CORPORATE COUNSEL
An ALM Website
corpcounsel.com | June 12, 2017

BATTENING DOWN THE SHIP, A 2017 CORPORATE INVESTIGATION PLAYBOOK

Dan Panitz, Esq.
dan.panitz@unitedlex.com
(212) 226-2928

BY DAN PANITZ, UNITEDLEX,
AND H. BRUCE GORDON,
TEVA PHARMACEUTICALS

Few things in life are as certain than death and taxes. While corporate investigations may not rise to these levels of life certainty, they create stormy seas resulting in unanticipated resource costs and financial damage/exposure to shareholders globally which can cripple a business, remove its C level suite or even spell the sinking of the ship.

This article opens a discussion on practical considerations for corporate investigations balanced against known trends in government enforcement in the waters that lie ahead.

Governmental Enforcement Weather Forecast

In 2016, the Department of Justice negotiated 35 corporate nonprosecution agreements and deferred prosecutions. Of the 35, 18 required a corporate monitor. In addition to the DOJ, many other federal, state and local agencies, including the state attorneys general, state financial regulators (e.g., the New York Department of Financial Services and New York Department of Insurance) and local agencies (e.g., the New York City Department of Investigation), impose monitors on corporations. Many other agencies, including the SEC, EPA, Department of Defense, Federal Reserve, OCC,and Federal Trade Commission impose monitorships.

Anti-bribery and corruption (ABC) investigations have become increasingly international. Cooperation among regulatory authorities around the world is now the norm and the great majority of DOJ FCPA settlements over the past three years have been with non-U.S. based companies. The DOJ is widening the industries it is investigating for FCPA,

particularly life sciences and financial companies.

On Feb. 8, The U.S. Department of Justice issued a document called evaluation of corporate compliance programs. This document includes 11 key compliance program evaluation topics, with a corresponding set of "common questions" that the DOJ considers relevant in assessing compliance programs within the context of a criminal investigation. According to Anthony Bosco, a N.Y.-based attorney and compliance expert, it is likely the DOJ views its guidance as a "floor" rather than a set of best practices. Bosco goes on point out that companies whose compliance programs don't exceed these guidelines cannot expect to receive maximum credit when it comes time to negotiate a plea with the government.

All prosecutorial and regulatory agencies are increasingly emphasizing enterprises' responsibility for monitoring risk posed by third-party vendors. To the extent the federal government backs off on regulatory enforcement, several key states are ready to step in, notably the attorneys general of California, New York and the New York Department of Financial Services. This trend, combined with the greater prevalence of whistleblower and bounty programs, will continue to generate a steady flow of corporate investigations.

U.S. government agencies are using increasingly sophisticated techniques to mine large databases to identify wrongdoing and bring cases. Companies that don't effectively analyze this data to build state of the art surveillance programs will come under increased regulatory pressure and face more severe sanctions.

Battening Down the Ship

Assuming a goal to stay out in front of problems, data analytics are the first step to obtaining and understanding the information needed to confront a potential corporate issue and create/maintain effective compliance monitoring programs. In a sea of ever-expanding digitized information, data analytics enable corporations to identify problem transactions in real-time and problem employees before they break the law.

Beyond solid corporate data retention/disposition schedules being established and enforced, what specific data monitoring practices help prepare for a corporate investigation at some point downstream? We believe a safe course would be to monitor and retain logs for 60-90 days on the following:

- All user login activity (both on network and remote VPN);
- Internet activity from corporate devices and BYOD devices on which corporate information resides; and
- All USB devices.

Other recommended buoyant practices include synchronizing all local file storage with network storage. This is particularly well suited for frequent corporate business travelers who need to take documents with them, yet need to ensure the latest copy is properly backed up to network storage the next time they are online. Corporate travelers should also use secure self-encrypted USB storage devices for the transfer of data—with asset tracking of all devices assigned to an individual. This eliminates the need to later search local hard drives if an investigation subsequently bubbles up.

Protecting The Family Jewels

It's no secret that IP theft can change the course of first

market mover advantage when one company operationalizes an innovation before another. The technology involved in self-driving vehicles might come to mind, but we see this issue in pharmaceuticals, manufacturing and even fintech to name a few verticals.

Locking down your IP should include reviewing and organizing all corporate network access rights assigned to individuals in order to minimize access to key network data stores. Set up appropriate active directory groups per department and sub teams so that data access is properly restricted to that which is needed to perform one's job duties. This access should be reviewed at least annually. Consider front-end web access to filter and restrict access to large back-end IP data stores and in the most draconian situational needs, block the use of external computer and laptop ports including Bluetooth and wireless connections.

Casting the Net

The complexity of collecting, processing and reviewing electronic data in a global investigation requires the establishment of a protocol, otherwise known as a scoping plan, for how custodial data is selected for preservation or collection.

• First categorize what data is available, where it is located and how the data can be collected and reviewed legally (Some jurisdictions have strict data privacy laws or blocking statutes: see our earlier Articles on Privacy Shield and GDPR).

• The location of data and the client's data storage architecture are paramount here. This includes, for example, the physical location of servers, backup tapes, returned laptops, external hard drives and cloud storage facilities.

• Third Party Information—Categorize third parties involved as to potential information available. The degree of control over these persons will likely vary from substantial to none and this will affect access to needed information. Decisions must also be made as to the extent to which the investigation must encompass such persons, who would typically be outside the scope of available privilege.

In the example of IP theft (and whistleblower investigations in part), we should include email and forensic device imaging and searching as well as login tracking, web surfing tracking, time card logs, and site badge access checking. We might also isolate and include attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; unauthorized use of a system for the transmission, processing or storage of data, and; exporting or making illegal copies or downloads of software.

What's In Davey Jone's Locker?

A new approach has been validated regarding data analysis methodology, eliminating uncertain total project costs from data hosting and review on which traditional e-discovery processes fail. Specifically, it's now possible to identify, analyze and isolate relevant data prior to data hosting and review costs being incurred.

This enables corporate investigational cost certainty from the outset of an investigation, which previously might have yielded open ended financial exposure.

With this innovation in investigational process cost certainty, as distinguished from wholly separate potential governmental fines/penalties or civil liabilities, individual and programmatic approaches to corporate investigations can now be achieved

at greatly reduced costs (in the range of 25 percent-plus cost reduction).

External Production and Disclosure

The DOJ and SEC have long encouraged companies to timely disclose any FCPA violation and cooperate during the government investigation process. The decisions of whether, when and how to self-report to the government or the investing public, however, should be made carefully, weighing all potential benefits and drawbacks. Counsel should consider numerous factors, including:

- The seriousness of the misconduct.
- The materiality of the amounts paid to the foreign official and the materiality of any contracts arguably tainted by the payments at issue.
- Whether the misconduct was endorsed by top executives or merely a rogue sales agent.
- Whether the government is likely to find out about the misconduct through its own investigations or a whistleblower.
- Whether the disclosure and potential government investigation is likely to subject the company to follow-on civil litigation.
- That self-reporting almost always triggers a formal government investigation, which may be expansive and costly, especially if the scope of the misconduct is not fully understood.
- In cases of minor violations by rogue actors, companies often will choose to investigate and self-remediate, carefully documenting their work. In cases of more serious misconduct, companies that self-report early, work on fixing the problem and cooperate in the government's investigation often are rewarded by lesser fines and avoiding charges. If counsel and the client decide self-reporting is the best route to take, however, they should consider the possible privilege implications, as well as any relevant requirements under the Sarbanes-Oxley Act of 2002 (SOX).

Sailing Safely Back Home

Utilizing sound data monitoring/analytics, proper data collection scoping strategies and cost reducing innovations to assess data, protocols can be established to batten down the ship and effectively navigate in front of problems before the issues become unmanageable.

Dan Panitz, UnitedLex VP, Global Legal Solutions*, is an experienced attorney based in New York with more than 20 years of combined legal, technology and corporate advisory experience. Having worked with SEC Enforcement and NASD (now FINRA) Arbitration, Dan also holds Anti-Bribery & Corruption specialty certifications for the PRC, UK and the US.*

H. Bruce (HB) Gordon *currently works for Teva Pharmaceuticals located in Horsham, Pennsylvania as their Manager, ESI Response Management. Prior to Teva, HB worked for Amerisource-Bergen Corporation as the IT Liaison to the Legal Department, and Rohm and Haas Company as the IT Manager for the Legal Department.*