IRS

Fraud alert: Fake IRS letters target cryptocurrency holders

Date: July 30, 2026

Contact: newsroom@ci.irs.gov

Washington — Fraudsters are mailing fake IRS letters to cryptocurrency holders in an attempt to steal personal information and digital assets. The letters direct recipients to a fraudulent website that mimics IRS.gov and instructs them to register for a nonexistent "Digital Asset Compliance Portal." If you receive a letter claiming to be from the IRS that instructs you to enroll in a Digital Asset Compliance Portal, don't respond. The IRS did not send it. The IRS does not operate a Digital Asset Compliance Portal. This is a scam.

"Criminals continue to exploit public trust in government agencies by creating convincing fake websites and official-looking correspondence," said IRS Criminal Investigation (IRS-CI) Chief Jarod Koopman. "Before responding to unexpected requests for personal information, stop, verify the source, and report potential fraud schemes to law enforcement."

Scheme details

Victims receive what appears to be an official IRS letter claiming they must enroll in a "Digital Asset Compliance Portal" before a deadline. The letter instructs them to scan a QR code that directs them to a fraudulent website designed to look like IRS.gov. The site may ask for personal information, cryptocurrency wallet information, exchange account credentials, or other sensitive data that criminals can use to steal identities or digital assets.

Protect yourself

Fraudsters increasingly use convincing websites, official-looking letters, and urgent deadlines to trick victims.

- Don't scan QR codes from unsolicited letters, emails, or text messages, especially those claiming to be from a government agency.
- Hang up if someone claims to be from a government agency and asks for payment or personal information. Contact the agency directly using information from its official website.

- Slow down and verify the situation; scammers create false urgency to push victims into quick decisions.
- Protect your personal and financial information, especially in response to unsolicited messages. Never share wallet recovery phrases or private keys.
- Consult a trusted family member, financial advisor, or attorney before sending money or making major financial decisions.
- Monitor financial accounts regularly and report suspicious activity immediately. Enable multifactor authentication on accounts.
- Be cautious of new online acquaintances and verify identities before engaging further.
- Report suspicious IRS-related communications immediately.

If you or someone you know has been impacted by a fraud scheme, stop communicating with the fraudster; change passwords for affected financial accounts; contact your financial institution or cryptocurrency exchange immediately if you shared credentials; preserve screenshots, emails, and letters; and report information to IRS-CI at IRS.gov/submitatip.

This fraud alert demonstrates the importance of public-private partnerships. Coinbase and its partners at DarkTower traced the infrastructure behind this campaign to a domain registered through a Hong Kong registrar. The domain was registered just days before the fake letters were mailed to crypto-holders. The site was hosted in Romania on a network known for hosting phishing pages fraudulently tied to financial institutions. Additional details about this fraud scheme can be found on Coinbase.com.

IRS-CI is the law enforcement arm of the IRS, responsible for conducting financial crime investigations, including tax fraud, narcotics trafficking, money laundering, public corruption, healthcare fraud, identity theft and more. It is the only federal law enforcement agency with investigative jurisdiction over violations of the Internal Revenue Code. IRS-CI has 18 field offices located across the U.S. and maintains an international presence through attaché posts abroad.