United States Secret Service [INFO]

February 16, 2019

[INFO] Information Only Alert – GIOC Reference #19-004-I

Contactless Skimmers on Automated Fuel Dispensers

On February 13, 2019, the U.S. Secret Service's Philadelphia Field Office was alerted to a new technique utilized by fraudsters to steal payment card information at gas pumps.

Gas stations are beginning to implement contactless payments at the pump to go along with traditional magnetic strip or EMV chip and PIN based payments. These contactless payments utilize a technology called near field communication (NFC), which exchanges wireless signals when held closely to a point-of-sale device. Some smartphones and contactless credit cards have already been issued to support contactless payments at fuel pumps. Contactless payment systems mask real credit card numbers with a special token known as a device account number which contains information that identifies both the mobile device used for payment and the payment card itself to the NFC reader.

This sophisticated technique involves a cellular relay skimmer located in the contactless NFC reader on the outside of a gas pump. When customers make a contactless payment, this skimming device picks up the contactless card primary account number over-the-air

[INFO] - Indicates informational or educational content.

before it reached the point of interaction, which means that it will even defeat point-to-point encryption. Since this skimmer contains a cellular relay, it can transmit stolen card data wirelessly via text message. Consequently, fraudsters can receive real-time transmissions of the stolen card data from anywhere in the world. Be aware that a small external cellular antenna may also be attached to this device.

Any questions relating to this alert can be directed to the GIOC at gioc@usss.dhs.gov or 202-406-6009.