[redacted]

PUBLIC SAFETY

CROSS-SECTOR

19 FEBRUARY 2025 **LIR 250219012**

Heightened Threat to Chief Executive Officers Following the Shooting of a Healthcare Sector Executive

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's New York and Portland Field Offices, in coordination with the Office of Private Sector (OPS), the Criminal Investigative Division, the Counterterrorism Division, and the Little Rock, Indianapolis, and Phoenix Field Offices, prepared this Liaison Information Report (LIR) to inform private sector partners about an increased threat to Chief Executive Officers (CEOs) following the 4 December 2024 shooting of UnitedHealthcare CEO Brian Thompson in New York, NY. On 9 December 2024, an identified individual was arrested for the suspected murder of CEO Thompson. Following these events, social media posts threatening executives, including posts referencing CEO Thompson's homicide, have risen across critical infrastructure sectors and industries. This rhetoric has displayed an elevated threat of violence to executives and highlighted a need for increased situational awareness among private sector partners.

Lone actors, unaffiliated with specific ideological groups, are using social media to intimidate high-profile employees. While these threats often fall short of federal prosecution, they create fear and highlight the need for heightened vigilance against potential copycat attacks.

- On 16 December 2024, a social media user calling for the death of corporate executives discussed the sale of playing cards titled, "Most Wanted CEOs." An online website reportedly sells playing cards that "unmask CEOs who rule our world." The cards include CEOs from real estate, healthcare, retail, finance, technology, media, weapons, oil, chemical, pharmaceutical, agriculture, and logistics companies.

- As of 12 December 2024, following company layoffs, former employees of a digital music distribution service had posted images and messages regarding the company's CEO. The posts included altered images and references to CEO Thompson's homicide; however, the posts did not meet federal prosecution criteria. The FBI referred the complaint to local law enforcement for further investigation.

- On 10 December 2024, multiple social media users' posts threatened to kill the CEO of a major U.S. energy company. One post stated, "I'll shoot the CEO of [U.S. Company] before I pay that light bill.

- On 10 December 2024, a social media user's post threatened healthcare CEOs and referenced Thompson's homicide. The post stated, "copycat killers identified," and named the CEOs of multiple major U.S. healthcare companies.

- On 8 December 2024, multiple social media users' posts threatened the CEO of a major U.S. online payment service. One post stated, "Corrupt CEOs should start watching the news." Another post stated the user planned to attend one of the company's shareholder meetings in February 2025.

- On 7 December 2024, a social media user posted a "hit list" of corporate executives; the post contained the words, "Wanted Dead or Alive," with "Alive" crossed out in red. Additionally, the post listed the names and photographs of several corporate executives. CEO Thompson's name was on the list with a red "X" over his photograph.

The following suspicious activities are potential indicators of a heightened threat environment against CEOs. A single indicator does not accurately identify a threat of violence; organizations should consider the totality of facts and circumstances, including message delivery and other relevant information, when reporting to security/law enforcement personnel.

- Online content or posts on websites or social media expressing the following:
  - o Explicit praise or discussion of tactics used in the killing of CEO Thompson in extremist online spaces;
  - o Requests for or sharing of attack tactics, techniques, and procedures;
  - o Development and dissemination of new methods to target high-profile executives nationwide;
  - o Sharing locations of an executive's workplace or home;
  - o Advocacy for violence as a necessary means to achieve ideological goals; or
  - o Increased use of concealment tactics for attack planning, such as using a VPN to hide the user's true location, posting attack plans or manifestos with fictious social media accounts, deleting or hiding social media accounts, and using disposable/burner phones;

- Threats addressed to a CEO or other executive via social media, phone, or email;
- Suspicious surveillance, such as repeated unauthorized visits, filming, photographing, or drone activity near corporate property or the private property of a corporate executive;
- Attempts to gather sensitive security details on personnel, entry points, or access controls without justification;
- Unauthorized access attempts at workplaces or residences of a high-profile executive;

- Doxing or swatting of a CEO or other high-level management;
- Trespassing on corporate or executive private property; or
- Individuals attempting to use false identification or impersonating employees to gain access to executive areas or executive-level conferences.

Private sector partners are encouraged to consider the following steps to address the heightened threat environment to CEOs:

- Coordinate with federal, state, tribal, and local law enforcement to establish communication channels for reporting public safety threats and developing response plans for emergencies, including clear roles and uniform communication methods.
- Create systems to alert employees about security incidents, provide resources for reporting suspicious behavior, and share relevant reports with external law enforcement when appropriate.
- Develop operational security plans for high-risk individuals to better safeguard them both at work and in their personal lives. Discuss with law enforcement how best to mitigate fraudulent calls for service to prevent swatting incidents at workplace or residential addresses.
- High-level executives should keep their personal social media accounts private. They should also separate public social media accounts from company marketing accounts and not highlight any personal information.
- Company websites should remove identifying information of executives from biography and team pages, such as town of residence and information on family members.
- Employees should not share their home address or phone number with parties who do not have a need to know it.

To report any threats or suspected criminal activity, you may visit https://tips.fbi.gov/ or contact your local FBI Office: https://www.fbi.gov/contact-us/field-offices. Please note, these websites cannot be used to report emergencies or immediate threats to life. For an emergency or immediate threat to life, please call 911.