

FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown

14-18 minutes : 6/8/2021

For Further Information, Contact:

Media Relations Director Kelly Thornton (619) 546-9726

SAN DIEGO – A wave of hundreds of arrests that began in Australia and stretched across Europe culminated today with the unsealing of a federal grand jury indictment in San Diego charging 17 foreign nationals with distributing thousands of encrypted communication devices to criminal syndicates.

The 500-plus arrests that took place during a worldwide two-day takedown were possible because of a San Diego-based investigation like no other. For the first time, the FBI operated its own encrypted device company, called “ANOM,” which was promoted by criminal groups worldwide. These criminals sold more than 12,000 ANOM encrypted devices and services to more than 300 criminal syndicates operating in more than 100 countries, including Italian organized crime, Outlaw Motorcycle Gangs, and various international drug trafficking organizations, according to court records.

During the course of the investigation, while ANOM’s criminal users unknowingly promoted and communicated on a system operated lawfully by the FBI, agents catalogued more than 27 million messages between users around the world who had their criminal discussions reviewed, recorded, and translated by the FBI, until the platform was taken down yesterday.

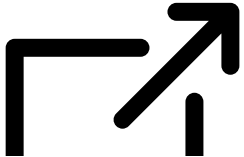
The users, believing their ANOM devices were protected from law enforcement by the shield of impenetrable encryption, openly discussed narcotics concealment methods, shipments of narcotics, money laundering, and in some groups—violent threats, the indictment said. Some users negotiated drug deals via these encrypted messages and sent pictures of drugs, in one instance hundreds of kilograms of cocaine concealed in shipments of pineapples and bananas, and in another instance, in cans of tuna, in order to evade law enforcement.

The indictment charges 17 alleged distributors of the FBI’s devices and platform. They are charged with conspiring to violate the Racketeer Influenced and

Corrupt Organizations Act (RICO), pertaining to their alleged involvement in marketing and distributing thousands of encrypted communication devices to transnational criminal organizations worldwide.

During the last 24 to 48 hours, in addition to the more than 500 arrests around the world, authorities searched more than 700 locations deploying more than 9,000 law enforcement officers worldwide and seized multi-ton quantities of illicit drugs.

[CLICK HERE - Video Messages from International Partners](#)



Grand totals for the entire investigation include 800 arrests; and seizures of more than 8 tons of cocaine; 22 tons of marijuana; 2 tons of methamphetamine/amphetamine; six tons of precursor chemicals; 250 firearms; and more than \$48 million in various worldwide currencies. Dozens of public corruption cases have been initiated over the course of the investigation. And, during the course of the investigation, more than 50 clandestine drug labs have been dismantled. One of the labs hit yesterday was one of the largest clandestine labs in German history.

“This was an unprecedented operation in terms of its massive scale, innovative strategy and technological and investigative achievement,” said Acting U.S. Attorney Randy Grossman. “Hardened encrypted devices usually provide an impenetrable shield against law enforcement surveillance and detection. The supreme irony here is that the very devices that these criminals were using to hide from law enforcement were actually beacons for law enforcement. We aim to shatter any confidence in the hardened encrypted device industry with our indictment and announcement that this platform was run by the FBI.”

“Today marks the culmination of more than five years of innovative and complex investigative work strategically aimed to disrupt the encrypted communications space that caters to the criminal element,” said Suzanne Turner, Special Agent in Charge of the Federal Bureau of Investigation (FBI) - San Diego Field Office. “The FBI has brought together a network of dedicated international law enforcement partners who are steadfast in combating the global threat of organized crime. The immense and unprecedented success of Operation Trojan Shield should be a warning to international criminal organizations – your criminal communications may not be secure; and you can count on law enforcement worldwide working together to combat dangerous crime that crosses international borders.”

“Operation Trojan Shield is a perfect example of an OCDETF case - an investigation driven by intelligence and maximizing the strengths of partner law enforcement agencies in coordinated efforts to dismantle command and control elements of criminal networks,” said OCDETF Director Adam W. Cohen. “Coordination is the cornerstone of the OCDETF program, and the impressiveness of the combined efforts of the U.S. Attorney’s Office, FBI, and our foreign partners cannot be overstated. This effort has created lasting disruptive impacts to these transnational criminal organizations.”

“The AFP and FBI have been working together on a world-first operation to bring to justice the organised crime gangs flooding our communities with drugs, guns and violence,” said AFP Commissioner Reece Kershaw APM. “The FBI provided an encrypted communications platform while the AFP deployed the technical capability which helped unmask some of the biggest criminals in the world. This week the AFP and our state police partners will execute hundreds of warrants and we expect to arrest hundreds of offenders linked to the platform. This is the culmination of hard work, perseverance and an invaluable, trusted relationship with the FBI.

We thank the FBI for their long and integral partnership with the AFP.”

Europol’s Deputy Executive Director Jean-Philippe Lecouffe: “This operation is an exceptional success by the authorities in the United States, Sweden, the Netherlands, Australia, New Zealand and the other European members of the Operational Task Force. Europol coordinated the international law enforcement community, enriched the information picture and brought criminal intelligence into ongoing operations to target organised crime and drug trafficking organisations, wherever they are and however they choose to communicate. I am very satisfied to see Europol supporting this operation and strengthen law enforcement partnerships by emphasizing the multi-agency aspect of the case.”

“I am exceptionally proud of our New Zealand Police staff who supported Operation Trojan Shield,” said New Zealand Police Commissioner Andrew Coster. “This operation will have an unprecedented impact on organised crime syndicates across the globe. We value our strong relationship with the FBI, AFP and Europol and it is through these partnerships and the unrelenting efforts by law enforcement agencies from multiple countries that this operation has seen such incredible success. This is a fantastic result and reiterates the importance of our transnational partnerships with law enforcement agencies across the globe in our common ongoing efforts to dismantle organised crime groups and the enormous harm they cause to our communities.”

“This remarkably successful operation demonstrates what can be accomplished when law enforcement agencies throughout the world work together,” said DEA Los Angeles Division Special Agent in Charge Bill Bodner. “Through strong relationships with our partners in more than 67 countries, professionals

throughout the DEA, including experts in the Los Angeles Division, supported this unprecedented collaboration and our own mission to disrupt and dismantle the criminal organizations that profit from the distribution of illegal drugs.”

According to the San Diego indictment, ANOM’s administrators, distributors, and agents described the platform to potential users as “designed by criminals for criminals” and targeted the sale of ANOM to individuals that they knew participated in illegal activities.

All defendants are foreign nationals located outside of the U.S. In total, eight of the indicted defendants were taken into custody last night. Authorities are continuing to search for the remaining nine defendants.

The indictment alleges the defendants knew the devices they distributed were being used exclusively by criminals to coordinate drug trafficking and money laundering, including in the U.S. The defendants personally fielded “wipe requests” from users when devices fell into the hands of law enforcement.

The FBI’s review of ANOM users’ communications worked like a blind carbon copy function in an email. A copy of every message being sent from each device was sent to a server in a third-party country where the messages were collected and stored. The data was then provided to the FBI on a regular basis pursuant to an international cooperation agreement. Communications such as text messages, photos, audio messages, and other digital information were reviewed by the FBI for criminal activity and disseminated to partner law enforcement agencies in other countries. Each user was using ANOM for a criminal purpose. Those countries have built their own cases against ANOM users, many of whom were arrested in takedowns in Europe, Australia and New Zealand over the last several days.

Intelligence derived from the FBI’s communications platform presented opportunities to disrupt major drug trafficking, money laundering, and other criminal activity while the platform was active. For example, over 150 unique threats to human life were mitigated.

This operation was led by the FBI and coordinated with the U.S. Drug Enforcement Administration, the U.S. Marshals Service, Australian Federal Police, Swedish Police Authority, National Police of the Netherlands, Lithuanian Criminal Police Bureau, Europol, and numerous other law enforcement partners from over a dozen other countries.

This investigation began after Canada-based encrypted device company Phantom Secure was dismantled by the FBI in 2018 through a San Diego-based federal RICO indictment and court-authorized seizure of the Phantom Secure platform, forcing many criminals to seek other secret communication methods to

avoid law enforcement detection. The FBI—along with substantial contributions by the Australian Federal Police—filled that void with ANOM.

When the FBI and the San Diego U.S. Attorney's Office dismantled Sky Global in March 2021, the demand for ANOM devices grew exponentially as criminal users sought a new brand of hardened encryption device to plot their drug trafficking and money laundering transactions and to evade law enforcement. Demand for ANOM from criminal groups also increased after European investigators announced the dismantlement of the EncroChat platform in July 2020. The ANOM platform - unlike Phantom Secure, EncroChat, and Sky Global - was exploited by the FBI from the very beginning of ANOM's existence and was not an infiltration of an existing popular encrypted communications company.

In October 2018, Phantom Secure's CEO pleaded guilty to a RICO conspiracy in the Southern District of California. He was sentenced to nine years in prison and ordered to forfeit \$80 million in proceeds from the sale of Phantom devices.

For further information, please see <https://www.justice.gov/usao-sdca/pr/chief-executive-communications-company-sentenced-prison-providing-encryption-services> and <https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices>.

Operation Trojan Shield is an Organized Crime Drug Enforcement Task Forces (OCDETF) investigation. OCDETF identifies, disrupts, and dismantles the highest-level drug traffickers, money launderers, gangs, and transnational criminal organizations that threaten the United States by using a prosecutor-led, intelligence-driven, multi-agency approach that leverages the strengths of federal, state, and local law enforcement agencies against criminal networks.

Assistant U.S. Attorneys Meghan E. Heesch, Joshua C. Mellor, Shauna Prewitt, and Mikaela Weber of the U.S. Attorney's Office for the Southern District of California are prosecuting the case, with assistance from Paralegal Specialist Tracie Jarvis. Former Assistant U.S. Attorney Andrew P. Young made invaluable contributions during his tenure on the case team.

Acting U.S. Attorney Grossman praised federal prosecutors and FBI agents and international law enforcement partners for their relentless pursuit of justice in this extraordinary case. Additionally, Acting U.S. Attorney Grossman thanked the coordinated efforts of the Department of Justice's Office of International Affairs which facilitated many international components of this complex investigation.

The charges and allegations contained in an indictment are merely accusations, and the defendants are considered innocent unless and until proven guilty.

DEFENDANTS 21-CR-1623-JLS COUNTRY

*Joseph Hakan Ayik (1)

DEFENDANTS 21-CR-1623-JLS	COUNTRY
Domenico Catanzariti (2)	Australia
*Maximilian Rivkin (3)	
Abdelhakim Aharchaou (4)	The Netherlands
*Seyyed Hossein Hosseini (5)	
Alexander Dmitrienko (6)	Spain
*Baris Tukul (7)	
*Erkan Yusef Dogan (8)	
*Shane Geoffrey May (9)	
Aurangzeb Ayub (10)	The Netherlands
James Thomas Flood (11)	Spain
*Srdjan Todorovic aka Dr. Djek (12)	
*Shane Ngakuru (13)	
Edwin Harmendra Kumar (14)	Australia
Omar Malik (15)	The Netherlands
Miwand Zakhimi (16)	The Netherlands
*Osemah Elhassen (17)	
*Fugitive	

SUMMARY OF CHARGES

Conspiracy to Conduct Enterprise Affairs Through Pattern of Racketeering Activity (RICO Conspiracy), in violation of 18 U.S.C. § 1962(d)

Maximum Penalty: Twenty years in prison

AGENCIES

Federal Bureau of Investigation

Drug Enforcement Administration

United States Marshals Service

Department of Justice, Office of International Affairs

Australian Federal Police

Swedish Police Authority

Lithuanian Criminal Police Bureau

National Police of the Netherlands

EUROPOL

For further information, please see

<https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication>



[https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-](https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime)

[smashes-organised-crime](https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime)

