Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Big Data's Big Impact In Financial Investigations

Law360, New York (May 28, 2015, 10:41 AM ET) -- While the banking system is one of the main vehicles for moving dirty money, it is not the only one. Trade-based money laundering (TBML), the use of international trade to move value across borders in the form of goods or commodities and disguise the illicit origins of the criminal proceeds, remains a common way for money launderers to move billions in illicit "funds" across borders. Detecting trade-based money laundering poses a significant challenge for financial institutions, other businesses, and law enforcement. Used properly, big data analysis can be an effective tool to detect trade-based money laundering and other illegal financial activity.

Big data is best defined as the emergence of new datasets with massive volume that change at a rapid pace that are very complex and exceed the reach of the analytical capabilities of commonly used data management tools.

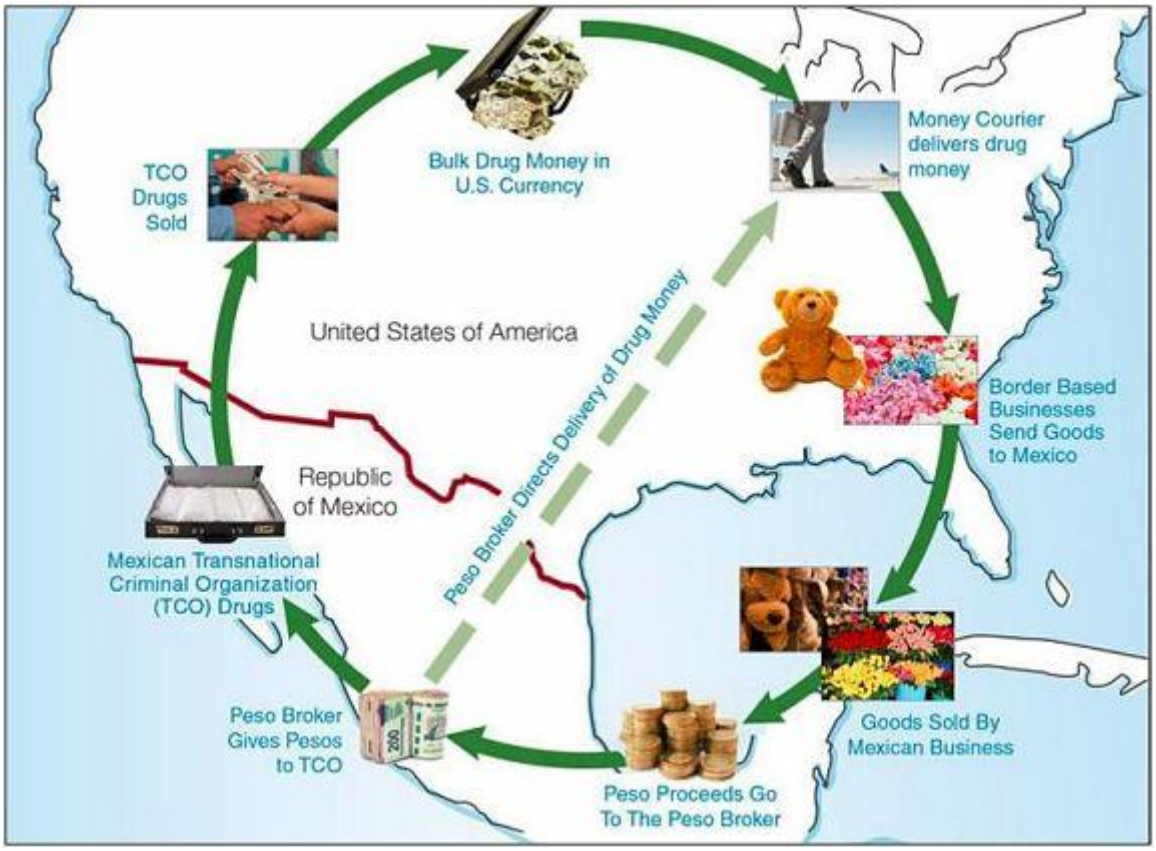
A series of high-profile decisions by the U.S. Department of Justice against BNP Paribas, JP Morgan Chase, Barclays and other large, global banks resulting in multibillion dollar fines has brought anti-money-laundering (AML) to the top of the financial services industry's priority list. However, financial institutions are not the only victims of money laundering schemes — many nonfinancial businesses are confronting money laundering risks as well, particularly those that engage in international trade. Due to the more extensive and effective AML controls that financial institutions are applying to fight money laundering schemes and financial system abuse, criminals are increasing their reliance on the time-tested method of trade-based money laundering because it proves tricky and more difficult to track. Analytical tools of modern data science can increase the efficiency and power of investigations of financial flows to uncover disguised, illicit transactions.

How It Can Work

Criminal and terrorist organizations and money launderers engaging in TBML are helped by the sheer magnitude of global trade, the growth of free trade zones, the large differences in financial and commercial controls in various countries, the ability to mingle legitimate and illicit funds, corruption and the low risk of detection. Sometimes the goal is to evade taxes; often it is to get dirty money into the banking system or move it from one person to another. Similar to directly laundering dirty money through the financial system, TBML typically occurs in three stages: placement, layering and integration.

Placement involves the introduction of criminally derived funds into a legitimate enterprise (e.g., purchasing the goods or commodities with the proceeds of illegal activity). Layering involves the movement of criminal proceeds to distance them from their source (e.g., shipping the goods or commodities to another country). Integration involves the reintroduction of criminal proceeds into the legitimate economy in a way that makes them appear legitimate (e.g., selling those goods or

commodities in the other country to generate “clean” proceeds in that country). This is an illustration of laundering drug proceeds through TBML:



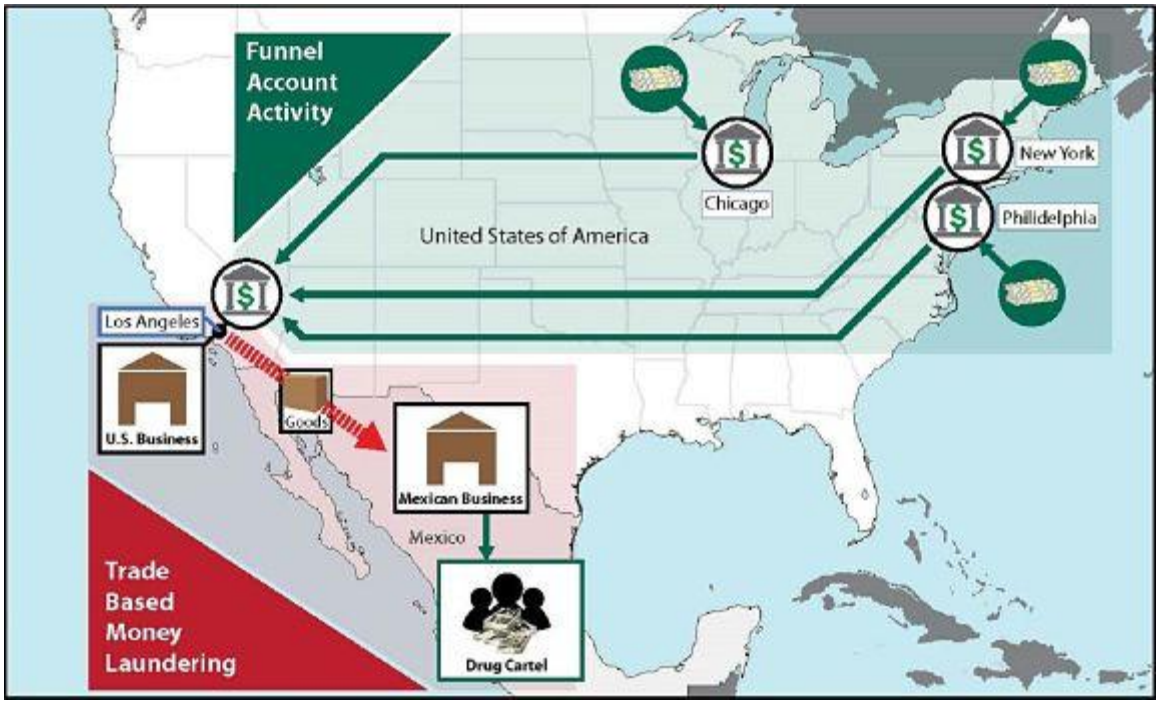
Source: Trade-Based Money Laundering Graphic from oag.ca.gov

One of the basic techniques is mis-invoicing. This is one of the oldest methods of fraudulently transferring value across borders and remains a common practice today. The key element of this method is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter. A front company for a cartel in country X might sell $1 million worth of products to an importer in country Y while creating paperwork for $3 million worth, giving it cover to send dirty $2 million back home.

Another common technique is multiple invoicing. This involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer is able to justify multiple payments for the same shipment of goods or delivery of services. Other common TBML techniques include over and under shipment, as well as false description of trade goods.

To help facilitate laundering dirty money, criminals may employ several tactics that include the use of shell companies, front companies and funnel accounts. A shell company can be loosely defined as a legal entity that exists primarily on paper, with no place of business or significant operations or assets. Shell companies help obscure money launderers’ identities while providing a business identity through which to create trade networks. Shell companies incorporated in tax havens can take advantage of those jurisdictions’ bank secrecy rules. Front companies on the other hand are actual functioning businesses that may be wholly or in part legitimate, but are controlled or operated on behalf of criminals. Criminals

may also employ funnel accounts — individual or business accounts in one geographic area that receive multiple cash deposits and from which funds are withdrawn in a different geographic area. This fragmented nature of trade financing arrangements, in which a single transaction may involve multiple banks in multiple roles, further limits any one institution's ability to design reliable identification tools. Funnel account usage looks like this:



Source: Trade-Based Money Laundering Graphic from oag.ca.gov

The annual dollar amount laundered through trade is estimated into the hundreds of billions. Between 2004 and 2009, approximately 17,000 suspicious activity reports were filed with the U.S. Treasury's Financial Crimes Enforcement Network regarding potential TBML aggregating over $276 billion.

Strategies for detecting TBML include: exploring whether financial flows are consistent with expected business activity; determining whether direct payments for the goods are being made to unrelated third parties; and distinguishing payment sources or beneficiaries that are hard to identify and/or are located in a high risk geography.

How Can Big Data Help?

Big data analytics can peel back the layers of a multibillion dollar industry and help financial institutions and other businesses find these illegal transactions. Whereas the boom in big data analytics has been largely driven by consumer information based ad targeting and marketing, similar tools can be applied usefully to money laundering and other data intensive fraud investigations.

The challenge lies in identifying the questionable transactions within the haystack of the massive global trade business. The mining of big data is a critical component of an effective anti-TBML program which involves extracting and analyzing data that is both structured and unstructured and that resides both in-house and externally. The ability to assemble, standardize and integrate massive amounts of transaction

level data from different sources is essential. Statistical techniques can then be used identify patterns and linkages potentially indicative of TBML activities that would be hidden or difficult to detect with traditional methods.

Integrating data from multiple sources into a single big data platform will expand the range of analytics that are possible. For example, linking email and financial transaction data, or more simply combining financial records from multiple countries or institutions. Uses of analytics that can help uncover anomalies or patterns that may be indicative of illicit activity include the following:

- Frequent transactions in round to whole dollars; negotiable instruments in round numbers under $3,000 used to fund transactions; sequential numbers or missing payee information;
- Discrepancies between descriptions of goods on transport docs, invoice or other shipping/packing documents;
- Patterns of international wires received as payment for goods into U.S. accounts or through U.S. correspondent or intermediary accounts;
- Ordering parties living in country different than originating country;
- Fund transfers into domestic U.S. accounts moved out in same amounts, often to high risk countries;
- Foreign businesses with U.S. accounts receiving payments from outside geographic customer base;
- Deposits showing evidence of funnel account activity; and
- Multiple cash deposits per day; particularly in multiple branches.

A key technique is to construct fuzzy metrics or probabilistic measures of suspect activity that do not depend on exact matching or require the source data to be complete or of high quality. Investigative analytics designed to identify financial flows and patterns of trade in the data can be very effective with identifying every transaction. Big data analytics can also be used to direct manual investigation efforts on certain activities that have the highest value probabilistic measures. Combining big data analytics with traditional investigative techniques may significantly reduce the number of false positives a financial institution devotes resources to needlessly investigating.

Network analytics can be used to map how emails or financial transactions between individuals or entities trace out chains of sequential communication and financial flows not otherwise easily visible. Graphical representation of network interconnections and flows can quickly identify important channels and intermediaries and identify new targets of investigation.

Another powerful, statistics-driven approach is transaction price analysis in which a bank's trade finance transaction details are benchmarked to detect unit prices anomalies outside global or regional norms. Unit-weight analysis can be employed to detect over or under shipment. Such discrepancies and outliers can help identify suspicious trading activity.

Data mining, network analysis and algorithms designed to assess probabilistic measures of suspicious activity in financial transaction data, can both improve the productivity of limited investigative resources and increase the power of investigations to uncover hidden patterns of fund flows. Whether used to after internal investigations or prior to them to monitor and prevent illicit activities, big data analytics and data science have wide applications to enhance anti-money laundering practices.

—By Mark Sarro, Rand Ghayad, Paul Hinton, The Brattle Group, and Kevin Rosenberg, Lowenstein & Weatherwax LLP

Mark Sarro is a principal in the Brattle Groups's Cambridge, Massachussetts office.

Rand Ghayad is an associate in The Brattle Group's Cambridge, office.

Paul Hinton is a principal in The Brattle Group's New York office.

Kevin Rosenberg is chairman of Lowenstein & Weatherwax's government investigations and white collar litigation group and is based in Los Angeles.