WRITTEN TESTIMONY

OF

Matthew Noyes
Cyber Policy & Strategy Director, Office of Investigations
United States Secret Service

BEFORE

Subcommittee on National Security, Illicit Finance, and International Financial Institutions
Committee on Financial Services
United State House of Representatives

ON

"Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry"

September 18, 2024
Washington, DC

Introduction

Good morning, Chairman Luetkemeyer, Ranking Member Beatty, and distinguished Members of this subcommittee. Thank you for the opportunity to appear before you today and discuss the ongoing efforts of the U.S. Secret Service (Secret Service), along with our partners, to counter the serious transnational criminal fraud schemes, including romance confidence scams.[1]

I serve as the Cyber Policy and Strategy Director for the U.S. Secret Service, Office of Investigations. I am responsible for leading the development of policy, strategy, planning, and budget for the Secret Service's global network of over 160 offices and 3,000 special agents and professional staff that execute the U.S. Secret Service's integrated mission of safeguarding the integrity of financial systems and protecting designated persons, locations, and events. This includes the operation of our 42 domestic Cyber Fraud Task Forces, located in our largest offices, and our National Computer Forensics Institute in Hoover, Alabama, which trains local law enforcement, prosecutors, and judges.

For more than 150 years, the Secret Service has conducted criminal investigations to protect the American public, financial institutions, private companies, and critical infrastructure from exploitation. Our investigative responsibilities encompass not only various forms of financial fraud,[2] but also computer and access device fraud.[3] In Fiscal Year 2023, Secret Service investigations resulted in over 1,300 arrests, $1.2 billion in cyber financial crime losses recovered, and over $464 million returned to victims of crime.

Transnational organized fraud schemes are a growing risk to Americans. Over the past 4 years, confidence scams involving digital assets have rapidly grown as a method used to defraud Americans. Since November 2022, the Secret Service has received over 8,000 complaints related to these schemes.[4] Often these reports appear to involve schemes commonly executed by scam camps operating in Southeast Asia in the Mekong region.[5]

The Threat Posed by Scam Camps

The threat posed by scam camps is significant and growing. The United States Institute of Peace (USIP) estimates revenue of over $43.8 billion a year for the criminal syndicates organizing these operations—a total that is nearly 40 percent of the estimated 2023 combined GDP of

---

[1] Various terms are used to describe these scams. For discussion on this, *See* Jack M. Whittaker, Suleman Lazarus, Taidgh Corcoran, "Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘)," Journal of Economic Criminology, Volume 3, 2024, 100052, ISSN 2949-7914. Accessed 28 August 2024 at: https://doi.org/10.1016/j.jeconc.2024.100052

[2] *See* subsection (b) of 18 U.S.C. § 3056 - Powers, authorities, and duties of United States Secret Service.

[3] *See* 18 U.S.C. § 1029, Fraud and related activity in connection with access devices, and 18 U.S.C. § 1030, Fraud and related activity in connection with computers.

[4] U.S. Secret Service, "Combatting the Illicit Use of Digital Assets." Accessed 2 September 2024: https://www.secretservice.gov/investigations/digitalassets

[5] Lindsey Kennedy and Nathan Paul Southern, "Inside Southeast Asia's casino Scam Archipelago," The Diplomat (2 August 2022). Accessed 5 September 2024 at: https://thediplomat.com/2022/08/inside-southeast-asias-casino-scam-archipelago/

Burma, Cambodia, and Laos.[6] Professor John Griffin and Kevin Mei at University of Texas Austin estimate that, between January 2020 and January 2024, at least $75.3 billion received in digital assets at digital asset exchange deposit addresses that are associated with scam camps in the Mekong region; this includes $15.2 billion sent from digital asset exchanges commonly used by Americans.[7] These criminal schemes are harming millions of people and continue to grow in impact to Americans. Substantial activity has been linked to transnational criminal organizations operating scam camps in Burma, Cambodia, and Laos.[8] Like most forms of illicit activity, estimating the total economic impact is difficult, as fraud victims may not realize they are victims or may not report the fraud to law enforcement. Further research and survey data is needed to better understand the scale of the problem.

The growth in fraud is not limited to scam camps operating in the Mekong region. The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) and the Federal Trade Commission's (FTC) Consumer Sentinel Network both report significant increases in financial losses from various types of fraud, including identity theft, online scams, and telemarketing fraud, that are not limited to activity in the Mekong region.[9] In 2023, U.S. law enforcement received reports of over $12.5 billion in losses due to a wide array of Internet scams.[10] This broader context underscores the urgent need for increased action to combat fraud. Fraud at the base level is an intentional act of deceit designed for profit or other gain. Increasingly these fraud schemes are operating transnationally and at scale, through use of information technology, to target a large number of victims. These fraudsters employ sophisticated social engineering techniques to deceive their victims. The scam camp operators force human trafficking victims to serve as accomplices in furthering these criminal schemes.

[6] USIP Senior Study Group, "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security." USIP, Washington DC (May 2024). ISBN: 978-1-60127-940-8. Accessed 2 September 2024 at: https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

[7] Griffin, John M. and Mei, Kevin, "How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering" (February 29, 2024). Accessed 5 September 2024 at: https://www.jgriffin.info/papers

[8] United Nations Office on Drugs and Crime, "Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat." (January 2024). Accessed 2 September 2024 at: https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html

[9] Federal Trade Commission, "Consumer Sentinel Network Data Book 2023." Washington DC (February 2024). Accessed 2 September 2024 at: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023

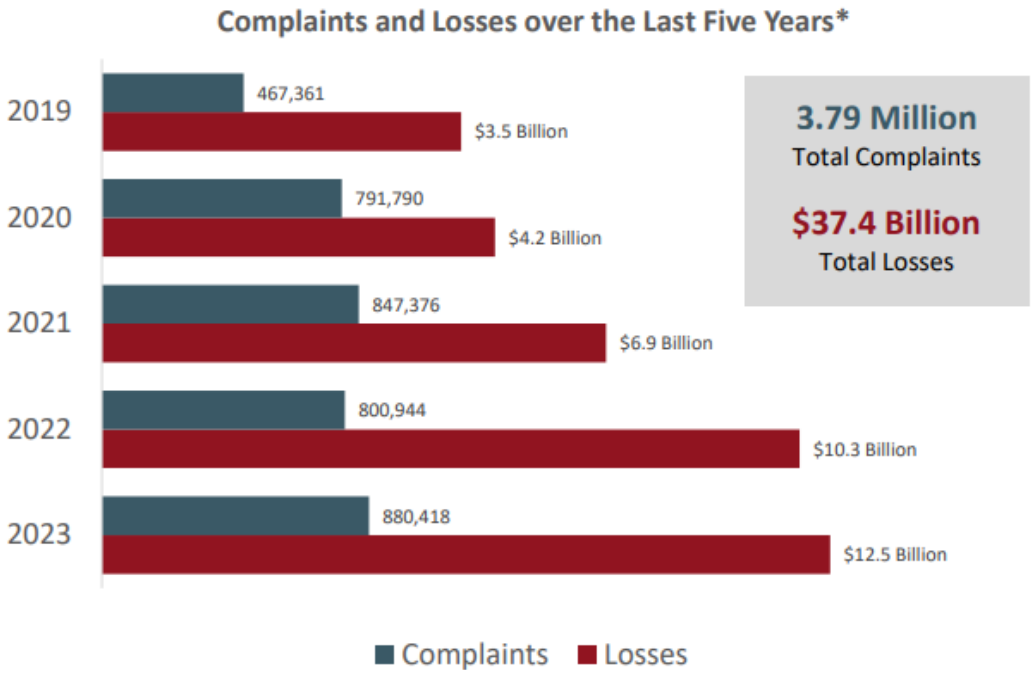

Figure 1: Yearly and aggregate data for complains and losses reported to IC3 over the years 2019 to 2023. (2023 IC3 Report, page 7)

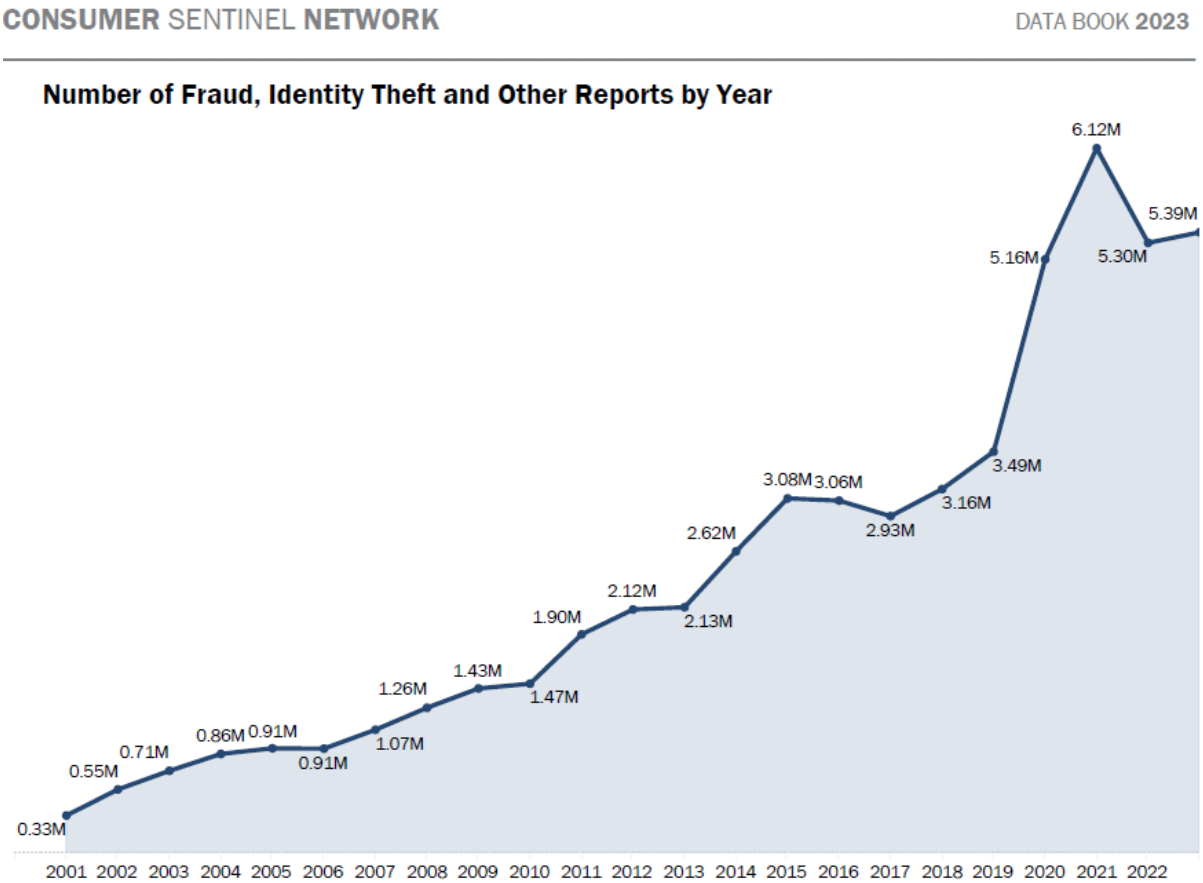

Figure 2: Number of Fraud, Identity Theft, and Other Reports by Year 2001-2023. (2023 Federal Trade Commission Consumer Sentinel Data Book, page 6)

The Typical Scam Camp Fraud Scheme

Scam camps operate multiple criminal schemes, targeting a range of demographics across multiple countries. Americans are frequently victimized by confidence scams that start with an unsolicited seemingly errant message sent through short messaging service (SMS), social media, professional networking website, dating application, or other electronic messaging services. After this initial contact, the scammers typically invite the victim to engage further on a different platform, where the scam operators entice their victims to make a series of financial transactions.

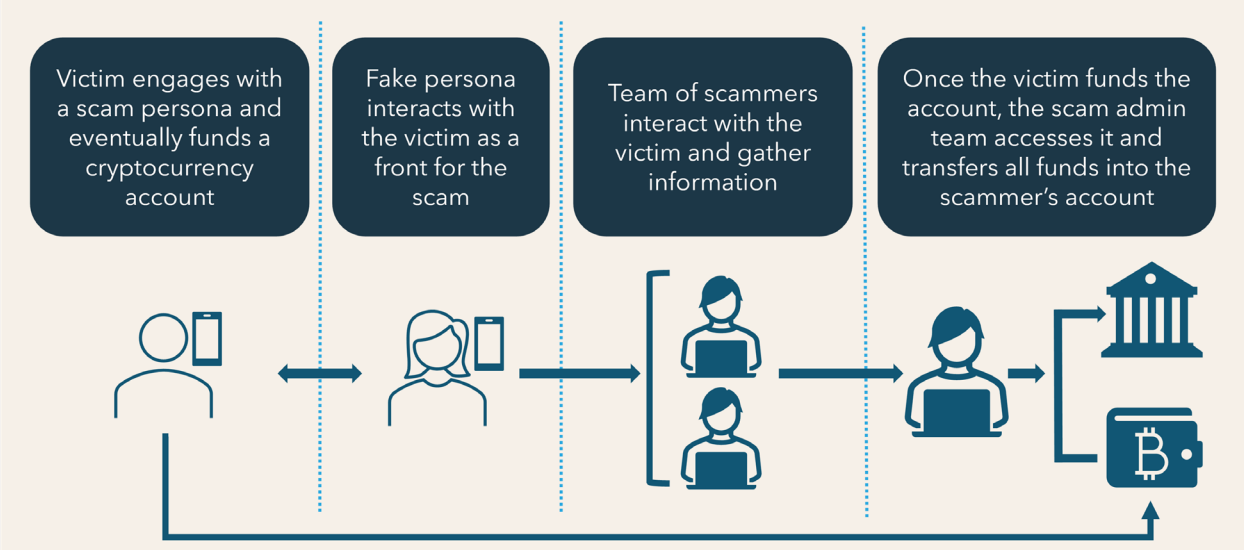

Figure 3: Summary of Scam Flow from Datos Insights.[11]

A Secret Service special agent recently received and engaged with an individual believed to be a scam operator; parts of these exchange are included in this testimony to illustrate how these schemes are often executed. For example, an initial exchange often begins:

[11] Mortensen, Jim "Slaughtering the Pig Butchers." Datos Insights (8 November 2023). Accessed 2 September 2024 at: https://datos-insights.com/blog/jim-mortensen/slaughtering-the-pig-butchers/

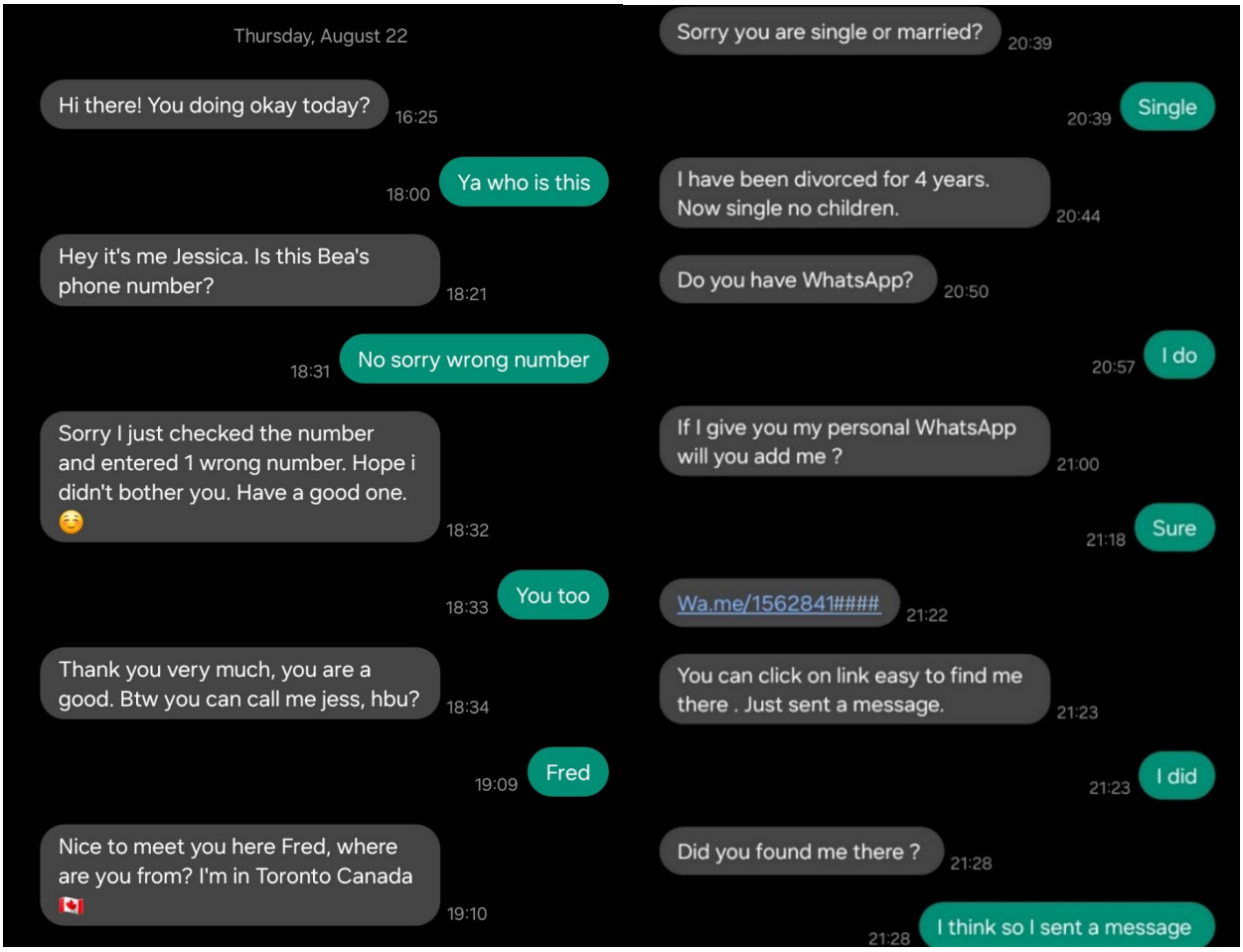

Figure 4: Example initial SMS exchange. This and subsequent 3 figures are from a conversation with a Secret Service special agent (August 2024).

In the operation of these scam camps, once engagement is transferred to the scam camps preferred Internet messaging platform, further engagement usually transfers from the team responsible for initial contact, to a different specialized team. Scam camps tend to use platforms that allow for multiple people to engage in the conversation at low cost and which the organizer assesses are susceptible to continued fraud schemes (e.g., Internet electronic messaging platforms with limited ability to detect illicit activity due to use of end-to-end encryption). For example, this transition may begin with:

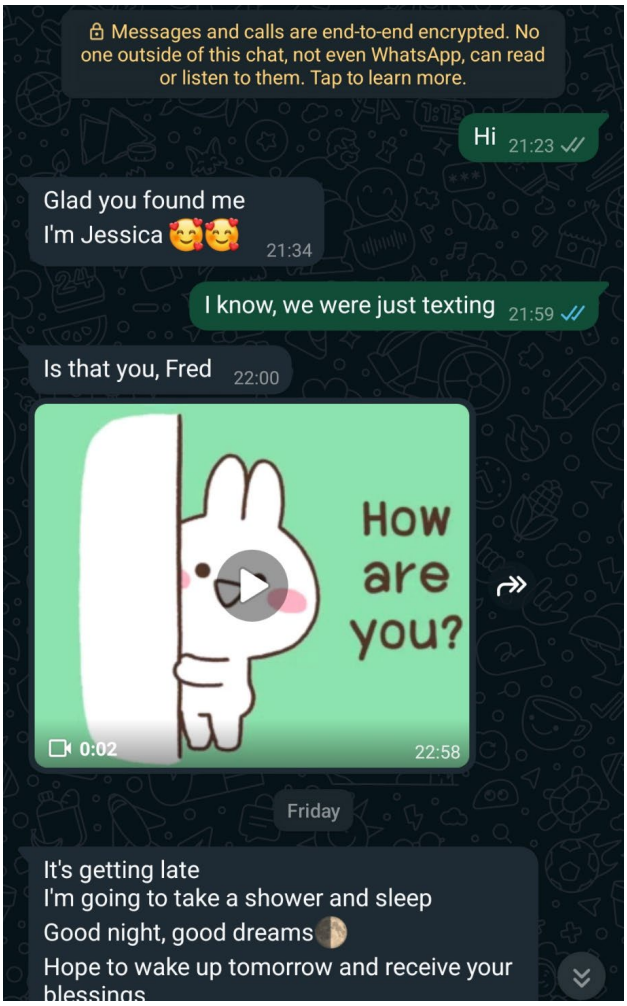

Figure 5: Example continuation of a conversation using WhatsApp.

Once on the scam camp's preferred communications platform, the scam operators engage in conversation intended to build trust or romantic interest. This may occur over the course of days or weeks, depending on the pace of the conversation and the interest the victim expresses. Scam camps use tested scripts that have demonstrated success at psychologically manipulating potential victims into trusting the scammer, even falling in love with the scammer. For example, this conversation revolves around earning money to travel. After a few days the pitch will start with showing massive profits from a potential investment opportunity. For example:

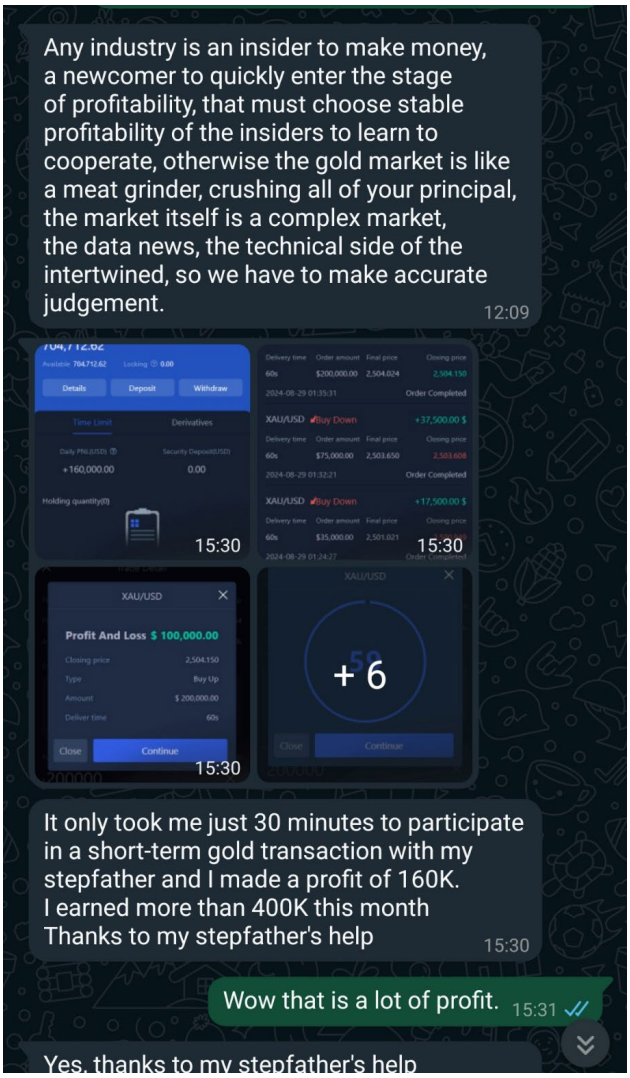

Figure 6: Example of conversation turning to investment advice.

Following introducing the victim to the potential for significant profit, the scam operator will recommend the victim join an investment opportunity. For example:

Figure 7: Example invitation to start investing.

The scam operator will often direct the potential victim to a fraudulent investment website or application. The fraudulent website or application will look very similar to a legitimate service and the scam operator will walk the victim through the process of investing money which often involves the victim transferring funds from their bank account to a bank account controlled by the scammers, a digital asset exchange, or some other transfer. Once the money is "invested," the scam operators will manipulate the fraudulent website or application to show large returns. The scam operators often suggest taking some money out to further gain the trust of the fraud victim.

Once the scam operator is confident that they both have the victim's trust and the victim believes they are earning large returns, then the scam operators will offer a time-limited investment opportunity with a large, guaranteed return, but requiring a substantial minimum investment. As part of this, the scam operator will seek to induce the victim to invest as much money as possible to reap the maximum benefits. This is where victims may empty their bank accounts, retirement accounts, ask friends and family to invest with them, take out loans to raise sufficient capital, and even engage in criminal activity themselves to raise funds. In the following weeks the victim

may realize they have fallen subject to a devastating fraud, leaving them impoverished and in severe psychological trauma.[12] Some victims require substantial assistance in coming to terms with the situation due to the affection they have developed for the scam operators.

The Scam Camp Operation

These cases are not isolated incidents but part of significant transnational criminal schemes involving skilled operators with heavily tested and refined scripts and operations. The scam operations are often conducted from secure compounds housing human trafficking victims forced to engage in these operations.[13] The operators run sophisticated information technology systems, involving multiple communication channels, including social media, messaging apps, and email. Financial fraud victims are often lured through romance or investment scams, and the stolen funds are laundered through complex financial networks. Although money laundering often involves various digital assets, traditional money laundering methods are also used. Some methods involve defrauding other victims by hiring someone as an account processor and the person will use a bank account to receive and transfer funds. They also use bulk cash smuggling, where a bank account will be remotely opened, and a person unknowingly or knowingly will go and withdraw cash and either pass it to another individual or deposit it at a different bank to further the obfuscation of the funds. Nearly all aspects of their operations are supported through a range of specialized services widely advertised on the Telegram communication service and other platforms.[14]

Scam camps operate predominately in Southeast Asia, particularly in Burma, Cambodia, and Laos.[15] These camps are often led by known leaders of transnational criminal organizations that have been active in the region for decades and are reported to exert a corrupt influence on local law enforcement and government officials.[16] The people working in these camps have often been defrauded by the promise of lucrative jobs, only to find themselves forced to work as scam operators. From these camps the workers send billions of unsolicited SMS and other electronic messages to lure victims into romance and digital asset scams. Scam camps are often involved in other forms of criminal activity.[17]

---

[12] For example, Department of Justice "Former CEO of failed bank sentenced to prison" (19 August 2024). Accessed 2 September 2024: https://www.justice.gov/usao-ks/pr/former-ceo-failed-bank-sentenced-prison

[13] Lindsey Kennedy and Nathan Paul Southern, "'Just as scared': Cyberscam victims in Cambodia find no freedom in rescue" Al Jazeera (24 November 2023). Accessed 5 September 2024 at: https://www.aljazeera.com/features/2023/11/24/just-as-scared-cyberscam-victims-in-cambodia-find-no-freedom-in-rescue

[14] Elliptic Research, "Huione Guarantee: The multi-billion dollar marketplace used by online scammers." Elliptic (10 July 2024). Accessed 2 September 2024 at: https://www.elliptic.co/blog/cyber-scam-marketplace

[15] Office of the United Nations High Commissioner for Human Rights (OHCHR) Regional Office for South-East Asia, "Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response" United Nations (August 2023). Accessed 6 September 2024 at: https://news.un.org/en/story/2023/08/1140187

[16] "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security," supra 6.

[17] Amanda Gore, Lindsey Kennedy, Nathan Southern, and Daan van Uhm, "Asian Roulette: Criminogenic casinos and illicit trade in environmental commodities in South East Asia." Global Initiative Against Transnational Organized Crime, Geneva Switzerland (July 2022). Accessed 5 September 2024 at:

Neighboring countries are increasingly concerned about the impact of these criminal activities on their nationals and the spillover effects of these operations. Thailand, Vietnam, Philippines, and China have all taken actions to liberate their citizens from these scam operations and disrupt the activities at scam camps. The working conditions in these scam camps are bleak, with scam operators who do not meet work quotas usually suffering physical abuse and sometimes death.[18] The families of those forced to stay in these scam camps are often extorted as they seek to free their loved ones from the scam camps.

https://theeyewitnessproject.wordpress.com/wp-content/uploads/2024/08/gitoc-apa-obs-asian-roulette-criminogenic-casinos-and-illicit-trade-in-environmental-commodities-in-south-east-asia.pdf

[18] Department of State, "2024 Trafficking in Persons Report" (August 2024). Accessed 3 September 2024 at: https://www.state.gov/reports/2024-trafficking-in-persons-report/

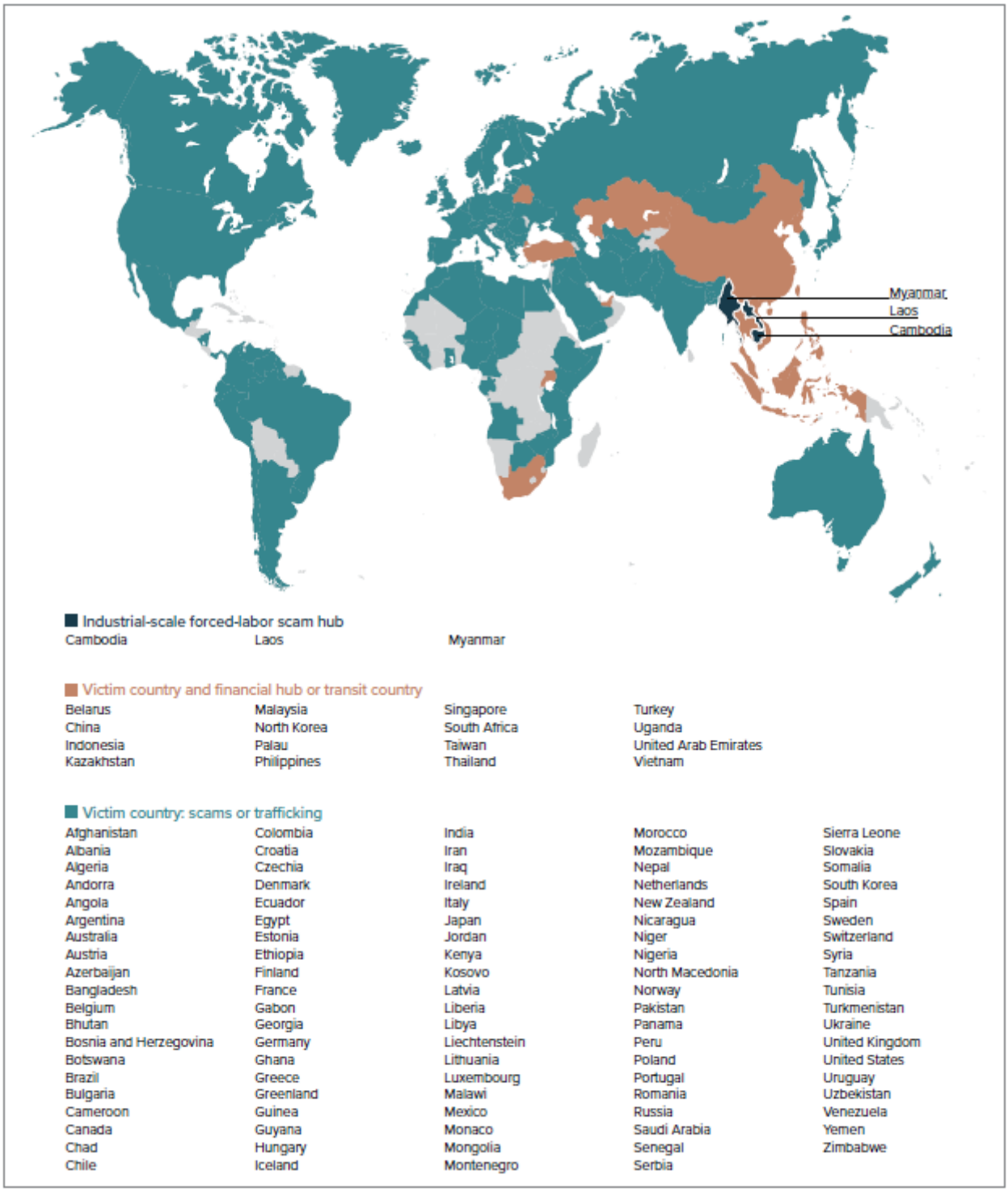

Figure 8: Global Impact of Scam Camp Operations. USIP Report, page 15.[19]

[19] "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security," supra 6.

The communication channels used by these scam operations vary due to some of the remote locations the scam centers operate in, but all make use of the Internet which involves various potential control points for analysis.[20] Some locations are old casino properties and have substantial computer networks; others simply use nearby wireless services. Internet access is often through nearby cell towers or Wi-Fi (sometimes provided across the border from Thailand), with communications ultimately routed across oceanic fiber optic cables. Increasingly, they are using satellite Internet connections (e.g. Starlink). A significant portion of scam camp Internet traffic is routed through a few Autonomous System Numbers (ASNs) assigned by the Asia Pacific Network Information Centre (APNIC). Potential victims in the U.S. are reached through electronic messaging primarily through social media platforms (e.g. dating services, LinkedIn, Facebook/Instagram) and the public switched telephone network by sending messages using North American 10-digit phone numbers. Ultimately, the scam camps are likely to utilize any connection and any messaging platform available to them to reach their potential victims while seeking to evade U.S. controls, such as those related to email[21] and phone calls.[22]

Victims of these scams come from diverse demographics, but certain groups seem to be particularly at risk. Often victimized are those seeking love or connection, those seeking employment, the elderly, and individuals with limited digital literacy. Nationwide surveys would be useful for better identifying victim demographics and overcoming the analytic challenge posed by disparate reporting of crimes to law enforcement across demographics. Improving public awareness of these schemes, and providing readily accessible reporting options, could help to reduce victimization. Various states have enacted laws,[23] and Congress has considered bills,[24] that provide for delay of certain financial transactions based on a reasonable suspicious of fraud. Such laws have the potential to reduce fraud losses to the specified protected populations.

The financial methods used to launder stolen funds are complex and varied.[25] Scam camps substantially exploit less stringent remote account opening rules in the U.S., whereby a U.S. financial institution opens an account after being presented a digital image of a passport (or other identity document, often of foreign origin) and image of a face (i.e., a "liveness/selfie" check). This remote account opening practice using foreign identity documents puts the U.S. at significant risk of criminal activity. Those involved in scam camp operations have told Secret Service investigators that as Singapore, EU, China, Malysia, and other jurisdictions implement new restrictions related to financial accounts, they are shifting their activity to focus on jurisdictions without such controls. Money mules (both witting and unwitting) and couriers are used by scam camp operators to obfuscate the transaction of fraudulent funds. Digital asset

---

[20] Clark, David D., Control Point Analysis (September 10, 2012). 2012 TRPC. Accessed 17 September 2024 at: http://dx.doi.org/10.2139/ssrn.2032124

[21] Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2023.

[22] TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act.

[23] For example, 720 ILCS 5/17-56. Accessed 5 September 2024 at: https://www.ilga.gov/legislation/ilcs/documents/072000050K17-56.htm

[24] H.R.500 - 118th Congress (2023-2024): Financial Exploitation Prevention Act of 2023. (2023, January 31). Accessed 2 September 2024 at: https://www.congress.gov/bill/118th-congress/house-bill/500

[25] For example, Department of Justice "Two Foreign Nationals Arrested for Laundering At Least $73M Through Shell Companies Tied to Cryptocurrency Investment Scams" (17 May 2024). Accessed 2 September 2024 at: https://www.justice.gov/opa/pr/two-foreign-nationals-arrested-laundering-least-73m-through-shell-companies-tied

exchanges, centralized digital asset issuers, and various other digital asset services, are often used to obfuscate transactions further and to quickly move funds transnationally. Cross-sector cooperation between companies that provide telecommunications, Internet services, and financial services is integral to combating and reducing fraud losses to these schemes.[26]

Finally, it is important to consider how scam camps and transnational fraud schemes enable a range of significant transnational criminal activity and national security threats. Through U.S. Secret Service investigations, and those of our partner law enforcement agencies, we have seen significant interplay between money launderers and the activities of significant national security threats, to include foreign efforts to evade sanctions, steal funds, profit from ransomware, and other criminal activity.[27]

Framing a Whole of Nation Response to Counter this Threat

At their core, transnational fraud schemes have four components: The individuals conducting the fraud, the channels they use to communicate with potential victims, the fraud victims themselves, and the financial mechanisms used to obtain and launder the proceeds of these schemes. All four of these components need to be addressed as part of a comprehensive whole of nation effort. This effort naturally requires supporting actions to foster international cooperation, strengthen the rule of law, and improve our ability to measure the nature and prevalence of fraud schemes harming Americans.

[26] For example, Match Group, "Tech Companies Announce A New Coalition To Fight Online Fraud & Pig Butchering Scams." PR Newswire (21 May 2024). Accessed 2 September 2024 at: https://www.prnewswire.com/news-releases/tech-companies-announce-a-new-coalition-to-fight-online-fraud--pig-butchering-scams-302149506.html

[27] For example, Department of Justice "International Money Launderer Sentenced to More Than 11 Years in Prison for Laundering Millions of Dollars in Cyber Crime Schemes" (8 September 2021). Accessed 2 September 2024 at: https://www.justice.gov/opa/pr/international-money-launderer-sentenced-more-11-years-prison-laundering-millions-dollars

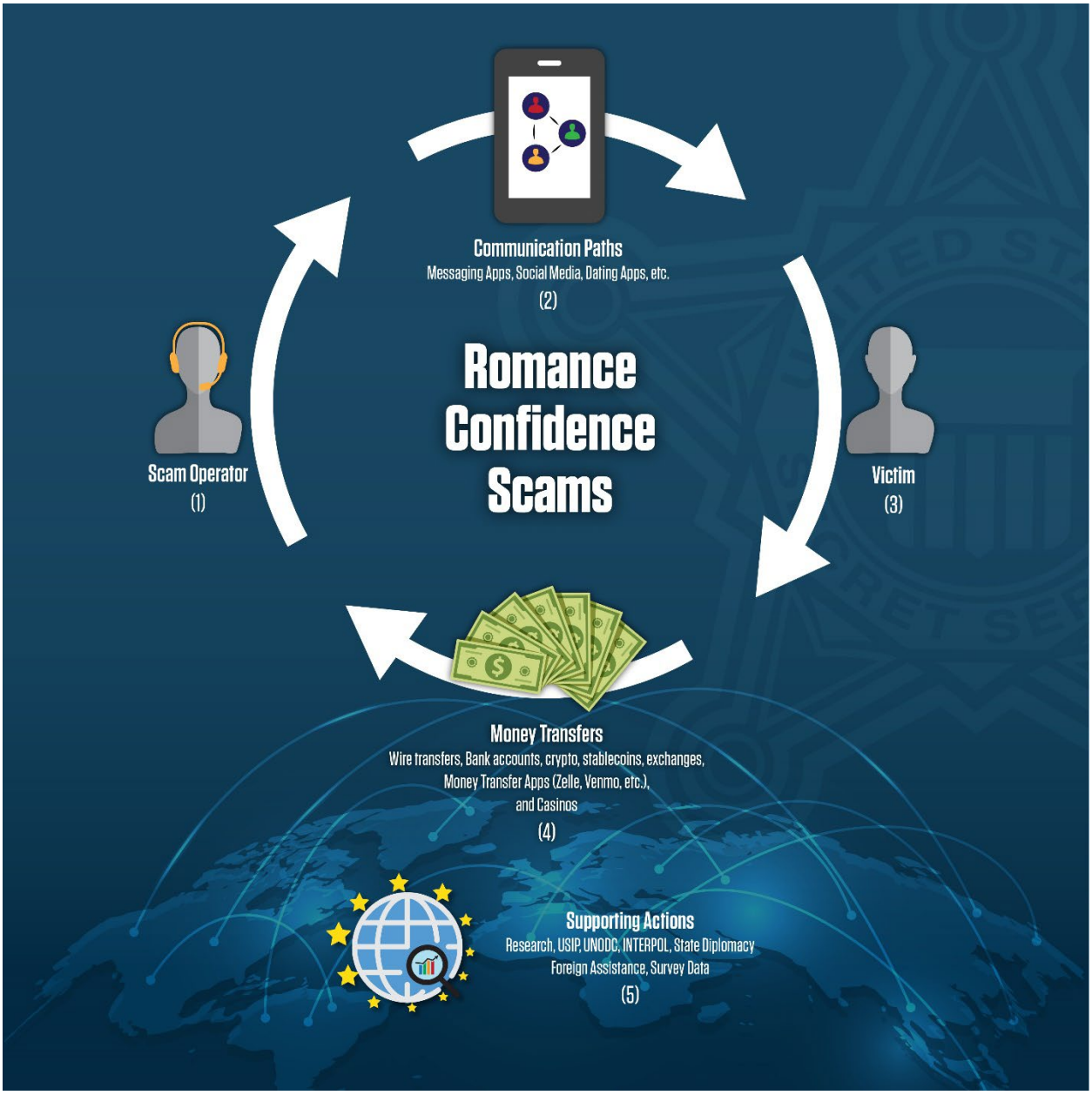

Figure 9: The five key elements for disrupting transnational fraud schemes.

1) Countering Scam Operators

The most direct action to counter fraud is by arresting the individuals criminally involved in these schemes and seizing their assets for return to victims. Working with international partners, the U.S. can achieve this while reinforcing the international rule of law. Interagency and international collaboration is vital to disassembling these types of criminal enterprises. The United States Secret Service will continue to work with the Department of Justice, the Department of State, Interpol, and other domestic and foreign law enforcement agencies, such as the Royal Thai Police, to combat human trafficking and financial crimes in the Mekong Region.

International law enforcement operations to address these scam centers should be executed as a sustained coordinated campaign to apprehend and prosecute the leaders of these operations, interdict new recruits to scam camps, and liberate all those already trapped inside of them. Cheap labor is critical to making these scam camps operationally viable. If the scam operators are cut off from their source of labor, the enterprise will lose a degree of profitability, leading to a natural decline in the scope of their operations. The State Department's 2024 Trafficking in Persons Report makes important recommendations to improve investigation and prosecution of human trafficking, which are particularly relevant to Burma, Cambodia, Laos, and other countries in the region and various other public and private organizations confronting the intersection of digital technology and human trafficking.[28]

More timely and effective enforcement of criminal laws is essential to countering scam camps. Law enforcement requires the investigative tools and training to swiftly detect fraud schemes involving digital technology, identify the nature of their operations, and support lawful action to swiftly end criminal activity. Effective resourcing of State, Local, Tribal, and Territorial (SLTT) law enforcement is an essential part of this, as they represent over 90 percent of the law enforcement in the United States. Our local partners perform an essential role in engaging directly with victims of these crimes. Resources like the National Computer Forensics Institute, which provided training to over 4,000 SLTT law enforcement in FY 23, are critical for our law enforcement partners to assist with investigating these types of cases.

2) Fortifying Communication Paths

A critical component to these schemes is the ability for the scam operators to use electronic messages to communicate internationally at scale to contact victims. Over the years, the U.S., and our foreign partners, have implemented various laws to address communications methods that have been used in fraud schemes: mail, wire, email, robocalling, etc. These sorts of laws are useful for enabling action to address the abuse of a communications service as part of a fraud scheme, but as new communications services emerge applying these disparate existing laws can present challenges in providing users their expected level of protection from harmful communications, regardless of the international communications technology used.

Voluntary industry action is important to detecting and reducing the spread of fraud schemes. Some social media companies, dating apps, and messaging platforms have begun to take steps to better protect their users from fraud schemes, and collaborate cross-sector to share information to do so.[29,30] Some of the websites and applications used in these schemes could be disrupted through actions by various information technology companies. Analysis by the National Cyber Forensics and Training Alliance[31] and other partners continues to be useful for identifying how these websites and applications function and opportunities to disrupt illicit activity involving them.

---

[28] "2024 Trafficking in Persons Report," supra 16.
[29] "Tech Companies Announce A New Coalition To Fight Online Fraud & Pig Butchering Scams," supra 23.
[30] U.K. Home Office, "Online Fraud Charter" (30 November 2023). Accessed 6 September 2024 at: https://www.gov.uk/government/publications/online-fraud-charter-2023
[31] Accessed 6 September 2024 at: https://www.ncfta.net/

Federal agencies working with the telecom industry, social media companies, and Internet access providers can seek to restrict scam operators' ability to communicate with victims. Fraud risk could be reduced through stricter customer verification, enhanced authentication, improving detection and reporting of suspicious activity, increasing record keeping, and improving cross-sector information sharing to identify and combat fraud. The Internet operations of scam camps could be substantially disrupted by addressing their abuse of Internet domain names and other Internet assigned names and numbers.

3) Preventing Victimization and Assisting Victims

Public education is critical to aiding Americans to avoid falling victim to various fraud schemes. The Global Anti-Scam Alliance,[32] American Bankers Association,[33] AARP,[34] Cyber Crime Support Network,[35] Stop Scam Alliance,[36] National Consumers League[37], and National Cybersecurity Alliance,[38] amongst others, all do important work to inform potential and current victims about various fraud schemes and what they can do to protect themselves.

However, the responsibility to avoid falling victim to fraud should not fall solely on potential victims. Businesses that provide technologies that are misused by fraudsters have a critical role to perform in informing and protecting the users of their technology from fraud schemes. This includes implementing effective measures to rapidly detect suspicious activity and potential victimization, alerting users of suspicious activity, providing effective reporting mechanisms for users, keeping records related to suspected criminal activity, and working to lawfully disrupt criminal abuse of their services. Private industry can perform a range of roles to protect their customers from fraud, for example: training checkout clerks on how to spot gift card schemes, having peer-to-peer (P2P) payment apps incorporate algorithms for detecting potentially coerced transactions, or implementing accessible methods to report and record suspicious communications on end-to-end encrypted messaging applications.

On the law enforcement side, SLTT are an essential mechanism for educating the public as they are often at the front line of victim engagement. Training for SLTT law enforcement on how to spot these types of crimes and help victims of these scams will aid in raising awareness and reduce the impact on Americans. Both SLTTT and Federal law enforcement also perform a critical role in recovering and returning assets to fraud victims. In FY 2023, the U.S. Secret Service returned over $464 million to crime victims.

When someone does fall prey to a romance confidence scam, they are too often confused on where to turn to get help. While it is useful for crime victims to have options on where to report (e.g., SLTT law enforcement agencies, federal law enforcement field offices, IC3, FTC, etc.), this can be overwhelming for a crime victim, resulting in reporting delays, and leading to duplicative

[32] Accessed 5 September 2024 at: https://www.gasa.org/
[33] Accessed 6 September 2024 at: https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money
[34] Accessed 3 September 2024 at: https://www.aarp.org/money/scams-fraud/
[35] Accessed 3 September 2024 at: https://fightcybercrime.org/
[36] Accessed 5 September 2024 at: https://www.stopscamsalliance.org/
[37] Accessed 3 September 2024 at: https://fraud.org/
[38] Accessed 3 September 2024 at: https://staysafeonline.org/

efforts. The financial and communication services that consumers have chosen to use are often best positioned to quickly receive a report, take immediate action (e.g., freezing a financial account, reversing a transaction, preserving relevant evidence, alerting other users), and aggregating relevant information for reporting to an appropriate government agency for action.

4) Disrupting the Illicit Financial Networks Utilized for Money Transfers

Disrupting the mechanism by which perpetrators profit from these scams is essential for reducing their prevalence. Under the Bank Secrecy Act, or BSA, and associated regulations, financial institutions are required to implement anti-money laundering and countering the financing of terrorism (AML/CFT) programs, which are critical to reducing the risk of fraud and to reporting suspicious activity. The growth of remotely accessible digital financial services has resulted in new opportunities for transnational fraudsters to evade customer identification requirements and increase exploitation of financial institutions with weak AML/CFT compliance measures.. In 2021, $212 billion in suspicious activity, approximately 42 percent of the total BSA reports that FinCEN received, involved suspicious activity related to identity.[39]

Transnational criminals are increasingly exploiting methods used at U.S. financial institutions for remote account opening, use of foreign identity documents in account opening, and the overreliance on one-time passwords (OTP) sent by SMS, and other messaging services, for authentication. Those involved in scam camp operations have told Secret Service investigators that as Singapore, EU, China, Malysia, and other jurisdictions implement new customer identification and authentication restrictions related to financial accounts, they are shifting their activity to target U.S. citizens and financial institutions in their transnational fraud schemes. Urgent action is needed to improve record-keeping by financial institutions of the identity documents used to open accounts,[40] improving standards on validating identity information presented, and reducing reliance in the U.S. on the public switched telephone network (PSTN) for authentication for high-value financial transactions.[41] Additionally, FinCEN has published "red flag" indicators to help detect, prevent, and report potential suspicious activity related to romance confidence scams, which are important for financial institutions to fully apply.[42]

Identifying and reporting suspicious activity is particularly useful in efforts to recover funds for return to victims. Money mule networks[43] are frequently involved in moving the proceeds of fraud, which often results in a mismatch between the beneficiary listed for a wire and the

[39] Financial Crimes Enforcement Network, "Financial Trend Analysis: Identity-Related Suspicious Activity: 2021 Threats and Trends" (January 2024). Accessed 3 September 2024 at: https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf

[40] 31 C.F.R. § 1020.220(a)(3) (2024). Accessed 17 September 2024 at: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020

[41] National Institute of Standards and Technology Special Publication 800-63B Natl. Inst. Stand. Technol. Spec. Publ. 800-63B, 79 pages (June 2017) CODEN: NSPUE2. Specifically, paragraphs 3.1.3.1, 3.1.3.3, and 3.2.9. Accessed 3 September 2024 at: https://doi.org/10.6028/NIST.SP.800-63b

[42] Financial Crimes Enforcement Network, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering'" FIN-2023-Alert005 (8 September 2023). Accessed 3 September 2024 at: https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf

[43] U.S. Secret Service, "Avoid Scams: Don't Be a Money Mule." Accessed 6 September 2024 at: https://www.secretservice.gov/investigations/mule

receiving account (e.g., a wire intended for a particular business going to a personal account). Financial institutions can often detect such mismatches and not execute such transactions. Improving cooperation amongst financial institutions and with law enforcement to rapidly freeze and return funds to victims of fraud is an essential part of addressing transnational crime. A particular priority is addressing jurisdictional arbitrage by encouraging countries to implement comprehensive AML/CFT supervisory regimes to hold accountable those organizations, financial institutions, and other jurisdictions that fail to sufficiently address illicit activity involving virtual assets. The Financial Action Task Force (FATF), which sets global standards for anti-money laundering laws, has published guidance regarding Virtual Asset Service Providers (VASPs), which are important to swiftly implement in lower-capacity jurisdictions where some major digital asset service companies claim to be located.[44]

5) Foundational Efforts to Understand and Build International Capability to Address

Currently, the prevalence of fraud impacting Americans is primarily measured through victim reporting. However, with sophisticated fraud schemes the victims may be unaware, or too embarrassed to report. A comprehensive measure of fraud impact would allow the U.S. government to better prioritize its efforts to counter the most significant criminal schemes. While the National Crime Victimization Survey distributes a fraud supplement, the scale, scope, and frequency of the survey is limited.[45]

Various researchers and journalists working in the Mekong region have done important work researching the growth and prevalence of scam camps. Their efforts have supported work by the United States Institute of Peace, United Nations Office on Drugs and Crime, Interpol, and others. Supporting continued research is important to improving understanding of romance confidence scams and related transnational criminal activity. This in turn will provide the basis for increasing international awareness and political will to address these crimes.

Finally, developing foreign law enforcement capability is essential for addressing criminal schemes like transnational fraud. The U.S. Government, and our partners, execute a range of programs to strengthen the rule of law, combat foreign law enforcement corruption, and build foreign law enforcement capability and willingness to assist in addressing transnational criminal activity.[46] These programs are essential in combatting transnational criminal activity.

Key Focus Points

The following are key focus points for improving our nation's ability to counter the threat posed by transnational fraud schemes:

---

[44] Financial Action Task Force, "Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs" (9 July 2024). Accessed 3 September 2024: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

[45] Bureau of Justice Statistics, "National Crime Victimization Survey" Department of Justice. Accessed 4 September 2024 at: https://bjs.ojp.gov/data-collection/ncvs

[46] Department of State, "U.S. Strategy on Countering Corruption Implementation Plan" (6 September 2024). Accessed 17 September 2024 at: https://www.state.gov/policy-issues/anti-corruption-and-transparency/

1) **U. S. Secret Service authority under 18 U.S.C. § 3056 to investigate various crimes related to digital asset transactions:** On 8 May 2023, the Administration proposed to Congress updates to 18 U.S.C. § 3056, which would enable the U.S. Secret Service to more effectively counter criminal activity involving illicit digital asset transactions. On 29 February 2024, the House Financial Services Committee passed H.R. 7156 in a 49-0 vote. On 18 July 2024, it was placed on the House Union Calendar. Similar legislation has been introduced in the Senate—S. 4830 and S. Amdt 2813 to the Senate National Defense Authorization Act (NDAA).

2) **U.S. law enforcement authority to address illicit use of digital assets:** Digital assets have become an essential financial tool used for scam camps, ransomware, and other transnational criminal activity. To safeguard Americans from transnational fraud schemes and other criminal activity, the Administration has developed a range of legislative proposals to improve law enforcement's ability to detect illicit activity online and deny criminals the proceeds of their illicit activity. These legislative proposals are described in the recommendations made by the Attorney General in his reports pursuant to Executive Order 14067, Ensuring Responsible Development of Digital Assets.[47]

3) **Abuse of modern electronic messaging:** In 2003, the U.S. enacted the CAN-SPAM Act to address abuse of email. Today, transnational criminals are more often using phone, social media, and other electronic messaging services, rather than email.[48] Existing laws do not adequately address abuse of international communications systems as part of transnational fraud schemes. Additionally, existing statute of limitations, absent an applicable option for tolling, creates significant challenges for law enforcement when encrypted information likely contains evidence of a crime.

4) **Support for state, local, tribal, and territorial law enforcement**: The continued support of the training and equipping of state, local, tribal, and territorial law enforcement is integral. The majority of U.S. law enforcement are state and local law enforcement, and they are an essential partner in addressing fraud schemes. Organizations like the National Computer Forensics Institute provide critical cyber investigation skills to our partners who are often the first responders to victims of criminal schemes and support and enable federal law enforcement action.[49]

5) **Improvement of identity and authentication practices:** U.S. government agencies, along with financial and commercial institutions, often rely on ineffective authentication methods. This reliance puts Americans at significant risk of identity theft and creates significant opportunities for transnational criminals to exploit. It is ineffective to authenticate someone merely by requiring demonstrating knowledge of a password, a social security number, presenting a digital image of a document, or knowledge of a collection of other static pieces

[47] U.S. Department of Justice, "The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets" (6 September 2022). Accessed 22 August 2024 at: https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network

[48] Anti-Phishing Working Group, "Phishing Activity Trends Report, 2nd Quarter 2024" (21 August 2024). Accessed 4 September 2024 at: https://apwg.org/trendsreports/

[49] U.S. Secret Service, "National Computer Forensics Institute." Accessed 4 September 2024 at: https://ncfi.usss.gov/

of information. Phishing-resistant multi-factor authentication is more effective.[50] Moreover, organizations using the public switched telephone network (PSTN) for authentication should quickly adopt more secure authentication methods, consistent with NIST SP 800-63B.[51] Using technology like passkeys as access devices has the potential to greatly improve security and reduce fraud and money laundering risks.[52] Adoption of more secure access devices and authentication practices would reduce our current substantial risk from reliance on our people and technology keeping secret some static piece(s) of information.[53,54]

6) **Collaboration is paramount:** We should continue to foster and strengthen the ability of U.S. law enforcement to work cooperatively with victims of cyber crime, private industry, and international partners to detect cyber criminal activity, seize assets related to cyber criminal activity, and arrest those responsible. It is critical to ensure victims of fraud and extortion attempts, and all those facilitating communications and financial transfers in criminal schemes, are fully engaged with, and cooperating with, appropriate law enforcement authorities. Fostering productive international law enforcement partnerships should remain a priority, particularly with countries in the Southeast Asia region. Continuing to strengthen and expand the Secret Services' international network of Cyber Fraud Task Forces increases U.S. ability to work collaboratively in countering transnational financial crimes.[55]

7) **Fraud as a money laundering risk:** Despite FinCEN clarifying that financial institutions can share information about fraud pursuant to the safe harbor created by section 314(b) of the USA PATRIOT Act, [56] some employees of U.S. financial institutions feel obliged to limit the information they share with other institutions about fraud under that authority. This inhibits efforts to identify and report on fraud. Moreover, some employees of U.S. financial institutions feel obliged to execute the transactions of customers despite reasonably believing those customers are victims of, or involved in, fraud schemes and do not timely report such activity to law enforcement either directly or through the suspicious activity reports they are obligated to provide. Treasury continues to emphasize the risk posed by fraud, for example writing, "Fraud remains the largest and most significant proceed-generating crime for which funds are laundered in or through the United States."[57] Financial institutions should take reasonable steps to identify fraud indicators, report in a timely manner suspicious activities,

---

[50] Cybersecurity and Infrastructure Security Agency, "Implementing Phishing-Resistant MFA" (October 2022). Accessed 4 September 2024 at: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[51] NIST SP 800-63B, supra note 41.

[52] FIDO Alliance, "Passkeys." Accessed 6 September 2024 at: https://fidoalliance.org/passkeys/

[53] 12 C.F.R. § 1005.2 (2024). Accessed 6 September 2024 at: https://www.consumerfinance.gov/rules-policy/regulations/1005/2/

[54] S.884 - 118th Congress (2023-2024): Improving Digital Identity Act of 2023, S.884, 118th Cong. (2023). Accessed 6 September 2024 at: https://www.congress.gov/bill/118th-congress/senate-bill/884/

[55] U.S. Secret Service, "Cyber Investigations." Accessed 4 September 2024 at: https://www.secretservice.gov/investigation/cyber

[56] Financial Crimes Enforcement Network, "Section 314(b)" U.S. Department of the Treasury. Accessed 6 September 2024 at: https://www.fincen.gov/section-314b

[57] Department of The Treasury, "National Money Laundering Risk Assessment (NMLRA)" (February 2024), at page 3. Accessed 17 September 2024 at: https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf

intervene to protect their customers from fraud, and delay financial transactions reasonably believed to involve fraud.

8) **Increase criminal enforcement to counter fraud:** Academic reports indicate Federal criminal enforcement related to fraud have substantially declined over the past 12 years.[58] Attention is needed to enhance U.S. capacity to enforce the law and hold fraudsters, particularly transnational criminal organizations, accountable.

Conclusion

I expect continued increase in the need for the U.S. Secret Service to detect and arrest those involved in scam camps and similar transnational criminal activity. We will have to meet this challenge while also addressing the dynamic protection requirements over the coming years. With the continued support of Congress, the Department of Homeland Security, and our partners, I am confident the Secret Service can meet the substantial demands of our integrated mission.

Thank you again for the opportunity to appear before you to discuss the Secret Service's ongoing efforts to counter scam camps and related transnational cyber-criminal activity. We welcome your partnership and counsel, and I look forward to answering your questions.

[58] TRAC Report, "White Collar Crime Prosecutions for April 2024" (17 June 2024). Accessed 4 September 2024 at: https://trac.syr.edu/tracreports/bulletins/white_collar_crime/monthlyapr24/fil/