Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

April 07, 2015

Alert Number
I-040715b-PSA

CRIMINALS HOST FAKE GOVERNMENT SERVICES WEB SITES TO ACQUIRE PERSONALLY IDENTIFIABLE INFORMATION AND TO COLLECT FRAUDULENT FEES

From May 2012 to March 2015, the FBI's Internet Crime Complaint Center (IC3) has received complaints regarding criminals hosting fraudulent government services websites in order to acquire Personally Identifiable Information (PII) and to collect fraudulent fees from consumers.

Although the volume and loss amounts associated with these websites are minimal to date, the victims are having their PII data compromised which may be used by criminals for any number of other illicit activities, ranging from the creation of fraudulent IDs and passports to fraudulent loans and tax refunds. The PII can include the victim's name, address, phone number, e-mail address, social security number, date of birth, and mother's maiden name.

This is how the scheme usually happens: victims use a search engine to search for government services such as obtaining an Employer Identification Number (EIN) or replacement social security card. The fraudulent criminal websites are the first to appear in search results, prompting the victims to click on the fraudulent government services website. The victim completes the required fraudulently posted forms for the government service they need. The victim submits the form online, believing they are providing their PII to government agencies such as the Internal Revenue Service, Social Security Administration, or similar agency based on the service they need. Once the forms are completed and submitted, the fraudulent website usually requires a fee to complete the service requested. The fees typically range from $29 to $199 based on the government service requested. Once the fees are paid the victim is notified they need to send their birth certificate, driver's license, employee badge, or other personal items to a specified address. The victim is then told to wait a few days to several weeks for processing. By the time the victim realizes it is a scam, they may have had extra charges billed to their credit/debit card, had a third-party designee added to their EIN card, and never received the service(s) or documents requested. Additionally, all of their PII data has been compromised by the criminals running the websites and can be used for any number of illicit purposes. The potential harm gets worse for those who send their birth certificate or other government-issued identification to the perpetrator.

Follow-up calls or e-mails to the perpetrator(s) are normally ignored and many victims report the customer service telephone numbers provided are out of service. The FBI recommends that consumers ensure they are communicating or requesting services/merchandise from a legitimate source by verifying the entity. When dealing with government websites, look for the .gov domain instead of a .com domain (e.g. www.ssa.gov and not www.ssa.com).

Below are some consumer tips when using government services or contacting agencies online:

- Use search engines or other websites to research the advertised services or person/company you plan to deal with.
- Search the Internet for any negative feedback or reviews on the government services company, their Web site, their e-mail addresses, telephone numbers, or other searchable identifiers.

	• Research the company policies before completing a transaction. • Be cautious when surfing the Internet or responding to advertisements and special offers. • Be cautious when dealing with persons/companies from outside the country. • Maintain records for all online transactions. As a consumer, if you suspect you are a victim of an Internet-related crime, you may file a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov.