Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

September 19, 2019

Alert Number
I-091919-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims For Financial Gain

Each year, millions of elderly Americans fall victim to some type of financial fraud, racking up more than $3 billion in losses annually. Criminals use a variety of methods to deceive these victims, including romance, sweepstakes, charity, technology support, grandparent, lottery, and government impersonation schemes, to name a few. In each case, perpetrators try to gain their targets' trust and may communicate with victims via computer, through the mail, in person, and by phone, TV, and radio. With the elderly population growing in the United States, it is likely perpetrators will find more and more victims.

Elderly individuals may encounter the following scams:

- **Romance Scam**: Perpetrators pose as interested romantic partners through dating websites to capitalize on their elderly victims' desire to find companions.
- **Tech Support Scam**: Perpetrators pose as technology support representatives and offer to fix non-existent computer issues—gaining remote access to victims' devices and, thus, their sensitive information.
- **Grandparent Scam**: Perpetrators pose as a relative—usually a child or grandchild—claiming to be in immediate dire financial need.
- **Government Impersonation Scam**: Perpetrators pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.
- **Sweepstakes/Charity/Lottery Scam**: Perpetrators claim to work for legitimate charitable organizations to gain victims' trust. Or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee."
- **Home Repair Scam**: Perpetrators appear in person and charge homeowners in advance for home improvement services that they never provide.
- **TV/Radio Scam**: Perpetrators target potential victims using illegitimate

advertisements about legitimate services, such as reverse mortgages or credit repair.

- **Family/Caregiver Scam**: Perpetrators are relatives or acquaintances of the elderly victims and take advantage of them or otherwise get their money.

Once successful, perpetrators will likely continue to target vulnerable elderly victims with these schemes because of the prospect of significant financial gain.

Defense and Mitigation

Taking the following steps may help protect yourself from being victimized:

- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.
- Resist the pressure to act quickly. Perpetrators create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.
- Be cautious of unsolicited phone calls, mailings, and door-to-door services offers.
- Never give or send any personally identifiable information, money, jewelry, gift cards, or checks—or wire information or funds—to unknown or unverified persons or businesses.
- Ensure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.
- If you receive a pop-up or locked screen on your device, immediately disconnect from the internet and shut down the affected device. Pop-ups are regularly used by perpetrators to spread malicious software. To avoid accidental clicks on or within a pop-up, enable pop-up blockers.
- Do not open any emails or click on attachments you do not recognize, and avoid suspicious websites.
- If a perpetrator gains access to a device or an account, take precautions to protect your identity; immediately contact your financial institutions to place protections on your accounts; and monitor your accounts and personal information for suspicious activity.

Filing a Complaint

If you believe you or someone you know may have been a victim of elder fraud, you should contact your local FBI field office. You can also file a complaint with the Internet Crime Complaint Center at www.IC3.gov.

When reporting a scam—regardless of dollar amount—be as descriptive as possible in the complaint by including:

1. Dates the perpetrator had contact with you, and the methods of communication.
2. Names of the perpetrator and company.
3. Phone numbers, email addresses, and mailing addresses used by the subject.
4. Websites used by the subject company.
5. Method of payment.
6. Account names and numbers and the financial institutions to which you sent funds, including wire transfers and prepaid card payments.
7. Descriptions of interactions with the perpetrator and the instructions you were given.

Complainants are also encouraged to keep all original documentation, emails, faxes, and logs of all communications. Because scams and fraudulent websites appear very quickly, individuals are encouraged to report possible internet scams and fraudulent websites by filing a complaint with the IC3 at www.ic3.gov.

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