RANE
Risk Assistance
Network + Exchange

RANE Interviews

Fraud Prevention as a Competitive Advantage

Jonny Frank, StoneTurn

February 22, 2016

Jonny Frank specializes in compliance controls and monitoring at StoneTurn Group, which provides forensic and expert services to attorneys, corporations and government officials on high-stakes legal and compliance matters. Frank serves as the DOJ-appointed Independent Compliance and Business Ethics Monitor to a Top 5 global investment bank. He previously served as the NYS Department of Financial Services-appointed Independent Compliance Monitor to the nation's largest non-bank mortgage servicer. He also serves as forensic adviser to a NHTSA-appointed Monitor of a Tier 1 automotive supplier and the DOJ-appointed FCPA Monitor of a $250 billion oil and gas conglomerate and $6 billion medical device manufacturer. Frank was previously a partner at PricewaterhouseCoopers, where he founded and led the firm's fraud risks and controls practice. He is a former executive assistant U.S. attorney for the Eastern District of New York, and has served on the faculties of the Yale School of Management, Fordham University Law School and Brooklyn Law School.

⇒ *On the critical, underappreciated difference between "good" fraud and "bad" fraud…*

"Bad" fraud is conduct for which the organization faces either civil or criminal liability or that hurts its reputation. When an organization can root out "good fraud," by contrast, it can cut costs, increase revenues and protect assets and brand value.

Most companies focus on bad fraud – and very little on good fraud.

In the international space, for example, companies spend considerable time and resources on so-called "ABC" – or "anti-bribery and corruption" – programs. But whether or not the misconduct is classified as corruption or fraud requires compliance officers to follow the money. If large sums are paid to public officials, it's corruption. If an employee misappropriates funds, it's fraud.

Companies spend all their time and effort on potential corruption risk. But, from a pure risk analysis perspective, it doesn't make sense. Even with numerous FCPA investigations, and when you think of all of the companies that conduct business abroad, very few get caught for

corruption, whereas, all of them are losing money on the other types of fraud. Companies are missing the opportunity to focus on the fundamental business issues at hand.

⇒ *On how uncovering good fraud can be a lucrative transactional diligence tool…*

When it comes to M&A, think of good fraud in operational terms. For example, in due diligence, you may uncover that a target company is leasing space from the CEO's brother-in-law at a higher cost than market rate. If you negotiate a better lease after you buy the company, you've made a better deal because you have just decreased operational costs and increased value. Bad fraud (e.g. fraudulent financial reporting), in contrast, makes the deal less valuable.

It's all part of moving away from the idea that fraud is solely a legal issue; it's also a business issue.

⇒ *On the challenges and costs of fraud…*

One of the challenges of fraud is determining how much money is being lost. An aspect of fraud, by definition, is concealment. According to one study, the average multinational company loses about one-to-two percent of earnings to fraud.

Another great challenge for companies is "ownership" around fraud risk. When I act as a compliance monitor, management acknowledges they "own" fraud risk. If you talk to those same people in an informal setting and ask them about their roles related to fraud, they typically say the internal audit or legal department owns fraud.

Another major cost of fraud is lost opportunities. According to a number of recent studies, over two-thirds of companies do not enter a given market because they don't know how to control fraud in that specific location. On the other hand, when a company already has a presence in a "high-risk" market, and leaders are conscious that others are being defrauded, they often think it won't happen in their organization.

⇒ *On why companies are typically better at fraud investigation than prevention…*

A lot of companies hire former prosecutors for compliance roles. Having once been a prosecutor and conducted investigations early on, I did not appreciate the distinct differences between investigations and preventative measures. With an investigation, there's typically an allegation or suspicion. It's much easier to investigate a specific allegation or suspicion than it is to prevent or detect fraud in the absence of one.

The complexity between the two concepts is exacerbated by the fact that for-profit companies are in business for one reason: to make money. If compliance controls hinder the company's ability to turn a profit, the business will reject them. So, compliance officers are in the difficult position of trying to mitigate risk, while not inhibiting the company from increasing profits.

⇒ *On why remediation is often an afterthought…*

In a typical scenario, the company hires outside professionals to handle investigations; once the investigation is over, the idea of 'remediation' is usually discussed. But, by that point, the

company is so fatigued from the investigation, it just wants closure. As a result, it becomes vulnerable to the very same fraudulent activity.

We had this experience with a client – the exact same fraud scheme happened in Brazil and, again, in the Middle East. The company thought it was a coincidence; it never occurred to leadership that something was wrong in the system.

⇒ *On the growing importance of using data to prevent fraud…*

Data analytics and data mining represent by far the biggest evolution or change I've seen in my 36 years of examining fraud. Stay tuned because there is more to come…

Fraud risk assessments identify schemes and scenarios that, if they arise, significantly impact the business. A forensics and risk and controls expert can then help to determine red flags, and use the company's data to build "smoke detectors."

Let me give you an example. Some years ago, the State of Vermont engaged StoneTurn because it suspected some state troopers were abusing overtime. We compared overtime records with radio calls on cruisers to see if the troopers were actually in their cars when they reported working overtime; we very quickly saw a pattern -- certain troopers were collecting 10 hours of overtime every week for a two years in a row -- or collecting overtime when they weren't even in their cruisers. In this case, the proper controls and connecting of dots were not in place. The good news is we were able to identify the scheme right away, as well as the perpetrators.

Companies use data for all sorts of reasons, but few think to slice it for this purpose. In five years, it will be commonplace. The next step will be predictive fraud analytics; that is, prediction of fraud even without red flags.

⇒ *On how regulators will increasingly expect companies to implement compliance "smoke detectors"…*

Sooner or later – likely sooner - the government will start asking why companies do not employ proactive compliance data analytics. For example, a company could use data to determine how many instances of corrupt payments occurred around the world and self-disclose this information to the government. This information would highlight potential risks, which could be monitored, and regulators would be less likely, therefore, to declare the company's compliance program as fatally flawed.

There is currently a lot of movement in this direction. Leslie Caldwell has stated in recent speeches that she intends to substantially raise the bar. In her view, computer compliance programs are all too often focused on yesterday's issues as opposed to tomorrow's scandals.

⇒ *On why companies fail to uncover misconduct…*

Companies typically fail to uncover misconduct for one of three reasons: 1) failure to identify the risk; 2) over reliance on ineffective controls; or 3) failure to connect the dots.

⇒ *On the common mistakes companies make …*

Comply with what? Too often companies focus on regulatory compliance as opposed to compliance with a "Capital C," which includes:

- Compliance with general laws and regulations (local, state, federal, international)
- Compliance with contractual provisions
- Compliance with company processes and policies