Crowe Horwath

January 2017

Building Defenses Against Fraud in the Commodities Sector

An article by Matthew R. Bowser, CIA, CISA and Doug Nisley, CPA

Commodities fraud is an ancient problem, prompting, for instance, injunctions in the Quran and Bible against dishonest weights. But while the commodities industry has a long history of confronting dishonesty, a rapidly changing catalog of fraudulent activities is straining its ability to guard against such theft. Modern trading and technology, among other factors, have expanded the threat from fraud and put fortunes at risk.

Compared to financial commodities industries such as banking, the physical commodities sector generally is under less regulatory pressure to protect against fraud, perpetuated either internally or by outside thieves. In the United States the *Sarbanes-Oxley Act* requires, among other measures, an assessment of fraud in publicly traded companies, and options markets face specific regulations, but few regulations protect private companies from trading fraud from within. As a result, many companies have been lax in erecting defenses.

Losses can range widely. For example, Dutch grain-trading company Nidera reported an annual loss in 2015, its first in five years, because of rogue trading – a practice in which an employee makes unauthorized market deals – in biofuels that the company said cost it almost $200 million.[1] AFGlobal Corp., a manufacturer that serves the oil and gas industry, said that in 2014 an email scam resulted in a loss of $480,000.[2]

In commodities companies, fraud also often is the result of a lack of controls over the processes linked to contracts. Fraudulent contracts, contracts without proper accounting, and misstated contract terms within financial reporting have been common within the industry. Because so much of the business focuses on contracting future activity, controls over contracts are crucial.

Of course, losses at any time can pose severe risks for a company, but adding to the urgency, the recent increase in volatility in prices for many commodities has eaten into profit margins, making a robust defense against fraud of all types even more vital for the industry.

The Changing Face of Fraud

In ancient China, merchants guarded against buying wheat that had been soaked in water to increase its weight or purchasing loosely woven silk, which increased a bolt's length while lowering quality. Romans were alert to wine adulterated with lead to make it sweeter. But these simple frauds pale in comparison to the variety and sophistication of theft perpetrated today.

Traditional white-collar crimes such as padded expense accounts and bribery are just the tip of the iceberg. With modern technologies and markets, internal threats now include misappropriation of assets, for example, by rogue trading practices; fraudulent reports that manipulate performance results to reach incentive targets; and hiding disadvantageous contract terms to complete a trade.

Rogue trading, which infamously brought down Barings Bank in 1995,[3] poses a particularly insidious risk. This type of fraud can start with efforts to cover a bad market position, but generally greed is a clear factor, as traders can reap large commissions and bonuses from these unauthorized activities. Efforts to cover rogue trading may include manipulating mark-to-market valuations, making unrecorded trades, substituting lower-quality products, misstating freight or other costs, or some combination.

In addition, external threats have become much more varied with the onset of cyber crime. In particular, social engineering – in IT terms, playing on emotions such as friendship or fear to extract information – is a growing threat. Using mass emails masquerading as a bank or other trusted correspondent to solicit user names, passwords, and other valuable information, a practice known as phishing, is on the rise, as are its variants: spear-phishing, which targets a smaller group with more personalized emails, and whaling, which targets senior executives.

Symantec Corp., a cybersecurity company, has estimated that about 1 in 2,225 emails received by mining companies in 2015 was a phishing attack, almost equal to the ratio of phishing attacks in the finance, insurance, and real estate sector. Among the industries the company studied, mining had the highest percentage of spam, 56.3 percent of total emails, and about 1 in 300 emails to mining companies contained malware, again almost identical to that of the finance, insurance, and real estate sector. The company also estimates that across industries, about 429 million identities were exposed by cyberattacks in 2015, up 23 percent from the previous year.[4]

Three Lines of Defense

Without regulatory pressure to build a bulwark against fraud, many commodities companies have taken a relaxed approach to these threats. But as the threats become more sophisticated, the attacks more frequent, and the value at risk higher, a more aggressive strategy is needed. Commodities companies must establish defenses.

In a 2013 position paper,[5] the Institute of Internal Auditors described a model for effective risk management and control consisting of lines of defense across three fronts:

- **Front line:** The first line of defense lies with operational managers who are responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. These managers should take direct ownership of identifying and managing risk.
- **Middle office:** The next line of defense comprises middle office functions, specifically financial control, security, enterprise risk management, credit management, risk management, and compliance. Specialists in these offices use their diverse skills to design appropriate processes and support the front line.
- **Independent assurance:** Internal auditors make up the final line of defense. These experts are independent from other functions and verify that risk controls are followed and effective.

With these three lines of defense staffed and ready, companies can implement an effective anti-fraud program that is tailored to each organization's unique situation. The plan should assign clear responsibilities throughout the organization and be flexible enough to adjust quickly to change.

Among the crucial components of an anti-fraud program are clear policies and monitoring processes. Periodic performance assessments help companies detect problems and vulnerabilities, while targeted training and communications can prevent problems before they start. Confidential hotlines for reporting fraud and careful questioning during exit interviews also can alert managers to potential problems.

Internal controls to detect and prevent fraud can include restrictions on access to computer systems, rigid approval processes for trading and accounting systems, and routine reviews of any exceptions granted to standard policies and access to sensitive systems. In addition, purchasing transactions and approvals should be examined regularly by an independent auditor.

Cyberthreats also require companies to put in place specific protections. For example, a cyber resiliency program is a proactive initiative designed to anticipate potential vulnerabilities, prevent attacks, and prepare responses needed to minimize any damage from a successful attack.

Final Thoughts

Fraud has plagued commodities traders for millennia, and perhaps because of its long history, much of the industry may have become complacent in its defenses against these crimes. But modern trading and new technologies have put much more value at risk, including, in extreme instances, a company's very existence. Companies cannot wait for regulators to mandate more robust protections. By understanding the new variants of fraud and building defenses across three lines, companies can begin now to erect a strong bulwark against these modern criminals.

Connect With Us

Matthew Bowser
Principal
+1 317 208 2432
matthew.bowser@crowehorwath.com

Doug Nisley
Partner
+1 574 389 2510
doug.nisley@crowehorwath.com

[1] Isis Almeida and Javier Blas, "Grain Trader Nidera Reveals $200 Million 'Rogue Trader' Loss," Bloomberg, June 29, 2016, http://www.bloomberg.com/news/articles/2016-06-29/grain-trader-nidera-discloses-200-million-rogue-trader-loss

[2] Brian Krebs, "Firm Sues Cyber Insurer Over $480K Loss," Krebs on Security, Jan. 18, 2016, http://www.krebsonsecurity.com/tag/business-email-compromise/

[3] Adam Bradbery, "Lessons of the Barings Bust," The Wall Street Journal, Oct. 2, 1996, http://www.wsj.com/articles/SB844199491848285500

[4] "2016 Internet Security Threat Report," Symantec, April 2016, https://www.symantec.com/security-center/threat-report

[5] "IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control," Institute of Internal Auditors, January 2013, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf