Farley M. Mesko

Written Statement for the Hearing On

"Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance"

Before the Task Force to Investigate Terrorism Financing

Of the House Financial Services Committee

February 3, 2016

Chairman Fitzpatrick, Ranking Member Lynch, and members of the Task Force, thank you for the opportunity to testify here today.

Detecting and preventing trade-based money-laundering (or TBML) schemes is a notoriously difficult task, because such schemes are by necessity deeply embedded in overt and legal trade flows. However, this dependency also presents an opportunity: in order to embed within overt systems of finance and commerce, TBML schemes require seemingly legitimate companies, which require paperwork, disclosures, sometimes even marketing and a web presence. This means the networks that perpetrate TBML schemes tend to leave a broad and publicly discoverable footprint, both digital and physical. Despite the many layers of obfuscation that may be built into a scheme, this footprint often leads directly back to an already-identified threat actor or network, particularly in the context of a sophisticated and persistent terror financing scheme.

TBML typologies evolve and change over time, but the key actors in the networks tend not to. This implies that even as public and private sector entities focus on identifying and screening for *typologies* of TBML, they also need to focus on identifying the *networks*.

I am going to use a case example to illustrate this point.

Case Study

In 2011, as part of a larger sanctions package targeting a Hizballah terror financing TBML scheme, the United States Treasury identified a Cotonou, Benin-based group of companies known as the "Elissa Group." In addition to its alleged participation in this terror financing scheme, the Elissa Group was deeply integrated into seemingly legal streams of international trade and commerce, acting as shipping agent for several large

international freight forwarders who specialized in maritime transport of new and used automobiles. By all accounts, this coordinated US government effort, which also included the designation of a Lebanese bank as a primary money laundering concern, was a success. However, patterns of economic activity subsequent to the designation, and patterns of later US government actions, suggest that this network continued to operate even in the face of exposure.

Treasury data from the original 2011 action indicate that at least six of the sanctioned companies shared an address in Cotonou, Benin, and further open source research revealed that several also shared the same phone number. Subsequent to the designation, a new company, Abou Merhi Lines, began to appear on maritime commercial listings linked to this same address and phone number, operating in the same industry segment as the Elissa Group. Reexamining publicly available bills of lading from prior to 2011 shows that this company owned and managed vessels used by the Elissa Group companies for hundreds of used vehicle shipments. Four years after the original Elissa designation, in October 2015, Treasury sanctioned Abou Merhi Lines for its alleged participation in the same TBML scheme identified in 2011. This suggests that the TBML network likely operated post-designation, through both new and old actors, for at least four years.

Even further, online trade data and public records from the Littoral Department Chamber of Commerce in Benin indicate that at the time of the original 2011 designation, at least six other companies and two individuals were active at the shared Cotonou, Benin address. One of these companies, Rmaiti SRL, was later identified in the 2013 FinCEN 311 designation of Kassem Rmeiti & Co For Exchange. Another company, never publicly identified, was actually listed "care of Elissa Group." These and others were active in used vehicle imports, the same industry used to disguise illicit financial flows in the scheme targeted by Treasury.

In sum, 13 companies and two individuals shared identifiers and selectors in Cotonou, Benin; between 2011 and 2015, eight of these 15 companies and individuals were either sanctioned by OFAC or identified in a FinCEN 311 action, in several cases operating openly for years after the initial identification of the scheme; of the remaining seven co-located companies and individuals, five were overtly involved in the used vehicle trade, and may be operating today.

I chose this example because it illustrates several key points about targeting TBML networks.

First, sanctions, 311 actions, and indictments are a starting point and not an endpoint in the government's efforts to target money launderers (particularly those involved in

complex networks and sophisticated schemes like TBML). Networks change over time in response to interventions from law enforcement and regulators, but they rarely go away.

Second, in addition to focusing on *typologies* of TBML, both public and private sector stakeholders need to focus on the *networks*. Proxies, shell companies, vessels, and other actors may change over time, but more often than not, there is a trail leading back to the same key players, whether it's a common director, shareholder, address, phone number, or otherwise. Further, many thousands of these key players have already been identified by governments worldwide, essentially providing the first level of lead generation for investigators and analysts in both the public and private sector.

Third, there is a tremendous amount of data available publicly to help detect and deter these schemes. Availability of course varies by jurisdiction, and most of these records are non-indexed, non-searchable, in local languages, and sometimes offline, but the information is there if you know where and how to look.

Finally, there are many stakeholders in this fight, from law enforcement and regulators to the transportation industry and the financial sector. Each of them holds some unique data, but nobody has the whole picture, and nobody is making full use of the range of data available to them in the public domain. The key to detecting and preventing increasingly complex TBML schemes is data integration, within government, within the private sector, between the two, and, for all the stakeholders, between proprietary and open data streams.

Thank you again for the opportunity to be here today, and I look forward to questions.