Dual-use or not? The next frontier in trade finance

David Pan **(CAMS), business solutions, risk & trade compliance, APAC at Accuity, answers questions surrounding dual-use goods, and what banks can do to identify such items.**

Starting with the UK Financial Conduct Authority's review of bank's control of financial crime risks in trade finance (July 2013), then the Singapore MAS guidance paper on anti-money laundering (AML) and counter-terrorist financing (CTF) in trade finance (October 2015) and the Hong Kong Association of Banks' guidance, published in February 2016, the regulatory focus on banks' need to identify dual-use goods has caused much discussion within the industry, specifically by banking professionals who must look into implementing a solution to help them comply with this need. Dual-use goods can be defined as any good or technology which can have both commercial applications as well as military.

A few challenges banks face when identifying dual-use goods specifically involve:

- Generic descriptions/multiple descriptions of goods
- Goods that are only dual-use if they meet certain specifics such as tensile strength
- Goods involving high-risk jurisdictions
- Uncertainty regarding implications once a real match is identified

Ultimately the fundamental questions are, "how do I look for dual-use goods" and "what do I do with it once I find what I'm looking for?"

How do I look for dual-use goods?

The answer to the first question is that the search can be conducted in a few ways. The simplest approach is to obtain a copy of the dual-use goods "list" and search on it using CTRL+F. The obvious pitfall here is if the commercial invoice description reads "law enforcement grade pepper spray" yet the dual-use goods list doesn't use the same language. For example, if the dual-use goods document states "riot control agents such as 'Bromobenzyl cyanide' or 'chloroacetophenone'" then it can be a frustrating task to investigate if they are the same thing. Another pitfall is that certain innocent goods may read las if they are dual-use goods (amorphous silicon common in solar panels) which will send the person investigating on a wild goose chase, ultimately ending up with nothing.

A more sophisticated approach is to digitise and place human intelligence into the data. This would then require a dedicated resource to study the dual-use list and adapt what can be adapted while enriching key terminology such as "riot control agent" equating to "tear gas" or "pepper spray". The pitfall here would be a need for this dedicated resource or team of resources to manually input data: the quality and practicality of this project would solely rest on the competency of the team putting this together.

The last option is to then pair the digitised "list" into a traditional watchlist filtering engine and hope that the algorithms (developed for name matching) are sufficient. Most watchlist filtering engines can easily spot letter transpositions, misspelled words and word proximity through "fuzzy" logic. This, when paired with a project team's dedication in digitising the list, may ease a compliance officer's concerns about their capabilities to spot dual-use goods.

What do I do if I find a dual-use good?

The second question of what to do next will inevitably arise if a bank's systems flag up a dual-use good. The MAS guidance merely states that staff should be aware of the risks of dual-use goods and capable of identifying red flags that suggest dual-use goods are supplied for illicit purposes. Banks should have policies and procedures to spot dual-use goods in transactions whenever possible but the guidance offers little in the way of concrete measures

as to how to proceed. Next steps would be based on the bank's own discretionary measures. However, the question still remains, what can the bank do? This will require a deeper dive into the origins of dual-use goods.

As we said, dual-use goods can be defined as any good or technology which can have both commercial applications as well as military. At the macro level this can be evident in a country's capacity to militarise, such as automotive factories converted to building tanks and airplanes during World War II or civilian nuclear power plants producing enriched uranium that can be weaponised. The same technologies as well as the supply chains to support heavy industry, nuclear power and space exploration can be redirected towards advancing military technology.

At the micro level, this can be the terrorist groups smuggling chemical fertilisers such as ammonium nitrate to be used as explosives. The same materials used in agriculture or industrial manufacturing can be extracted and repurposed in biological or chemical weapons of mass destruction. Thus, international consortiums have joined together and offered guidance on the items that can have dual-use properties.

These are: the Missile Technology Regime (MTR) which covers delivery systems for weapons of mass destruction; the Organisation for the Prohibition of Chemical Weapons (OPCW) that identifies certain chemical compounds which can be weaponised into three schedules; the Nuclear Suppliers Group which seeks to prevent proliferation of materials, equipment and technology used in nuclear weapons; the Australia Group that seeks to identify exports which can contribute to the spread of chemical and biological weapons; and the Wassenaar Arrangement that promotes transparency in the movement of conventional arms and dual-use technologies.

Thus, the European Commission's Dual-Use Goods list (as well as other countries' controlled goods lists such as Singapore's Strategic Control List) combines the aforementioned list of items and segregates them into various categories. There are a total of 10 categories such as Category 0: Nuclear Materials, Facilities, and Equipment, Category 2: Materials Processing, Category 9: Aerospace and Propulsion, etc.

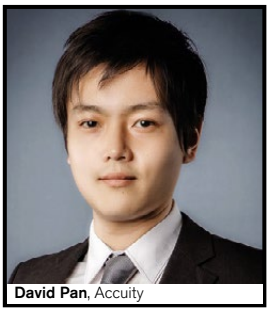
We see the reality of dual-use goods reflected in news headlines. Ball bearings found in a chocolate mixer confiscated in Port Ashdod before going to the Palestinian territories or ammonium nitrate-based fertiliser smuggled across the border to Afghanistan would fall into the low-tech terrorism-derived category for dual-use technology. While graphite rods shipped to Syria from North Korea (2012) and the Pyongyang Bio-technical Institute (a pesticide factory rumoured to be capable of producing military batch sizes of Anthrax) are clear examples of higher-technology dual-use goods meant to advance rogue state actors and their weapons of mass destruction.

Given these examples of the real end uses of dual-use technology, the question of how to proceed when alerted to the presence of dual-use goods is to treat it as a red flag. A red flag that will require the bank to put on an investigator's hat and place some context around the transaction including asking the right questions:

- Are the companies involved capable of producing weapons-grade dual-use goods or is this a false positive? For example, vacuum pumps produced by a retail appliance manufacturer would have different implications than ones produced by a company that also has a defence contract
- Is the nature of the dual-use good high technology or low technology? If low technology (radio micro-controllers or explosive/volatile materials), is it going to an active conflict zone or a country with close cultural ties around the conflict zone and in what quantities? If it is high technology (nuclear, ballistic missile, space) is it going to a country with an active arms embargo or sanctions?
- If the good has been clearly identified as dual-use and perhaps is seemingly going to violate embargoes, did the exporter provide the right customs documentation and export licences?

"At times, if enough red flags have been identified, a simple question by the bank may uncover further suspicious patterns of behaviours."

David Pan, Accuity



David Pan, Accuity

The dual-use good red flag can also be used to raise additional questions. Rogue state actors such as North Korea are known for evading embargoes by setting up complex agents and companies located in places such as Russia, Hong Kong, Macau, Vietnam and Singapore. At times, if enough red flags have been identified, a simple question by the bank may uncover further suspicious patterns of behaviours.

Although the main gatekeepers stopping proliferation of weapons of mass destruction through dual-use technology should be the exporters themselves, banks will nevertheless finance these transactions. Thus banks are in a unique position, with the leverage to stop proliferation by means of cutting off financing. Perhaps this is the reason that financial regulators are so interested in trade finance and have placed obligations on the banks to be aware of and, when possible, assist in this fight.

ACCUITY

Learn more about how Accuity helps banks identify dual-use goods at **www.accuity.com**

Come and meet us in September at Sibos 2016 at Booth A39 where you can test your knowledge on which everyday items could also have a military application.

We also look forward to being part of **GTR Asia** Trade & Treasury Week 2016 in Singapore and to taking part in **GTR** Mauritius Trade & Export finance Conference 2016 in November.