NEWS RELEASE

DATE: 03/11/2025

FOR IMMEDIATE RELEASE

CONTACT: **Michael W. Martel**
TITLE: **Postal Inspector/National Public Information Officer**
PHONE: **1-877-876-2455**
EMAIL: **ISMediaInquiries@uspis.gov**

Postal Inspectors Warn of Ransomware Scam Letters

Washington, DC – The U.S. Postal Inspection Service remains committed to preventing the use of the U.S. Postal Service by criminals to perpetuate criminal activity. To that end, the Postal Inspection Service is working jointly with the Federal Bureau of Investigations (FBI) to inform businesses of a recent ransom scam that could potentially disrupt their daily operations by threatening the security of their infrastructure.

Criminals, claiming to be from a ransomware group, are using the U.S. Postal Service to send letters containing ransom threats to corporate executives. Stamped "Time Sensitive Read Immediately," the letters at issue claim the "BianLian Group" gained access into the organization's network and stole thousands of sensitive data files. The letters threaten publication of the victim's data to BianLian's data leak sites if the recipient does not pay between $250,000 and $500,000 within 10 days utilizing the included QR code linked to a Bitcoin wallet. The letter states the group will not negotiate with the recipient of the letter.

The FBI believes the letters are an attempt to scam organizations into paying a ransom. The letter contains a U.S.-based return address of "BianLian Group" in Boston, Massachusetts. No connections have been made between the mailer of the letters and the known BianLian ransomware and data extortion group. Postal inspectors are investigating the portion of this scam touching the Postal Service and its customers.

Tips to Protect Yourself: Both the FBI and the Postal Inspection Service recommend individuals take the following precautions:

- Notify organization executives of the scam for awareness.
- Ensure employees are educated on what to do if they receive a ransom threat.
- If you or your organization receive one of these letters, ensure your network defenses are up to date and that there are no active alerts regarding malicious activity.
- If you discover you are a target of this scam, please visit the FBI's Joint Cybersecurity Awareness Bulletin for recent tactics, techniques, and procedures and how to detect network breaches to help organizations protect against ransomware.

The FBI requests victims report receipt of the above letters to your local FBI Field Office or the Internet Crime Complaint Center (IC3).

###