‘Pay The Fine Now’—Feds Issue Text Warning For iPhone And Android Users

Zak Doffman May 03, 2026, 04:24am EDT

These texts are dangerous.
getty

This is a multi-billion-dollar threat to American smartphone owners — and it’s getting worse. Despite security innovations on both iPhone and Android, criminal gangs have started using AI to power “dramatically faster and effective" attacks.

This is a global text scam industry that has now prompted countless U.S. federal agency warnings. “It starts with a text message with a QR code,” the FTC warned two weeks ago, just as a new attack started to spike. “The message says you need to scan it to pay for a traffic violation to avoid court.” You are given two options. Attend the (fake) court hearing to appeal your innocence or "pay the fine now.”

“*Pay the fine now*.” If you see one of those texts, the FTC says, “don’t respond, and don’t scan the QR code. If you think the message might be real, check the court’s website for case information or call the court directly — but use a website or phone number you know is correct, not info from the text message.”

A traffic violation is just one potential lure. Last week, the FTC warned “that job offer text is probably a scam” as well. “There’s a new text scam the FTC is hearing about. It involves fake recruiters offering fake jobs, stealing real money.”

The FTC’s advice is broadly the same. “They’ll ask you to reply with ‘YES’ or ‘INTERESTED.’ Don’t do this, no matter how ’professional’ the graphics or message looks and sounds. They want you to engage so they can scam you.”

This global scam industry is rooted in South East Asia and powered by China’s organized criminal gangs. In a new report, the U.S.-China Economic and Security Review Commission warns that “American losses from industrial-scale scam centers operated by Chinese criminal groups in Southeast Asia continue to mount. The U.S. government estimates that Americans lost at least $10 billion

to Southeast Asia-based scams in 2024—with losses projected to have grown further in 2025."

The Prompt: Get the week's biggest AI news on the buzziest companies and boldest breakthroughs, in your inbox.

There's a nasty twist here. China's authorities are cracking down on the criminals, USCC says, but only where they target Chinese citizens. "In December 2025, China's Ministry of Public Security published a list of 100 high-level criminals wanted for scams 'targeting Chinese citizens,'" but Beijing "continues to turn a blind eye to criminal activity targeting foreigners."

Forbes 'Action Is Needed'—Microsoft Changes Windows Update In 10 Days By Zak Doffman

And so the FBI's comprehensive warning on text scams remains as relevant now as ever — notwithstanding new security innovations on our phones. Do not reply to warning texts unless you can independently verify the sender. Do not click links or make any payments. Report and then delete all such texts right away.

Even texts that seem to come from the FBI or other law enforcement agencies can be scams. You cannot take any such messages at face value. Put simply, you need to adopt a zero trust position to texts at all times: Never trust, always verify.