OFFICE of PRIVATE SECTOR
Liaison Information Report (LIR)

CROSS-SECTOR

19 DECEMBER 2024 **LIR 241219007**

International Organized Theft Groups Target Athletes

References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI. The FBI does not and will not target people based on their race or ethnicity.

The FBI Criminal Investigative Division, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform U.S. professional athletic associations about international organized theft groups, often emanating from South America, targeting the U.S. homes of athletes, particularly while they are at games or on travel. These homes are targeted for burglary due to the perception they may have high-end goods like designer handbags, jewelry, watches, and cash.

International organized theft groups conduct physical and technical surveillance in preparation for these burglaries. The perpetrators also use publicly available information and social media to identify a pattern of life for a prospective victim and often know in advance where valuables are kept in a home. These preparation tactics enable theft groups to conduct burglaries in a short amount of time. Organized theft groups bypass alarm systems, use Wi-Fi jammers to block Wi-Fi connections and disable devices, cover security cameras, and obfuscate their identities.

- Between September and November 2024, organized theft groups allegedly burglarized the homes of at least nine professional athletes and targeted entry points including glass rear doors, windows, and second-story doors.

- In April 2024, an organized theft group of Chilean nationals stole a safe from a residence and covered up security cameras to avoid detection. The same burglary ring conducted multiple residential burglaries within a two-month timeframe and stole jewelry, collectibles, cufflinks, and other valuables. While this group did not target the homes of athletes, its tactics are consistent with other international organized theft groups who allegedly do so.

The following suspicious activities observed on or near residential property are potential indicators of targeting for theft. A single indicator does not accurately identify if individuals are targeting an athlete's home for theft; personnel and organizations should consider the totality of facts and circumstances, including message delivery and other relevant information, before reporting to security/law enforcement personnel.

- A small group of unvetted individuals accessing one's property with face coverings and hoodies.
- Vehicles and/or persons not regularly seen outside one's home.

- Individuals with technical surveillance tools such as drones, signal jammers, GPS devices, lawn cameras, thermal imaging devices, and other burglary tools such as picklocks, crowbars, screwdrivers, and slide hammers.
- Irregular delivery vehicles/companies frequenting the area.
- Individuals following athletes to their homes, posing as lawncare workers, food delivery persons, or mechanics/repairmen.

Increased awareness among leagues, including athletes, regarding international organized theft groups will help sensitize potential victims to the need for greater safeguarding of their property and valuables. Increased reporting of suspicious activity and home burglaries will help law enforcement understand and combat these burglaries. Leagues should consider educating athletes and staff on efforts to target their homes for burglaries and the tactics these criminals employ. They should also consider encouraging personnel to take the following mitigation steps:

- Keep records of valuables, inventorying items and their whereabouts.
- When traveling out of town, employ and arm surveillance and alarm systems, employ additional security, and engage with private security and homeowners' association security.
- Engage with the local police department about this potential threat and report suspicious activity.
- Exercise caution while using social media, to include refraining from posting pictures of valuables, the interior of one's home, and real-time posts when on vacation.

While many burglaries occur while homes are unoccupied, some burglaries occur while residents are home. In these instances, individuals are encouraged to seek law enforcement help and avoid engaging with criminals, as they may be armed or use violence if confronted.

The FBI's Office of Private Sector disseminated this LIR. If league personnel have feedback or information on historic and current burglaries and tactics used to employ these crimes, please contact your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP: RED  For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP: RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP: RED information with anyone else. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.
TLP: AMBER  Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP: AMBER+STRICT restricts sharing to the organization only.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP: AMBER+STRICT.
TLP: GREEN  Limited disclosure, recipients can spread this within their community.	Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
TLP: CLEAR  Recipients can spread this to the world, there is no limit on disclosure.	Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.