

United States Senate  
Washington, DC 20510-1304

October 15, 2015

The Honorable James B. Comey  
Director  
Federal Bureau of Investigation  
935 Pennsylvania Ave., NW  
Washington, DC 20535

Dear Director Comey:

I write to seek clarification regarding the FBI's views on the security of credit and debit cards.

On October 8, the FBI posted an advisory entitled "New Microchip-Enabled Credit Cards May Still Be Vulnerable To Exploitation By Fraudsters." The advisory discussed payment cards that are now being issued in the United States with microchips pursuant to the Europay MasterCard Visa (EMV) security standard, and noted that "although EMV cards will provide greater security than traditional magnetic stripe cards, they are still vulnerable to fraud." The advisory then discussed the use of Personal Identification Numbers (PINs) for payment cards, recommending that "when using the EMV card at a PoS [point of sale] terminal, consumers should use the PIN, instead of a signature, to verify the transaction." The advisory also said "merchants are encouraged to require consumers to enter their PIN for each transaction, in order to verify their identity."

The FBI's recommendations for PIN usage by both consumers and merchants appeared to be sound from a fraud prevention standpoint, as PIN card transactions have a fraud rate far lower than non-PIN card transactions and as the requirement of chip-and-PIN in overseas markets has significantly limited fraudsters' ability to take advantage of lost or stolen payment cards.

However, on October 9 the FBI withdrew its October 8 advisory. According to an October 9 article in *Computerworld*, the FBI withdrew the advisory after being contacted by the American Bankers Association (ABA). ABA senior vice president of payments and cybersecurity policy Doug Johnson was quoted in the *Computerworld* article saying that the FBI advisory "was not really reflective of the U.S. marketplace" and that "PIN is not going to be adopted in the U.S."

On October 13, the FBI issued a revised version of the October 8 advisory that no longer included the recommendations for consumers and merchants to use PINs. While noting that "an EMV chip does not stop lost and stolen cards from being used in stores," the October 13 advisory simply observed that "currently, not all EMV cards are issued to consumers with the PIN capability and not all merchant PoS terminals can accept PIN entry."

The revisions to the FBI advisory raise significant questions about whether current EMV security technology is adequately protecting consumers and whether the FBI is taking appropriate steps to warn against and deter payment card fraud involving lost or stolen cards. Accordingly, I ask that you please provide answers to the following questions.

1. Please provide information on the annual dollar amount of payment card fraud associated with lost and stolen cards in the United States.
2. In the FBI's view, is enabling a payment card with the option of a PIN an effective step to help reduce the occurrence of, and costs from, fraud in relation to payment card transactions?
3. In the FBI's view, what is the annual dollar amount of lost-and-stolen payment card fraud that could be averted if the use of a PIN was a standard requirement for U.S. payment card transactions (as is currently the case with ATM withdrawals)?
4. Did representatives of the American Bankers Association contact the FBI between the issuance of the October 8 advisory and the release of the revised advisory? If so, did the American Bankers Association request that the advisory's recommendations for consumers and merchants to use PINs be removed?
5. EMV is a set of security specifications established by EMVCo, an organization owned and run by six giant payment card networks: American Express, Discover, MasterCard, Visa, JCB (a Japanese-based payments company) and UnionPay (a Chinese bankcard association). EMVCo is essentially the payment card industry's effort to establish its own standard for card security technology. Did EMVCo or any of the six card networks that own EMVCo contact the FBI between the issuance of the October 8 advisory and the release of the revised advisory? If so, did EMVCo or any of the six card networks request that the advisory's recommendations for consumers and merchants to use PINs be removed?
6. The FBI's revised October 13 advisory states, correctly, that "currently, not all EMV cards are issued to consumers with the PIN capability and not all merchant PoS terminals can accept PIN entry." In order to help reduce fraud involving lost and stolen cards, does the FBI believe that EMV cards should be issued to consumers with PIN capability and that merchant PoS terminals should be able to accept PIN entry?
7. Is the FBI aware that payment card networks and banks in the United States have an incentive to dissuade consumers and merchants from using PINs because the fees that networks and banks receive on non-PIN transactions are higher than on PIN transactions? Is the FBI concerned that this incentive may cause card networks and banks to set security specifications that seek to maximize fee revenue instead of maximizing fraud prevention?
8. Is the FBI committed to overseeing the security specifications established by EMVCo on an ongoing basis to ensure that these specifications are adequately protecting U.S. consumers against fraud?

Please provide responses to these questions as soon as possible, and no later than November 15, 2015. Thank you for your attention to this request, and I look forward to hearing from you.

Sincerely,



Richard J. Durbin  
United States Senator