

MANAGING AN FCPA INVESTIGATION BY THE US GOVERNMENT

The US Department of Justice, the Securities and Exchange Commission and the FBI have shifted enforcement of the FCPA from self-reported violations to active investigations, resulting in five times more FCPA-related actions since 2004.

Robert Brown reports

Increasingly, Foreign Corrupt Practices Act (FCPA) investigations focus on a range of US corporations doing business across international borders. The highest concentration of recent FCPA investigations have targeted companies doing business in countries known for corruption. However, the FCPA has been applied to executives, international partners and joint ventures, as well as companies based outside of the US that issue securities or publicly-traded bonds in US markets.

An FCPA or related investigation is a high profile case involving government officials, at times from multiple jurisdictions, and it is the collective responsibility of IT, risk and security managers to mitigate exposure by understanding the law and its applications as well as preparing a best-practices response. The nature of electronic data and communications compounds the issues facing corporations and executives charged with the self-investigation process. Developing an appropriate strategy in response to an FCPA investigation must take into account various local and international regulations, compliance and legislative procedures. This can be particularly difficult in light of more robust privacy and intellectual property laws.

As business interests expand into global markets and information technology continues to evolve, even the most astute legal professionals are challenged by the broad language and vague guidelines of the FCPA. One of the best safeguards in preparing an appropriate response to an FCPA investigation is securing capable and experienced partners. Partnering with a comprehensive, single-source vendor that is not only familiar with the technical aspects of data

collection, review management and production, but also with the litany of local and international laws is essential.

Introducing multiple vendors compounds risk as the intersection of responsibilities can be vague and each process is dependent on the previous processes. Misunderstandings can lead to the impression of non-compliance. The consequences of poor compliance are not limited to bad publicity and large penalties. A corporation found to be less than fully cooperative will lose both logistic and strategic control of the process and at times of its data, resulting in the potential disclosure of valuable information such as intellectual property and trade secrets.

When a company controls the review and disclosure process, the data produced to an investigative body is limited to specific custodians and issues. Conversely, when the review is performed by an outside entity, the business impact of having to expose an entire data set could be catastrophic.

There are a number of key legal and logistical issues to consider in preparing for and responding to the unique challenges of an FCPA investigation:

- understand your compliance objective and the legislative issues involved;
- implement a proactive response including a repeatable discovery process;
- identify, isolate and manage the appropriate information;
- develop a legally defensible strategy for collecting and preserving data;
- recognise the limits of local and international law;
- anticipate a potential disruption to general business operations; and
- plan an appropriate post-investigation stance.

The most important element in responding to an FCPA investigation is a demonstrated and informed readiness to cooperate. The greatest threat is not enforcement actions, but losing the confidence of investigators and compromising the control of the investigative process. It is in every corporation's best interest to evaluate operating and data management procedures to formulate a comprehensive strategy. ■

Robert Brown is Technical Expert with First Advantage.