STATEMENT OF
GREGORY HEEB
DEPUTY ASSISTANT DIRECTOR
CRIMINAL DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
JOINT ECONOMIC COMMITTEE

AT A HEARING ENTITLED,
"The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters"

PRESENTED
March 25, 2026

STATEMENT OF
GREGORY HEEB
DEPUTY ASSISTANT DIRECTOR
CRIMINAL DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
JOINT ECONOMIC COMMITTEE

AT A HEARING ENTITLED,
"The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters"

PRESENTED
March 25, 2026

Chairman Schweikert, Vice Chair Schmitt, and other members on the committee, thank you for having me here today.

My name is Gregory Heeb, and I am the Deputy Assistant Director of the Criminal Division for the Federal Bureau of Investigation (FBI). I appreciate the opportunity to speak with you today about the FBI's efforts to combat overseas scam compounds.

The Scam Landscape

In the past decade, the FBI's Internet Crime Complaint Center (IC3) has reported exponential growth in scam victimization of U.S. citizens, particularly through cyber-enabled fraud, which the FBI defines as the use of the internet and digital technologies to conduct scams. Fraud is the broader legal category. Scams are a subset, typically involving social engineering, and deception to induce the voluntary transfer of funds.

Preliminary 2025 data from the IC3 underscores the magnitude of this problem. Last year alone, IC3 received approximately 456,000 cyber scam-related complaints, with reported losses exceeding $17.7 billion. We know these figures are underreported, so the statistics published by the IC3, while staggering, only represent part of the whole. Many people never report these scams. They may be embarrassed, afraid of losing independence, not believe law

enforcement can help, or not realize they were scammed. Some worry it will cause family conflict, or are impacted by memory issues making it difficult to explain what happened.

While reported victimization increased modestly over the past several years, reported dollar losses increased dramatically — roughly 350% since 2019. In other words, the financial impact per victim has escalated sharply. The $17.7 billion lost last year equates to nearly $48 million lost per day, or more than $2 million per hour. These are retirement accounts, college funds, and lifetime savings flowing to organized criminal enterprises operating abroad.

While Americans across all age groups are affected by cyber-enabled fraud, adults aged 60 and older accounted for approximately 24% of complaints and 42% of losses last year.

This growth in victimization has not been random. It has been driven by structural shifts in technology, finance, and global criminal organization. Over the past fifteen years, overseas criminal organizations have exploited successive waves of U.S. financial innovation. As transactions became faster and more digital —from peer-to-peer platforms to cryptocurrency — fraud became more scalable and anonymous.

What began as decentralized fraud has consolidated into vertically-integrated call centers and scam compounds operating abroad. These enterprises combine professionalized social engineering teams, financial laundering units, cryptocurrency conversion capability, and management hierarchies — all operating around the clock and targeting Americans at a rapidly-expanding scale.

While low-dollar scams may originate from a mix of domestic and overseas actors, the overwhelming majority of high-dollar scam losses — particularly investment scams, business email compromise, tech support scams, and romance fraud — are executed by organized transnational criminal enterprises.

These criminal enterprises are not randomly dispersed. Certain regions have become hubs for specific scam typologies. West Africa has long been associated with romance and confidence schemes. The Caribbean is a hotbed for lottery scams. South and Southeast Asia have emerged as epicenters for tech support scam schemes and large-scale cryptocurrency investment fraud and scam compounds, in some cases fueled by corruption and linked to human trafficking. Other regions host infrastructure supporting business email compromise and laundering operations.

Also driving the growth in scam victimization is our nation's demographic shift. By 2030, one in five Americans will be over 60. Aging increases cognitive decline, and older Americans hold a disproportionate share of national wealth. Over the coming decades, $30–68 trillion will transfer between generations. This will be the largest wealth transfer in history, one

that economists have termed "The Great Wealth Transfer." That convergence of vulnerability and concentrated assets creates extraordinary opportunity for transnational fraud actors.

The Impact of Victimization

The consequences of scam victimization to the U.S. economy are profound. This is not simply consumer fraud. American productivity, intellectual capital, and lifetime earnings are being converted into revenue streams for organized criminal networks beyond our regulatory reach. These funds can be reinvested into corruption, trafficking, and other destabilizing activities.

For victims, the impact can be devastating. Many lose retirement savings, home equity, or their entire life savings. Victimization can be particularly more devastating to older adults living on fixed incomes. Beyond financial loss, victims experience shame, isolation, depression, and lasting psychological harm. Some cases result in suicide. This crime robs individuals not only of money, but of security, dignity, and peace of mind. In some cases, financial damage is compounded by tax liabilities on stolen retirement funds.

Tradecraft

The success of modern scams is rooted in tradecraft, specifically social engineering; psychological manipulation, including heightened emotion, urgency, and isolation; and often, revictimization. Scammers adapt rapidly. Blended schemes and evolving narratives are now common. Criminals exploit emotion, authority, and trust. Heightened emotion and urgency drive panic, which places the targeted victim into "fast thinking" mode. As a result, the victim will act without thinking. Panic overrides deliberation. By targeting victims who may already be isolated from others and urging targeted victims to maintain secrecy over the interaction, the scammer minimizes the likelihood others will intervene to stop the scam attempt. This increases the prospect the victim will fall for another scam attempt.

Increasingly, scammers use artificial intelligence (AI) to enhance credibility and scale deception. AI tradecraft includes the use of deepfake voice, video, and image technology, as well as the creation of grammatically-correct correspondence.

Scam Compounds in Southeast Asia

Investment fraud remains the dominant scam typology, accounting for 48% of all cyber-enabled fraud losses in 2025. From 2019 to 2025, victim and dollar losses to investment scams sharply increased; victimization and losses increased 1,725% and 3,793%, respectively, outpacing every other fraud category, driven by the scalable industrialized scam compound model and the widespread use of cryptocurrency.

Investment fraud is predominately perpetrated by organized criminal enterprises operating scam compounds located in Southeast Asia, which rely on victims of human trafficking to serve as forced labor to run the scam operations.

Cryptocurrency investment fraud is a sophisticated long-term scheme using psychological manipulation, the appearance of legitimacy, and exploitation of cryptocurrencies to deceive victims into investing large sums of money. Cryptocurrency investment fraud was the highest source of financial losses to Americans in 2025, representing 41% ($7.2 billion) in all cyber-enabled fraud losses in 2025.

The scammers typically initiate contact through text messages, social media sites, advertisements, or dating applications and then quickly move the conversation to a messaging platform. Often, the victims are introduced to investment groups representing themselves to be knowledgeable industry insiders offering guidance on trading or investing in cryptocurrency or gold. The victims are enticed to send cryptocurrency to fake investment scam platforms or applications and are shown fake profits and offered loans to encourage larger investments. Eventually, when the victims try to withdraw their money, they will be charged taxes and fees as a final attempt to exploit money from the victims before the scammers disappear with all the victim funds. Victims are also targeted in recovery scams, claiming to help recover lost funds.

There has also been a rise in investment scams utilizing social media platforms and messaging service applications, also executed by threat actors based in Southeast Asia-based scam compounds. This scam type intersects investment scams and stock market manipulation, and it is defrauding Americans at an alarming rate. The scheme, known as a "ramp-and-dump" stock manipulation, targets U.S. investors through online engagement, often via social media advertisements or messages promoting an "investment club" of fellow investors, some of which may be bots or fake accounts. These promotions typically direct victims to secure messaging apps where the group operates. To appear credible, perpetrators may impersonate legitimate brokerage firms or well-known stock analysts. They secretly control a large volume of a low-priced stock and coordinate efforts to inflate its price ("ramp up") by encouraging club members to purchase shares over a period of several weeks or months. Once the price is artificially elevated, the criminals sell off ("dump") their shares at a profit, leaving unsuspecting investors with significant losses as the stock value collapses.

Combatting the Threat

The FBI has been aggressively combating scams on every front through our international presence, participation in the Scam Center Strike Force, enterprise investigations, public awareness campaigns, and partnerships.

One of the FBI's strengths is its global reach, with 90 overseas offices and coverage for over 200 countries, territories, and islands. Through our strong relationships with foreign law enforcement, our investigative teams have worked with partners in more than 60 countries, dismantling global fraud networks and seizing assets. We have personnel located in identified epicenters of specific scam types, such as Accra, Ghana; New Delhi, India; and Bangkok, Thailand.

These personnel coordinate operational efforts with local law enforcement to disrupt, dismantle, and deter criminal syndicates, collect intelligence, and recover victim funds. This international coordination is critical: the threat is global, so our response must be as well.

Since 2022, the DOJ, FBI, and IC3 have collaborated with law enforcement in India, to include the Central Bureau of Investigation (CBI) in New Delhi and local Indian states, to combat cyber-enabled financial crimes and transnational call center fraud. The collaborative efforts of the FBI and CBI have resulted in over 1,200 exchanges of information to support criminal investigations, with more than 475 arrests across 27 joint operations.

The FBI is a proud partner of the United States Attorney's Office, District of Columbia Scam Center Strike Force ("Strike Force"). The purpose of the Strike Force is to disrupt scam center targets and facilitators, leverage subject matter expertise, and utilize an entire government approach. The Scam Center Strike Force is also engaged with the U.S. Intelligence Community (USIC) on the threat. The United States Secret Service and DOJ Criminal Division are also key partners on the Strike Force.

The Strike Force is targeting the leaders and organizers of major cryptocurrency investment fraud compounds located in Laos, Burma, and Cambodia. In August 2025, FBI Chicago supported the disruption and prosecution of 38 suspects who supported five scam centers located in in Bali, Indonesia, targeting American citizens. In November and December 2025, multiple web domains, used to facilitate scams and linked to a scam compound in Burma, were seized. One seized domain was disguised as a legitimate investment platform to lure victims into unknowingly depositing their funds, showing fraudulent returns on what they believed to be lucrative investments.

The FBI takes a whole-of-government approach to target, investigate, and disrupt transnational scam enterprises through partnerships with federal law enforcement and international counterparts. We focus not just on individual actors, but on dismantling the broader criminal ecosystem by focusing on the financial enablers and key infrastructure. These investigations are initiated through our partnerships with federal and international law enforcement partners, the USIC, the private sector, or open-source intelligence.

Prevention remains critical. Across our 56 field offices, we conduct outreach and awareness initiatives to educate the public on scam indicators and psychological manipulation tactics. Our campaigns, such as Take a Beat, emphasize pausing, verifying, and resisting urgency-based manipulation. Although awareness alone is not sufficient, it is a necessary first layer of defense.

The IC3 remains the central hub for reporting cyber-enabled crime. It aggregates complaints, publishes public advisories and annual reports, and disseminates investigative referrals to domestic and international partners. This reporting infrastructure is essential to identifying patterns, connecting victims, and building enterprise-level cases.

The IC3's Recovery Asset Team works directly with financial institutions to freeze fraudulent wire transfers using the Financial Fraud Kill Chain process. In 2025, the team handled approximately 3,900 incidents representing over $1.1 billion in attempted theft, freezing more than $679 million. These interventions do not eliminate the threat, but they significantly reduce victim harm.

The FBI is committed to aggressively pursuing and returning stolen funds to victims. Victim fund recovery restores more than money; it restores dignity to victims, reinforces public trust in institutions, and prevents long-term financial destabilization, especially for vulnerable populations like senior citizens. Effective recovery efforts also disrupt criminal networks' economic models, making them a core component of deterrence and national financial security. In 2025, the FBI returned more than $336 million to victims.

The FBI has robust relationships with the private sector. Our private sector collaboration is essential because the private sector often sees fraud first and controls the platforms, transactions, and data that scammers exploit. We bring our investigative authority, disruption capabilities, international reach, and the ability to dismantle criminal networks.

Minimizing Victim Harm

The FBI proactively identifies victims of cryptocurrency investment fraud and works to disrupt the activity to prevent further financial loss. The "Operation Level Up" initiative, launched in January 2024, uses sophisticated techniques to identify victims who are actively being defrauded. The FBI intervenes by calling those victims directly and informing them of the scam activity. Since inception of the initiative, the FBI has notified 8,390 victims of cryptocurrency investment fraud. Of those victims, 77% were unaware they were being scammed. The estimated savings to victims is over $529 million. Eighty-five victims were referred to an FBI victim specialist for suicide intervention. Around 1,000 foreign victims were identified, and respective law enforcement entities were contacted for further action deemed necessary; over 1,600 illicit scam domains, emails, numbers, and accounts were identified and

disseminated to Meta, Google, Apple, and Microsoft for action; and over $101 million in cryptocurrency was frozen and/or seized. The success of this initiative demonstrates that timely intervention can materially reduce harm.

Closing

The Department of Justice and the FBI are unwavering in their commitment to halt cyber-enabled scams. With the recently issued Executive Order entitled "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens", we are confident that all components of the federal government will join together to achieve maximum disruption of Southeast Asian scam centers to combat cybercrime, fraud, and predatory schemes against Americans.[1]

Awareness and education are paramount, but they are not sufficient to prevent victimization. Law enforcement alone cannot solve a threat that is global, digital, highly adaptive, and financially incentivized. Addressing transnational scam enterprises requires sustained coordination across the government, law enforcement, the private sector, and international cooperation: reducing victimization; disrupting criminal infrastructure; and strengthening national financial resilience.

The FBI greatly appreciates the Committee's interest in this vital effort and the steps we are taking to address overseas scams. This is not simply about fraud prevention. It is about protecting Americans, safeguarding our nation's wealth, and defending the integrity of our infrastructure. Thank you for inviting me here today. I am available to answer questions you have.

[1] Executive Order 14390 of March 6, 2026 (Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens), see https://www.govinfo.gov/content/pkg/FR-2026-03-11/pdf/2026-04826.pdf; President Trump's Cyber Strategy for America, March 2025, see https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf