Cooperation: The Defendable Investigation

Reprinted with permission. An extract from *The Asia-Pacific Investigations Review 2018* published by Global Investigations Review

In simple terms, an investigation is all about finding the facts. This includes the identification of the who, what, where, when, why and how. But the reality for a company and their legal counsel to find the answers to these questions is usually complex, especially when a regulator is involved. While the underlying conduct that has caused the regulatory investigation to commence is a key point in deciding what action a regulator will take against a company, so too are self-reporting, cooperation and remedial efforts. This article deals with cooperation, and specifically, considerations for a company and their legal counsel in conducting a defendable internal investigation.

Whether the company is responding to a regulator for alleged breaches of anti-corruption laws like the US Foreign Corrupt Practices Act of 1977 (FCPA) and the UK's Bribery Act 2010, sanctions, money laundering or violations of other white-collar crime regulatory concerns, cooperation is effectively built on the company's response to the regulator about its internal investigation methodology and protocol.

Whether the company is responding to a regulator for alleged breaches of anti-corruption laws like the US Foreign Corrupt Practices Act of 1977 (FCPA) and the UK's Bribery Act 2010, sanctions, money laundering or violations of other white-collar crime regulatory concerns, cooperation is effectively built on the company's response to the regulator about its internal investigation methodology and protocol.

In their co-publication with the US Department of Justice (DOJ), titled 'A Resource Guide to the US Foreign Corrupt Practices Act', the US Securities and Exchange Commission (SEC) states that cooperation means, among others, 'providing SEC staff with all information relevant to the underlying violations'. With the DOJ, they specify that cooperation includes 'the company's willingness to provide relevant information and evidence'.

In addition, the DOJ discuss cooperation in guidance for their FCPA enforcement pilot programme. Notably, they mention a company under investigation should demonstrate, among others, 'Proactive cooperation, rather than reactive; that is, the company must disclose facts that are relevant to the investigation, even when not specifically asked to do so, and must identify opportunities for the government to obtain relevant evidence not in the company's possession and not otherwise known to the government.'

Although the scale of bribery differs, a contrast in cooperation is illustrated in two FCPA cases involving inappropriate conduct in Asia. The first involves a French power and transportation company, which in late 2014 paid a fine of over US$700 million to settle charges that it violated the FCPA in Indonesia, Taiwan and other countries. The criminal fine, which is the largest imposed to date in an FCPA case, was so large in part due to the company's refusal to fully cooperate with the DOJ's investigation for several years. It only began cooperating after the DOJ publicly charged several of its executives.

In the second case, a US technology company self-disclosed to both the SEC and DOJ that bribery had been committed by their China subsidiary in dealings with officials of state-owned entities. Despite the fact that bribery had been committed, the DOJ announced in 2016 that the company would not be subject to any penalty while the SEC announced a non-prosecution agreement. The DOJ noted the company's 'prompt voluntary self-disclosure of the misconduct, the thorough investigation and fulsome cooperation' and the SEC stated they 'cooperated extensively'.

What do you do with all the data that is collected? The use of a centralised review platform can expedite a company's obligations to identify the who, what, where, when and how. With potentially millions of records to review, utilising a platform that allows the ability to quickly search for key people, words and dates is mandatory.

So what does a thorough, and thus defendable, internal investigation look like? In the case of the US technology company, the DOJ specified it included 'identifying all individuals involved in or responsible for the misconduct and by providing all facts relating to that misconduct'. While engaging legal counsel is a necessity to help the company navigate its interactions with regulators and other legal aspects, they will generally require assistance with identifying and reporting on the facts. Such assistance can be provided by incorporating a forensic response.

The Forensic Response

Fraud, bribery and many forms of misconduct associated with white-collar crime are usually identified in, and evidenced through, the financial and accounting records of a company. As such, forensic accountants are often engaged to assist with financial data analysis and other fact-finding tasks. The forensic accountants should work at the direction of counsel to maintain attorney–client privilege over the investigation so as to avoid involuntary disclosure of investigation findings. The in-depth and objective analysis that a forensic accountant performs will help uncover trends that bring to light the issues that have caught the attention of the regulator. This may involve reconstructing a series of transactions or checking the appropriateness of how any improper activity may have been reflected in the financial statements. Key witnesses and subjects will also need to be interviewed to provide information regarding the issues.

But the forensic accountant does not act alone. Other professionals will be involved to ensure evidence is identified, forensically collected and thoroughly analysed. An overview of the additional skillsets that round out the forensic response is provided below.

Computer Forensics and E-discovery

The validity, defensibility and objectivity of evidence are crucial in responding to a regulator. Computer forensics specialists – experts in handling and analysing digital evidence – collect, analyse, and report on digital evidence in a forensically sound manner (ie, collected, analysed, handled and stored in a manner that is acceptable by the law).

Digital evidence is crucial in investigating key subjects and understanding their conduct that has seen the investigation arise. It also helps identify additional key players. Such digital evidence is obtained from multiple sources (eg, the company's email servers, from the cloud, or personal devices such as laptops, mobile phones or tablets for SMS and other messaging applications). This can be voluminous and unwieldly. Collecting digital evidence, which is volatile, can be challenging. Without proper care, data spoliation may occur. This in turn may open undesired regulator queries as to the validity and objectivity of the evidence being presented by the company. In proving or disproving key facts, utilising computer forensic specialists mitigates the risk of key digital evidence being discounted, providing defensibility.

What do you do with all the data that is collected? The use of a centralised review platform can expedite a company's obligations to identify the who, what, where, when and how. With potentially millions of records to review, utilising a platform that allows the ability to quickly search for key people, words and dates is mandatory. Applying analytics that are integrated into a review platform is also critical. Examples include:

- Deduplication, near deduplication, email threading: the removal of duplicated emails or documents so that an investigation team is only reviewing one copy of an email. This also groups similar documents together, for example, multiple versions of a contract Word document, or groups a 'back-and-forth' email chains. This saves time and costs;
- Concept clustering: using the contents of communication between key players, concept clustering groups conceptually-like documents together. For example, all documents related to sales opportunities, expenses, transactions, or outliers – perhaps suspicious – are grouped together for review; or
- Artificial intelligence and predictive coding: with the millions of records, a sample of this population is reviewed by senior members of the investigation or legal team for 'hot' documents. That sample is then applied to the remaining population and the artificial intelligence system predicts and returns similarly 'key' documents. This saves time and costs, whereby the entire population does not need to be reviewed, and in some instances, provides for greater accuracy.

Data Analytics

Data analytics are an essential part of an investigation. Using targeted querying of the company's databases, patterns can be efficiently identified that may be signatures of improper activity.

Data analytics involves the transformation, analysis, and visualisation of complex data to reveal actionable insight in an investigation. It is used to provide a deep understanding of the company's financial data and how the data is collected and used by the company. This data will provide additional insight through complex analysis, data mining for specific transactional activity, and the ability to define relationships across multiple disparate data sources, both internal and from third parties.

Typically, data analytics in an investigation will involve:

- Identifying, acquiring and normalising relevant data;
- Identifying the relationships between multiple sources and data points;
- Designing and implementing appropriate tests and triggers to identify suspected transactions; and
- Providing a platform for the review and investigation of these transactions by the forensic accountants and potentially counsel and other stakeholders in the investigation.

Business Intelligence

Not all investigations are created equal. At the early stages of a regulatory investigation, the investigation team will generally have good and quick access to internal data, financial and accounting records and other information. But there are many instances where they do not and other means are required in order to progress the investigation. One of the key components to help progress an investigation is the use of business intelligence.

Business intelligence effectively involves an investigator discreetly gathering actionable intelligence externally related to key subjects or entities without unnecessarily alerting employees and others. The discreet nature of the methodology used also lowers the risk of evidence being destroyed that could be material to the investigation. Such intelligence may include identifying corporate information (including key principals and shareholders or ultimate beneficiaries), track record, business reputation, business and political connections, financial health, business strategies, involvement in nefarious activities (money laundering and bribery and corruption), involvement in litigation and bankruptcy or at the very least verify the bona fide of the company. It could be crucial in identifying additional key subjects for the investigation.

Undertaking investigations in more challenging jurisdictions, where publicly available and reliable information is limited, requires a well-structured and often times creative intelligence gathering exercise to allow the investigator to identify any undisclosed business relationships or interests as well as ascertain the source of wealth and possibly assets if asset recovery is required.

Having experienced investigators with a good understanding of local cultural context as well as the necessary language capabilities cannot be over-emphasised. Experience has shown that such capabilities speed up the investigation process and allow the intelligence-gathering exercise to progress efficiently. It also allows the investigators to fully appreciate the context of the information identified and decide on its relevance before allocating the necessary resources.

Determining the Scope and Approach

A company's internal investigation requires more than just incorporating a forensic response in order to demonstrate proactive cooperation to a regulator. Thought must be applied in determining the scope to ensure the skillsets described above are deployed appropriately. Determining the scope may involve formulating theories to prove or disprove allegations and reaching appropriate conclusions. This should involve thinking outside the box to devise a thorough investigation work plan. In turn, this will enable the facts to be presented in a clear manner that is understandable and properly supported by the evidence.

Experience shows that if you are able to clearly articulate and demonstrate an innovative approach, especially one that is technology-driven, regulators will be more than willing to listen, as they know that this will bring greater clarity and new insights. Below are examples of innovative approaches involving a forensic response that have helped companies demonstrate their cooperation by conducting defendable internal investigations.

Experience shows that if you are able to clearly articulate and demonstrate an innovative approach, especially one that is technology-driven, regulators will be more than willing to listen, as they know that this will bring greater clarity and new insights.

Just Too Big

A multinational pharmaceutical company was required to investigate whistleblower allegations of improper payments made in China. The nature of the allegations, along with the scale of the company – involving thousands of employees – and the duration of the investigation – spanning multiple years – created a vast population of millions of transactions. This was a clear situation where the volume of data would simply be overwhelming for a manual paper-based approach.

The solution developed focused on using technology to accelerate the review process. The investigation started with using data analytics to risk rank the employee expenses. For each employee selected for further review, a dashboard provided a detailed review of their respective transactions including trend lines of their expenses over time and the identification of specific transactions of risk that required further testing. Counsel was also able to incorporate the dashboards into their interview preparation process. The regulator understood the magnitude of the work required to complete a more traditional 'paper' review and were able to support the alternative 'data' approach.

Is There a Problem

Media reports implicated the company in a major corruption scandal that was making headlines across the globe. The company wanted its investigatory response to consider expenditure at one of its overseas facilities to identify potential indicators of bribes being paid. Given the volume of transactions at this particular facility, it was not practical for every payment to be scrutinised. Accordingly, a risk categorisation was developed for each of the 1,500 vendors used by the facility in order to understand the relative risk for each respective company–vendor relationship. This risk ranking, developed by way of a Heatmap, included a review of the overall risk presented by each vendor and risks related to each of the specific payment transactions made to each respective vendor.

To build the Heatmap, data analytics were deployed. Tests across all transactions considered payments with round values, high-dollar and those that were with one-time vendors. They also considered whether payments to a particular vendor in total were below a certain threshold. In addition, tests considered keyword hits based on the payment description, the corruption risk that may be associated with the type of goods or services provided, and the reputation of each vendor identified through business intelligence analysis that considered any historical misconduct, fraud or corruption allegations. The vendors were then ranked according to their risk ranking. This relative risk ranking was used to understand which vendors should be subject to further scrutiny to assist with selecting the sample of transactions for forensic testing and thus ascertain whether bribes were being paid by the facility's management.

Spread Out

In a US export compliance investigation, the regulators ultimately needed to understand the scale of the controlled parts that originated in the US that were shipped to sanctioned countries by a technology company. In this case, defining that vast scale proved challenging. The majority of the information needed by the regulators was not readily apparent by looking at the paper documentation. Instead, it was spread throughout the company's IT infrastructure. Furthermore, all of these resided in separate IT systems that did not speak to each other. Getting the answer required connecting customer, shipping, manufacturing, procurement, and compliance data.

Once the data from the various IT systems was able to be connected, the process was documented so the regulators could better grasp how the company operated and what it was doing. Following this, robust data analytics techniques were applied to generate the required insights into the shipments to sanctioned countries by the company and what these shipments contained. Finally, the method- ology was validated using detailed testing by forensic accountants in order to confirm the data-driven approach. This was then followed up with a series of detailed presentations to educate and guide the regulators on the approach.

The majority of the information needed by the regulators was not readily apparent by looking at the paper documentation. Instead, it was spread throughout the company's IT infrastructure. Furthermore, all of these resided in separate IT systems that did not speak to each other. Getting the answer required connecting customer, shipping, manufacturing, procurement, and compliance data.

Determining the Value

An oil and gas company received a 'please explain' from a regulator after they became embroiled in a corruption scandal. Among others, the 'please explain' requested the company to specifically quantify the amount of bribes that had been paid. This was challenging for two reasons. Firstly, the bribes paid were contained in line items of invoices from a subcontractor the company engaged. These line items were not individually captured in the company's accounting system and the supporting documents were stored in a warehouse in a remote location. Secondly, the line items on the subcontractor's invoices were described in both a mix of common words used to describe bribes and local slang equivalents.

The solution to respond to the regulator's request involved building a database that listed all of the subcontractor's invoices paid by the company while the supporting documents for each payment were scanned. In turn, forensic accountants reviewed the scanned documents and identified the line items in the invoices that likely reflected the bribes being paid. This information was then inputted in the database, including the words used to describe the bribes. The database allowed the company to not only quantify the bribes paid but also assist with determining how and when they were paid. This approach enabled the company to demonstrate to the regulator the effort it was making to respond to the question as accurately as possible given the circumstances.

Conclusion

Should the unthinkable happen and the company find itself subject to regulatory scrutiny, the contrasting examples of the investigation responses discussed earlier and how that impacted the penalties imposed demonstrates why a company should cooperate. Appropriately incorporating a forensic response under the direction of counsel can help with making the company's internal investigation be defendable. This will enable the company to demonstrate cooperation by responding to the regulator with appropriate analysis and relevant facts. In turn, this should assist the company in its efforts to minimise or avoid any penalty and assist with a swifter resolution of the regulatory issues that are under investigation.

An extract from The Asia-Pacific Investigations Review 2018 published by Global Investigations Review
http://globalinvestigationsreview.com/edition/1001055/the-asia-pacific-investigations-review-2018

The authors wish to acknowledge the contributions of Jason Liew, Senior Managing Director, and Gino Bello, Senior Director, in drafting this article.

Jarrod Baker
Senior Managing Director
+65 6831 7802
jarrod.baker@fticonsulting.com

Brett Clapp
Senior Managing Director
+852 3768 4729/+65 6831 7890
brett.clapp@fticonsulting.com

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.