Technologies on the horizon

In our first “Fraud EDge” column in this series we discussed how essential it is for all fraud examiners to be cognizant of the many potentially useful technologies that are effective in fraud examinations. In our first four columns, we explored the cutting edge of high tech in the fight against fraud — from the exploration of how natural language processing can extract names from unstructured text for the construction of complex relationship maps, to how underlying emotional tones in written communications help detect deception before a single email is even read. The columns have also illustrated how artificial intelligence can enhance human intelligence to achieve intelligence augmentation.

In this column we share our view of some new technologies that have the most promise of providing major value to future fraud examiners. We also discuss the significant role colleges and universities must play in educating professional fraud examiners of the future. Colleges and universities have unique and excellent opportunities to provide students with the functional and technical knowledge and skills they need to successfully compete in the professional world. — Les E. Heitger, Ph.D., Educator Associate

Current technologies
The most common fraud analytics tools fraud examiners use focus on data extraction, analysis, visualization and keyword-search based tools for unstructured data. Software companies design these technologies for examiners who don’t have information technology backgrounds. Therefore, organizations of all sizes have adopted fraud analytics and digital forensics — tools previously only available through experts.

Fraud examiners still need help to implement the concepts we discussed in the previous columns. However, many of the current stand-alone technologies are becoming integrated into single-source solutions that encompass all the uses we’ve listed.

Transformative future technologies
Tackling a topic about the future of technology is difficult. We can easily veer off into what appears to be pure science fiction. Regardless, two seemingly unattainable technologies — intelligence augmentation (using technology to enhance human abilities) and detecting fraud via emotional tones — fall into this category. However, fraud examiners haven’t universally adopted them so they might be considered “future tech” for some.

Here we’ll focus on two emerging concepts sure to influence the future of fraud examinations: cognitive analytics and the “Internet of Things.”

Fraud detection via cognitive analytics
Traditional computer-assisted fraud analytics systems — “expert” systems that attempt to emulate human experts to assess data and “decision support” systems that assist examiners in decision making based on a set of rules for a given situation — at their core rely on sets of rules to anticipate a wide range of possible conditions or occurrences. These systems provide the platform of predictive analytics — using past experiences to evaluate current data to make predictions about future events.

These systems, which are heavy on statistics, are becoming more commonplace in fraud examinations. However, these rule-based systems are only as good as the human experts who populate their databases with knowledge. While rules-based systems help automate detection in very large data sets, they fail to be adaptive to things previously unseen or too subtle for detection with earlier methods.

The emerging area of cognitive analytics, alternatively, leverages artificial intelligence, machine learning and natural language processing (using machine learning to understand the meaning of communications and
text) in ways that transcend traditional expert systems. Working together, these components achieve a form of “machine cognition” that includes making inferences, and sensing and predicting deception or anomalous events that could be indicative of fraud — all without being pre-configured with specific rules to detect them. (When a machine reaches cognition it attains a level of awareness about the context surrounding the data it’s analyzing, which allows it to make inferences, predictions and judgments much like a human.)

These systems also can retain knowledge and apply it to future data. Soon, the systems will be capable of asking people questions to help in learning. (See “Adding ‘augmented intelligence’ and ‘data visualization’ to the mix,” Fraud Magazine, November/December 2014, http://tinyurl.com/kpb7xat.)

While not common in fraud examinations, cognitive analytics is far enough along that CFEs likely will implement it routinely in the next five years. Already, IBM’s Watson system has achieved much of the requirements to be “cognitive,” as it initially demonstrated on the “Jeopardy” game show and has since been incorporated into more practical uses such as the fight against cancer.

Eventually, such systems will be able to digest millions of documents and emails, extract correlations and patterns that humans can’t detect and then teach us what it found. At that point, the student will indeed have become the teacher.

Conversely, more sophisticated, organized crime and fraud rings might use cognitive systems to help perpetrate frauds in ways that appear normal to the examining cognitive detection system. For example, competing, autonomous algorithms that ran amok caused the “flash crash” of the stock market in 2011. WIRED magazine’s October 2014 article, “The Future of Fraud,” by Ori Eisen (http://tinyurl.com/k7rr6rk) included a hint of this increasingly organized, systemic fraud.

The Internet of Things
“The Internet of Things” (IoT) describes the interconnectivity of physical objects in a manner similar to the Internet. Futurists paint visions of a world in which buildings talk to each other, biological ecosystems help researchers diagnose imbalances and cars drive themselves — reacting to other vehicles like schools of fish.

It might not sound like any of this could apply to fraud examination, but it can. Physical objects within a business entity connected to a network are capable of generating data; they create a massive new pool of data from which CFEs can perform analytics.

Consider what we could do if every item of inventory could report its movement and location in real time, doorframes could distinguish who passes through them and vehicles could record virtually every condition leading up to an accident. This concept of “disruptive technology” has the potential to tip the balance in favor of fraud examiners. The challenge is effectively harnessing the enormous volume of generated data.

The drawback to a world in which everything is connected and generating statistics is that “Big Data” will only get bigger. With such massive, high-quality and unique data, red flags and anomalies potentially could be buried within much larger pools of data. This problem is already plaguing fraud examiners who don’t have the abilities to harness, store and analyze current datasets. We can mitigate this problem with artificial intelligence, intelligence augmentation, statistical-based fraud detection and cognitive analytics.

Preparing for the future
Fraud examiners have always been on the forefront of embracing technology since financial analysis jumped from paper to spreadsheets and later to computer-assisted audit and analysis tools. Growth in data available for analysis is approaching exponential rates. The movement toward more open data sources and the IoT will hasten this growth.

Future fraud examiners will need to embrace this data growth and have a working understanding of the tools and technologies, all designed to distill meaning from massive data, which we discussed in the last several columns in this series. (See a recap of these tools and methodologies in the sidebar on page 18.)

Future fraud examiners also will need to understand how to extract, normalize and access this data before beginning to analyze it. They might even need to move accumulated data on central topics from disparate systems and deposit it into special-purpose data warehouses (a means by which to accumulate data regarding...
a central topic or use from disparate systems into a single location).

College and universities are ideal environments to tackle the early challenges of combining the need for understanding and managing massive data infrastructures and the tools needed to analyze the data. Budding fraud examiners at these higher-ed institutions are eager to learn and differentiate themselves from their peers. These institutions also have multiple departments containing experts of all levels.

Incorporating elements such as programming, information systems, graphic design, accounting, psychology and others into forensic accounting curricula will help equip the fraud examiners of tomorrow with the skills they need to embrace technology and stay on the cutting edge of high tech.

**Advanced fraud tools and techniques**

- Social Network Analysis (SNA).
- Predictive coding.
- Natural language processing.
- Analysis of unstructured data.
- Intelligence augmentation.
- Data visualization.
- Predictive analytics.
- Statistical-based detection.
- Cognitive analytics.

The era of “human-machine cooperation” is soon to be a reality — not necessarily a matter of choice but one of necessity. 

**Les Heitger, Ph.D., Educator Associate**, is BKD Distinguished Professor of Forensic Accounting in the School of Accountancy at Missouri State University in Springfield. He’s chair of the ACFE Higher Education Advisory Committee. His email address is: LesHeitger@MissouriState.edu.

**Jeremy Clopton, CFE, CPA, ACDA**, is senior managing consultant in the Forensics Practice of BKD, LLP. His email address is: jclopton@bkd.com.

**Lanny Morrow, EnCE**, is a managing consultant in the Forensics Practice of BKD, LLP. His email address is: lmorrow@bkd.com.

---

**IFP | Institute for Fraud Prevention**

Improving the Ability of Business and Government to Combat Financial Fraud Crimes

**Become a member today.**

Contributions and memberships are tax deductible.

An industry/university cooperative research effort dedicated to:

- multi-disciplinary research
- education
- prevention of fraud & corruption
- providing cutting-edge research to detect and deter fraud

Visit www.theifp.org to get involved or for more information