OFFICE of PRIVATE SECTOR
Liaison Information Report (LIR)

CROSS-SECTOR

22 March 2023 **LIR 230322006**

Nationwide Takedown of Catalytic Converter Theft Ring

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. An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The FBI's Sacramento and Newark Field Offices, in coordination with the FBI's Chicago and Detroit Field Offices, the Office of Private Sector (OPS), and Criminal Investigative Division, prepared this LIR to inform private sector partners about the effects of the November 2, 2022, nationwide takedown of DG Auto Parts LLC (DG Auto). DG Auto was one of the leading criminal actors and businesses participating in the theft, sale, and illegal transportation of catalytic converters throughout the United States. In total, 21 individuals in 5 states have been arrested in connection with this case for their involvement in the transaction of $575 million in stolen material in the United States. This LIR should be read in conjunction with LIR 210810006 titled "Criminal Actors Committing Interstate Transportation of Stolen Catalytic Converters," 10 August 2021, highlighting the rise in criminal actors transporting stolen catalytic converters across state lines. The FBI assessed criminal actors and organized crime groups would continue to target catalytic converters for theft, sale, and illegal transport as a low-risk opportunity to profit from soaring prices of platinum, palladium, and rhodium.

In 2020, FBI Sacramento initiated an Asian organized crime investigation on an illegal catalytic converter fencing operation in Sacramento, California. Vang Auto Core was first identified as a large-scale fencing operation, which sold its stolen converters to DG Auto in New Jersey. After DG Auto bought the converters, they were sold to a Japanese company, DOWA Metals and Mining Co. The proceeds from the sale of the converters were laundered and distributed to DG Auto and its national network of affiliates. At that time, the financial investigation revealed DG Auto sent wire transfers to Vang Auto Core to purchase stolen catalytic converters, totaling approximately $38,000,000 in a three-year period. Financial records belonging to DG Auto revealed wire deposits to DG Auto totaling in excess of $300,000,000 from a precious-metals recycler, identified as DOWA Metals and Mining America (subsidiary). Since the initiation of the investigation on DG Auto, FBIHQ established a major theft national initiative, which identified several businesses affiliated with DG Auto in several states (Pennsylvania, Virginia, New Jersey, Minnesota, Oklahoma, Nevada, California, Texas, Florida, Tennessee, Mississippi, and Wisconsin).

Following the takedown of DG Auto and associates, the FBI assesses a power vacuum will occur due to the risk versus profit-potential and the continued high prices of platinum group metals found in catalytic converters. The FBI expects mid-level associates and networks to replace the void left by the takedown of DG Auto. While catalytic converter thefts will continue, the FBI believes that associates and groups attempting to fill the power vacuum will not reach the sophistication or the international relationships created by DG Auto.

Due to the DG Auto takedown, another large catalytic converter recycler based in the United States reportedly exercised caution when dealing with customers who did not have a pre-existing relationship to the recycler. Additionally, following the takedown, a different recycling plant located in Pennsylvania refused to purchase catalytic converters from individuals based in New Jersey. Out of concern for law enforcement scrutiny, the Pennsylvania plant is no longer taking new customers and is now requiring existing customers attempting to sell catalytic converters to provide a driver's license.

The FBI is interested in information regarding continued organized criminal activity targeting catalytic converters and other vehicle components. The FBI recommends reporting suspicious information to your facility security office and local Law Enforcement to include your local FBI field office.

The FBI's Office of Private Sector disseminated this LIR. Direct any requests and questions to 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.