Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 13, 2015

Alert Number
I-100815(REVISED)-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 hundreds of millions of traditional credit and debit cards, which rely on data stored on magnetic strips, with new payment 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 no one technology eliminates fraud and cybercriminals will continue to look for opportunities to steal payment information.

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.

With traditional credit cards, the magnetic strip on the back of the card contains static personal information about the cardholder. This information is used to authenticate the card at the point of sale (PoS) terminal, before the purchase is authorized. When a consumer uses an EMV card at a chip PoS terminal, that transaction is protected using the technology in the microchip. Additionally, consumers will be able to continue to use the magnetic strip on the EMV card at retailers who have not yet implemented chip PoS terminals. When the card is equipped with a personal identification number (PIN), which is known only to the cardholder and the issuing financial institution, issuers will be able to verify the user's identity. Currently, not all EMV cards are issued to consumers with the PIN capability and not all merchant PoS terminals can accept PIN entry. EMV transactions at chip PoS terminals provide more security of consumers' personal data than magnetic strip PoS transactions. In addition, EMV card transactions transmit 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 criminal activity while the data is transmitted from the chip enabled PoS to the issuing bank.

THREAT

Although EMV cards provide greater security than traditional magnetic strip cards, an EMV chip does not stop lost and stolen cards from being used in stores, or for online or telephone purchases when the chip is not physically provided to the merchant, referred to as a card-not-present transaction. Additionally, the data on the magnetic strip of an EMV card can still be stolen if the merchant has not upgraded to an EMV terminal and it becomes infected with data-capturing malware. Consumers are urged to use the EMV feature of their new card wherever merchants accept it to limit the exposure of their sensitive payment data.

DEFENSE

Consumers should closely safeguard the security of their EMV cards and PINs. This includes being vigilant in handling, signing, and activating a card as soon

	as it arrives in the mail, reviewing statements for irregularities, and promptly reporting lost or stolen credit cards to the issuing bank. Consumers should also shield the keypad from bystanders when entering a PIN, as PINs are vulnerable to cybercriminals who work to steal these numbers to commit ATM and cash-back crimes. 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 and debit 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 or through online means should be protected by the retailer to include encrypting digital information and securely disposing written credit card information. 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.