



# Protecting Americans from China-Linked Scam Centers

## An Update on Emerging Trends

MARCH 5, 2026

### Key Findings

- » 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.
- » In recent months, the U.S. government has taken steps to protect Americans from scam centers in Southeast Asia by sanctioning criminal kingpins and launching an interagency Scam Center Strike Force. Yet Chinese criminal organizations are moving quickly to stay ahead of the crackdowns by embracing advanced technologies and exploiting cryptocurrency to launder stolen assets across national borders with virtual impunity.
- » Scam centers are rapidly adopting artificial intelligence (AI) tools to scale their operations, increase the sophistication of scams, and evade traditional detection methods. These AI-powered scams make it difficult for even the most discerning potential victims to distinguish fact from fraud.
- » In response to Beijing's selective crackdowns on scam centers in Southeast Asia, many Chinese criminals are returning home and opening smaller-scale scam operations inside China that exclusively target foreigners—an alarming new trend known in Chinese as "foreigner butchering."
- » Chinese criminal organizations are also globalizing their scam operations. New clusters of scam centers are emerging in the Pacific Islands, South Asia, the Middle East, and West Africa. Building on its playbook from Southeast Asia, China is exploiting the globalization of scam centers to expand its security presence throughout these regions.

## Introduction

In July 2025, a Florida woman named Sharon received what appeared to be a distraught call from her daughter, who had been detained after a car accident and urgently needed \$15,000 to pay bail. “There is nobody that could convince me that it wasn’t her,” Sharon said later. “I know my daughter’s cry.”<sup>1</sup> As it turns out, Sharon had fallen victim to a sophisticated scam that used AI-powered voice cloning technology to replicate her daughter’s voice, likely using snippets of audio from social media.<sup>2</sup> Her case illustrates a disturbing trend. The crime syndicates behind these operations are rapidly embracing AI tools—among other new tactics—to create dramatically faster and effective scamming operations and stay ahead of the possible crackdowns.

In July 2025, the Commission published a [report](#) on *China’s Exploitation of Scam Centers in Southeast Asia*, which analyzed how scam centers operated by Chinese criminal groups defraud Americans of billions of dollars annually. The Commission found that Beijing is exploiting the growing crisis of scam centers—which spread across Southeast Asia with *at least* implicit backing from elements of the Chinese government—to expand its security footprint in the region. As with the fentanyl crisis, Chinese criminal networks are inflicting enormous harm on Americans while Beijing selectively enforces only when it serves its own interests. Since the Commission published its findings, the U.S. government has sanctioned individuals and entities involved in scam centers and announced the formation of an interagency Scam Center Strike Force. Nevertheless, the scam crisis only continues to escalate. The U.S. Department of the Treasury now estimates that Americans lost \$10 billion to Southeast Asia-based scams in 2024—and losses are projected to have exceeded that figure in 2025.<sup>3</sup>

This Commission issue brief analyzes three developments that pose challenges to U.S. efforts to combat scam centers:

1. Scammers’ adoption of AI and AI-enabled tools and exploitation of cryptocurrency.
2. The rise of scam operations inside China that exclusively target foreigners.
3. The globalization of China-linked scam centers beyond Southeast Asia.

The success of U.S. efforts to protect Americans from scams will depend on whether authorities can move to enact policies to stay ahead of these emerging trends and cooperate on enforcement efforts with other governments.

## New Measures Cracking Down on Scam Centers

The U.S. government has taken several steps to begin addressing the scam crisis.

- In September 2025, the Treasury Department sanctioned numerous entities and individuals behind major scam hubs in Burma and Cambodia.<sup>4</sup>
- In October 2025, the United States and the UK imposed coordinated sanctions on the Prince Group, a transnational criminal organization that operates large-scale scam centers across Cambodia.<sup>5</sup> At the same time, the U.S. Department of Justice indicted Chen Zhi, the mastermind behind the Prince Group, and seized approximately \$15 billion in Bitcoin—the largest forfeiture action in U.S. history.<sup>6</sup> The Justice Department’s indictment of Chen Zhi also revealed new evidence of the complicity of Chinese officials in scam centers. The Prince Group bribed

officials from China’s Ministry of Public Security and Ministry of State Security for protection and advanced notice of raids, and Chen Zhi and his associates often bragged that their connections with Chinese officials ensured their protection.<sup>7</sup>

- In November 2025, the Justice Department announced the creation of an interagency Scam Center Strike Force to combat scams perpetrated by Chinese criminal organizations in Southeast Asia.<sup>8</sup>

Although the United States has taken initial measures to tackle the scam center crisis, Chinese criminal syndicates are evolving their operations to stay ahead of crackdowns—first and foremost by accelerating their adoption of advanced technologies, including AI.

### Selective Crackdowns by China and Several Southeast Asian Countries Have Not Stopped the Growth of the Scam Crisis

China and several Southeast Asian governments have also launched crackdowns targeting scam centers, but their selective measures often serve political purposes and have not stemmed the growth of the region’s scam industry. The Cambodian government launched a highly publicized crackdown on scam centers in July 2025, but analysts cautioned that it was a choreographed “show crackdown” designed to stave off international pressure, not a serious attempt to disrupt the scam industry.<sup>9</sup> In December 2025, China’s Ministry of Public Security published a list of 100 high-level criminals wanted for scams “targeting Chinese citizens,” offering a reward of 200,000 renminbi (RMB) (\$28,400) for information leading to an arrest.<sup>10</sup> In January 2026, China secured the arrest and extradition to China of the U.S.-indicted scam center’s kingpin, Chen Zhi, from Cambodia.<sup>11</sup> However, Beijing continues to turn a blind eye to criminal activity targeting foreigners.<sup>12</sup>

## AI Is Turbocharging Scam Centers

Generative AI is revolutionizing the scam industry. Within weeks of the release of OpenAI’s ChatGPT in November 2022, cyber security analysts observed scammers using it to create more convincing personas for online romance scams.<sup>13</sup> While most popular generative AI tools are designed to refuse requests to facilitate illegal activity, studies have found that it is relatively easy for criminals to evade these guardrails—often simply by telling the prompt that they are conducting research or writing a novel about scam operations.<sup>14</sup> According to Ken Westbrook, a former CIA officer and founder of the nonprofit Stop Scams Alliance, criminal groups are reinvesting their profits “to fund a huge development of artificial intelligence.”<sup>15</sup> A 2025 Reuters report based on interviews with people who had worked in scam compounds in Burma found that ChatGPT is “the most-used AI tool to help scammers do their thing.”<sup>16</sup> OpenAI has publicly documented instances in which it disrupted scam centers that were using ChatGPT, including one case in which Chinese-language actors operating out of Cambodia had used ChatGPT to generate and disseminate tailored content in multiple languages for romance scams, fraudulent job offers, and fake investment firms.<sup>17</sup>

### Scammers Use AI to Scale Their Operations

Generative AI tools enable scammers to scale their operations. First, scammers use large language models (LLMs)

and AI image generation software to create convincing social media profiles that evade traditional detection techniques such as reverse image searches. The scammers then use these fake profiles to churn out enormous quantities of AI-generated initial contact messages.<sup>18</sup> After establishing contact with potential victims, generative AI tools enable individual scammers to engage with larger pools of victims simultaneously. According to the UN Office on Drugs and Crime, the adoption of generative AI is “significantly amplifying the scale” of scam operations—enabling a single scammer to defraud people on a scale that previously would have required an entire team.<sup>19</sup> AI tools have also contributed to the growing scale of online scams by lowering the technical barriers to entry for would-be cybercriminals, facilitating what some have termed the “democratization” of cybercrime.<sup>20</sup> For example, AI coding tools enable mid-level developers to create “scamming kits” that make SMS phishing campaigns “easy, extremely effective, scalable, and affordable for cybercriminals.”<sup>21</sup>

The scam industry’s embrace of AI has not reduced the vast scale of human trafficking into Southeast Asia’s scam centers. At least thus far, scam centers primarily use AI to enhance the efficacy of human scammers rather than to replace them altogether.<sup>22</sup> In fact, the crime syndicates behind scam centers are using AI tools to expand their human trafficking operations, both by using AI models to scrape social media platforms in search of vulnerable individuals and to generate more realistic fake job advertisements to lure victims into scam centers.<sup>23</sup>

### AI-Enhanced Scams Are Increasingly Difficult to Recognize

AI-powered technologies also enable scammers to increase the believability of their scams, making it difficult for even highly discerning potential victims to distinguish fraud from reality. The Federal Bureau of Investigation has warned that criminals are using “vocal cloning” technologies and AI-generated imagery to engage in real-time conversations and video chats with victims in which they impersonate loved ones or company executives.<sup>24</sup> Scam centers in Southeast Asia are investing in these technologies. One Chinese-language advertisement posted on an encrypted messaging service claimed to have installed “face-swapping” software at more than 1,000 compounds and promised 24/7 support and “door-to-door delivery” throughout Cambodia.<sup>25</sup>

AI tools have also made it possible for scammers to target victims more effectively across linguistic and cultural barriers. For instance, a man from Kenya who had been trafficked into the notorious KK Park scam compound in Burma reported that he impersonated cattle ranchers in Texas and soybean producers in Alabama by using ChatGPT to generate idiomatic local expressions and credible responses to detailed questions.<sup>26</sup>

## Cryptocurrency Fuels the Global Scam Industry

The explosive growth of online scams into a massive global criminal industry has also been facilitated by crime syndicates’ exploitation of cryptocurrency. FTC data indicates that in a recent calendar quarter, about one third of all cash lost by Americans to scammers involved cryptocurrency transfers.<sup>27</sup> Like other transnational criminal organizations, scam centers exploit cryptocurrency as an effective tool for international money laundering that makes it difficult to detect and trace their illicit activities. In one common approach, scammers contact victims under false pretenses—such as claiming to be a bank representative or government official—and instruct them to withdraw cash and deposit it into a Bitcoin or cryptocurrency ATM to avoid financial penalties or legal troubles, a tactic that sends funds directly to the scammer’s digital wallet with no way for banks to reverse the transaction.<sup>28</sup> This method disproportionately affects older adults, who often do not distinguish crypto ATMs from traditional bank ATMs and are guided through the process by fraudsters taking advantage of the kiosks’ speed, anonymity, and lack of regulatory oversight.<sup>29</sup>

Another tactic that is becoming increasingly common is for scammers to exploit the lure of cryptocurrency as an exciting investment opportunity to ensnare victims.<sup>30</sup> The goal of many newer scams is to convince victims to “invest” in fake cryptocurrency platforms, which mimic the appearance of legitimate sites with professional design, customer service, and two-factor authentication.<sup>31</sup> Scammers often allow victims to withdraw “earnings” during the early stages of the scam to reassure them that the platform is legitimate and encourage further investment.<sup>32</sup>

After obtaining a victim’s funds, crime syndicates hire money laundering services that employ vast networks of “mules” to transfer stolen assets across many different crypto wallets until the funds are eventually returned to the original scam group “clean” and ready to be spent in the legitimate economy.<sup>33</sup> By transacting in cryptocurrency, scammers can move funds rapidly across borders, bypassing oversight from traditional financial intermediaries.<sup>34</sup> Although crypto transactions are permanently recorded on blockchains, criminals deploy services called “mixers” and “tumblers” that pool and redistribute crypto assets, enhancing anonymity and obscuring the origin of funds.<sup>35</sup> Moreover, since criminals can rapidly transfer crypto overseas, law enforcement investigations encounter significant challenges tracing transactions across multiple jurisdictions.<sup>36</sup> Chinese money laundering networks (CMLNs) are playing an increasingly large role in laundering the proceeds from scams and other criminal activities and now process approximately 20 percent of all illicit crypto funds.<sup>37</sup>

**Figure: Cryptocurrency and Online Scams**



Source: Visualization generated using an AI tool based on the text and citations of the preceding two paragraphs.

## Repatriated Scammers Set Up Shop in China

As discussed in the original [“Commission Spotlight” on scam centers](#), over the past several years, Beijing’s selective crackdowns on scam centers that target Chinese victims have caused Chinese criminal groups to conclude that they can make more money with less risk by targeting Americans instead.<sup>38</sup> These crackdowns are now driving an alarming new trend: Chinese criminals that have been arrested and repatriated from Southeast Asian scam centers are opening small-scale scam operations inside China itself that exclusively target foreigners.

China’s selective raids on scam centers in Southeast Asia have led to a wave of scam center “alumni” setting up shop in China.<sup>39</sup> In 2024, Chinese authorities prosecuted approximately 78,000 people for online fraud—a 54 percent increase over the previous year.<sup>40</sup> According to China’s Ministry of Public Security, more than 8,000 Chinese nationals were repatriated from scam centers in Southeast Asia in 2025.<sup>41</sup> While China has meted out harsh punishment to some of the kingpins behind scam centers, “ordinary participants” in online fraud typically receive comparatively short prison sentences ranging from a few months to a few years.<sup>42</sup> As a result, tens of thousands of people previously arrested for participating in online scams are being released back into Chinese society with little money, few skills apart from online scamming, and a criminal record that makes it nearly impossible to find legitimate employment.<sup>43</sup> Increasingly, these “alumni” of Southeast Asian scam centers are opening stealthy, small-scale scam operations out of apartments and office buildings in cities across China.<sup>44</sup>

### From “Pig Butchering” to “Foreigner Butchering”

To evade scrutiny, these small domestic scamming operations often exclusively target foreign victims—a new criminal trend that is referred to in Chinese as “foreigner butchering” (*sha yang pan*). As described by Chinese official

#### “Chinese Don’t Scam Chinese”

The phrase “Chinese don’t scam Chinese” is popular online slang in China—an expression used to mean “you can trust me on this one.”<sup>45</sup> Yet this cheeky phrase can be tied to the rise of foreigner butchering scams at first in Southeast Asia and more recently inside China itself.<sup>46</sup> In March 2021, China’s Ministry of Public Security released a video—which went viral on Chinese social media—depicting dozens of young Chinese men who had been arrested for online fraud in Burma chanting in unison: “We conducted scams in northern Burma. Now we have returned to the motherland’s embrace... We are Chinese. Chinese don’t scam Chinese.”<sup>47</sup> A few months later, China’s Supreme People’s Court issued an opinion stating that “engaging in telecom and online fraud from outside the country targeting residents inside the country” violated China’s Criminal Law—language that appeared to exclude situations in which the fraud victims were located outside of China.<sup>48</sup> For Chinese criminal organizations, the message was clear: They could continue constructing massive scam compounds dedicated to industrial-scale fraud—as long as their targets were foreigners, not Chinese. Almost immediately, Chinese scam groups in Southeast Asia began to pivot from targeting Chinese people to targeting foreigners, and some organizations adopted the phrase “Chinese don’t scam Chinese” as a motto.<sup>49</sup>

media, foreigner butchering is a “mutation of pig butchering”<sup>50</sup> and a “new form of telecommunications and online fraud in which criminals make foreigners their targets, use translation software and messaging apps to feign romance with foreign men, and then swindle the victim’s money after gaining their trust.”<sup>50</sup>

Despite recent changes to Chinese law explicitly criminalizing scams targeting foreigners, in practice the Chinese perpetrators of foreign butchering scams rarely face consequences. In July 2024, China’s Supreme People’s Court issued an opinion clarifying that online fraud targeting victims outside of China also violated the Criminal Law.<sup>51</sup> In practice, however, enforcement remains extremely difficult. Foreign victims almost never report these crimes to Chinese authorities, leaving prosecutors with little hard evidence.<sup>52</sup> As a result, high-level bosses are rarely caught, and low-level scammers arrested in raids often receive little if any punishment.<sup>53</sup> While there have been at least 40 legal cases involving foreigner butchering operations inside of China in recent years, these likely represent only a small fraction of the scale of the problem—Chinese criminals recognize that they remain far less likely to face legal consequences if they target victims overseas.<sup>54</sup> Foreigner butchering is apparently so widespread that Chinese authorities and Chinese Communist Party (CCP) media have launched publicity campaigns to remind people that “scamming foreigners is also a crime.”<sup>55</sup>

Emulating the strategy of scam centers operated by Chinese crime syndicates in Southeast Asia, the criminals running new foreigner butchering operations inside China also cloak their scams in patriotic rhetoric.<sup>56</sup> According to a Chinese lawyer who has worked with numerous people accused of participating in scams targeting foreigners, many believe that “defrauding foreigners out of money is not illegal” and even that “this is patriotic behavior.”<sup>57</sup> In one revealing case, Chinese police arrested four men who were running a scamming operation out of an apartment in Jiangxi Province that specifically targeted Japanese men.<sup>58</sup> Upon being apprehended, the men proudly stated that they only targeted Japanese victims because “Chinese don’t scam Chinese.”<sup>59</sup> When the case became public, the perpetrators received an outpouring of support on Chinese social media, with some netizens calling them “anti-Japanese heroes” and others saying that they should be granted leniency because they acted patriotically.<sup>60</sup>

## The Globalization of Scam Centers

As a hedging strategy against crackdowns in Southeast Asia, Chinese criminal organizations have also begun expanding their scam operations around the world, targeting countries with high rates of corruption and limited government capacity.<sup>61</sup> Interpol has tracked the expansion of scam centers from the “original hub” of Southeast Asia to the Middle East, Central America, and West Africa, noting that West Africa in particular “could be developing into a new regional hub.”<sup>62</sup> The UN Office on Drugs and Crimes has likewise reported on the “spillover” of scam networks into South Asia and select Pacific Island countries.<sup>63</sup> As of March 2025, approximately 26 percent of victims trafficked into scam centers were sent to compounds outside of Southeast Asia.<sup>64</sup>

As scam centers spread across Southeast Asia during the pandemic, Chinese officials initially looked the other way as Chinese crime syndicates expanded throughout the region.<sup>65</sup> After scam centers operated by these criminal groups had taken root, Beijing exploited the problem by pressuring regional countries to allow Chinese security forces to lead crackdowns inside their territories—a key part of China’s larger strategy of using internal security cooperation to increase its leverage over Southeast Asian governments.<sup>66</sup> Although framed as assistance to combat

\* Originating in Chinese criminal slang, the term “pig butchering” (*sha zhu pan*) refers to scams in which the scammers build personal relationships with victims over weeks or months (“fattening the pig”) before stealing their money by convincing them to invest in fraudulent financial schemes (“slaughtering the pig”). U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia*, July 18, 2025. <https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia>.

scams and transnational crime, these arrangements often involve China providing equipment, training, and surveillance technologies that strengthen authoritarian control by host governments, deepen their dependence on Chinese security services, and reduce their willingness to cooperate with the United States.<sup>67</sup> Beijing is now deploying this same playbook in regions such as the Pacific Islands and Africa.<sup>68</sup>

### **Beijing Is Using Organized Crime to Infiltrate the Pacific Island Country of Palau**

In the Pacific Islands, U.S. officials have assessed that Beijing is using organized crime to infiltrate Palau, a country that recognizes Taiwan diplomatically and hosts important U.S. military facilities.<sup>69</sup> In 2019, Broken Tooth—a notorious criminal kingpin behind scam centers in Southeast Asia with close ties to the CCP—visited Palau and met with government leaders with the stated aim of leasing land for a casino.<sup>70</sup> While Palau’s government halted the project after learning about Broken Tooth’s criminal background, Chinese criminal networks have nevertheless managed to establish numerous scam centers in the country.<sup>71</sup> An April 2025 Reuters investigation found that hundreds of foreign nationals have entered Palau via China and Southeast Asia to work in scam centers, which have “continued to thrive” in the country despite its attempts to crack down.<sup>72</sup>

### **Beijing Exploits Scam Centers to Expand Its Security Influence in Africa**

Since early 2024, scam centers linked to Chinese nationals have been uncovered in the African countries of Angola, Namibia, and Zambia.<sup>73</sup> In all three countries, Beijing has used the growing problem of scam centers to press for greater security access. In June 2024, China’s Embassy in Angola announced that it would cooperate with Angolan authorities to combat online scams by “increasing police cooperation,” “deepening joint law enforcement,” and “coordinating crackdowns.”<sup>74</sup> That same month, Namibian officials traveled to China to participate in an anti-transnational crime working group meeting to discuss strengthening law enforcement cooperation and joint crackdowns on scams.<sup>75</sup> More recently, in October 2025, Chinese Embassy officials met with Zambia’s Inspector-General of Police Graphel Musamba to discuss efforts to strengthen security cooperation to combat transnational crime.<sup>76</sup> The following month, China’s Prime Minister Li Qiang traveled to Zambia and expressed China’s willingness to strengthen “judicial, police, and law enforcement cooperation” with the country.<sup>77</sup>

### **China-Linked Scam Centers in Nigeria**

Over the past year, Nigeria has become a hotspot for Chinese criminal networks diversifying their operations out of Southeast Asia. In December 2024, Nigerian officials arrested 148 Chinese nationals in a raid on a seven-story scam compound in Lagos.<sup>78</sup> According to the officials, these Chinese criminals had recruited and trained hundreds of local Nigerians to conduct pig butchering scams targeting victims in North America and Europe.<sup>79</sup> In a January 2025 raid on a scam compound in the capital of Abuja, Nigeria arrested four Chinese nationals who had allegedly recruited and trained 101 Nigerians to conduct scams targeting the UK.<sup>80</sup>

The Chinese government is exploiting the spread of scam centers to press for greater security influence in Nigeria. In March 2025, China’s Ambassador to Nigeria Yu Dunhai met with Nigerian police and offered to send a Chinese working group to the country to assist with “evidence collection” and “fraud tracing.”<sup>81</sup> In July 2025, the Chinese Embassy further proposed “joint operations” targeting scams and other transnational crimes.<sup>82</sup> Most recently, in September 2025, Nigeria’s Inspector-General of Police visited China to discuss greater security cooperation and intelligence sharing with officials from China’s Ministry of Public Security.<sup>83</sup> Nevertheless, Nigerian analysts have expressed concern that such security arrangements could grant China “undue influence” in the country.<sup>84</sup>

## Considerations for Congress

- The Commission's [2025 Annual Report](#) included a [recommendation](#) that Congress direct the President to create an interagency task force on scam centers. While the Administration recently created a Scam Center Strike Force, codifying a task force into law will ensure that it is permanent, accountable to Congress, and focused on the national security risks posed by China's involvement in the scam crisis.
- The Commission's 2025 [recommendation](#) called for greater cooperation between the U.S. government and U.S. technology companies to detect and stop scams. Reports indicate that scam-linked ads may be driving significant revenue to some technology intermediaries, indicating a need for more extensive cooperation in this space.<sup>85</sup>
- The Commission's 2025 [recommendation](#) on scam centers called for creation of a national public awareness campaign and for enhancing law enforcement training on scams. There continues to be a significant victim reporting gap. State and local law enforcement agencies are often the first point of contact when Americans fall victim to scam centers, but most departments lack the training and resources to identify these cases as part of transnational criminal operations linked to China. Too often, cases are filed as isolated fraud incidents and never reach the federal investigators who could connect them to broader scam center networks. Congress should consider directing the Scam Center Strike Force to establish information-sharing mechanisms and training programs—particularly for departments serving communities with large elderly populations—that enable state and local agencies to identify, document, and refer scam center-linked cases to federal authorities.
- As the United States seeks to ensure it is the global leader in AI and cryptocurrency, the U.S. government has both an economic and moral imperative to stop criminal organizations from weaponizing these technologies to steal from Americans. Congress should consider ways to strengthen protections built into AI tools to prevent their use for scams.
- The Commission's 2025 [recommendation](#) called for greater cooperation between the U.S. government and financial intermediaries to detect and stop scams, particularly relating to cryptocurrency. Given their increasing use by criminal organizations to move large sums of money rapidly outside of the United States, Congress should also consider whether existing regulation of cryptocurrency ATMs is sufficient and should encourage states to strengthen oversight of cryptocurrency ATM operators, which are often subject to minimal state-level licensing requirements.
- The U.S. government's seizure of approximately \$15 billion in Bitcoin from the Prince Group demonstrates that scam center proceeds can be identified and recovered through blockchain analysis. Congress should consider establishing a reward program that incentivizes cryptocurrency tracing firms and other private sector actors to identify and report stolen assets linked to scam center operations, modeled on existing whistleblower frameworks at the Securities and Exchange Commission and the Internal Revenue Service.
- Scam centers rely on spoofed phone calls, SMS phishing campaigns, and social media platforms to make initial contact with potential victims. Congress should consider requiring telecommunications carriers and social media platforms to implement stronger verification and detection measures targeting scam center-linked activity. Existing anti-spoofing frameworks such as STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using toKENS)—which require carriers to verify that caller ID information is legitimate before a call reaches the recipient—have helped combat domestic caller ID spoofing but were not

designed to address the international calls, text messages, and social media outreach that scam centers predominantly use to target Americans. Congress should consider expanding the scope of these frameworks to close these gaps.

- Given the scale of the scam center problem, the U.S. anti-money laundering regime may be ill-equipped for the challenge of stopping transnational crime syndicates from exploiting cryptocurrency to launder the billions of dollars they steal from Americans each year. Congress should consider if U.S. anti-money laundering policies should be updated in light of the growth of scam centers and consider ways to expand cooperation with allies and partners to coordinate enforcement across borders.
- When scam center assets are successfully recovered, Congress should consider directing that the proceeds be prioritized for victim restitution rather than flowing into the general Assets Forfeiture Fund. These are stolen savings, disproportionately taken from elderly Americans, and victims should be first in line when assets are recovered.
- Chinese criminal networks have responded to crackdowns in Southeast Asia by globalizing their operations. In order to stop new clusters of scam centers from emerging in other regions, the United States should act proactively to make disrupting the development of scam centers beyond Southeast Asia a priority for U.S. diplomacy, intelligence gathering, security cooperation, and foreign assistance.
- Scam centers run by Chinese criminal organizations threaten the wellbeing of Americans and the security of the United States. The U.S. government should treat the scam crisis, alongside the fentanyl epidemic, as a priority issue in bilateral negotiations with Beijing and the governments of countries where scam centers operate.

---

*The Commission extends special thanks to Jack Neubauer, former Senior Policy Analyst on the Security and Foreign Affairs team, for significant contributions to this report.*

# Endnotes

- <sup>1</sup> Georgia McCarthur, "Hillsborough Woman Conned Out of \$15K after AI Clones Daughter's Voice," *WFLA News Channel 8*, July 17, 2025. <https://www.wfla.com/news/hillsborough-county/hillsborough-woman-duped-out-of-15k-after-ai-clones-daughters-voice/>.
- <sup>2</sup> Jeffrey M. Allen, "The Rise of the AI-Cloned Voice Scam," *American Bar Association*, September 10, 2025. [https://www.americanbar.org/groups/senior\\_lawyers/resources/voice-of-experience/2025-september/ai-cloned-voice-scam/](https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-september/ai-cloned-voice-scam/).
- <sup>3</sup> U.S. Attorney's Office for the District of Columbia, *USA Pirro and LEO Announces Scam Center Strike Force to Go After Crypto Investment Fraudsters*, November 12, 2025. <https://www.youtube.com/live/Ke6CxXQ7QrQ>.
- <sup>4</sup> U.S. Department of the Treasury, *Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams*, September 8, 2025. <https://home.treasury.gov/news/press-releases/sb0237>.
- <sup>5</sup> U.S. Department of the Treasury, *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia*, October 14, 2025. <https://home.treasury.gov/news/press-releases/sb0278>; United Kingdom's Foreign, Commonwealth & Development Office et al., *UK and US Take Joint Action to Disrupt Major Online Fraud Network*, October 14, 2025. <https://www.gov.uk/government/news/uk-and-us-take-joint-action-to-disrupt-major-online-fraud-network>.
- <sup>6</sup> U.S. Department of Justice, *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes*, October 14, 2025. <https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged>.
- <sup>7</sup> *United States of America v. Approximately 127,271 Bitcoin ("BTC") Previously Stored at the Virtual Currency Addresses Listed in Attachment A, and All Proceeds Traceable Thereto*, No. 1:25-cv-05745 (E.D.N.Y., October 14, 2025). <https://www.justice.gov/usao-edny/media/1416266/dl>.
- <sup>8</sup> U.S. Attorney's Office for the District of Columbia, *New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans*, November 12, 2025. <https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting>.
- <sup>9</sup> Jacob Sims, "Reform Theater: Don't Be Taken In by Cambodia's Cybercrime Crackdown Promises," *Diplomat*, July 17, 2025. <https://thediplomat.com/2025/07/reform-theater-dont-be-taken-in-by-cambodias-cybercrime-crackdown-promises/>.
- <sup>10</sup> Hao Ping and Liang Qiuping, "公安机关公开通缉100名电信网络诈骗犯罪在逃金主和骨干人员" [Ministry of Public Security Releases Wanted List of 100 Fugitive Financial Backers and Key Players in Telecommunications and Online Fraud], *People's Daily Online*, December 9, 2025. <https://web.archive.org/web/20251219212657/https://society.people.com.cn/n1/2025/1209/c1008-40620582.html>.
- <sup>11</sup> Helen Regan, "Alleged Cybercrime Kingpin Arrested and Extradited from Cambodia to China," *CNN*, January 8, 2026. <https://edition.cnn.com/2026/01/07/asia/chen-zhi-arrest-extradition-cambodia-china-intl-hnk>.
- <sup>12</sup> Jeff Horwitz and Engen Tham, "Meta Tolerates Rampant Ad Fraud from China to Safeguard Billions in Revenue," *Reuters*, December 15, 2025. <https://www.reuters.com/investigations/meta-tolerates-rampant-ad-fraud-china-safeguard-billions-revenue-2025-12-15/>.
- <sup>13</sup> Thomas Brewster, "Armed with ChatGPT, Cybercriminals Build Malware and Plot Fake Girl Bots," *Forbes*, January 6, 2023. <https://www.forbes.com/sites/thomasbrewster/2023/01/06/chatgpt-cybercriminal-malware-female-chatbots/>.
- <sup>14</sup> Steve Stecklow and Poppy McPherson, "We Set Out to Craft the Perfect Phishing Scam. Major AI Chatbots Were Happy to Help," *Reuters*, September 15, 2025. <https://www.reuters.com/investigates/special-report/ai-chatbots-cyber/>.
- <sup>15</sup> Phelim Kine, Giselle Ruhyyih Ewing, and Daniella Cheslow, "US Hits China Scamwall," *Politico National Security Daily*, November 21, 2025. <https://www.politico.com/newsletters/national-security-daily/2025/11/21/us-hits-china-scamwall-00665347>.
- <sup>16</sup> Poppy McPherson, "ChatGPT Was Used 'To Help Scammers Do Their Thing' in Asia Fraud Scheme," *Reuters*, September 15, 2025. <https://www.reuters.com/investigations/chatgpt-was-used-help-scammers-do-their-thing-asia-fraud-scheme-2025-09-15/>.
- <sup>17</sup> "Disrupting Malicious Uses of AI: An Update," *OpenAI*, October 2025, 18–22. <https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf>; "Disrupting Malicious Uses of AI: June 2025," *OpenAI*, June 2025, 41–45. <https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf>; "Disrupting Malicious Uses of Our Models: An Update, February 2025," *OpenAI*, February 2025, 18–22. <https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf>.
- <sup>18</sup> Simon Moseley, "Automating Deception: AI's Evolving Role in Romance Fraud," *Centre for Emerging Technology and Security*, 21–23. [https://cetas.turing.ac.uk/sites/default/files/2025-04/cetas\\_briefing\\_paper\\_-\\_automating\\_deception\\_2.pdf](https://cetas.turing.ac.uk/sites/default/files/2025-04/cetas_briefing_paper_-_automating_deception_2.pdf).
- <sup>19</sup> United Nations Office on Drugs and Crime, *Emerging Threats: The Intersection of Criminal and Technological Innovation in the Use of Automation and Artificial Intelligence in the Cybercrime Landscape of Southeast Asia*, September 2025, 13. [https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC\\_Report\\_Emerging\\_threats\\_-\\_The\\_intersection\\_of\\_criminal\\_and\\_technological\\_innovation\\_in\\_the\\_use\\_of\\_automation\\_and\\_AI.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf).
- <sup>20</sup> "Scammers, Spies, and Triads: Inside Cyber-Crime's \$15tn Global Empire," *Financial Times*, December 18, 2025. <https://www.ft.com/content/bdc7797a-90a0-4e86-91a6-9505d10f1712>.
- <sup>21</sup> "Scammers, Spies, and Triads: Inside Cyber-Crime's \$15tn Global Empire," *Financial Times*, December 18, 2025. <https://www.ft.com/content/bdc7797a-90a0-4e86-91a6-9505d10f1712>; "Smishing on a Massive Scale: 'Panda Shop' Chinese Carding Syndicate," *Resecurity*, May 5, 2025.
- <sup>22</sup> United Nations Office on Drugs and Crime, *Emerging Threats: The Intersection of Criminal and Technological Innovation in the Use of Automation and Artificial Intelligence in the Cybercrime Landscape of Southeast Asia*, September 2025, 13.

[https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC\\_Report\\_Emerging\\_threats\\_-\\_The\\_intersection\\_of\\_criminal\\_and\\_technological\\_innovation\\_in\\_the\\_use\\_of\\_automation\\_and\\_AI.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf).

<sup>23</sup> United Nations Office on Drugs and Crime, *Emerging Threats: The Intersection of Criminal and Technological Innovation in the Use of Automation and Artificial Intelligence in the Cybercrime Landscape of Southeast Asia*, September 2025, 16. [https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC\\_Report\\_Emerging\\_threats\\_-\\_The\\_intersection\\_of\\_criminal\\_and\\_technological\\_innovation\\_in\\_the\\_use\\_of\\_automation\\_and\\_AI.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf); Organisation for Security and Co-operation in Europe, *New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons*, November 2024, 18–19. <https://www.osce.org/files/f/documents/7/d/579715.pdf>.

<sup>24</sup> U.S. Federal Bureau of Investigation, *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, December 3, 2024. <https://www.ic3.gov/PSA/2024/PSA241203>.

<sup>25</sup> Will Jackson, “How South-East Asia’s Pig Butchering Scammers are Using Artificial Intelligence Technology,” *Australian Broadcasting Corporation*, May 15, 2024. <https://www.abc.net.au/news/2024-05-16/pig-butcher-scams-artificial-intelligence-ai-face-swapping-/103804830>.

<sup>26</sup> Poppy McPherson, “ChatGPT Was Used ‘to Help Scammers Do Their Thing’ in Asia Fraud Scheme,” *Reuters*, September 15, 2025. <https://www.reuters.com/investigations/chatgpt-was-used-help-scammers-do-their-thing-asia-fraud-scheme-2025-09-15/>.

<sup>27</sup> Jack Caporal, “Crypto and Investment Scam Statistics for 2026: Investment scams are costing consumers millions, and cryptocurrency is a top payment method,” *The Motley Fool*, January 12, 2026. <https://www.fool.com/research/crypto-investment-scams/>.

<sup>28</sup> U.S. Federal Trade Commission, *Scammers Use Bitcoin ATMs to Steal Your Money*, September 3, 2024. <https://consumer.ftc.gov/consumer-alerts/2024/09/scammers-use-bitcoin-atms-steal-your-money>.

<sup>29</sup> U.S. Department of the Treasury, Financial Crimes Enforcement Network, *FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity*, August 4, 2025, 3–4. <https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf>; U.S. Federal Trade Commission, *Scammers Use Bitcoin ATMs to Steal Your Money*, September 3, 2024. <https://consumer.ftc.gov/consumer-alerts/2024/09/scammers-use-bitcoin-atms-steal-your-money>.

<sup>30</sup> U.S. Federal Trade Commission, *What to Know about Cryptocurrency and Scams*, May 2022. <https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams>.

<sup>31</sup> U.S. Federal Bureau of Investigation, *Cryptocurrency Investment Fraud*, accessed January 15, 2026. <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud>.

<sup>32</sup> U.S. Federal Bureau of Investigation, *Cryptocurrency Investment Fraud*, accessed January 15, 2026. <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud>.

<sup>33</sup> Selam Gebrekidan and Joy Dong, “The Scammer’s Manual: How to Launder Money and Get Away with It,” *New York Times*, March 23, 2025. <https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html>.

<sup>34</sup> U.S. Federal Bureau of Investigation Internet Crime Complaint Center, *Cryptocurrency*, accessed January 15, 2026. <https://www.ic3.gov/CrimelInfo/Cryptocurrency>.

<sup>35</sup> Sanjeev Bhasker, Michael Grady, and Kevin Mosley, “Cryptocurrency: Anti-Money-Laundering Enforcement and Regulation,” *Criminal Justice Magazine*, July 15, 2023. [https://www.americanbar.org/groups/criminal\\_justice/resources/magazine/archive/cryptocurrency-anti-money-laundering-enforcement-regulation/](https://www.americanbar.org/groups/criminal_justice/resources/magazine/archive/cryptocurrency-anti-money-laundering-enforcement-regulation/).

<sup>36</sup> U.S. Federal Bureau of Investigation Internet Crime Complaint Center, *Cryptocurrency*, accessed January 15, 2026. <https://www.ic3.gov/CrimelInfo/Cryptocurrency>.

<sup>37</sup> Chainalysis, “Chinese Language Money Laundering Networks Emerge as Major Facilitators of the Illicit Crypto Economy, Now Driving 20% of Laundering Activity,” January 27, 2026. <https://www.chainalysis.com/blog/2026-crypto-money-laundering/>.

<sup>38</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia*, July 18, 2025. <https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia>.

<sup>39</sup> Jason Tower, “Exporting Fraud: China’s Acquiescence to Myanmar’s Military Regime Fuels ‘Foreigner Butchering’ Scam Epidemic,” *Global Initiative against Transnational Organized Crime*, October 10, 2025. <https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/>.

<sup>40</sup> China’s Supreme People’s Procuratorate, 最高检：2024年检察机关起诉电诈犯罪7.8万人·同比上升53.9% [Supreme People’s Procuratorate: In 2024 Prosecutor’s Offices Prosecuted 78,000 People for Online Fraud, Up 53.9%], March 8, 2025. [https://web.archive.org/web/20251116181050/https://www.spp.gov.cn/spp/2025zqjzbg/202503/t20250308\\_688215.shtml](https://web.archive.org/web/20251116181050/https://www.spp.gov.cn/spp/2025zqjzbg/202503/t20250308_688215.shtml).

<sup>41</sup> China’s Ministry of Public Security, 重拳出击通力协作中柬老缅泰越六国将联合打击跨国电信网络诈骗犯罪 [A Strong Attack with Coordinated Efforts: Six Countries of China, Cambodia, Laos, Myanmar, Thailand and Vietnam Unite to Crackdown on Transnational Telecommunications and Online Fraud], November 14, 2025. <https://web.archive.org/web/20251116214525/http://www.mps.gov.cn:9080/n2253534/n2253535/c10300471/content.html>.

<sup>42</sup> China’s Supreme People’s Procuratorate, 依法惩治跨境电信网络诈骗及其关联犯罪典型案例 [Model Cases for Punishing Cross-Border Telecommunications and Online Fraud and Related Crimes According to the Law], July 26, 2024. [https://web.archive.org/web/20251116154415/https://www.spp.gov.cn/xwfbh/wsfbh/202407/t20240726\\_661524.shtml](https://web.archive.org/web/20251116154415/https://www.spp.gov.cn/xwfbh/wsfbh/202407/t20240726_661524.shtml); China’s Supreme People’s Procuratorate, 最高检发布6起依法惩治妨害国（边）境管理犯罪典型案例 [Supreme People’s Procuratorate Issues 6 Model Cases for Punishing the Crime of Undermining the Administration of National Borders According to the Law], July 7, 2022. [https://web.archive.org/web/20250516091449/https://www.spp.gov.cn/xwfbh/wsfbt/202207/t20220707\\_562224.shtml#2](https://web.archive.org/web/20250516091449/https://www.spp.gov.cn/xwfbh/wsfbt/202207/t20220707_562224.shtml#2).

<sup>43</sup> Jason Tower, “Exporting Fraud: China’s Acquiescence to Myanmar’s Military Regime Fuels ‘Foreigner Butchering’ Scam Epidemic,” *Global Initiative against Transnational Organized Crime*, October 10, 2025. <https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/>.

- <sup>44</sup> Jason Tower, "Exporting Fraud: China's Acquiescence to Myanmar's Military Regime Fuels 'Foreigner Butchering' Scam Epidemic," *Global Initiative against Transnational Organized Crime*, October 10, 2025. <https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/>; Wangtu Qiulin, Huang Shiyun, and Zhang Yinglin, "隐匿的杀洋盘：‘领导说是帮外国用户保管虚拟币’ [Concealed Foreigner Butchering: 'Boss Said They Were Helping Foreigners Manage Virtual Currency']," *Southern Weekly*, June 13, 2025. <https://web.archive.org/web/20251107162830/https://www.infzm.com/wap/#/content/295555?source=131>.
- <sup>45</sup> "中国人不骗中国人，这是什么梗？" [What Is the Neologism 'Chinese Don't Scam Chinese?'], *Creader*, March 13, 2022. <https://web.archive.org/web/20251123022459/https://news.creaders.net/society/2022/03/13/2460629.html>.
- <sup>46</sup> "中国人不骗中国人，这是什么梗？" [What Is the Neologism 'Chinese Don't Scam Chinese?'], *Creader*, March 13, 2022. <https://web.archive.org/web/20251123022459/https://news.creaders.net/society/2022/03/13/2460629.html>.
- <sup>47</sup> "诈骗犯认错称‘中国人不骗中国人’网民批：没有一句真话" [Fraudsters Admit Wrongdoing, Saying "Chinese Don't Scam Chinese"—Netizens Comment: Not One Word of Truth], *Lianhe Zaobao*, March 7, 2021. <https://www.zaobao.com.sg/realtime/china/story20210307-1129405>.
- <sup>48</sup> China's Supreme People's Court, Supreme People's Protectorate, and Ministry of Public Security, 关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二） [Opinion on Some Questions Regarding the Appropriate Law for Handling Telecommunications and Online Fraud Criminal Cases (2)], June 17, 2021. [https://web.archive.org/web/20251107145119/https://www.gov.cn/zhengce/zhengceku/2021-06/22/content\\_5620164.htm](https://web.archive.org/web/20251107145119/https://www.gov.cn/zhengce/zhengceku/2021-06/22/content_5620164.htm).
- <sup>49</sup> Lezhi County Committee Political and Legal Affairs Commission, 中国人不骗中国人？乐至警方捣毁一专骗外国女性电诈团伙 [Chinese Don't Scam Chinese? Lezhi Police Demolish Telecom Fraud Group Specialized in Scamming Foreign Women], January 8, 2025. <https://web.archive.org/web/20251107154312/https://www.lz.ziyangpeace.gov.cn/pajs/20250108/2938956.html>; Hou Wenchang et al., "揭秘境外电信诈骗犯罪新动向" [Uncovering New Trends in Overseas Telecommunications Fraud Crimes], *Procuratorate Daily*, September 18, 2023. [https://web.archive.org/web/20251107150144/https://newspaper.jcrb.com/2023/20230918/20230918\\_004/20230918\\_004\\_1.htm](https://web.archive.org/web/20251107150144/https://newspaper.jcrb.com/2023/20230918/20230918_004/20230918_004_1.htm).
- <sup>50</sup> Zhao Hongqi, Wang Rui, and Zhang Shengli, "‘杀洋盘’电诈数额该如何认定？" [How to Determine the Amount in "Foreigner Butchering" Telecom Fraud], *Legal Daily*, April 26, 2024. [https://web.archive.org/web/20251107185252/http://www.legaldaily.com.cn/legal\\_case/content/2024-04/26/content\\_8989536.html](https://web.archive.org/web/20251107185252/http://www.legaldaily.com.cn/legal_case/content/2024-04/26/content_8989536.html).
- <sup>51</sup> China's Supreme People's Court, Supreme People's Protectorate, and Ministry of Public Security, 关于办理跨境电信网络诈骗等刑事案件适用法律若干问题的意见 [Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases Such as Cross-Border Telecommunications and Internet Fraud], July 26, 2024. [https://web.archive.org/web/20260211215349/https://www.spp.gov.cn/xwfbh/wsfbh/202407/t20240726\\_661523.shtml](https://web.archive.org/web/20260211215349/https://www.spp.gov.cn/xwfbh/wsfbh/202407/t20240726_661523.shtml); Chen Hongxiang and Wang Suzhi, "《关于办理跨境电信网络诈骗等刑事案件适用法律若干问题的意见》解读" [Interpreting Opinion on Some Questions Regarding the Appropriate Law for Handling Cross-Border Telecommunications and Online Fraud Criminal Cases], *People's Judicature*, no. 25 (2024): 27, 30.
- <sup>52</sup> Wangtu Qiulin, Huang Shiyun, and Zhang Yinglin, "隐匿的杀洋盘：‘领导说是帮外国用户保管虚拟币’ [Concealed Foreigner Butchering: 'Boss Said They Were Helping Foreigners Manage Virtual Currency']," *Southern Weekly*, June 13, 2025. <https://web.archive.org/web/20251010175550/https://www.nfnews.com/content/5385x1Le6B.html>.
- <sup>53</sup> Wangtu Qiulin, Huang Shiyun, and Zhang Yinglin, "隐匿的杀洋盘：‘领导说是帮外国用户保管虚拟币’ [Concealed Foreigner Butchering: 'Boss Said They Were Helping Foreigners Manage Virtual Currency']," *Southern Weekly*, June 13, 2025. <https://web.archive.org/web/20251107162830/https://www.infzm.com/wap/#/content/295555?source=131>.
- <sup>54</sup> Wangtu Qiulin, Huang Shiyun, and Zhang Yinglin, "隐匿的杀洋盘：‘领导说是帮外国用户保管虚拟币’ [Concealed Foreigner Butchering: 'Boss Said They Were Helping Foreigners Manage Virtual Currency']," *Southern Weekly*, June 13, 2025; Chen Hongxiang and Wang Suzhi, "《关于办理跨境电信网络诈骗等刑事案件适用法律若干问题的意见》解读" [Interpreting Opinion on Some Questions Regarding the Appropriate Law for Handling Cross-Border Telecommunications and Online Fraud Criminal Cases], *People's Judicature*, no. 25 (2024): 27, 30.
- <sup>55</sup> Jason Tower, "Exporting Fraud: China's Acquiescence to Myanmar's Military Regime Fuels 'Foreigner Butchering' Scam Epidemic," *Global Initiative against Transnational Organized Crime*, October 10, 2025. <https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/>; Legal Daily, "中国人骗外国人没事？‘杀洋盘’也是违法犯罪" [Chinese People Scamming Foreigners Is No Big Deal? "Foreigner Butchering" Is Also a Crime], *Global Times*, June 27, 2025. <https://web.archive.org/web/20251116173809/https://hqttime.huanqiu.com/article/4NGN2sysSec>.
- <sup>56</sup> Jason Tower, "Exporting Fraud: China's Acquiescence to Myanmar's Military Regime Fuels 'Foreigner Butchering' Scam Epidemic," *Global Initiative against Transnational Organized Crime*, October 10, 2025. <https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/>; Legal Daily, "中国人骗外国人没事？‘杀洋盘’也是违法犯罪" [Chinese People Scamming Foreigners Is No Big Deal? "Foreigner Butchering" Is Also a Crime], *Global Times*, June 27, 2025. <https://web.archive.org/web/20251116173809/https://hqttime.huanqiu.com/article/4NGN2sysSec>.
- <sup>57</sup> Wangtu Qiulin, Huang Shiyun, and Zhang Yinglin, "隐匿的杀洋盘：‘领导说是帮外国用户保管虚拟币’ [Concealed Foreigner Butchering: 'Boss Said They Were Helping Foreigners Manage Virtual Currency']," *Southern Weekly*, June 13, 2025. <https://web.archive.org/web/20251107162830/https://www.infzm.com/wap/#/content/295555?source=131>.
- <sup>58</sup> "抠脚大汉假扮‘援交女’诈骗日本人·被抓时霸气解释：不骗中国人" [Burly Men at Home Pretend to Be 'Sugar Babies' to Scam Japanese People, When Caught Proudly Declare That They Don't Scam Chinese], *NetEase*, July 26, 2022. <https://web.archive.org/web/20251116162718/https://www.163.com/dy/article/HD7EDGGH0550TA0M.html>; 四名男子伪装成“援交女”·称专骗日本男网友, [Four Men Posing as 'Escort Girls' Claim to Only Have Scammed Japanese Men], *Paper*, April 29, 2022. <https://archive.ph/9zw8L>.
- <sup>59</sup> "抠脚大汉假扮‘援交女’诈骗日本人·被抓时霸气解释：不骗中国人" [Burly Men at Home Pretend to Be 'Sugar Babies' to Scam Japanese People, When Caught Proudly Declare That They Don't Scam Chinese], *NetEase*, July 26, 2022. <https://web.archive.org/web/20251116162718/https://www.163.com/dy/article/HD7EDGGH0550TA0M.html>; 四名男子伪装成“援交女”·称专骗日本男网友, [Four Men Posing as 'Escort Girls' Claim to Only Have Scammed Japanese Men], *Paper*, April 29, 2022. <https://archive.ph/9zw8L>.

- <sup>60</sup> “抠脚大汉假扮‘援交女’ 诈骗日本人·被抓时霸气解释：不骗中国人” [Burly Men at Home Pretend to Be ‘Sugar Babies’ to Scam Japanese People, When Caught Proudly Declare That They Don’t Scam Chinese], *NetEase*, July 26, 2022. <https://web.archive.org/web/20251116162718/https://www.163.com/dy/article/HD7EDGGH0550TA0M.html>; 四名男子伪装成“援交女”·称诈骗日本男网友, [Four Men Posing as ‘Escort Girls’ Claim to Only Have Scammed Japanese Men], *Paper*, April 29, 2022. <https://archive.ph/9zw8L>.
- <sup>61</sup> United Nations Office on Drugs and Crime, *Cyberfraud in the Mekong Reaches Inflection Point*, UNODC Reveals, April 21, 2025. <https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html>.
- <sup>62</sup> “INTERPOL Releases New Information on Globalization of Scam Centres,” *Interpol*, June 30, 2025. <https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres>.
- <sup>63</sup> United Nations Office on Drugs and Crime, *Cyberfraud in the Mekong Reaches Inflection Point*, UNODC Reveals, April 21, 2025, 8–10. <https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html>.
- <sup>64</sup> “INTERPOL Releases New Information on Globalization of Scam Centres,” *Interpol*, June 30, 2025. <https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres>.
- <sup>65</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia*, July 18, 2025. <https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia>.
- <sup>66</sup> U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia*, July 18, 2025. <https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia>.
- <sup>67</sup> U.S.-China Economic and Security Review Commission, “Crossroads of Competition: China and Southeast Asia,” in *2025 Annual Report to Congress*, November 2025. [https://www.uscc.gov/sites/default/files/2025-11/2025\\_Annual\\_Report\\_to\\_Congress.pdf](https://www.uscc.gov/sites/default/files/2025-11/2025_Annual_Report_to_Congress.pdf).
- <sup>68</sup> Virginia Comolli, “Who Is Policing the Pacific?” *Global Initiative against Transnational Organized Crime*, November 21, 2025. <https://globalinitiative.net/analysis/who-is-policing-the-pacific/>; U.S.-China Economic and Security Review Commission, *China’s Exploitation of Scam Centers in Southeast Asia*, July 18, 2025. <https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia>; Paul Nantulya, “China’s Growing Police and Law Enforcement Cooperation in Africa,” *National Bureau of Asian Research*, June 1, 2022. <https://www.nbr.org/publication/chinas-growing-police-and-law-enforcement-cooperation-in-africa/>.
- <sup>69</sup> Pete McKenzie and Hollie Adams, “Inside the U.S. Battle with China over an Island Paradise Deep in the Pacific,” *Reuters*, April 30, 2025. <https://www.reuters.com/investigations/inside-us-battle-with-china-over-an-island-paradise-deep-pacific-2025-04-30/>.
- <sup>70</sup> Pete McKenzie and Hollie Adams, “Inside the U.S. Battle with China over an Island Paradise Deep in the Pacific,” *Reuters*, April 30, 2025. <https://www.reuters.com/investigations/inside-us-battle-with-china-over-an-island-paradise-deep-pacific-2025-04-30/>.
- <sup>71</sup> Pete McKenzie and Hollie Adams, “Inside the U.S. Battle with China over an Island Paradise Deep in the Pacific,” *Reuters*, April 30, 2025. <https://www.reuters.com/investigations/inside-us-battle-with-china-over-an-island-paradise-deep-pacific-2025-04-30/>.
- <sup>72</sup> Pete McKenzie and Hollie Adams, “Inside the U.S. Battle with China over an Island Paradise Deep in the Pacific,” *Reuters*, April 30, 2025. <https://www.reuters.com/investigations/inside-us-battle-with-china-over-an-island-paradise-deep-pacific-2025-04-30/>.
- <sup>73</sup> United Nations Office on Drugs and Crime, *Cyberfraud in the Mekong Reaches Inflection Point*, UNODC Reveals, April 21, 2025, 9–10. <https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html>.
- <sup>74</sup> China’s Embassy in Angola, 提醒：当心电信诈骗，远离网络赌博 [Reminder: Look Out for Telecommunications Fraud, Stay Away from Online Gambling], June 19, 2024. [https://web.archive.org/web/20251114183733/https://ao.china-embassy.gov.cn/chn/lsw\\_0/tsvj/202406/t20240619\\_11438566.htm](https://web.archive.org/web/20251114183733/https://ao.china-embassy.gov.cn/chn/lsw_0/tsvj/202406/t20240619_11438566.htm).
- <sup>75</sup> Tianjin Public Security Bureau, 国际刑警组织打击电信诈骗犯罪全球行动“曙光行动2024”线下总结会在津成功举办 [Concluding Meeting for INTERPOL’s “Operation First Light 2024” Global Action against Telecommunications Fraud Successfully Convened in Tianjin], June 27, 2024. [https://web.archive.org/web/20251114190944/https://ga.tj.gov.cn/sy/gabsyccs/gaywgh/202406/t20240628\\_6663213.html](https://web.archive.org/web/20251114190944/https://ga.tj.gov.cn/sy/gabsyccs/gaywgh/202406/t20240628_6663213.html).
- <sup>76</sup> Augustine Sichula, “China Reaffirms Commitment to Strengthening Security Cooperation with Zambia,” *Zambia Monitor*, November 1, 2025. <https://www.zambiamonitor.com/china-reaffirms-commitment-to-strengthening-security-cooperation-with-zambia/>.
- <sup>77</sup> China’s Ministry of Foreign Affairs, 李强同赞比亚总统希奇莱马会谈 [Li Qiang Meets with Zambia’s President Hakainde Hichilema], November 20, 2025. [https://web.archive.org/web/20251122160521/https://www.mfa.gov.cn/zyxw/202511/t20251120\\_11757152.shtml](https://web.archive.org/web/20251122160521/https://www.mfa.gov.cn/zyxw/202511/t20251120_11757152.shtml).
- <sup>78</sup> Nigeria’s Economic and Financial Crimes Commission, *EFCC Bursts Syndicate of 792 Cryptocurrency Investment, Romance Fraud Suspects in Lagos ... Arrests 193 Chinese, Arabs, Filipinos, Others*, December 17, 2024. <https://www.efcc.gov.ng/news/efcc-bursts-syndicate-of-792-cryptocurrency-investment-romance-fraud-suspects-in-lagos-arrests-193-chinese-arabs-filipinos-others>.
- <sup>79</sup> Nigeria’s Economic and Financial Crimes Commission, *EFCC Bursts Syndicate of 792 Cryptocurrency Investment, Romance Fraud Suspects in Lagos ... Arrests 193 Chinese, Arabs, Filipinos, Others*, December 17, 2024. <https://www.efcc.gov.ng/news/efcc-bursts-syndicate-of-792-cryptocurrency-investment-romance-fraud-suspects-in-lagos-arrests-193-chinese-arabs-filipinos-others>.
- <sup>80</sup> Nigeria’s Economic and Financial Crimes Commission, *EFCC Arrests 105 Suspected Internet Fraudsters in Abuja*, January 10, 2025. <https://www.efcc.gov.ng/news/efcc-arrests-four-chinese-101-others-for-suspected-internet-fraud-in-abuja>.
- <sup>81</sup> Nigeria’s Economic and Financial Crimes Commission, *Chinese Working Group to Collaborate with EFCC in Tackling Cybercrime*, March 4, 2025. <https://www.facebook.com/officialefcc/posts/chinese-working-group-to-collaborate-with-efcc-in-tackling-cybercrime-worried-by/113282604547264/>.
- <sup>82</sup> Bridget Chiedu Onochie, *Telecom, Online Fraud: China Warns Citizens against Illicit Activities*, *Guardian* (Nigeria), July 9, 2025. <https://guardian.ng/news/nigeria/national/telecom-online-fraud-china-warns-citizens-against-illicit-activities/>.
- <sup>83</sup> Abdulzeez Seyifunmi, “IGP Represents Nigeria in Global Security Talks in China,” *Guardian* (Nigeria), September 15, 2025. <https://guardian.ng/news/igp-represents-nigeria-in-global-security-talks-in-china/>.
- <sup>84</sup> Timothy Obiezu, “Nigeria, China, Crack Down on Chinese Nationals in Financial Crimes,” *Voice of America*, March 6, 2025. <https://www.voanews.com/a/nigeria-china-crack-down-on-chinese-nationals-in-financial-crimes/8001570.html>.

<sup>85</sup> Jeff Horwitz, "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show," *Reuters*, November 6, 2025. <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/>.