OFFICES OF HOMELAND SECURITY AND CIVIL DEFENSE
Inasiguran I Tano' Guahan/Ufisinan Difensia Sibet
221-B Chalan Palasyo, Agana Heights, Guam 96910
Tel: (671) 475-9600 / Fax: (671) 477-3727
Website: www.ghs.guam.gov

Esther J. C. Aguigui
Homeland Security Advisor
Charles V. Esteves
Administrator

For Immediate Release
February 6, 2025, 5 p.m. (ChST)

Community Advised to Be Wary of AI Scams

The Offices of Guam Homeland Security and Civil Defense, along with the Mariana Regional Fusion Center (MRFC), continue to receive reports of purported scams to unassuming recipients. The community is advised to be cautious of generative artificial intelligence (AI) videos, commonly referred to as "deepfake," to include ones seemingly from known individuals congratulating you on winning a sweepstake or trying to gather personal or financial information from you. By using deepfakes, criminals can target a larger audience and use more realistic methods to disguise their illicit activities.

AI-Generated scams can be conducted through:

- Text: Often used to distribute messages to multiple victims containing convincing information, such as those seen in romance and investment scams, as well as to create fraudulent social media accounts.
- Images: Commonly used to create believable photos such as fake social media profiles, fake photos in a social media library, or a fake driver's licenses, used to trick the victim into thinking they are communicating with a real person.
- Audio: Commonly used to impersonate public figures or someone close to the victim to solicit payments such as a loved one's voice asking for immediate financial aid or to pose as a business representative to obtain sensitive information.
- Videos: Frequently utilized to impersonate public figures for fraudulent activities, such as sending videos claiming the victim has won a sweepstakes or lottery. Additionally, they are used to trick victims into believing they are interacting with a real person during live video chats.

Remain vigilant and follow these tips to avoid falling victim to scams:

- Do not give your personal or financial information to someone you've only met over the phone or online. Pay close attention to any suspicious tone or word choice of the person if you receive a call.
- Avoid giving gift cards, money, or cryptocurrency to people you do not know or have only met over the phone or online.
- Keep your social media accounts private or limit the number of people allowed to follow you.
- If you receive a video, look out for irregular facial movements such as distorted or abnormal movement of the eyes or mouth or any delay between the words.
- Before providing money or personal information, talk to someone you trust. Scam artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, conduct an online search, consult an expert – or contact the MRFC.

The MRFC analyzes data and trends to identify scams and fraudulent patterns. Your report may help law enforcement identify the people behind AI-generated scams. When making a report, provide as much detail about the incident, including the day and time you were contacted, phone numbers, photos, names, email addresses, even if you think it might be fake, or specific instructions you were given.

Report any suspicious activity relating to the subject to the MRFC at (671) 475-0400 or via email at mrfc@ghs.guam.gov, following the Department of Homeland Security's campaign, "If You See Something, Say Something." Information that is provided to the MRFC will be recorded and properly disseminated to all pertinent authorities.

-###-