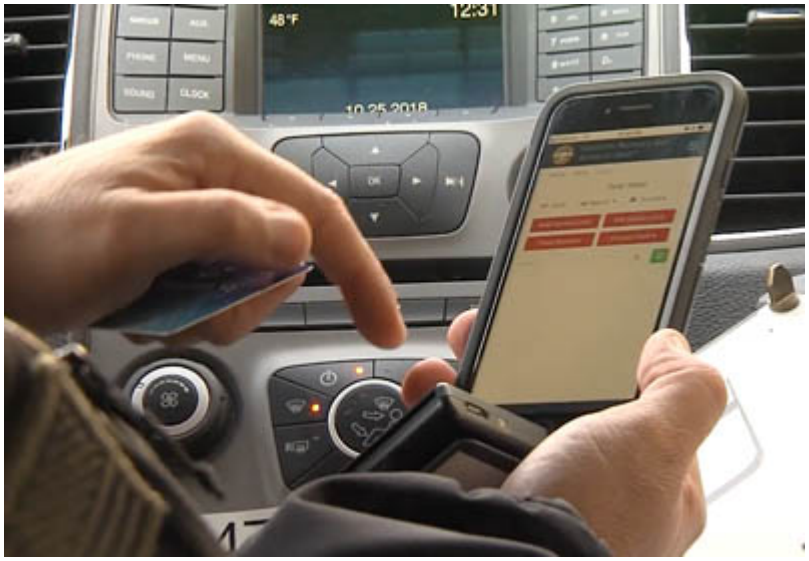
---

Video Highlights Technology to Provide Information on Suspicious Prepaid Money Cards

A recent video highlights technology designed to help law enforcement obtain information on suspicious prepaid money cards.

Large amounts of money can be programmed onto prepaid cards and used for illicit purposes. Cards with magnetic stripes such as bank credit and debit cards, gift cards and hotel card keys can be turned into prepaid cards.

The Electronic Recovery and Access to Data (ERAD) Prepaid Card Reader is a small, handheld device that wirelessly allows law enforcement officers in the field to identify and check the balance of suspicious cards, and to put a temporary hold on the linked funds until a full investigation can be completed.



Available since 2015, ERAD is used by state and local law enforcement in 48 states, as well as by federal and international law enforcement agencies, according to the U.S. Department of Homeland Security Science and Technology Directorate, (DHS S&T), which coordinated development of the technology.

Previously, law enforcement had to contact each bank to determine whether a card was lost, stolen, bogus or cloned. In the recent video, Alan Walker, certified fraud examiner,

Maricopa County (AZ) Attorney's Office, describes a case for which ERAD would have been helpful.

"We had a situation from the city of Scottsdale involving 6,000 cards which were obviously cloned cards or bogus cards," Walker said. "As we began to assist in the investigation, we realized that going through each card one at a time, contacting the banks individually, doesn't work. It took nine months to conclude that. We began to look for a better method, a better way. What we found was ERAD."

In the video, Det. Vince Porter, Financial Crimes Unit, Fairfax County (VA) Police Department, notes that patrol officers making a stop for some other kind of incident can come across a number of cards in the driver's possession that have different names embossed on them or no names at all.

Using the portable ERAD device attached to a smart phone, the officer can run the card through the device onsite. The device sends a signal to ERAD, which will identify the card and information about it, and email it back to the law enforcement officer.

"We are trying to verify that the information that comes up on the mag strip, is the same information that is on the face of the card," Porter said. "If we run a card and the card comes back not to match, we are able to freeze those assets that are on the card using ERAD itself."

The system also includes a USB-enabled scanner that users can connect to a desktop computer, so an investigator with a large number of cards can scan them at his or her computer. ERAD produces a detailed report on the status of each card and associated data.

The system has been a valuable asset for linking the suspicious cards to crimes. In the video, Walker notes that, “For every seizure we’ve had, we have seen 20 separate, unrelated criminal cases investigated, instigated or created because of the card identifying identity theft, drug trafficking, money laundering, child prostitution, sex trafficking, human trafficking.”

To read more about the technology and view the video, go to this link. Also, email first.responder@hq.dhs.gov for information.

Article photo: U.S. Department of Homeland Security/Science and Technology Directorate

Main photo: U.S. Department of Homeland Security/Science and Technology Directorate