TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Senate Special Committee on Aging

Made in China, Paid by Seniors: Stopping the Surge of International Scams

NATHAN PICARSIC

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
January 14, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

I would like to thank Chairman Scott, Ranking Member Gillibrand, and committee members for the opportunity to join today's hearing and offer testimony alongside my esteemed co-witnesses. I would also like to thank the committee members and staff for convening this hearing and dedicating effort to crafting thoughtful legislation to support American elders and families impacted by elder scams.

According to FBI analysis, the elder scam marketplace already accounts for billions of U.S. dollars in harm annually. China and Chinese-linked operations play an outsize role in executing and supporting these international scams. That constitutes a direct threat to America's elderly population and to American society.

In this testimony, I hope to convey three points about the threat: The strategic implications of international scam operations and their relevance to great power competition between the United States and China; the complicit nature of the Chinese government in the proliferation of scams that target elderly populations in the United States; and the need for legislation and federal government leadership to empower coordination between federal authorities, law enforcement, and the financial ecosystem that can disrupt and deter China-linked scams against Americans.

Elder Scams and Strategic Competition

The strength of the United States, both domestically and as it stacks up against international competition, is a function of the whole of American society. America is at its greatest when confident in its domestic cohesion. That cohesion has historically stemmed from a social contract that provides opportunity for life, liberty, and the pursuit of happiness; it requires trust backed by the rule of law, transparency, and justice. Those features set America apart. They make everything from our capital markets to our universities to our farms the envy of the world. But American institutions and the American experiment writ large did not emerge without struggle, and they will not be sustained without vigilance.

America should lead. Leading requires, on the one hand, openness to the world and, on the other, concomitant investment in protecting against the risks that openness invites. Mastering that balance is a key to American greatness. Nothing better reflects the importance of getting that balance right — and signals to our competitors our sincerity and resolve — than how we protect our most vulnerable.

Social cohesion is a pivotal battleground in today's international contest. Defending against external attacks targeting our vulnerable, including our elderly, is a fundamental, if nontraditional, requirement for succeeding in long-term, peacetime competition.[1]

[1] Emily de La Bruyère and Nathan Picarsic, "Wanted: A Strategy for Long-term Peacetime Competition with China," *Foundation for Defense of Democracies*, June 1, 2020. (https://www.fdd.org/analysis/2020/06/01/strategy-for-peacetime-with-china)

China understands this. And China deliberately positions itself to foment fissures within American society and to tease at American vulnerabilities.[2] It is not uncommon to hear about this Chinese tack in the context of malign foreign influence in narrative and media, foreign investment that carries national security risk, or efforts to capture elites across American society. The same underlying, competitive ambitions that propel those hydra heads of China's global influence campaign also propel the transnational criminal forces that execute, guide, and redeem proceeds from elder scams in the United States. Chinese criminal actors have been prosecuted for roles in leading elder scams in the United States. But recognition of the full scope of this threat lags. So, too, does marshaling a right-sized response.

State-Backed Scamming

Scams targeting elderly Americans know no political or socio-economic boundaries. If you have an aging parent, grandparent, or neighbor, you've certainly heard the harrowing tales and very likely also know the implications, personally, of these attacks. Elder scams generate stress and devastation for targets, victims, and their families all across the United States.

These scams also know no borders. Scam operations are big business. And they are international. China plays an outsize role in the expansion, proliferation, and nefarious success of these scams. China plays this role both in scams that originate in China itself and outside, in hotspots across Southeast Asia, where scam operations exist and scam compounds operate under Chinese leadership. Chinese-linked scam operations feed into a broader network of transnational criminal efforts. Those efforts are permitted and, at times, abetted by the Chinese state and its ruling Communist Party.

China's broader transnational criminal enterprise benefits from a permissive state apparatus in Beijing. The leaders of the Chinese Communist Party would much rather see criminal acts perpetrated against foreign targets than against China's own aging population. Accordingly, the Chinese government has allowed China's cottage industry of scam operations, including those that target elder victims, to exist — and to refine tactics, techniques, procedures, and international positioning that enable professional and adaptive performance.

China's scam networks are best-in-class, just as China's hackers have matured to pose persistent threats to critical global cyber networks. Unfortunately, global — and American — vigilance has not kept pace. And China has several fundamental advantages that make catching up in this hider-finder game a daunting task for relevant American authorities.

First, China's transnational criminal networks benefit from advanced technology — and the Chinese state's support for developing, fielding, and scaling that technology. Beijing pursues a "network great power" strategy.[3] The strategy is built on a backbone of communications network, including telecommunications network, capabilities that are directly transferable to transnational

[2] RADM (Ret.) Mark Montgomery and Annie Fixler, "China has a cyberspace campaign plan. Does Washington?" *Washington Examiner*, December 5, 2022. (https://www.washingtonexaminer.com/news/2871713/china-has-a-cyberspace-campaign-plan-does-washington)

[3] Emily de La Bruyère, "The Network Great-Power Strategy," *Asia Policy*, APRIL 2021, pages 5-16. (https://www.jstor.org/stable/27023967)

criminal operations and the tactics of common elder scams. For instance, Chinese industrial and technological capacity in networking equipment, cloud computing, artificial intelligence, and big data all help Chinese transnational criminal organizations generate, share, refine, and distribute English-language scripts for social engineering calls and chats that feed elder scams. Moreover, China's telecommunications champions have internationalized, along with Beijing's so-called "Belt and Road." This provides regional bastions from which Chinese criminal organizations can operate — and that the Chinese state can use for an added buffer of plausible deniability.

Second, China's banking sector has followed the same "Go Out" playbook as China's corporate sector. This has laid the financial foundation for Chinese scam networks to internationalize. China's rise as a global banking power allows China-linked criminal networks to transfer money across borders, obfuscate the flow of funds, and evade regulatory authorities. Chinese criminal networks often use bank outposts in Hong Kong to transfer ill-gotten gains and to obfuscate their ultimate destinations. As long as funds are flowing over Chinese bank channels, international — including U.S. — authorities are hard-pressed to guarantee compliance with basic anti-money laundering requirements, let alone keep pace with emerging threats like those presented by cryptocurrency.

The net impact of China's positioning is a new, global, and highly efficacious phenomenon of state-backed scamming. This phenomenon will continue to benefit from scale, technology, and a complicit banking ecosystem in China. As China increases its investments in advanced networking and communications and financial technologies, including crypto, China's criminal networks will benefit. They will become more adept at executing, and profiting, from elder scams. America's seniors will suffer the consequences.

Commendable work by the U.S. Department of Justice has documented how China's capabilities come together today to create a large-scale threat and commensurate impact.[4] Elder scams executed by Chinese-linked networks prey on a variety of populations but prioritize those known to be vulnerable targets — namely, individuals who are retired, have ample savings, and lack digital fluency. How do scam networks identify those targets? Through data brokers trafficking lists from previous hacks, including insurance hacks. And those hacks, in turn, are often the work of Chinese state-backed hackers.

"Pig butchering" (杀猪盘) has emerged as a term to describe certain cyber-enabled scams that frequently target elderly victims. That term traces back to Chinese, underscoring the foundational role of Chinese entities in shaping the tactics and networks that dominate the international scam marketplace.[5] "Pig butchering" scams originated in China. But today, they have been scaled in the United States, in many cases by Chinese operations, and target American citizens.

[4] U.S. Department of Justice, "Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse," October 2025. (https://www.justice.gov/elderjustice/media/1416301/dl?inline)

[5] The term was even included among a set of "top 10 new terms in Chinese media in 2019" and reportedly was first coined by Chinese online commenters: Ying Ni, "2019年度中国媒体十大新词出炉 夜经济、极限施压等入列 [The top 10 new terms in Chinese media in 2019 have been released, including 'night economy' and 'maximum pressure']," *China News* (China). (https://www.chinanews.com.cn/gn/2019/12-16/9034981.shtml)

For example, in May 2024, the U.S. Attorney's Office for the Eastern District of Texas brought charges against a Chinese national who allegedly attempted to commit wire fraud and money laundering crimes to move "millions of dollars." He had allegedly acquired those funds by convincing unwitting victims that they were investing in legitimate business opportunities via cryptocurrency.[6] That is just one case. In July 2024, the U.S. Attorney's Office in the Southern District of California brought charges against five Chinese nationals accused of "a massive, complex fraud and money laundering scheme." That case featured $27 million in funds alleged to have been acquired by fraud, with more than 2,000 American seniors among the victims of the indicted network.[7]

Dozens of additional cases of a similar scope have been brought to light over the past few years. But those cases risk being the tip of the iceberg. The true scale of Chinese-linked attacks is unknown; it is safe to assume that some multiple of the number of cases that have been discovered and prosecuted has actually played out — and that the pace of growth in Chinese-tied elder scams, whether measured in victims or value, will continue to accelerate in the years ahead.

Compounding the threat posed by Chinese-tied tactics and perpetrators is the power of the Chinese financial system in propelling them. Take, for instance, one "business email confidence" case in which the Department of Justice sought to recover funds that had been deployed through U.S.-based "mules." That case saw upwards of 5 million U.S. dollars fraudulently attempted to be routed out of the United States. In that case, the destinations for transfer of ill-gotten funds were allegedly Bank of China, Standard Chartered in Hong Kong, and Singaporean accounts.[8] And the problem isn't just that this internationalized Chinese banking system exists as a channel for funds. Worryingly, this channel makes it nearly impossible to reclaim stolen funds. Victims of elder crime often have little recourse after funds have been offshored and may see their entire savings drained. Moreover, those funds, in turn, become fuel for additional criminal activity. Technological advances across telecommunications networking and cryptocurrency will add additional fuel to this fire.

The systemic nature of China's scamming enterprise amounts to great power stakes. The U.S. — government, technology companies, and banks — cannot afford to stand by as Chinese-linked criminal networks deplete American social trust and bank accounts.

Defending American Elders

A whack-a-mole response will not solve the challenge at hand. State-backed, international scam networks have the resources and flexibility to outfox both their targets and the law enforcement authorities that are invariably playing catch-up once alerted to a case. To offset this imbalance, the United States needs to erect protections and sensing — akin to the use of anti-virus software — that provide early warning. The U.S. government needs to increase awareness of these risks and

[6] U.S. Attorney's Office, Eastern District of Texas, Press Release, "Chinese national charged in "pig butchering" scheme," May 21, 2024. (https://www.justice.gov/usao-edtx/pr/chinese-national-charged-pig-butchering-scheme)
[7] U.S. Attorney's Office, Southern District of California, Press Release, "Five Chinese Nationals Indicted for Scamming Seniors Out of More Than $27 Million," July 31, 2024. (https://www.justice.gov/usao-sdca/pr/five-chinese-nationals-indicted-scamming-seniors-out-more-27-million)
[8] See: United States v. Approximately $143,586.44 Seized From JPMorgan Chase, No. 1:24-cv-11467, June 5, 2024. (https://www.justice.gov/usao-ma/media/1354406/dl)

the common tactics leveraged by scammers to inoculate our most vulnerable and the institutions that support them. And the U.S. government must enforce aggressively against perpetrators to send a deterrent signal.

Legislation can help. In particular, the National Strategies for Combating Scams Act offers an orienting call for strategy. Its requirement for the rapid development of a national strategy aligns with the urgency of the risk. That bill's mandate to drive coordination across over a dozen relevant federal agencies will spur necessary interagency collaboration and information sharing. Similarly, the Scam Compound Accountability and Mobilization Act addresses the sprawling, global layout of scam networks that operate across Southeast Asia with backing from China-linked actors and that benefit from opportunities to launder proceeds through China's banking system. The act's tasking to the secretary of state will compel additional coordination across the interagency and enable targeting of Chinese equities through the proposed Enabling Country List mechanism.
Those efforts can go a long way toward activating federal resources and coordination. That is a necessary first step to empowering law enforcement and local actors who stand on the front lines of supporting elder Americans and their families as they confront a tidal wave of China-linked scammers. Additional effort will be necessary to properly resource and provide information to those subnational and non-federal authorities.

At the same time, the great power stakes of the threat to America's elderly population underscore that, ultimately, protective measures need to deliver a deterrent effect in the adversary's system. In order to orient toward that objective, U.S. federal authorities across the interagency should prepare for and signal to Chinese counterparts the political will and practical capacity to effectively target the core nodes of the Chinese banking system that aid and abet crimes against American elders. Those nodes of the Chinese banking system are the same ones that fund China's military-civil fusion ecosystem and that move money to support coordination between Chinese chemical companies and international drug cartels. Imposing costs on those pillars of China's system would not just be good defense of America's elders, but rather it would be good strategy. Signaling resolve in this direction could be conveyed by documenting assets of high-risk Chinese financial institutions and their leaders that may be held in the United States and, as such, could be subject to seizure under authorities that could be triggered by the International Emergency Economic Powers Act (IEEPA).

Thank you for the opportunity to contribute to today's hearing and for the important work of the committee on these timely issues.