Fraud in a World of Advanced Technologies

The Possibilities are (Unfortunately) Endless

By Mark A. Nickerson

In Brief

For many years, internal controls have been the focus of auditors' risk assessment as they seek to attest that the control environment is working effectively to minimize the potential for fraud. As standards have evolved to focus more on fraud, so has technology. Innovations such as artificial intelligence (AI), robotic process automation (RPA), and blockchain have been touted as tools that will assist in identifying fraud; however, what if they actually make that job much more difficult by enabling potential fraudsters to perpetrate more robust and harder-to-detect crimes? The author investigates this question and arrives at some disturbing conclusions.

From 2000 to 2002, corporate accounting and financial scandals rocked investors, ultimately costing individuals billions of dollars, collapsing major corporations, and drastically upsetting confidence in U.S. securities markets. Companies such as Enron and WorldCom, among many others, were embroiled in financial scandal. Off–balance sheet loans, manipulation of commodity prices, improper accounting practices, falsified financial results—these improprieties all centered on the relatively unregulated environment at the time.

That supposedly changed on July 30, 2002, with the passage of the Sarbanes-Oxley Act (SOX). Prior to SOX's enactment, auditors operated in a self-regulated, peer-reviewed environment whose standards were set by FASB and overseen by the AICPA. SOX mandated SEC oversight and created the PCAOB, which was charged with establishing auditing and related attestation, quality control, ethics, and independence standards and rules to be used by registered public accounting firms in the preparation and issuance of audit reports. SOX also took numerous steps to reform the public accounting profession, which included establishing standards for auditor independence, requiring enhanced financial disclosures, and promising criminal fraud accountability.

But the accounting profession was not the only institution that needed to change. Corporations themselves were forced by SOX to address boardroom failures that led,

or at the very least contributed, to these scandals, including their lackluster “deferred maintenance” attitude to the system of internal controls over financial reporting (ICFR). Improving corporate governance and executive fiduciary responsibility were paramount to SOX’s success in curbing future improprieties, and it took those items head on by directly addressing loans to related parties, management oversight, due diligence by directors, and compensation of officers, as well as requiring independent audit committees and an ethics code for financial officers. Title III of SOX specifically requires both the CEO and CFO to certify not only that they have reviewed financial reports, but also that they believe the financials fairly represent the company’s financial position. If, at a later date, financial statements must be reissued due to noncompliance with GAAP, executives must return any bonuses received for that year, hopefully eliminating any financial incentive to inflate earnings.

More than 15 years later, the debate still rages as to whether SOX has been effective enough to justify the hefty cost public corporations incur annually to remain in compliance. While the cost/benefit equation is certainly the most highly debated topic, the lack of impact surrounding internal controls should be a much larger concern to the public. According to a 2015 Audit Analytics study (Derryck Coleman, *The Impact of SOX on Financial Restatements, Audit Analytics,* Feb. 28, 2017, http://bit.ly/2JVJ7WK), the number of companies that have disclosed ineffective ICFR declined drastically in the years following the implementation of SOX section 404(b), though that percentage has risen recently (*Exhibit 1*).

The decline in ineffective ICFR disclosures is almost certainly a result of SOX section 404(b) becoming effective for fiscal years ending on or after November 15, 2004. Section 404(b) requires companies to have external auditors not only report on financial statements themselves, but also attest to the effectiveness of the internal control environment. During that first year of implementation, 15.7% of companies were required to disclose ICFR material weaknesses. Over time, the percentage of companies disclosing ICFR declined dramatically, to a low of only 3.4% of companies in 2010. This data is fairly misleading, however, as the majority of these material weaknesses were only disclosed after companies had already restated their financials. As of 2014, the PCAOB had determined that an astounding 80.4% of companies issuing financial statement restatements had audits that determined effective internal controls prior to those restatements. Therefore, it was the restatements themselves, brought about by financial accounting discrepancies or oversight, that forced auditors to change their previous reports, changing the evaluation of the internal controls from effective to ineffective. In other words, the reliability of ICFR evaluations is questionable, leading one to ask whether SOX section 404(b), and thereby ICFR, is any deterrent to fraud.

Internal controls are themselves not a deterrent when power, influence, greed, and corporate malfeasance rule the corner offices.

Source of ICFR Risk: The Room Where It Happens

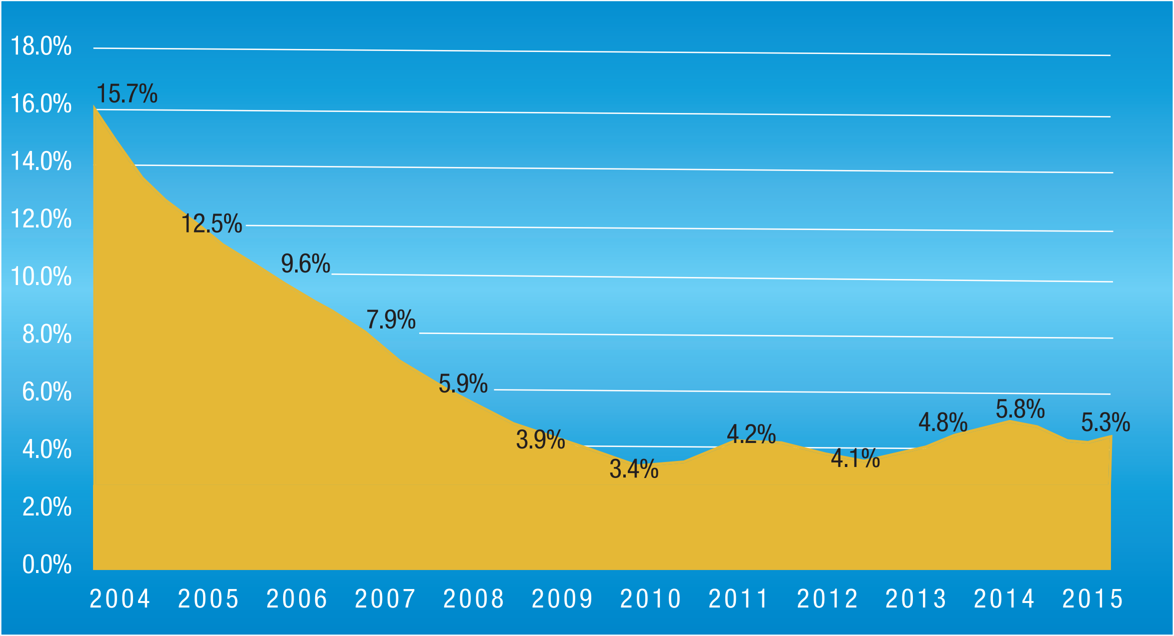
The question then remains: if internal controls and their respective audits are not identifying accounting-related frauds, why not? The answer, it seems, lies in the research detailing where these frauds actually occur. Frauds largely do not occur amongst employees or managers, who are mainly subjected to internal controls such as segregation of duties, establishment of responsibility, or independent internal verification. These acts are, for the most part, not perpetrated in the accounting departments of large corporations. Rather, they still overwhelmingly occur in the corner offices of CEOs and CFOs.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) sponsored a study, *Fraudulent Financial Reporting: 1998–2007, An Analysis of U.S. Public Companies,* which detailed the fraudulent activities investigated by the SEC (Mark Beasley et al., May 2010, http://bit.ly/2KmdNzS). The report showed that 89% of fraud cases included some level of CEO or CFO involvement, up from 83% during 1987–1997. Of that 89%, 20% had been indicted within two years, and 60% of those indicted were convicted.

In 1973, American criminologist Donald Cressey identified three factors that are present in fraud; this theory has come to be known as the fraud triangle. Cressey theorized that for fraud to exist, an ordinary individual must encounter financial pressure or incentive to commit fraud, have the opportunity to commit the act, and be capable of rationalization of their fraudulent activities. While the profession has tended to use these factors as a base for assessing and determining internal controls, the risk assessment of where large-scale frauds are most prevalent has been ignored. Internal controls are themselves not a deterrent when power, influence, greed, and corporate malfeasance rule the corner offices.

There is no greater role in a company than CEO or CFO, and correspondingly no greater opportunity or pressure to commit fraud. Take, for example, the role of equity-based compensation in fraud. As executive compensation packages shifted from cash-based to equity-based during the 1980s and 1990s, the likelihood of financial

Exhibit 1
Companies Disclosing Ineffective Internal Controls over Financial Reporting



Source: Audit Analytics

statement restatements increased dramatically. As John Coffee pointed out in *Gatekeepers: The Professions and Corporate Governance,* the leading factor for restatements was the presence of significant stock-based incentives in the hands of executives (Oxford University Press, 2006). Coffee determined that "if a CEO held options equaling or exceeding 20 times his or her annual salary (a substantial number of CEOs did), the likelihood of a restatement (an indicator of financial fraud) increased by 55%."

These statistics were substantiated in the most recent Association of Certified Fraud Examiners (ACFE) *Report to the Nations—2018 Global Study on Occupational Fraud and Abuse* (http://bit.ly/2BIITfH). According to the study, while only 19% of total frauds were perpetrated by executives, their median loss of $850,000 per occurrence was more than 17 times greater than the median loss of frauds perpetrated by low-level employees. In addition, 65% of these frauds involved corruption, and 27% were shown to directly involve financial statement fraud. Furthermore, 66% of executive frauds involved collusion, which has been shown throughout various studies to render internal controls ineffective if present.

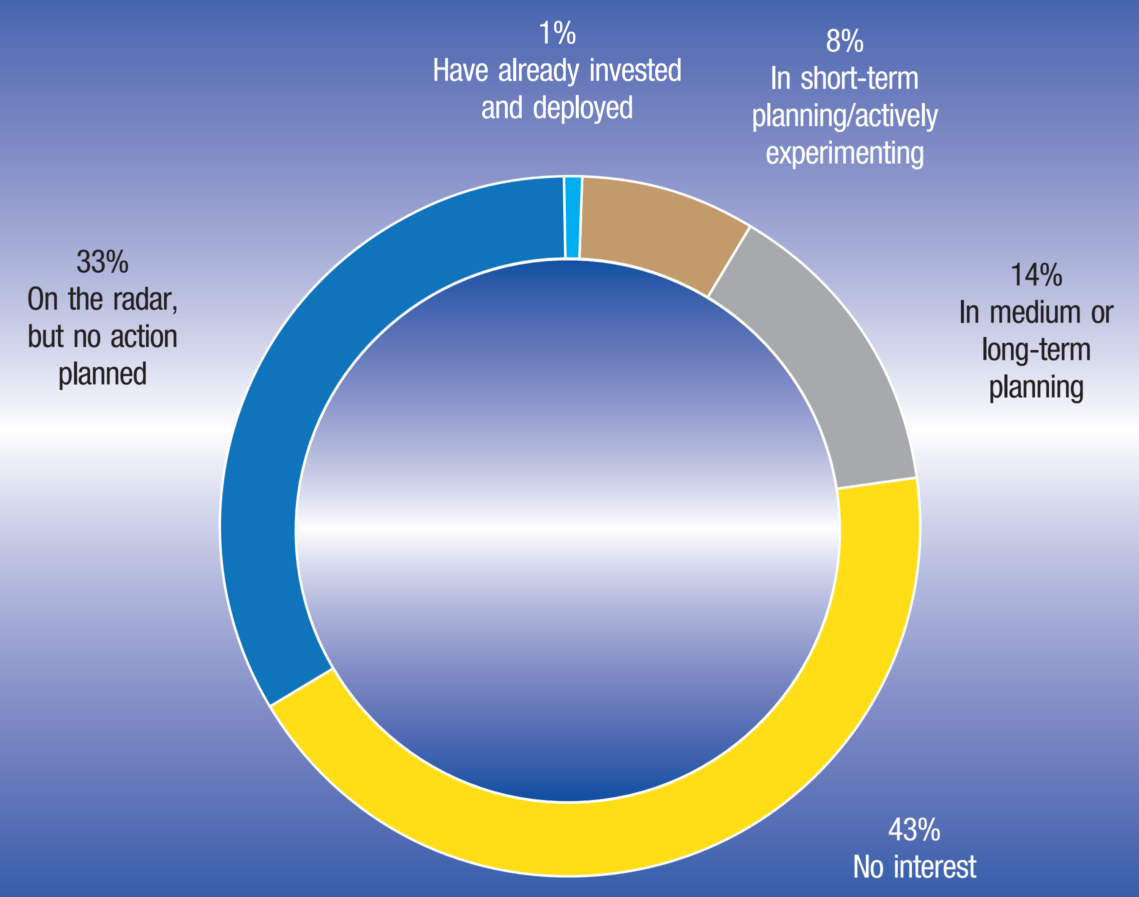
Enter the Robots: The Good, the Bad, and the Potentially Ugly

How these frauds have been committed varies widely, from more sophisticated techniques involving improper accounting recognition, off–balance sheet financing, and related party sales to simply making up the numbers. While many auditing standards have been changed or created in the past decades, so has technology. If companies such as GE, Enron, Wells Fargo, and Chesapeake Energy can perpetrate large-scale frauds simply by manipulating accounting techniques or outright lying, imagine what could be possible with the manipulation of AI to their benefit. Sam Antar, a key player in the "Crazy Eddie" fraud of the 1980s (see below), speaking at the 2019 Williamsburg Fraud Conference, said that he believed today is "the golden age of fraud."

Numerous articles have touted the emergence of AI, blockchain, data analytics, and RPA as tools to be used by auditors to combat fraud. Consider, however, this thought: fraudsters will look to take advantage of the same technologies to commit more damaging and robust frauds than have previously been possible.

Blockchain, for instance, has been lauded as a fraud-resistant superhero whose presence will eradicate evildoers in the financial accounting realm. This position, however, ignores many of blockchain's current drawbacks. First, blockchain usage itself amongst companies, including those with imminent plans to implement, is almost nonexistent (*Exhibit 2*). According to Gartner's 2018 CIO Survey, only 1% of respondents indicated current adoption of blockchain within their company, while 77% stated they had no interest or no current action plan to further investi-

Exhibit 2
Blockchain Deployment Plans



Source: Gartner 2018 CIO Survey

gate or develop the technology for use within their organizations ("Gartner Survey Reveals the Scarcity of Current Blockchain Deployments," May 3, 2018, https://gtnr.it/2XlmspD).

Second, many experts agree that blockchains generally represent targeted solutions to specific problems, making fraud more difficult in those instances, but also disregard blockchain as the complete fraud prevention tool that many have made it seem. Eric Wall, cryptocurrency blockchain lead at Cinnober, recently pointed out some of blockchain's fallibilities (David Cowan, "Blockchain is Not a Reliable Silver Bullet for Fraud Prevention," *Raconteur*, Sept. 6, 2018, http://bit.ly/2EMpdcs). The validation process for blockchain, says Wall, is inherently slow: "It can only see an order and process it; what it can't understand is the trading context and see if fraud is involved." In addition, as previously discussed, individuals with opportunity (e.g., power, influence, control), pressure (spending habits, meeting earnings goals), and rationalization (justifying greed and other behaviors) are the ones actually committing large-scale frauds. CEOs or persons with overwhelming authority, or those colluding with them, will be able to find a way to input fraudulent data. "Any information processing system that has bad input provides bad output," Wall continues. "The blockchain can only be aware of the inputs, not the reality. The blockchain will track it as valid data, so if you have the authority to input bad data, then the blockchain will validate the bad data. You still have a dependency on the real world, trusted sources of data and authorization. If you corrupt that, then you corrupt the process." Simply put, if those in power still seek to perpetrate frauds, especially those that involve collusion, blockchain may not be a deterrent.

In addition, cryptocurrencies continue to emerge and evolve, which also may contribute to the furtherment of more substantial and advanced financial frauds. Jamie Dimon, CEO of JPMorgan Chase & Co., has previously referred to Bitcoin as a fraud, although he has since softened his stance. While new cryptocurrencies move toward initial coin offerings (ICO), however, it is possible that these offerings themselves may bring new technologically savvy scammers to the table.

Contrary to what some may believe, these currencies are not unreachable by hackers. Recently, the digital currency exchange Coinbase discovered a fraud of over $1 million within the blockchain ledger for the cryptocurrency Ethereum Classic. The fraud was perpetrated by a "double-spending" attack, wherein the same token is used more than once. Essentially, the hackers were able to enter and rewrite a reportedly permanent ledger within the blockchain, a feat that most blockchain novices deemed impossible (Russell Brandom, "Why the Ethereum Classic Hack Is a Bad Omen for the Blockchain," *Verge*, Jan. 9, 2019, http://bit.ly/2MtT7Zk). CEOs with the ability to double spend while falsifying the blockchain ledger and accounting records could potentially perpetrate frauds costing investors and the economy billions.

While the SEC issued its long-awaited *Framework for Investment Contract Analysis of Digital Assets* in April 2019 (http://bit.ly/2JPRSBu), it also stated that the document itself is not exhaustive: "The framework is not intended to be an exhaustive overview of the law, but rather, an analytical tool to help market participants assess whether the federal securities laws apply to the offer, sale, or resale of a particular digital asset" (Public statement, Apr. 3, 2019, http://bit.ly/2wAoPcu). Moreover, it is important to note that while this is a step in the right direction, the framework is merely guidance and in no way legally binding.

There is another risk to these new technologies, one more troubling than the hackability of the blockchain. Technologies thought to protect investors against frauds and help auditors identify those activities, such as AI and RPA, could actually *assist* executives in committing fraud, or even learn to commit the frauds themselves. These technologies can be utilized in a number of different ways; most companies that have instituted AI in their organizations so far have done so with a focus on predictive analytics, machine learning, or natural language processing. It is important to keep in mind that these systems do not learn independently, but rather use human-programmed algorithms to process millions of provided data points. As these algorithms have been programmed by humans—who are prone to bias, greed, and sometimes lax moral standards—and the corresponding data points are generated by human interaction, algorithmic bias in AI is inevitable.

Technologies thought to protect investors against frauds and help auditors identify those activities could actually assist executives in committing fraud, or even learn to commit the frauds themselves.

There are already numerous reports of AI software exhibiting bias across racial and gender divides. For example, an image-recognition software built by a University of Virginia professor learned to exhibit sexist views of women through machine learning. Another study, by an assistant professor at the University of Massachusetts Amherst, showed that AI systems learned to exclude some African-American individuals from datasets based solely upon vernacular. In 2015, Google Photos, backed by machine learning, exhibited extremely racist and objectionable behavior when it began tagging photos of black people as gorillas. While these examples involve societal issues, what happens when AI can be manipulated or learns to exhibit those biases that lead to fraudulent behavior? What happens when the software thought to help combat fraud is instead assisting the perpetrators?

A recent report from Google's DeepMind AI division (Leibo et al., "Multi-agent Reinforcement Learning in Sequential Social Dilemmas," Proceedings of the 16th International Conference on Autonomous Agents and Multiagent Systems, 2017, http://bit.ly/2Igmn0l) showed how technology can become both greedy and aggressive over time. The division utilized two video games, played head-to-head by AI agents after being trained in deep reinforcement learning. The first game, called Gathering, requires each competitor to gather as much digital fruit as possible. Over the course of 40 million turns, researchers began to notice two scenarios being played out. If there were enough digital fruit to gather, both players were satisfied; however, when fruit was scarce, the AIs used lasers to combat their opponents and seize all of the apples. While the lasers were programmed into the system by humans, they were deeply embedded and remained unused by simpler AIs. As more intelligent AIs emerged, however, they seized any opportunity to gather all of the fruit. Google researchers believe that, as the AIs grew more intelligent, they also determined what resources were available and how to best manipulate those resources to their advantage. This again shows a pattern of sufficiently advanced AI exhibiting the worst of human behavior traits—greed, selfishness, aggression—over time. It is important to note that the AI were not programmed with a reward to use the lasers and were not taught to use them as an advantage per se. Those ideas were solely learned traits.

The second test placed three AI agents in the game Wolfpack, two acting as wolves and one as prey. By the rules of the game, if one wolf overcomes the prey by itself without losing the carcass to scavengers, it receives the entire reward, but at a greater risk. If both wolves agree to cooperate in capturing the prey—that is, if they collude—they can better protect the carcass from scavengers and both receive rewards. As the AI agents learned the benefits of cooperation, the rate of lone-wolf captures decreased dramatically.

While systems such as Google's Deepmind are still being developed, imagine how these systems learning greed, aggression, and collusion in order to receive a greater reward could impact financial and accounting frauds in the future. CPA firms, including most of the Big Four, have already made and discussed openly substantial investments in AI while looking to cut human time spent on audit engagements. Ernst & Young has definitively started using machine learning to help analyze and identify potentially fraudulent transactions. What if that AI system figures out that auditors have shifted focus away from identifying fraudulent transactions and towards the efficiency of internal controls within an organization?

Forewarned Is Forearmed

Luckily, scholars have also started to pay attention to the potential negative impacts of AI. Recently, a group of experts from six major universities, independent think tanks, and nongovernmental organizations released a report titled "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation." (Miles Brundage et al., February 2018, http://bit.ly/318dQoC). Its executive summary is, this author believes, serves as a warning to CPAs:

> Artificial intelligence and machine learning capabilities are growing at an unprecedented rate. These technologies have many widely beneficial applications, ranging from machine translation to medical image analysis. Countless more such applications are being developed and can be expected over the long term. Less attention has historically been paid to the ways in which artificial intelligence can be used maliciously. This report surveys the landscape of potential security threats from malicious uses of artificial intelligence technologies, and proposes ways to better forecast, prevent, and mitigate these threats. We analyze, but do not conclusively resolve, the question of what the long-term equilibrium between attackers and defenders will be. We focus instead on what sorts of attacks we are likely to see soon if adequate defenses are not developed.

The researchers go on to make four high-level recommendations regarding the current use and expansion of AI moving forward, the first of which is most relevant and important to the accounting profession. They advise that "policymakers should collaborate closely with technical researchers to investigate, prevent, and mitigate potential malicious uses of AI." FASB, the PCAOB, SEC, IRS, and all of the profession's governing bodies should be acting quickly to set standards as to how and when AI and other technologies should be used within the profession. CPAs must also work to understand how to properly address an engagement when a client is using such technologies and what additional work may be needed to ensure accurate financial reporting. In addition, university accounting departments nationwide must begin, if they have not already, including these technological advances and issues into their curricula. Suggested methods include encouraging faculty education, assigning research projects on emerging technologies, and developing group projects with the possibility of multidisciplinary interaction on the subject matter (Sean Stein Smith, "Integrating Blockchain and Artificial Intelligence into the Accounting Curriculum" *Journal of Accountancy*, Nov. 14, 2017, http://bit.ly/2MroVhu).

Imagine how these systems learning greed, aggression, and collusion in order to receive a greater reward could impact financial and accounting frauds in the future.

One step in the right direction was the PCAOB's recent issuance of Auditing Standard (AS) 3101, *The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion,* which includes the phrase "whether due to error or fraud" when describing reasonable assurance as to the financial statements being free from material misstatement. This wording will now coincide more closely with Auditing Standard (AS) 1001, *Responsibilities and Functions of the Independent Auditor,* which states that auditors must "plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud." While these are both steps in the right direction, auditors, with or without any additional standards dictating their requirements, must return to seeking out and identifying fraudulent transactions, discharging their responsibility as gatekeepers. Identifying these fraudulent transactions, especially when companies employ AI or RPA, will be paramount in ensuring that these technologies are actually benefiting stakeholders instead of placing them at an elevated risk. After all, the technologies will learn from human behavior, so humans need to teach them well. ❑

__Mark A. Nickerson, CPA, CMA,__ is a lecturer at the State University of New York at Fredonia and owner of Mark A. Nickerson CPA PLLC, Buffalo, N.Y.