Curtis C. Verschoor, CMA, Editor

New Report Shows Changing Fraud Environment

The latest *Kroll Global Fraud Report* shows that the incidence and cost of fraud have decreased over the last year, yet fraud still remains an important issue for all companies around the world. And a DOJ suit against Standard & Poor's highlights the need for oversight of the credit rating industry.

For the past six years, security consulting firm Kroll Advisory Solutions has commissioned the Economist Intelligence Unit to perform a global survey of fraud incidence. The 2012-2013 *Kroll Global Fraud Report* is based on a poll of 839 worldwide senior executives from a broad range of industries and functions—financial and professional services; retail and wholesale; technology, media, and telecommunications; healthcare and pharmaceuticals; travel, leisure, and transportation; consumer goods; construction, engineering, and infrastructure; natural resources; and manufacturing. More than half the respondents were from the C-suite, and about half represented companies with annual revenue of more than $500 million. All areas of the world were represented, with 26% from North America.

Although the incidence of fraud has decreased overall from 2011, 61% of companies reported they were still hit by fraud at least once. That's a decline from 75% in last year's report. The cost of fraud also decreased, going from 2.1% of revenues to 0.9%. Interestingly, global improvement wasn't particularly mirrored in the results from companies in the United States. Incidence in the U.S. dropped less dramatically, from 65% to 60%, while cost decreased from 1.9% of revenues to 1.1%, which is higher than the global average. Despite this favorable news, the incidence and cost of fraud are still significant issues for a majority of companies. Doing business requires trust in order to operate economically and effectively.

The three types of fraud that caused loss and were most commonly reported globally were theft of physical assets (24%), information theft (21%), and management conflict of interest (14%). Because of vigilance, the reductions in fraud are mostly seen in procurement fraud, internal financial fraud, corruption, and bribery. In the U.S., the same major causes of loss from fraud were reported, but in a different order: information theft (26%), theft of physical assets (24%), and management conflict of interest (16%). These were largely unchanged from last year, reflecting the more modest reductions in fraud incidence and cost in the U.S. compared with the rest of the world.

The *Kroll Report* warns against becoming complacent toward fraud. Findings show that reported fraud concerns are dropping faster than fraud instances, and this becomes dangerous if it means respondents are giving greater credit to fraud-fighting efforts than is appropriate. Compared to last year, the global proportion of companies that describe themselves as highly or moderately vulnerable to the three most reported types of fraud declined significantly, and Kroll suggests that the results seem to be directly related to whether or not the company experienced some kind of fraud in 2012. The percentage of companies that described themselves as vulnerable to theft of physical assets declined from 46% in last year's report to 26%. For information theft, the percentage went from 50% down to 30%. And those that reported being vulnerable to management conflict of interest fell from 44% to 23%.

In the U.S., the declines were somewhat less dramatic: Information theft went from 52% to 33%,

theft of physical assets declined from 36% to 20%, and management conflict of interest fell from 34% to 25%. Again, these results seem to be directly related to whether or not the company experienced some kind of fraud in 2012. The difference between the U.S. and global percentages could suggest that more attention is given to fraud vulnerabilities in the U.S. than elsewhere in the world.

The report also shows that the rising trend of insider involvement is accelerating. The key perpetrator or one of the leading culprits of 67% of frauds reported in 2012 was an insider, an increase from 60% last year and 55% in 2010. In 84% of reported frauds, only one perpetrator was involved. This suggests that following the internal control requirement that individuals with sensitive responsibilities should take forced vacations while someone else performs their duties should be effective in preventing many types of fraud.

Another major finding is that information theft remains a significant and multifaceted threat to which respondents feel most vulnerable. The endless range of information technology (IT) frauds continues to increase in variety, frequency, and sophistication, according to the report. Security breaches include undetected malware, a misplaced mobile device, and a hacker taking sensitive data hostage. These weaknesses make business assets such as trade secrets, financial and customer data, and intellectual property increasingly more vulnerable to cyber-attacks, and 30% of respondents noted that IT complexity is the leading cause of increasing fraud risk.

According to Tim Ryan of Kroll Advisory Solutions, "Cyber-based data destruction events are increasingly common. Rather than stealing a corporation's intellectual property, these attackers forensically destroy data. This causes enormous injury to companies, including lost production, lost revenue, remediation costs, and reputational damage." Mike DuBose, another Kroll expert, notes, "We are seeing more economic espionage, much of it originating in Eastern Europe and Asia."

The *Kroll Report* notes that the popular misconception that hackers are the biggest risk today is untrue. Employees, either as culprits or as a point of weakness, are far more responsible than hackers for information loss. In 51% of the cases where information was lost, the loss was caused by the theft of a technology device (phone or computer) or an employee mistake. Employee malfeasance was involved 35% of the time, whereas external hacking was the issue in only 17% of the reported cases.

Perhaps the most positive and uplifting portion of the report states that taking anticorruption more seriously is paying dividends for companies. Even though a small number of companies have more work to do, far more have taken steps to improve their compliance with anticorruption legislation. These steps include integrating corruption issues into their due diligence activities, training senior managers appropriately, and performing an entity-wide risk assessment. During the past year, the prevalence of corruption has declined from 19% to 11%, with companies that have active compliance programs benefiting the most. Only 7% of companies with active compliance programs reported suffering an incident of corruption compared to 13% of all other companies.

In short, a strong ethical culture supported by effective compliance brings many dividends for a company.

For guidance in applying the *IMA Statement of Ethical Professional Practice* to your ethical dilemma, contact the IMA Ethics Helpline at (800) 245-1383 in the U.S. or Canada. In other countries, dial the AT&T USA Direct Access Number from www.usa.att.com/traveler/index.jsp, then the above number.

Need for Credit Rating Oversight

On February 4, 2013, the U.S. Department of Justice (DOJ) filed a fraud lawsuit against credit rating agency Standard & Poor's (S&P), seeking $5 billion in damages. The U.S. Securities & Exchange Commission (SEC) didn't join in the suit, once again appearing to side with issuers of securities rather than with investors. (See the January 2013 column, "Credit Rating Agency Performance Needs Improvement.")

The DOJ complaint against S&P outlined the methodology the company utilized to assign credit ratings to mortgage securities, including subprime and other mortgages wrapped into complex structured debt instruments. Some of these were purely speculative (synthetic) instruments. In some cases, mortgage data provided by

the securities issuer was passed through an apparently proprietary financial model known as the "Loan Evaluation and Estimate of Loss System." Results were shared with the issuer, who would provide additional data if it were needed to improve the rating. A committee certified the system's result, and an analyst presented a summary to a rating committee. This practice seemed quite perfunctory, as the complaint states: "Most rating committees took less than 15 minutes to complete. Numerous rating committees were conducted simultaneously in the same conference room." The complaint sets forth many examples of how S&P personnel viewed their services as highly profitable assistance to the issuer who had employed them rather than as an independent opinion.

The DOJ asserted that S&P committed fraud by falsely claiming its ratings were objective while it inflated ratings and understated risks associated with mortgage-backed securities, actions driven by a desire to gain more business from the investment banks that issued those securities. "Put simply, this alleged conduct is egregious—and it goes to the very heart of the recent financial crisis," said Attorney General Eric Holder.

Securities markets operate on the basis of trust that the information provided to investors is presented fairly. Without effective oversight of the agencies providing assurance of the creditworthiness of debt instruments, these markets won't be able to operate effectively. Since 2009, the Council of Institutional Investors has advocated the formation of a Credit Agency Oversight Board. Professionalization of the credit rating agency industry should be undertaken by an independent board under the oversight of the SEC or some other agency. This would involve setting standards of performance and ethical behavior and then monitoring compliance. This is the most efficient way to bring about effective assurance of the published credit risks inherent in debt instruments. **SF**

Curtis C. Verschoor, CMA, is the Emeritus Ledger & Quill Research Professor, School of Accountancy and MIS, and an honorary Senior Wicklander Research Fellow in the Institute for Business and Professional Ethics, both at DePaul University, Chicago. He was selected by Trust Across America as one of North America's Top Thought Leaders in Trustworthy Business Behavior 2013. His e-mail address is curtisverschoor@sbcglobal.net.