SAU
SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2630 Chicago, IL 60602 V. 312.603.8180

Toni Preckwinkle, *President - Cook County Board of Commissioners*
Michael G. Masters, *Executive Director*

Date: 19 November 2014
No. 02

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: DUTY.DESK@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

IC3 PUBLIC SERVICE ANNOUNCEMENT
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 November 2014
Alert Number
I-111414-PSA

Criminals Post Fraudulent Online Advertisements For Automobiles, Recreational Vehicles, Boats, And Other Outdoor Equipment Leading To Financial Losses In Excess of $20 Million

From June 2009 to June 2014 the Internet Crime Complaint Center (IC3) received over 6800 complaints regarding criminals targeting online consumers by posting false advertisements for high priced items such as automobiles, boats, heavy equipment, recreational vehicles, lawn mowers, tractors, and other similar items. These complaints total more than $20 million in reported losses.

The scam initiates when the criminals post a false advertisement offering the item for sale. The advertisement usually includes a fraudulent photo to entice the consumer to purchase the item. Within the advertisement, the criminal includes a contact telephone number. The consumer leaves a message and the perpetrator responds via text message. The text message normally requests that the consumer provide an e-mail address. Once the e-mail address is provided the consumer is sent additional details to include multiple images of the item for sale. The perpetrator provides logical reasons for offering the item at such a discounted price such as moving to another location; therefore, the item needs to be sold quickly; the sale was part of a divorce settlement; or overseas deployment.

Consumers normally negotiate a price. Many scammers advise the consumer the transaction will be conducted through Ebay to ensure a safe and easy transaction. In reality the scammer is only pretending to use Ebay. The consumer receives a false e-mail that appears to be legitimate from Ebay. The e-mail provides instructions on how to complete the transaction. The perpetrator provides the consumer with all the information necessary to

complete the wire transfer - the bank account name, address, and account number. The scammer provides a fraudulent toll-free Ebay customer service number for the consumer to use when they are ready to wire the money. These numbers were also used by many victims to confirm a successful wire transfer or to check transaction status and shipping information. After the transaction, the consumer is sent a false Ebay confirmation e-mail that includes the fraudulent transaction or confirmation number and the expected delivery date of the item.

Any follow-up calls, text messages or e-mails to the perpetrator(s) are normally ignored and many victims report the toll-free customer service telephone numbers provided are constantly busy. As a result, the consumer never receives the purchased item(s) and suffers a financial loss.

The FBI recommends that consumers ensure they are purchasing the actual merchandise from a reputable source by verifying the legitimacy of the seller. Below are some consumer tips when purchasing items online:

- Use search engines or other websites to research the advertised item or person/company selling the item.
- Search the Internet for any negative feedback or reviews on the seller, their e-mail addresses, telephone numbers, or other searchable identifiers.
- Research the company policies before completing a transaction. For example, ensure the seller accepts payments via credit card as Ebay does not conduct wire transfers and only uses PayPal to conduct transactions.
- Be cautious when 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.

Source: http://www.ic3.gov/media/2014/141114.aspx

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

2. The holder of the information will comply with access and dissemination restrictions.

3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

1.0730	2. 0830