Stop Trafficking!
AwarenessAdvocacyAction

Anti-Human Trafficking Newsletter • May 2025 • Vol. 23 • No. 5

FOCUS: This newsletter focuses on Human Trafficking and Cyber Scam Operations.

Cyberfraud is considered the newest form of human trafficking. According to the **2023 Trafficking in Persons report**, nongovernmental organizations in Southeast Asia estimate that there are tens of thousands of trafficking victims being forced to work as cyber scammers. They are locked in former casino complexes or vast office parks and compounds under armed guard. These trafficked workers, from at least 40 countries, are forced to work 12-15 hours a day in illegal activities, used to perpetrate a range of online fraud on a second set of victims scattered around the world. The schemes include investment fraud, romance scams, and frauds linked to cryptocurrency investing and online gambling. If they do not meet their quota for the day, they are subject to beatings, sexual exploitation, torture, and rape.

The Growth of Cyber Scamming

Covid and its related restrictions led to a significant lack of revenue in all areas of the world. However, some operators saw an opportunity with widespread unemployment and started recruiting people online with fake ads, promising job opportunities in countries such as Burma, Cambodia, Laos, Malaysia, the Philippines, Ghana, Turkey, and China. Scam operations target educated people with exploitable skills, like English or Chinese proficiency or technological background, and promise attractive salaries for customer service jobs, IT, computer programming, and related industries.

Scam operators usually pay for workers' travel but confiscate the victims' passports upon arrival. The victims are locked in a guarded compound and forced to run internet scams 12-15 hours a day. They befriend people on social media and dating apps and persuade them to invest their money in cryptocurrency scams, illegal online gambling, and investment schemes. They may also be forced into romance scams, entering into fake online relationships with and extracting money from unsuspecting targets.

They are subjected to a wide range of abuses and violations, including the imposition of arbitrary debt; restricted access to food, water, medicine, communication, and movement; and threats, beatings, electric shocks, or uses for organ harvesting. There are widespread reports of suicide and casino-based cyber scam operators brutally murdering workers who try to escape.

Some female victims are made to serve as models in video chats with prospective scam victims or forced into sex work if unable to meet their scamming quotas. Scammers who have already been forced into the situation may be forced to lure more victims to join the company. In some cases, the trafficker will "resell" the victims to other scam operations or subject them to sex trafficking if they refuse to work as a scammer.

It is estimated that the scamming industry defrauds the world of tens of billions of dollars per year, so there is a lot of incentive for these criminal organizations to continue operating.

Awareness

Location

Casinos and shell companies, often operating in unused hotels and other rented commercial spaces, have become hotspots for scam centers. These entities sometimes provide a cover for criminal activities, allowing traffickers to operate under the guise of legitimate businesses.

The shift of the cyber-scam industry towards human trafficking was prompted by Cambodia's ban on online gambling in 2019. This ban significantly reduced the revenues of casinos and hotels, decreasing real estate prices in Southeast Asian casino towns. In response, some owners of these establishments conspired with criminal groups to convert unused space into scamming compounds.

The Office of the United Nations High Commissioner for Human Rights (OHCHR) estimated that upwards of 100,000 victims are being held in compounds in Sihanoukville City, Cambodia, alone. There are likely thousands more victims across Southeast Asia, as well as in the United Arab Emirates.

In Korea, organized crime has built compounds that are similar to small cities for the express purpose of scamming.

Despite the successful shutdown of some scam centers and the rescue of trafficking victims through coordinated law enforcement efforts, it's important to note that criminal gangs are proving to be highly adaptable. Their ability to quickly relocate their operations to evade detection and government crackdowns poses a significant and ongoing challenge to law enforcement agencies.

Though media coverage often focuses on Southeast Asia, scam centers have been discovered as far away as Ghana, Peru, the United Arab Emirates, and Mexico. The emergence of copycat centers would represent a worrying expansion of this issue, introducing entirely new criminal organizations and tactics to an elusive threat. For more information, please click here.

Who are the Scammer Trafficking Victims?

Scamming usually has two sets of victims: those trafficked to scam others and those scammed.

The United Nations Office on Drugs and Crime (UNODC) reports that initially, trafficking victims for scamming centers needed to speak Chinese. However, language skills are being surpassed by a need for victims with information technology skills who can develop new programs, such as sophisticated malware or fraudulent websites, to aid in the perpetration of the scams.

INTERPOL similarly found that the keywords mentioned in the fake work advertisements have evolved, expanding from requiring basic skills such as “phone operator” for “call center” jobs

“People who are coerced into working in these scamming operations endure inhumane treatment while being forced to carry out crimes. They are victims. They are not criminals. In continuing to call for justice for those who have been defrauded through online criminality, we must not forget that this complex phenomenon has two sets of victims.”

UN High Commissioner for Human Rights, Volker Türk

to requiring technical skills to supposedly recruit "information technology workers" and "digital sales executives."

The U.S. Department of State's 2024 Trafficking in Persons (TIP) Report specifically highlights the trafficking of victims from Ghana, Nigeria, Uganda, Kenya, Peru, Brazil, and the United Arab Emirates (UAE), among other countries. Many of these victims are young and tech-savvy and hail from regions with high unemployment rates and a surplus of new tech graduates. It is estimated that more than 220,000 trafficking victims are held in scam operations in Myanmar and Cambodia alone. Most are not citizens of the countries in which the trafficking occurs.

Who are the victims being scammed?

The scams conducted by those in the compounds have a global reach, targeting people worldwide, especially those from the Western world, North America, and Western Europe, as well as people in Hong Kong, Taiwan, and Thailand.

The United States Institute of Peace estimates that Americans lost $3.5 billion to scams specifically originating in Southeast Asia in 2023, highlighting that "U.S. residents are now a top target of the crime networks' financial crimes." This vast financial loss prompted the U.S. Department of the Treasury to publish an alert in September 2023 warning financial institutions and the public about pig butchering scams. Further, Americans may be at risk of being trafficked to work in fraud factories. While there is little publicly available data on Americans being trafficked, the FBI issued a warning to U.S. citizens about false job advertisements linked to labor trafficking at scam compounds, suggesting it is a rising concern.

Center for Strategic and International Studies

'Pig Butchering Scam'

The term "pig butchering scam" comes from the Chinese. It refers to the first phase of the scam, gaining the victims' trust and comparing it to fattening the pigs before slaughtering them. The scheme started in China around 2016, originally finding their victims on same-sex dating sites.

Today's scammers target victims throughout the world, catfishing victims, creating fake profiles on dating sites or social media and building personal, and often romantic relationships. Many of these operations rely on AI-generated visuals, commonly known as deepfakes, to deceive their victims. Recent developments in artificial intelligence and large language models like ChatGPT are also reportedly being leveraged by online scam centers. At the same time, language translation software is used to target victims in countries not represented by trafficked workers.

The scheme often starts with a simple "hi" or a seemingly innocent wrong number text on messaging platforms like WhatsApp. The scammers utilize carefully crafted scripts to 'fatten up' their unsuspecting targets. They groom these individuals with a blend of romance and financial promise, skillfully drawing them into investment schemes usually involving cryptocurrency investments, making them difficult to trace and recover. When the moment is ripe, they execute the "slaughter," ruthlessly divesting their victims of their hard-earned money, and then disappear. Many will lose their life savings by the time they realize they were scammed. The accurate measure of pig butchering losses is unknown because victims are often too embarrassed to report these crimes to authorities. Please click here for more information.

Advocacy

Tactics Used

How are human trafficking victims forced to scam and defraud other victims of their money? It typically looks like the following:

The scammer contacts the target through social media or a fake 'wrong number' text. The scammer develops trust with the target by sharing personal information, such as a fake name, a fabricated personal story, or even a manipulated photo, generating empathy and emotional pressure. During this time, the scammer assesses the target's financial position.

Once trust is acquired, the scammer gradually introduces the topic of cryptocurrency investment and convinces the target to invest. The scammer persists in encouraging investment until the target transfers a significant amount to the fraudulent investment platform.

In romance scams, scammers specifically target vulnerable seniors who have recently lost a spouse or gone through a divorce, knowing they may be emotionally fragile and have access to cash. According to the FTC's Protecting Older Consumers Report Protecting Older Consumers (2022-2023), older adults reportedly lost nearly $240 million to romance scams in 2022. Scammers again work to gain a victim's trust and then provide false information or misrepresentation to gain a financial benefit by relying on the compassion of the victim. These schemes are constantly evolving and becoming more innovative. Cryptocurrency, bank wires, gift cards, and payment apps may be payments.

Many victims of scams have lost substantial amounts of money, sometimes even their entire life savings, leaving them in dire financial straits. The shame and humiliation of being scammed are often compounded by societal attitudes that blame and shame the victim, making them feel even more isolated and desperate. This can make it difficult for victims to seek help or talk about their experience with loved ones or law enforcement, leading to feelings of isolation and despair.

The psychological toll of being scammed can be devastating, with many victims suffering from anxiety, depression, and other mental health issues as a result. In some extreme cases, victims have even taken their own lives in the aftermath of being scammed.

Even if it's too late to recoup your losses, reporting details may help others avoid becoming victims. Call the HSI Tip Line at 877-4-HSI-TIP to report suspicious criminal activity, including possible romance scams. Your call could prevent someone else from falling victim. Callers may remain anonymous. For more information, please click here.

In 2023, the Heartland Tri-State Bank in Kansas failed due to the CEO embezzling $47 million after he got caught up in a cryptocurrency scheme

*To address this increasingly global threat related to scamming, **INTERPOL** is calling for greater intelligence exchange between law enforcement, non-governmental organizations, financial intelligence units and relevant private sector companies to support the rescue of trafficking victims and dismantle the money laundering activities that facilitate these activities.*

***There are reports** that government officials in the countries where these centers are operating indirectly or directly benefit from their continued operation. Some benefit from the economic growth generated by criminal leaders' investments in legitimate businesses and real estate development. Moreover, it is reported that a scam compound in Cambodia is indirectly owned by a governing party representative, and it is believed that there are ties between the families of influential politicians and scam compounds.*

The absence of rule of law along the Thailand-Myanmar border in Karen State has resulted in direct connections between the scammers and the military.

Protection of Victim Scammers

Identifying individuals coerced into illegal acts such as scamming is crucial. It ensures compliance with the UN Office on Drugs and Crime's (UNODC) non-punishment principle, which states that trafficking victims should not be punished for crimes committed as a direct result of being trafficked. Survivors who managed to escape often face criminal charges for immigration violations rather than being identified as trafficking victims and receiving protection services. This underscores the urgent need for better support systems. It's crucial that embassies, as representatives of their nationals, are more responsive to victim complaints and engage more effectively with local law enforcement on their behalf. Please click here to learn more.

When 33-year-old Ali saw the social media ad for a digital marketing job in Cambodia, he immediately said yes. Ali was among thousands of workers who have fallen prey to human traffickers running cyber scam syndicates in Cambodia and other countries in Southeast Asia. Ali shares, "It was terrifying. We tried to survive the harsh physical torture for us to get out of the compound. I was forced to scam five people daily and entice them to join cryptocurrency investment schemes or deposit money into gaming accounts." I felt helpless taking money away from other people. There were many nights I couldn't sleep well because of guilt, but I had no other choice."

https://ijm.org.au/blog/scam-centres-run-by-human-trafficking/

Scammers Embrace Latest Technology

In their attempts to avoid detection, scammers have used custom software to conceal their activity. This may involve using virtual private networks (VPNs) and other tools to protect their anonymity. ChatGPT helps scammers craft more authentic-sounding messages to gain victims' trust.

Custom software is particularly effective for scammers, enabling them to create a false trail that leads investigators away from their true location or identity. By using advanced technology and tools, scammers can also manipulate data and create fake identities that are difficult and often impossible to trace.

In January 2024, the UN Office of Drugs and Crime (UNODC) reported that scammers are using deepfake technology to "execute social engineering scams with alarming success rates, exploiting people's trust and emotions." This technology helps scammers conduct investment fraud, create deepfake pornography, and carry out schemes impersonating police officers, celebrities, and family members.

According to the Center for Strategic and International Studies, criminals are using advanced technologies to bypass digital verification systems and know-your-customer measures. This threat to financial institutions adds to the challenges related to "money-muling," or the transfer of illegally acquired money on behalf of someone else.

FraudGPT is an AI bot on the dark web explicitly made to write scam pages, spear phishing emails, and even create password-cracking tools. This allows a scammer with only a basic understanding of technology to conduct advanced scams.

Further, according to the UNODC, criminal actors are using malware, including information-stealing malware (infostealers). Infostealers steal sensitive and personally identifiable information such as login details and financial information. The People's Republic of China (PRC) cracked down on an organized crime group based in Myanmar that trafficked Chinese nationals and forced them to commit sextortion fraud. In an incident involving sextortion, scammers first coerced victims into installing malware that allowed them to steal the victims' mobile phone contacts. Then, scammers pressured the victim to participate in graphic video calls.

Finally, they threatened to share the videos with the stolen contacts unless the victim paid a fee According to the Center for Strategic and International Studies, criminals can buy infostealers for as little as $50–250 and recruit money mules to launder funds and purchase sensitive personal information. This has allowed criminal groups to specialize, building upon their technical strengths while outsourcing other services.

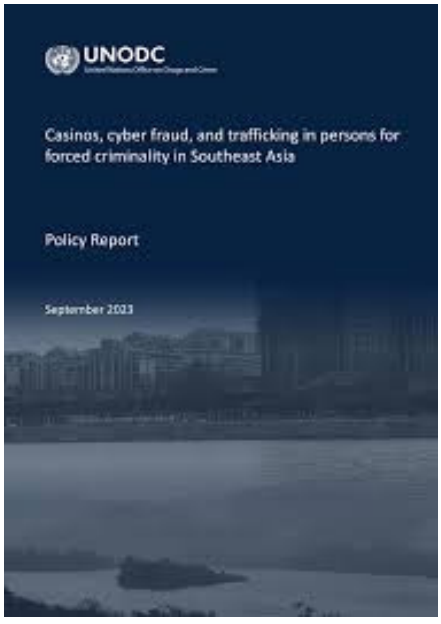
CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Human trafficking victims tortured into scamming innocent people

60 Minutes Australia

Inside the global scamming factories. Adam Hegarty reports on the frightening way new A.I. technology is being used to steal billions of dollars from unsuspecting victims. Please click **here** to view this YouTube video.

Please click **here** to access the UNODC latest report on casinos, money laundering and transnational organized crime in East and Southeast Asia.



How can you protect yourself?

Scams can target anyone, but with a deeper understanding of their tactics, you can empower yourself and your loved ones to spot and avoid them. The scam is built over time, and the initial payments appear to be successful investments, often allowing the victim to harvest some of their initial gains to build confidence and trust.

Banks and payment providers should look for specific red flags and intervene before all is lost when working with the right technology. They need to establish formal anti-scam programs and take a creative approach to deter scammers, collaborate to share information, and encourage victims to report scams.

One of the most effective ways to protect yourself online is by setting strict privacy settings. Remember, everything you post online is in the public domain, so take control of your online presence and limit the information available to potential scammers.

Beware of strange friend requests. Only accept a friend or follow requests from people you know. Traffickers typically reach out to strangers to 'chat' via social media.

One of the most important precautions to take is to never give out sensitive information unless you are certain you are on a legitimate website. Be wary of advertisements that seem too good to be true, as traffickers often provide vague details about the company's credentials or terms of employment. Phishing scams, which aim to obtain login credentials, are a common tactic used by scammers. To avoid falling victim to these scams, it's crucial to double-check the URL of any website you visit.

If you encounter someone on social media who is harassing you or making you uncomfortable, don't hesitate to unfriend, block, or report them. Take screenshots of any messages or posts that make you uneasy. If you suspect you've been targeted by a scam or have fallen victim to one, it's crucial to report it to your local authorities and the cryptocurrency community. Reporting such scams can prevent others from falling victim to the same scam, and authorities can take action to investigate and shut down fraudulent operations.

Click **here** to learn more.

Action

Scam Artist or Human Trafficking Victim?

Inside a Scam Farm

Feature by the United Nations

Scams are causing damage worldwide and spreading rapidly thanks to rapid technological developments. Following the trail of scam victims forward leads to stories of immense suffering—and so does following the trail backwards to the scammers, who engage in large-scale human trafficking, torture and enslavement so they can profit on the loss of others. Who is behind this trade in lies and deceit? How do they perpetrate their crimes?

And how can they be stopped? Please click here to view this 10-minute video.

Please click **here** to view a 3 minute video from Voice of America news on how victims of trafficking are treated in the scamming industry.

In 2023, the United Nations Office for Drugs and Crime published *Key Indicators of Trafficking in Persons for Forced Criminality to Commit Cyber Enabled Crimes* which may be accessed by clicking **here**.

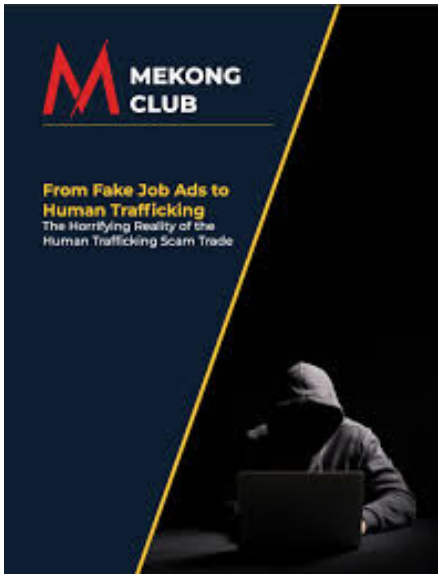
Operation Shamrock convenes social media companies, the financial sector, law enforcement, and nongovernmental organizations to combat online scamming. Operation Shamrock's mission is to raise awareness of pig butchering with everyone, everywhere, all the time. Their goal is to educate the public, mobilize collective action, and disrupt the operations networks of transnational organized criminals to prevent further harm.

The Tech Against Scams Coalition brings together large social media, dating apps and cryptocurrency companies such as Meta, Match Group (owner of Hinge and Tinder), and Coinbase, as well as the Global Anti-Scam Organization, to share intelligence and exchange best practices.

A romance scam victim speaks to Homeland Security about her experience being the target and gives advice for others who may be targets. Please click here to view this informative 6-minute video.

From Fake Job Ads to Human Trafficking by Mekong Club

This publication provides a comprehensive analysis of a new crime that emerged in 2022. It involves fraud, human trafficking, modern slavery, cryptocurrencies and money laundering, hereby referred to as the 'human trafficking scam trade'.

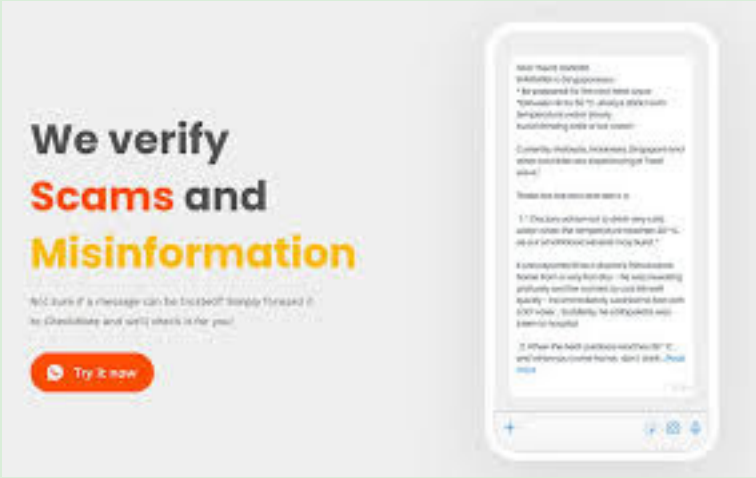


Cyber Scams and Human Trafficking in Cambodia and Vietnam

The United States Institute for Peace hosted a webinar on cyber scams and Human Trafficking in Cambodia and Vietnam. Concerned by the impact of organized crime on governance, local conflict and global security, the United States Institute of Peace formed a study group to explore the dimensions and nature of Southeast Asia's China-originating criminal networks and the scourge of online scamming they are now spreading globally. They found an alarming rise of criminal cyber scam centers that exploit forced labor, human trafficking and online "pig butchering" techniques to defraud victims of billions of dollars.

Please click here to view this video of their findings.

CheckMate is a free WhatsApp bot that can identify scams and disinformation. CheckMate uses AI to classify messages in one of seven different categories, such as "scam," "legitimate," or "spam." It then asks if it can include the message in a national scams database, which could provide up-to-date examples for public awareness campaigns. This program is relatively new but, if scaled up, could enable victims to identify scams more easily.



ALLIANCE TO END HUMAN TRAFFICKING

Founded and Supported by U.S. Catholic Sisters

Click on the links below to visit the websites of our sponsors

- Adorers of the Blood of Christ
- Adrian Dominicans
- Benedictine Sisters of Chicago
- Benedictine Sisters of Mount St. Scholastica, Atchison, KS
- Benet Hill Monastery
- Congregation of Notre Dame
- Congregation of Sisters of St. Agnes
- Congregation of S. Joseph
- Daughters of Charity, Province of the West
- Daughters of Charity, Province of St. Louise
- Daughters of the Holy Spirit
- Dominican Sisters of Houston, TX
- Dominican Sisters of Mission San Jose, CA
- Dominican Sisters of Peace
- Dominican Sisters of San Rafael, CA
- Dominican Sisters of Sinsinawa, WI
- Dominican Sisters of Sparkill
- Dominican Sisters of Springfield, IL
- Felician Sisters of North America
- Franciscan Sisters of Peace
- Franciscan Sisters of Perpetual Adoration
- Franciscan Sisters of the Sacred Heart
- Holy Spirit Missionary Sisters
- Institute of the Blessed Virgin Mary
- Marianites of Holy Cross
- Maryknoll Sisters
- Medical Mission Sisters
- Medical Missionaries of Mary
- Missionary Sisters of the Society of Mary
- Northern California Catholic Sisters Against Human Trafficking
- Our Lady of Victory Missionary Sisters
- Presentation Sisters, Aberdeen
- Presentation Sisters, San Francisco
- Racine Dominicans
- Religious of the Sacred Heart of Mary
- Religious Sisters of Charity
- School Sisters of Notre Dame, North America
- School Sisters of St. Francis of Christ the King
- Sisters of Bon Secours
- Sisters of Charity of Cincinnati
- Sisters of Charity of Halifax
- Sisters of Charity of Leavenworth
- Sisters of Charity of New York
- Sisters of Charity of St. Joan Antida
- Sisters of Charity of the Blessed Virgin Mary
- Sisters of Charity of the Incarnate Word - Houston
- Sisters of Charity of Nazareth
- Sisters of Charity of Seton Hill
- Sisters of Christian Charity Mendham, NJ & Wilmette, IL
- Sisters of Mercy Catherine's Residence
- Sisters of Mercy of the Americas
- Sisters of Notre Dame of the United States
- Sisters of Notre Dame de Namur, USA
- Sisters of Providence, Mother Joseph Province
- Sisters of St. Chretienne
- Sisters of St. Dominic - Racine, WI
- Sisters of St. Francis of Clinton
- Sisters of St. Francis of Colorado Springs
- Sisters of St. Francis of Dubuque
- Sisters of St. Francis of Philadelphia
- Sisters of St. Francis of Redwood City
- Sisters of St. Francis of the Providence of God
- Sisters of St. Francis Rochester, MN
- Sisters of St. Joseph of Baden
- Sisters of St. Joseph of Carondelet
- Sisters of St. Joseph of Chestnut Hill Philadelphia
- Sisters of St. Joseph of Cluny, USA & Canada Provinces
- Sisters of St. Joseph of Concordia, KS
- Sisters of St. Joseph of Orange
- Sisters of the Blessed Sacrament
- Sisters of the Divine Savior
- Sisters of the Good Shepherd
- Sisters of the Holy Cross
- Sisters of the Holy Family
- Sisters of the Holy Names of Jesus and Mary
- Sisters of the Humility of Mary
- Sisters of the Precious Blood
- Sisters of the Presentation of the Blessed Virgin Mary
- Sisters of the Sacred Hearts
- Sisters of the Sorrowful Mother
- Society of the Divine Savior
- Society of the Holy Child Jesus
- Society of the Sacred Heart
- Southern CA Partners for Global Justice
- St. Mary's Institute of O'Fallon
- Tri-State Coalition Against Human Trafficking & Slavery
- U.S. Ursuline Sisters of the Roman Union

The Anti-Trafficking Newsletter is dedicated exclusively to fostering an exchange of information among Alliance members, organizations and concerned persons collaborating to eliminate all forms of human trafficking. Click here to access previous issues of Stop Trafficking! To contribute information, please contact: stoptrafficking@feliciansisters.org. Editor: Maryann Agnes Mueller, CSSF. Layout & Design: Mary Francis Lewandowski, CSSF. Translated into Spanish by Amelia Breton, SBS.