Kim Komando: “Tech Alert”

The second sting

Image: ChatGPT/Kim Komando

TL;DR:

- Scammers are impersonating the FBI to target people who already lost money to fraud once.
- They use AI-generated videos of real FBI officials, fake agent profiles and copycat versions of ic3.gov to look legitimate.
- If you or someone you love has ever reported a scam or lost money to one, you’re exactly who they’re looking for.

📖 **Read time:** 2 minutes

This is alarming. Scammers are impersonating the FBI itself, specifically the people who handle Internet Crime Complaint Center reports. And they hunt one group above all others: Americans who already lost money to a scam.

The pitch sounds like mercy: We recovered your funds. We can help you file to get them back. Simply cover the fee.

🎭 Why it looks so real

The bureau updated this alert, and the upgrade is the ugly part. Criminals run AI-generated videos of senior FBI officials. They build social media profiles for agents who never existed. They stand up copycat sites that mimic the complaint center's hub at ic3.gov, issue official-looking case reference numbers and move it all to Telegram.

A security firm spotted one Facebook page calling itself "Ic3 Scam Recovery Inc.," complete with invented testimonials promising a professional case assessment.

Here's how they find you. They read the public posts. Somebody vents in a Facebook group about losing eight grand, and within a day, a polite stranger slides into their direct messages.

The numbers explain the effort. The IC3 logged more than a million complaints in 2025 with losses topping nearly $21 billion, a 26% jump in a single year. Americans 60 and older absorbed more than $7.7 billion of that. Government impersonation alone drew over 32,400 reports and nearly $800 million in losses.

🛑 Burn these four rules into your brain

One. The IC3 has no social media presence. None. Any Facebook page, X account or Instagram profile claiming to be IC3 is fake, full stop.

Two. The FBI will not call, email or text you offering to recover your money. That call is a scam.

Three. Type ic3.gov into the address bar yourself. Skip the search results, especially the sponsored ones. Confirm the address ends in .gov before you type a single detail.

Four. Nobody legitimately charges you a fee to get your own money back. The second somebody mentions crypto, gift cards or a wire transfer, hang up.

If this has already happened to you or someone you love, report it at [ic3.gov](ic3.gov). And for people 60 or older, the Justice Department runs an Elder Fraud Hotline at 1-833-372-8311, staffed by real people who walk you through the filing.

Getting scammed is not a character flaw. Professionals did this to you, and they do it all day. The only shame in this story belongs to them.

✅ Get proactive

Recovery scammers don’t guess who to target. They buy lists.

Data brokers package your name, your age, your phone number and your home address into a file, then sell it to anyone with a credit card, including the people running the scam you just read about.