Issued 2/19/18

Fraudulent Online Vehicle Sales

The FBI is issuing warnings regarding the fraudulent online sale of cars, recreational vehicles, boats, and other outdoor equipment. Criminals are posting online advertisements of items that are not, nor have ever been, within their possession. From May 2014 through December 2017, the IC3 received approximately 26,967 complaints with adjusted losses of $54,032,396 related to these types of fraudulent sales.

Technical Details

The fraudulent advertisements usually include photos matching the description of the vehicle for sale and a phone number or email address to contact the supposed seller. Once the initial contact is established, the criminal sends the intended buyer additional photos along with a seemingly logical explanation for the item's discounted price and the time-sensitive nature of the transaction. Common explanations given by the perpetrators include (but are not limited to):

- Seller is moving to another location or being deployed by the military
- Seller received the vehicle as part of a divorce settlement
- Vehicle belonged to a relative who has died

The criminal makes the fraud appear legitimate by deceptively claiming partnership with reputable companies, such as eBay, and using the names of these third parties with whom they have no actual association. The criminal assures the buyer that the transaction will occur through a third party's Buyer Protection Program; the criminal then immediately sends an email to the buyer with a fraudulent toll-free number that impersonates the

third party. The buyer is told to purchase prepaid gift cards in the amount of the agreed upon sale price and is instructed to share the prepaid card codes with the criminal. The criminal notifies the buyer they will be receiving the vehicle within a couple of days. After the transaction goes through, the criminal typically ignores all follow-up calls, text messages, or emails from the buyer or demands additional payments. The vehicle is not delivered and the buyer is never able to recuperate their losses.

Defense and Mitigation

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

- When it comes to making any purchases, be cautious of items being advertised well below their market value. Remember, if the deal appears too good to be true, it probably is.
- Use the Internet to research the advertised item and the seller's name, email addresses, telephone numbers, and other unique identifiers.
- Use the Internet to research the company's contact information and its shipping and payment policies before completing a transaction. Ensure the legitimacy of the contact information and that the company accepts the requested payment option.
- Avoid sellers who refuse to meet in person or who refuse to allow the buyer to physically inspect the vehicle before the purchase. For high-priced purchases, insist on speaking to the seller over the phone to establish their legitimacy.
- Ask for the vehicle's VIN number, license plate (if possible), and the name of the individual to whom the car is currently registered.
- If you are suspicious or unsure about an email that claims to be from a legitimate business, locate the business online and contact it directly. Criminals take extra effort to disguise themselves and may include familiar or recognizable words in their email address or domain name.

Filing a Complaint

Individuals who believe they may be a victim of, or have knowledge of, an online scam (regardless of dollar amount) can file a complaint with the IC3 at www.ic3.gov.

When filing with the IC3, please be as descriptive as possible in the complaint and include the following information:

1. All identifying subject information: names, phone numbers, email addresses, IP addresses, and any websites used.
2. Account names, numbers, addresses, and financial institutions that received any funds (e.g., wire transfers, prepaid card payments).
3. Description of interaction with the subject: dates, advertisement websites, vehicle types, means of communication, payment methods, and anything that stood out as odd or suspicious.

Complainants are also encouraged to keep all original documentation, emails, faxes, and logs of communications.

Because scams and fraudulent websites can emerge and change very quickly, individuals are encouraged to report any possible Internet scams and fraudulent websites by filing a complaint with the IC3 at www.ic3.gov.

To view previously released PSAs and Scam Alerts, visit the IC3 Press Room at www.ic3.gov/media/default.aspx.