C22 Skimmer Forensics: The Identification, Seizure, and Analysis of These Problematic Little Devices

James Darnell, BS, US Secret Service, University of Tulsa, Fisher Hall, 2821 E 8th Street, Tulsa, OK 74104; and John Simonello, MSc, United States Secret Service, 335 Adams Street, Ste 3200, Brooklyn, NY 11201*

The goal of this presentation is to educate attendees on identifying, seizing, and examining credit and debit card skimmers.

This presentation will impact the forensic science community by illustrating how an examiner must resolve the stored information on these devices to actual account numbers, otherwise there is nothing with which to charge the subject of the investigation.

When magnetic card readers are used to steal Personal Identity Information (PII) (e.g., credit or debit card numbers), they are known as skimmers. Many people still associate a skimmer as the hand-held device a waiter or waitress uses to steal a person's credit card number when paying for dinner in a restaurant, but the world of skimmers has matured and evolved. They are custom made and can be placed inside gas pumps, on top of ATMs and point-of-sale terminals, or even secreted inside door access readers. With the emergence of Bluetooth® skimmers, the suspect no longer has to retrieve the device but only has to be in close proximity to pair to the Bluetooth® and retrieve the stolen numbers. To further complicate matters, the manner in which the information is stored on the skimmer can be widely varied using different types of modulation, encoding, and encryption. So even if the odd electronic components of a skimmer, when mashed together, look "illegal," if an examiner is not able to resolve any stored information on the device to actual account numbers, there is nothing with which to charge the person who had the device.

Skimmers are created with various designs, form factors, and architectures and are intended to be hidden from the victim, so they are not necessarily easily identified. Once identified, the seizure, handling, and packaging of skimmers differ from that of other digital evidence and, given their unique nature, there is a lack of vendor tools and processes available to examine skimmers. All of these issues combined equate to one general problem — skimmers present a challenge for law enforcement and the banking system.

Due to the responsibility of enforcing Title 18, USC, Section 1029 — Fraud and related activity in connection with access devices (yes, a credit card or debit card account number is an "access device") — the United States Secret Service created a process for examining credit card skimmers. Not only does the Secret Service process these devices for examination, but educates other state, local, and federal agencies in regard to the methodology. This presentation will walk attendees through skimmer identification, seizure, and analysis. Chip-off processes, python scripting with examiner validation, and Bluetooth® module interrogation will all be discussed. Future work for encrypted skimmers and the emergence of shimmers (a skimming device designed to compromise Europay, MasterCard℠, and Visa℠ (EMV) chip cards) will also be presented.

Much of the material presented will be incorporated into updated versions of a Scientific Working Group on Digital Evidence (SWGDE) document and an American Society for Testing and Materials (ASTM) standard practice, both derived from the United States Secret Service's skimmer examination process.[1,2]

Reference(s):

1. SWGDE. Best Practice's for Examining Magnetic Card Readers. 2015.
2. ASTM E3017. Standard Practice for Examining Magnetic Card Readers. 2015.

Skimmer, Credit Card Fraud, Digital Evidence

*Presenting Author