COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Border Security & Enforcement Subcommittee Ranking Member Lou Correa (D-CA)

Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans

April 21, 2026

Today's hearing is an important one. Every single day Americans of all ages and backgrounds are victims of scams and cyber crimes that aim to hurt them or their loved ones. Cyber criminals and transnational criminal organizations (TCOs) are no longer confined by borders or limited to the number of victims they can target. Everyone is a possible target in their eyes. This topic isn't a Democrat or Republican problem, it's an everyone problem. Cyber criminals target all Americans, including the most vulnerable in our communities.

Today's cyber criminals are sophisticated and organized enterprises, leveraging corruption, cutting-edge technology, and human trafficking to generate vast streams of illicit revenue. This comes at our expense. Large, organized criminal gangs, especially in China and Southeast Asia, build large scamming centers to target our community members and critical infrastructure.

According to the FBI, cyber-enabled fraud in 2025 led to over $17.6 billion dollars' worth of reported losses. Transnational Criminal Organizations use a variety of schemes to target everyday Americans. Romance and sexploitation scams, fake cryptocurrency investment schemes, and government impersonation communications defraud Americans out of billions each year. We also see artificial intelligence (AI) helping transnational criminal organizations to scale their operations and increase their success rates.

They can generate highly personalized phishing messages, deploy sophisticated password-cracking tools, and create convincing deepfakes that blur the line between reality and deception. I bet most of us in this room have been the target of these scams and phishing messages. Cybercriminals also use a wide variety of digital weapons to target the businesses, public services, and daily necessities we rely on.

We've seen cyberhackers use ransomware and other tools to conduct data breaches, disrupt hospital operations, delay emergency services, and take down energy grids, threatening the services we rely on every day. No sector is off-limits. Ransomware remains a serious threat to U.S. critical infrastructure. Over 2,100 ransomware incidents targeting critical infrastructure were reported in 2025.

Their methods are varied, constantly evolving, and increasingly difficult to detect. The use of digital platforms and underregulated financial instruments allow these criminals to operate with a high degree of anonymity, complicating efforts to track, attribute, and prosecute their crimes. At a time when these threats are growing more sophisticated and pervasive, the Trump Administration is failing to respond and is weakening our ability to counter cyber criminals.

This Administration has strained critical resources dedicated to combating cyber scams and financial fraud. Over the last year-and-a-half, the White House gutted the Cybersecurity and Infrastructure

Security Agency (CISA) in the name of government efficiency. Roughly a third of its workforce has been cut, its leadership has been embroiled in controversy, and CISA's funding has been redirected towards immigration enforcement instead of cybersecurity. The President's Fiscal Year 2027 proposes additional cuts that threaten the very systems and institutional expertise we rely on to protect our citizens from cyber criminals. Similarly, over the past year, Homeland Security Investigations agents dedicated to combating child exploitation and digital financial crimes have been redirected to immigration enforcement, limiting our capacity to fight cyber criminals.

The schemes and damage caused by cyber criminals demonstrate that we face a dynamic, well-resourced, and well-organized adversary that DHS must be equipped for and ready to combat. I hope my Republican colleagues join Democrats in calling for the Trump administration to stop cutting personnel at CISA and other cyber agencies, as well as redirecting law enforcement specialized in combatting these crimes, and instead provide the resources needed to help fight these cyber criminals and keep Americans safe from these threats.

I look forward to hearing from our witnesses and engaging in a productive discussion on how we can meet this challenge head-on.

# # #

Media contact