檔　　號:
保存年限:

金融監督管理委員會保險局 函

地址：220232新北市板橋區縣民大道2段7號17樓
承辦人：李漢勝
電話：02-8968-0791
傳真：

受文者：中華民國人壽保險商業同業公會(代表人陳慧遊先生)

發文日期：中華民國114年9月26日
發文字號：保局(綜)字第11404303191號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：檢送美國務院及財政部制裁東南亞網路詐騙集團等事如附件，請依說明二、三辦理，請查照。

說明：

一、依據駐美國代表處經濟組114年9月9日經美字第1140000917號函副本辦理，併檢送前揭函文如附件。

二、請持續關注及更新相關制裁資訊，注意相關交易之風險，並採取適當控管措施。如發現疑似洗錢或資恐(資武擴)之情形，應向法務部調查局申報。

三、對於依「資恐防制法」第4條第1項或第5條第1項指定制裁之個人、法人或團體，應依同法第7條規定辦理。

正本：臺灣產物保險股份有限公司（代表人李泰宏先生）、兆豐產物保險股份有限公司（代表人梁正德先生）、富邦產物保險股份有限公司（代表人許金泉先生）、和泰產物保險股份有限公司（代表人蔡伯龍先生）、泰安產物保險股份有限公司（代表人李松季先生）、明台產物保險股份有限公司（代表人矢持健一郎先生）、南山產物保險股份有限公司（代表人蔡漢凌先生）、第一產物保險股份有限公司（代表人李正漢先生）、旺旺友聯產物保險股份有限公司（代表人洪吉雄先生）、新光產物保險股份有限公司（代表人吳昕紘先生）、華南產物保險股份有限公司（代表人涂志佶先生）、國泰世紀產物保險股份有限公司（代表人蔡鎮球先生）、新安東京海上產物保險股份有限公司（代表人藤田桂子女士）、中國信託產物保險股份有限公司（代表人許東敏先生）、中央再保險股份有限公司（代表人戴錦銓先生）、美商安達產物保險股份有限公司台灣分公司（代表人曾增成先生）、法商法國巴黎產物保險股份有限公司台灣分公司（代表人蔡端賢先

1142395022

生）、法商科法斯產物保險股份有限公司台灣分公司（代表人朱玲儀女士）、德商科隆再保險股份有限公司台灣分公司（代表人曾蕙芬女士）、英屬百慕達商美國再保險股份有限公司台灣分公司（代表人何軒傑先生）、新加坡商美國國際產物保險股份有限公司台灣分公司（代表人廖曉俐女士）、比利時商裕利安宜產物保險股份有限公司台灣分公司（代表人游振東先生）、臺銀人壽保險股份有限公司（代表人張志宏先生）、台灣人壽保險股份有限公司（代表人許舒博先生）、保誠人壽保險股份有限公司（代表人劉添先生）、國泰人壽保險股份有限公司（代表人熊明河先生）、凱基人壽保險股份有限公司（代表人王銘陽先生）、南山人壽保險股份有限公司（代表人尹崇堯先生）、新光人壽保險股份有限公司（代表人魏寶生先生）、富邦人壽保險股份有限公司（代表人林福星先生）、三商美邦人壽保險股份有限公司（代表人翁肇喜先生）、遠雄人壽保險事業股份有限公司(孟嘉仁先生)、宏泰人壽保險股份有限公司（代表人李啓賢先生）、安聯人壽保險股份有限公司（代表人陶奕馥女士）、中華郵政股份有限公司（代表人王國材先生）、第一金人壽保險股份有限公司（代表人楊棋材先生）、合作金庫人壽保險股份有限公司（代表人徐錫漳先生）、台新人壽保險股份有限公司（代表人林維俊先生）、全球人壽保險股份有限公司（代表人林文惠女士）、元大人壽保險股份有限公司（代表人翁健先生）、安達國際人壽保險股份有限公司（代表人李崇言先生）、英屬百慕達商友邦人壽保險股份有限公司台灣分公司（代表人侯文成先生）、法商法國巴黎人壽保險股份有限公司台灣分公司(代表人黃宥甄女士)

副本：中華民國人壽保險商業同業公會(代表人陳慧遊先生)、中華民國產物保險商業同業公會(代表人陳萬祥先生)、本局綜合監理組 電子公文交換章 2025/09/26 16:26:09

裝 訂 線

檔　　號:
保存年限:

駐美國代表處經濟組 函

地址：4201 Wisconsin Avenue, N.W.,
Washington D.C. 20016, U.S.A.
承 辦 人：張旨華
聯絡電話：1-202-686-1691
電子郵件：chhchang@sa.moea.gov.tw

受文者：金融監督管理委員會

發文日期：中華民國114年9月9日
發文字號：經美字第1140000917號
速別：普通件
密等及解密條件或保密期限：
附件：如文（c65ea4_1140000917R1.pdf、c65ea4_1140000917R2.pdf）

主旨：有關美國務院及財政部制裁東南亞網路詐騙集團事，報請查參。

說明：

一、美國務院及財政部於本(114)年9月8日對東南亞之網路詐騙集團實施制裁，分別發布新聞稿，綜整要點如下：

(一)東南亞詐騙案激增，據美國政府估計，2024年美國人因東南亞詐騙集團損失至少100億美元，比前一年增加66%。

(二)美國本次制裁包括9個緬甸實體及10個柬埔寨實體：

1、9個緬甸實體參與Shwe Kokko詐騙中心行動，Shwe Kokko是惡名昭彰之虛擬貨幣投資詐騙中心，並在已受美國制裁之犯罪組織Karen National Army(KNA)保護下運作，KNA係一跨國犯罪組織，協助針對美國人之網路詐騙活動，且強迫勞動。

2、另制裁柬埔寨之4名個人及6個實體，因渠等在柬埔寨透過強迫勞動方式，強迫工人對美國、歐洲、中國與

金管會 銀行局
1140147263 114/09/10

其他地區受害者進行虛擬貨幣投資詐騙。

(三)美國財政部負責恐怖主義與金融情報之次長John K. Hurley表示，東南亞網路詐騙產業不僅威脅美國人福祉及財務安全，另使成千上萬人淪為現代奴隸。

(四)本次制裁將阻止犯罪網路執行大規模詐欺、強迫勞動、身體和性虐待以及竊取美國人積蓄，進而保護美國人免受網路詐騙活動威脅。

(五)本次制裁行動針對實施此類詐騙的所有者和運營者，並依據相關行政命令，包括針對大型跨國犯罪組織及其支持者(第13851號)、針對從事惡意網路活動之行為者(第13694號)、針對嚴重侵犯人權行為者(第13818號)、針對威脅緬甸和平、安全與穩定之個人(第14014號)。

(六)制裁之影響：

1、上述受制裁實體在美國境內或由美國公民持有或控制之所有財產及財產權益均被凍結，並須向美國OFAC報告。

2、另由一名或多名被制裁人員直接或間接、單獨或合計擁有50%或以上權益(股權)之實體亦被凍結。

3、除獲OFAC頒發特定許可授權或取得豁免，依OFAC規定，禁止美國公民或在美國境內(或過境)者進行涉及被凍結人員任何財產或財產權益之所有交易。

4、金融機構與其他人員可能因參與涉及被制裁人員之某些交易或活動而面臨制裁風險，這些禁令包括禁止任

何被制裁人員向金融機構或其他人員提供或捐贈資金、貨物或服務、或禁止金融機構或其他人員接受任何受制裁者提供之捐贈資金、貨物或服務。

5、違反美國制裁可能導致美國人與外國人遭受民事或刑事處罰。OFAC之經濟制裁執行指南提供更多相關資訊(請見美財政部新聞稿連結)。

二、檢送美國務院及財政部新聞稿如附件，受制裁實體名稱請見財政部新聞稿，另各受制裁實體之詳細資訊可上OFAC網站查詢https://sanctionssearch.ofac.treas.gov/。以上，併請卓參。

正本：經濟部國際貿易署
副本：行政院經貿談判辦公室、內政部、交通部、金融監督管理委員會(均含附件)

電子公文交換章 2025/09/10 07:51:53

An official website of the United States Government Here's how you know

Imposing Sanctions on Online Scam Centers in Southeast Asia

PRESS STATEMENT

MARCO RUBIO, SECRETARY OF STATE

SEPTEMBER 8, 2025

Criminal actors across Southeast Asia have increasingly exploited the vulnerabilities of Americans online. In 2024, Americans lost at least $10 billion to scam operations in Southeast Asia, according to a U.S. government estimate.

In response, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today imposed sanctions on nine targets involved in operations in Shwe Kokko, a scam center hub in Burma operating under the protection of the already sanctioned criminal organization Karen National Army (KNA). The KNA is a transnational criminal organization that facilitates online scam operations that target Americans and exploit workers in forced labor.

Additionally, OFAC sanctioned four individuals and six entities for their roles operating forced labor compounds in Cambodia, where workers are forced to carry out virtual currency investment scams against victims in the United States, Europe, China, and elsewhere.

These sanctions protect Americans from the pervasive threat of online scam operations by disrupting the ability of criminal networks to perpetuate industrial-scale fraud, forced labor, physical and sexual abuse, and theft of Americans' hard-earned savings.

The Department of the Treasury's sanctions designations were taken pursuant to Executive Order (E.O.) 13581, as amended by E.O. 13863, E.O. 14014, E.O. 13818, and E.O. 13694, as amended. For more information, see Treasury's ***Press Release*** .

Cookie Settings

TAGS

Bureau of East Asian and Pacific Affairs | Bureau of Economic and Business Affairs | Fraud | Office of the Spokesperson | The Secretary of State

An official website of the United States government Here's how you know

U.S. DEPARTMENT OF THE TREASURY

Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams

September 8, 2025

Southeast Asia-based scams skyrocket, costing Americans over $10 billion last year

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) implemented sanctions against large network of scam centers across Southeast Asia that steal billions of dollars from Americans using forced labor and violence. The action includes nine targets operating in Shwe Kokko, Burma, a notorious hub for virtual currency investment scams under the protection of the OFAC-designated Karen National Army (KNA), as well as ten targets based in Cambodia.

"Southeast Asia's cyber scam industry not only threatens the well-being and financial security of Americans, but also subjects thousands of people to modern slavery," said **Under Secretary of the Treasury for Terrorism and Financial Intelligence John K. Hurley**. "In 2024, unsuspecting Americans lost over $10 billion due to Southeast Aisa-based scams and under President Trump and Secretary Bessent's leadership, Treasury will deploy the full weight of its tools to combat organized financial crime and protect Americans from the extensive damage these scams can cause."

Today's action targets the ownership structures and operators that perpetuate these scams and builds on a series of actions, including in the last several months, taken by Treasury to combat cyber scams and the serious human rights abuse that enables them. The sanctions authorities used today include Executive Order (E.O.) 13851, as amended by E.O. 13863 ("E.O. 13851, as amended"), which targets large transnational criminal organizations and their supporters; E.O. 13694, as amended by E.O. 14144 and E.O. 14306 ("E.O. 13694, as amended"), which targets actors engaged in malicious cyber-enabled activities; E.O. 13818, which targets those engaged in serious human rights abuse; and E.O. 14014, which targets persons who threaten the peace, security, and stability of Burma.

CYBER SCAMS TARGETING AMERICANS

Transnational criminal organizations (TCOs) based in Southeast Asia are increasingly targeting Americans through large-scale cyber scam operations. A U.S. government estimate

reported Americans had lost at least $10 billion in 2024 to Southeast Asia-based scam operations, a 66 percent increase over the prior year. Southeast Asia-based criminal organizations often recruit individuals to work in scam centers under false pretenses. Using debt bondage, violence, and the threat of forced prostitution, the scam operators coerce individuals to scam strangers online using messaging apps or by sending text messages directly to a potential victim's phone.

According to a September 2023 alert from Treasury's Financial Crimes Enforcement Network (FinCEN) on virtual currency investment scams, the coerced perpetrators of these scams often use the promise of potential romantic relationships or friendships to gain the trust of their victims. They then convince their targets to make purported "investments" in virtual currency on websites that are designed to look like legitimate investment platforms, but are actually controlled by the scammers themselves. Ultimately, these scammers steal the funds deposited on the platforms. The scam operators specifically look to recruit individuals with English language skills to target American victims. Former scammers have reported that they were directed to specifically target Americans, and some even had quotas for the number of targets per day.

These designations follow multiple Treasury actions undertaken to combat these scams. On May 29, 2025, OFAC sanctioned Funnull, which sold IP (internet protocol) addresses in bulk to cybercriminals to operate scam websites. On May 5, 2025, OFAC designated the KNA as a TCO, along with its leader Saw Chit Thu and his two sons Saw Htoo Eh Moo and Saw Chit Chit, for their roles in facilitating cyber scams that harm U.S. citizens, human trafficking, and cross-border smuggling.

On May 1, 2025, FinCEN identified Huione Group, a southeast Asian financial institution, as a primary money laundering concern pursuant to section 311 of the USA PATRIOT Act. Huione Group has served as a critical node for laundering proceeds of cyber heists carried out by the Democratic People's Republic of Korea (DPRK) and for TCOs in Southeast Asia perpetrating digital asset investment scams, commonly known as "pig butchering" scams, as well as other types of cyber scams. In September 2024, OFAC sanctioned Ly Yong Phat, his conglomerate L.Y.P. Group, and four of his hotels and resorts for their role in serious human rights abuse related to the mistreatment of trafficked workers in scam centers.

SCAM CENTER IN SHWE KOKKO

Treasury's designations today target a major scam hub in Burma sheltered by the KNA. The KNA is headquartered in Shwe Kokko, Myawaddy Township, in Burma's southeast Karen State along the border with Thailand. Through the KNA's collaboration with the Burmese

military, it gained control of territory in eastern Myanmar's Karen State, where KNA leaders profit from transnational crime including cyber scam centers run with trafficked labor, and from the sale of utilities used to provide energy to those same scam operations.

Yatai New City is a prominent compound of scam centers in Shwe Kokko, created by **She Zhijiang** and Saw Chit Thu. In eight years, they transformed a small village on the Moei River into a resort city custom built for gambling, drug trafficking, prostitution, and scams targeting people around the world, particularly Americans. Scam operators at Yatai New City reportedly have lured recruits from around the world under false pretenses, only to detain and physically abuse them, while forcing them to work for crime syndicates as online scammers. Escaped victims have reported being held captive until ransoms are paid by their families, beaten for failing to make quotas, and forced into commercial sex work.

KNA INVOLVEMENT IN YATAI NEW CITY

Saw Chit Thu, as the leader of the KNA, has entrusted different aspects of the operations to trusted subordinates, such as **Tin Win** and **Saw Min Min Oo**. Tin Win and Saw Min Min Oo control property that hosts the scam centers, provide security for those facilitating illicit money flows, and personally run entities that control and support scam compounds in Karen State.

Tin Win runs **Shwe Myint Thaung Yinn Industry & Manufacturing Company Limited**, the company that has historically contracted with energy suppliers to keep the lights on and the scams running in Shwe Kokko. In 2023 and 2025, Thailand shut off power to Yatai New City in an effort to close the scam centers down.

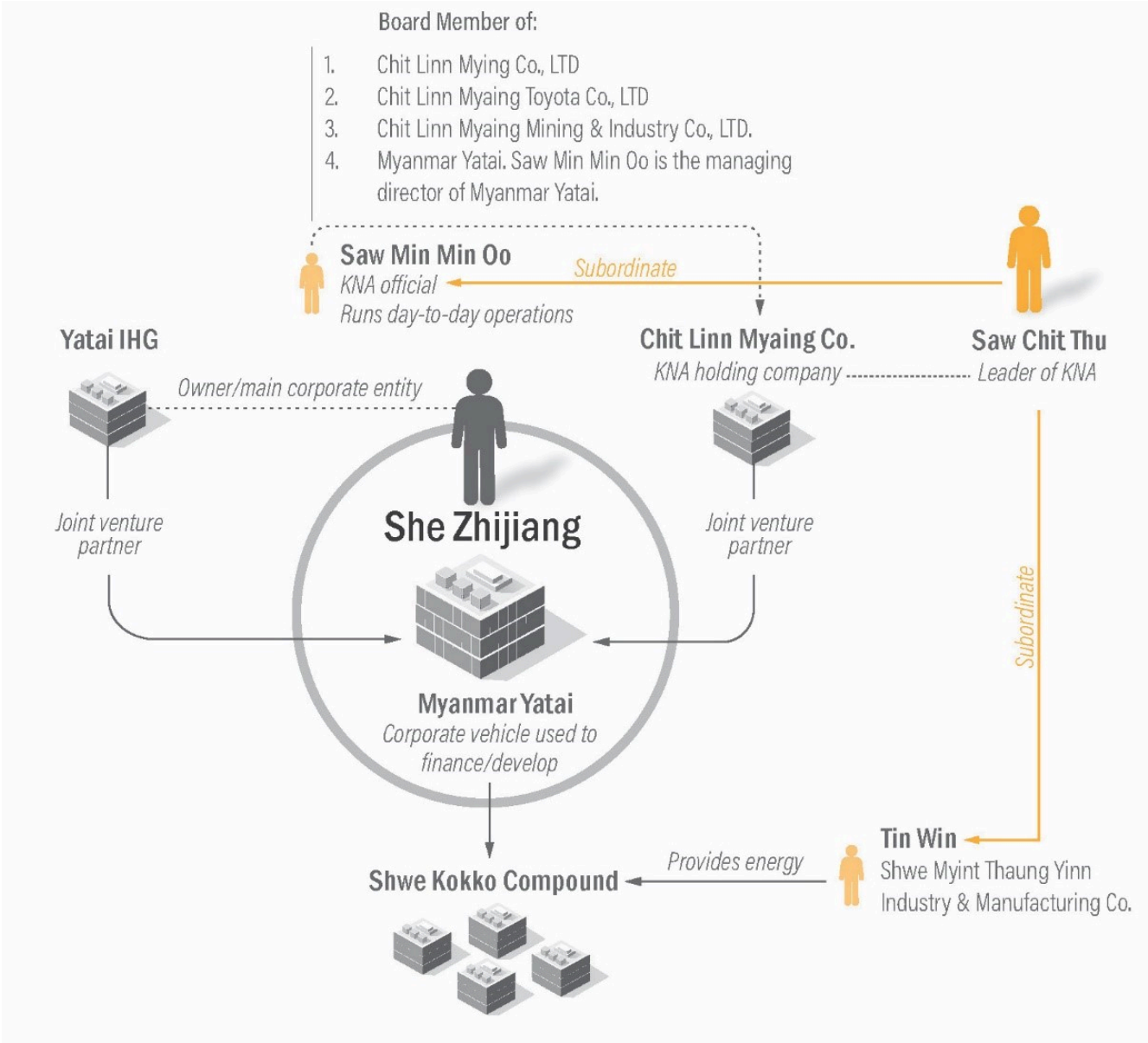
Saw Min Min Oo is a KNA official, and former Colonel in the KNA, who runs and manages various KNA affiliated companies. He is on the board of **Chit Linn Mying Co., Ltd** (CLM Co.), **Chit Linn Myaing Toyota Company Limited**, **Chit Linn Myaing Mining & Industry Company Limited**, and **Myanmar Yatai International Holding Group Co., Ltd**.

SHE ZHIJIANG'S SCAM CENTER EMPIRE

She Zhijiang is the creator and largest shareholder of the Yatai New City compound. Adopting Burmese and Cambodian citizenship, he has operated for years under a plethora of pseudonyms. In 2022, She Zhijiang was arrested in Thailand based on an Interpol Red Notice issued by China, which has continued to seek his extradition from Thailand ever since.

Myanmar Yatai International Holding Group Co., LTD. (Myanmar Yatai) is a joint venture between CLM Co., the KNA's holding company, and She Zhijiang's **Yatai International**

Holdings Group Limited (Yatai IHG). This venture, which is 70 percent owned by Yatai IHG and 30 percent by CLM Co., owns, operates, and profits from Yatai New City and the scam activity happening within. Day-to-day business operations of Yatai New City are run in part by Managing Director Saw Min Min Oo. Yatai IHG is She Zhijiang's main corporate vehicle for his business activities in Southeast Asia.



OFAC is designating Tin Win, Saw Min Min Oo, and Chit Linn Myaing Co., pursuant to E.O. 13581, as amended, and pursuant to E.O. 14014, for having acted or purported to act for or on behalf of, directly or indirectly, the Karen National Army.

OFAC is designating Chit Linn Myaing Toyota Company Limited and Chit Linn Myaing Mining & Industry Company Limited, pursuant to E.O. 13581, as amended, and pursuant to E.O. 14014, for having acted or purported to act for or on behalf of, directly or indirectly, Saw Chit Thu.

OFAC is designating Shwe Myint Thaung Yinn Industry & Manufacturing Company Limited pursuant to E.O. 13581, as amended, and pursuant to E.O. 14014 for having acted or

purported to act for or on behalf of, directly or indirectly, Tin Win.

OFAC is designating She Zhijiang, Yatai International Holdings Group Limited, and Myanmar Yatai International Holding Group Co., Ltd pursuant to E.O. 13818, for being foreign persons who are responsible for or complicit in, or who have directly or indirectly engaged in, serious human rights abuse.

CASINOS-TURNED-CRIMINAL COMPOUNDS IN SIHANOUKVILLE

Treasury is also targeting groups of scam centers in Cambodia. Many of these centers were built as casinos by Chinese criminal actors but became hubs for virtual currency investment scams when that activity proved to be more profitable. **T C Capital Co. Ltd.** (T C Capital) is a company located in Sihanoukville, Cambodia that owns a complex of buildings, including the Golden Sun Sky Casino and Hotel, from which virtual currency scams and other illegal activities have been carried out, sometimes by victims of human trafficking. The complex's casino functions also serve to launder the proceeds of the criminal activity taking place in adjacent buildings. T C Capital was founded by **Dong Lecheng** (Dong), an investor in several Sihanoukville real estate developments linked to modern slavery and virtual currency scams. Before moving to Cambodia, Dong was convicted of money laundering in China in 2008 and has been investigated for bribery, as well as for operating illegal online gambling rings advertised to Chinese nationals.

K B Hotel Co. Ltd. (K B Hotel) is another Sihanoukville company that owns a complex of buildings, including office blocks and a hotel and casino, where enslaved workers are forced to conduct virtual currency scams. K B Hotel was co-founded by **Xu Aimin** (Xu), a naturalized Cambodian citizen who has used his relationships with politically connected Cambodian individuals to avoid scrutiny for K B Hotel and his other businesses. Before moving to Cambodia, Xu was sentenced to 10 years in prison in China in 2013 for operating an illegal billion-dollar online gambling ring, was the subject of an INTERPOL Red Notice, and was wanted in Hong Kong for laundering $46 million of the proceeds through its banks. Xu also owns **K B X Investment Co. Ltd.** (K B X Investment), a Cambodian real estate development company.

CYBER SCAM NETWORKS ACROSS CAMBODIA

Another member of K B Hotel's board is **Chen Al Len** (Chen), who is also a director of **Heng He Bavet Property Co. Ltd.** (Heng He Bavet). Heng He Bavet owns the Heng He Casino and an associated complex of buildings in Bavet, Cambodia. The company, which is involved in

virtual currency scams and forced labor, has received workers from Sihanoukville who were previously linked to cyber scams. Heng He Bavet is co-directed by **Su Liangsheng** (Su), who also sits on the board of **M D S Heng He Investment Co. Ltd.** (M D S Heng He). M D S Heng He is the developer of a large virtual currency scam compound in Pursat Province in Cambodia. The company is chaired by Try Pheap, a Cambodian tycoon previously designated by OFAC. Additionally, Chen and Su are together the majority owners of **HH Bank Cambodia plc** (HH Bank), a Cambodian financial institution.

OFAC is designating T C Capital, K B Hotel, Heng He Bavet, M D S Heng He, Dong, Xu, Chen, and Su pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of cyber-enabled activities originating from, or directed by persons located, in whole or substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose of or involve causing a misappropriation of funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

OFAC is designating K B X Investment pursuant to E.O. 13694, as amended, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Xu. OFAC is designating HH Bank pursuant to E.O. 13694, as amended, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Chen, and also pursuant to E.O. 13694, as further amended, for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Su.

GLOBAL MAGNITSKY

Building upon the Global Magnitsky Human Rights Accountability Act, E.O. 13818 was issued on December 20, 2017, in recognition that the prevalence of human rights abuse and corruption that have their source, in whole or in substantial part, outside the United States, had reached such scope and gravity as to threaten the stability of international political and economic systems. Human rights abuse and corruption undermine the values that form an essential foundation of stable, secure, and functioning societies; have devastating impacts on individuals; weaken democratic institutions; degrade the rule of law; perpetuate violent conflicts; facilitate the activities of dangerous persons; and undermine economic markets. The United States seeks to impose tangible and significant consequences on those who commit serious human rights abuse or engage in corruption, as well as to protect the financial system of the United States from abuse by these same persons.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated or blocked persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of blocked persons.

Violations of U.S. sanctions may result in the imposition of civil or criminal penalties on U.S. and foreign persons. OFAC may impose civil penalties for sanctions violations on a strict liability basis. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. economic sanctions. In addition, financial institutions and other persons may risk exposure to sanctions for engaging in certain transactions or activities involving designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated or blocked person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons List (SDN List), but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, or to submit a request, please refer to OFAC's guidance on Filing a Petition for Removal from an OFAC List.

Click here for more information on the persons designated today. To report internet crime to the FBI, click here.

###