DOJ'S USE OF DATA ANALYTICS FOR PROSECUTIONS BECOMES THE "NORM"

The Fraud Division of the U.S. Justice Department unsealed an indictment recently that charged three traders associated with a global U.S.-based bank with a racketeering conspiracy that involved alleged manipulation of the precious metals markets through "spoofing." The indictment alleges numerous specific instances of spoofing, over an approximately eight-year period, intended to improperly affect prices for precious metals and related options. The U.S. Commodity Futures Trading Commission filed a parallel civil action against the three traders as well, likewise charging violations of commodities law reflecting attempts at market manipulation.

In announcing these charges, the head of DOJ's Criminal Division, Brian Benczkowski, said this prosecution demonstrated the results of DOJ's and the FBI's increasing use of data analytics to develop prosecutorial leads. Speaking to reporters, Benczkowski said that he "expect[ed]to use it more in looking at other financial products and other trading behavior at desks at major financial institutions." He emphasized that "[t]his is the type of case and the use of data that we expect to become the norm in the Criminal Division in the future." (*Law360*, 9/16/19)

According to the press report, Benczkowski also encouraged banks, trading firms and other financial institutions to begin scrutinizing their own trading data, so that these institutions can detect possible misconduct and self-report it to the relevant authorities if appropriate – before it gets discovered by the authorities through a whistleblower or other means. The type of historical review suggested, often called a "look back," permits a financial institution or trading firm to ensure that it has rooted out any particularized historical misconduct, and that it has in place sound trading and surveillance systems that comply with applicable laws and regulations.

The need for timely self-reporting by financial institutions is particularly acute, given their obligations to supervisory agencies such as the Securities and Exchange Commission, Office of the Comptroller of the Currency, Federal Reserve, or New York State Department of Financial Services. Indeed, last year, New York DFS granted significant cooperation credit to Deutsche Bank AG in connection with its self-reporting of various trading misconduct in its foreign exchange business – including spoofing.

In our experience, conducting look backs of trading or transaction data may identify particularized misconduct or compliance deficiencies that can elude ordinary surveillance systems and protocols. A look back typically involves:

- Gaining an understanding of the financial institution's systems and controls for the relevant trading or transactional system;
- Conducting a tailored review of the relevant data by the analytics team;
- Counseling from the consultant on deficiencies that may be identified and the means to improve them;
- If requested or appropriate, a written report laying out the results of the historical review and written recommendations for improvement.

Done properly, a look back can be relied upon when dealing with government authorities or self-regulatory organizations. In light of the recent guidance issued by DOJ for evaluation of corporate compliance programs in connection with DOJ investigations, a reliably performed look back may best position an institution to minimize the consequences of a possible enforcement action by DOJ or another enforcement agency.