Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 08, 2015

Alert Number
I-100815-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

NEW MICROCHIP-ENABLED CREDIT CARDS MAY STILL BE VULNERABLE TO EXPLOITATION BY FRAUDSTERS

By October 2015, many U.S. banks will have replaced millions of traditional credit cards, which rely on data stored on magnetic strips, with new credit cards containing a microchip known as an EMV chip. While EMV cards offer enhanced security, the FBI is warning law enforcement, merchants, and the general public that these cards can still be targeted by fraudsters.

TECHNICAL DETAILS

What is an EMV credit card? 

The small gold chip found in many credit cards is most often referred to as an EMV chip. Cards containing this chip are known as EMV cards, as well as "chip-and-signature," "chip-and-pin," or "smart" cards. The name "EMV" refers to the three originators of chip-enabled cards: Europay, MasterCard, and Visa. EMV chips are now the global standard for credit card security. Unlike traditional credit cards that store data on a magnetic strip, EMV cards store card data in tiny integrated circuits and are authenticated when the cardholder inputs a PIN into a PoS terminal.

With traditional credit cards, the magnetic strip on the back of the card contains data and personal information about the cardholder. This information is used to authenticate the card at the point of sale (PoS), before the purchase is authorized. While most EMV cards still retain the traditional magnetic strip and the cardholder's signature on the back of the card, they offer the additional enhancement of the microchip embedded into the card. This allows merchants to verify the card's authenticity by the cardholder's personal identification number (PIN), which is known only to the cardholder and the issuing financial institution. In addition, EMV cards

transmit transaction data between the merchant and the issuing bank with a special code that is unique to each individual transaction. This provides the cardholder greater security and makes the EMV card less vulnerable to hacking while the data is transmitted from the PoS to the issuing bank.

THREAT

Although EMV cards will provide greater security than traditional magnetic strip cards, they are still vulnerable to fraud. EMV cards can be counterfeited using stolen card data obtained from the black market. Additionally, the data on the magnetic strip of an EMV card can still be stolen if the PoS terminal is infected with data-capturing malware. Further, the EMV chip will likely not stop stolen or counterfeit credit cards from being used for online or telephone purchases where the card is not physically seen by the merchant and where the EMV chip is not used to transmit transaction data.

DEFENSE

Consumers should closely safeguard the security of their EMV cards. This includes being vigilant in handling, signing, and activating a card as soon as it arrives in the mail, reviewing credit card statements for irregularities, and promptly reporting lost or stolen credit cards to the issuing bank. When using the EMV card at a PoS terminal, consumers should use the PIN, instead of a signature, to verify the transaction. This fully utilizes the security features built within the EMV card. Consumers should also shield the keypad from bystanders when entering their card PIN.

Merchants are encouraged to require consumers to enter their PIN for each transaction, in order to verify their identity. If a consumer uses a signature, merchants should ask to also see a government-issued photo identification card to verify the cardholder's identity.

The FBI encourages merchants to handle the EMV card and its data with the same security precautions they use for standard credit cards. Merchants handling sales over the telephone or via the Internet are encouraged to adopt additional security measures to ensure the authenticity of cards used for transactions. At a minimum, merchants should use secure servers and payment links for all Internet transactions with credit cards, and information should be encrypted, if possible, to avert hackers from compromising card information provided by consumers. Credit card information taken over the telephone should be encrypted, and any written copies of the card information should be securely disposed.

If you believe you have been a victim of credit card fraud, reach out to your local law enforcement or FBI field office, and file a complaint with the Internet

	Crime Complaint Center (IC3) at www.IC3.gov.