

Spring 2019

# Using Machine Learning to Detect Financial Fraud

Josh Baker

*Elizabethtown College, bakerj1@etown.edu*

Follow this and additional works at: <https://jayscholar.etown.edu/busstu>

Part of the [Accounting Commons](#)

---

## Recommended Citation

Baker, Josh, "Using Machine Learning to Detect Financial Fraud" (2019). *Business: Student Scholarship & Creative Works*. 6.  
<https://jayscholar.etown.edu/busstu/6>

This Student Research Paper is brought to you for free and open access by the Business at JayScholar. It has been accepted for inclusion in Business: Student Scholarship & Creative Works by an authorized administrator of JayScholar. For more information, please contact [kralls@etown.edu](mailto:kralls@etown.edu).

# Using Machine Learning to Detect Financial Fraud

By

Josh Baker

Primary Advisor: Professor Terrie Riportella

Secondary Advisor: Professor Jeffrey Gabriel

This thesis is submitted in partial fulfillment of the requirements for Honors in the Discipline in Accounting and the Elizabethtown College Honors Program

May 1, 2019

Thesis Advisor (signature required) 

Second Reader (if applicable) 

Third Reader (if applicable) \_\_\_\_\_



## Honors Senior Thesis Release Agreement Form

The High Library supports the preservation and dissemination of all papers and projects completed as part of the requirements for the Elizabethtown College Honors Program (Honors Senior Thesis). Your signature on the following form confirms your authorship of this work and your permission for the High Library to make this work available. By agreeing to make it available, you are also agreeing to have this work included in the institutional repository, JaxScholar. If you partnered with others in the creation of this work, your signature also confirms that you have obtained their permission to make this work available.

Should any concerns arise regarding making this work available, faculty advisors may contact the Director of the High Library to discuss the available options.

### Release Agreement

I, as the author of this work, do hereby grant to Elizabethtown College and the High Library a non-exclusive worldwide license to reproduce and distribute my project, in whole or in part, in all forms of media, including but not limited to electronic media, now or hereafter known, subject to the following terms and conditions:

### Copyright

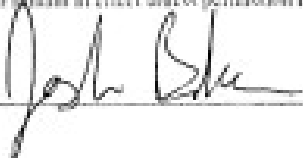
No copyrights are transferred by this agreement, so I, as the author, retain all rights to the work, including but not limited to the right to use in future works (such as articles or books). With this submission, I represent that any third-party content included in the project has been used with permission from the copyright holder(s) or falls within fair use under United States copyright law (<http://www.copyright.gov/help/faq/faq1.html#107>).

### Access and Use

The work will be preserved and made available for educational purposes only. Signing this document does not endorse or authorize the commercial use of the content. I do not, however, hold Elizabethtown College or the High Library responsible for third-party use of this content.

### Term

This agreement will remain in effect unless permission is withdrawn by the author via written request to the High Library.

Signature:  Date: 5/1/19

# Table of Contents

<b>I. Literature Review</b> .....	5
The History of Artificial Intelligence .....	5
The Right of Privacy .....	6
Artificial Intelligence’s Role in Accounting .....	8
Artificial Intelligence in Auditing .....	9
A Description of Fraud.....	13
Using Artificial Intelligence to Detect Fraudulent Activity ...	15
<b>II. My Proposal For a New Tool</b> .....	18
Sample Scorecard.....	22
Obstacles .....	30
<b>III. Conclusion</b> .....	35
<b>IV. Thoughts from Professionals</b> .....	35
<b>V. References</b> .....	44

In 1950, Alan Turing said, “We may hope that machines will eventually compete with men in all purely intellectual fields” (Turing 433). Nearly seventy years later, his dream may become a reality. Banks, telecommunications, and information technology, as well as accounting firms, use artificial intelligence for routine and data-oriented tasks that once required hours of human labor. As companies continue to invest in artificial intelligence, they are still ignoring what has impacted 49% of organizations, as reported in a 2018 PricewaterhouseCoopers (PWC 4) survey: **fraud**.

According to Elaine Pofeldt of CNBC, U.S. businesses lose \$50 billion per year to employee theft, also known as asset misappropriation. Asset misappropriation cases have ranged from a loss of \$1 million due to misappropriation, up to approximately \$55 million to vendor fraud with an average loss of \$1.13 million, while 28.7% of the cases went undetected for more than five years (Pofeldt). Though humans do not always have the time to search for these types of schemes, artificial intelligence can expose fraudulent activity without the need for as much human input.

# I. Literature Review

## **The History of Artificial Intelligence**

Artificial intelligence (AI), a term Norvig describes as “the science and engineering of machines that act intelligently”, has made significant leaps since the creation of the term in the early twentieth century (Norvig 2). The Turing test, as we call it now, is Turing’s proposal for assessing a machine’s intelligence. Turing’s test says a person, called the participant, communicates with two beings, a machine and another human, each on the other side of a door. Using written communication, the human, machine, and participant slide their messages underneath the doors to each other. For example, should the human ask, “Which type of pie is your favorite?” The machine may answer, “Pi is equal to 3.14159265,” the mathematical representation of the symbol  $\pi$ , while the human may answer, “Apple pie is my favorite.” Therefore, this machine would not be considered intelligent, as it is obvious to the participant that the machine answered the question incorrectly (Turing 433).

Andrew Hodges raises a valid question: did Turing disregard imagination, or freedom to think, as a component of intelligence (Hodges 1)? Peter Norvig agrees emotion and imagination are substantial pieces of intelligence in the use of AI, but refutes the suggestion that emotion can be mimicked through machine learning. Norvig points out that though emotion and imagination cannot be created, they can be imitated using equations (Norvig 5). Just as we infer the tone of voice in a book, AI can analyze the words and their order to predict the emotion of its author.

AI has advanced significantly since Turing’s paper was published in 1950. In 2011, IBM’s Watson, a form of AI, challenged two of Jeopardy’s most successful contestants to a

game. Although Watson struggled at times to answer questions precisely, the machine won convincingly with a score of \$77,147 to \$24,000 to \$21,600. In fact, Ken Jennings, who won Jeopardy 74 straight times, conceded on the final question, writing “I, for one, welcome our new computer overlords,” as his answer (Markoff).

Machine learning, a modern form of AI, uses machines to complete a task by teaching itself using existing data provided by the engineer or the internet. Tomáš Saloky and Jaroslav Šeminský define machine learning in their paper, “Artificial Intelligence and Machine Learning”, as “the capability of an AI system to improve its performance over a period of time.” Machine learning improves over time as it amasses more data so that the algorithm the machine uses becomes accurate (Saloky and Seminsky 2). For now, machine learning is one of the closest existing resemblances to artificial intelligence and is considered its own subclass of artificial intelligence itself (Marr). Machine learning presents the opportunity for a tool that runs on prior data, or in this case, prior cases of fraud, to create a model that can predict the likelihood of fraud based on financial pressures and rationalization.

### **The Right of Privacy**

*New York Times* journalist Farhad Manjoo writes about the privacy issues surrounding technology in his opinion piece titled, “It’s Time to Panic About Privacy.” To illustrate the thin line between using technology as an aid and the invasion of privacy, he provides the example of a doorbell camera. This camera, though a security measure for many homes, matches the faces of visitors to its internal memory system. A repeated facial recognition means the person is likely friendly, while a new face could be a threat of an intruder. Of course, to work, the camera must be able to identify the faces of those walking by or towards the door, meaning it is storing data on every individual.

Manjoo goes on to propose that some families may begin posting pictures of these suspicious faces on social media websites, which then law enforcement may find and match against their criminal databases. All of the sudden, the harmless picture meant to simply protect the family is being used and spread by various sources. Additionally, the video feed poses a threat of being obtained by the home's internet provider, the company who owns the doorbell technology, or anyone able to obtain access to the home's private network (Manjoo).

Wall Street Journal writer Te-Ping Chen says in her article, "Workers Push Back as Companies Gather Fingerprints and Retina Scans," that lawsuits have been filed against employers for not disclosing how the employee's biometric data is being used. These employees claim that their private information is being put at risk. Illinois, specifically, passed the 2008 Biometric Information Privacy Act that requires a company to obtain consent from employees to collect biometric data and describe its use, how it is stored, and for how long it will be stored. Florida and New York are looking to add similar laws, while Texas and Washington already do. Chen says the biometric data is being stored using cloud technology, then given to third parties that may be subject to unauthorized access from a hack or breach (Chen).

According to Matthew Heller of CFO.com, Democrats are proposing the Algorithmic Accountability Act that would expand testing on algorithms through Federal Trade Commission regulations to reduce susceptibility to "race, gender, or other discriminatory biases." One example of bias in the recent past stemmed from Facebook ads that, as Heller puts it, "steered black families away from certain neighborhoods in New Jersey. I would be concerned that this well-intended bill would not be able to prevent discrimination, as other variables may need to be considered. For example, if there is a correlation between a certain race and age class, would the discrimination still exist even if race is not specifically identified (Heller)?"



## Artificial Intelligence's Role in Accounting

Hussein, Ting, and Miklos describe AI as an intelligent machine that is aware of its surroundings, which is also capable of game-playing, language translation, language learning, pattern recognition, and problem solving. (Hussein, Ting, & Miklos 2). In fact, the Big Four accounting firms - Deloitte, Klynveld Peat Marwick Goerdeler (KPMG), PricewaterhouseCoopers (PWC), and Ernst & Young (EY) - have all heavily invested in AI research. KPMG partnered with IBM in 2016 to use Watson for its tax practice, which uses AI to identify projects eligible for research and development tax credits (Brown & Rainey). Deloitte is working with Kira Systems to create a data-analyzing tool that can read documents and flag relevant information. Currently, Deloitte is using the tool to help clients comply with the IFRS 16 lease accounting standard using contract analysis (Kira Systems). PWC is also using a data-analysis tool, DeNovo, for clients to extract pertinent financial information. This tool covers banking services, investment and wealth management, capital markets, insurance, and transaction and payment services (PWC). EY, in addition to announcing a \$1 billion increase on investments in new technology, has collaborated with Arria NLG to create a natural language generation portal. This portal, an internal tool, "turns raw data into insightful narratives" for employees to use in decision-making (Nesfield & Taggart).

Artificial intelligence is becoming much more popularized and debated. According to Marina Krakovsky's "The New Jobs," robots replaced approximately 670,000 employees over a seventeen-year span of 1990 to 2007 (Krakovsky 1). Kletzer adds that 30% of tasks can be automated in six out of every ten occupations (Kletzer). Accounting, specifically, has a 94% probability to be computerized according to Hussein, Ting, and Miklos in 2016 (Hussein, Ting, & Miklos 14).

## Artificial Intelligence in Auditing

Gale Crosley and Alan Anderson's guest column in the Public Accounting Report, "The Audit of the Future: Daring, Disruptive and Data-Driven but Poised to Add Significant Value to Firms and Clients," focuses its attention on potential changes to the audit field. Crosley and Anderson, unlike other sources, look at the field from a broad spectrum over the next hundred years rather than focusing on any specific change (Anderson and Crosley 2). This article clearly shows the rapid advancement of auditing but proposes a dilemma: the struggle of implementing multiple technological advancements at once. The majority of studies addressing the addition of artificial intelligence to the accounting field have focused on the current capabilities of the technology.

Crosley and Anderson claim that data analytics has practically eliminated the need for sampling, as computers can process the full data set (Anderson and Crosley 1). Their point is worth noting, as there is less of a need for sampling using the traditional method of randomly selecting from the population. If Crosley and Anderson are implying that the AI will test the full population and then send a human user the outliers for further testing, it can be argued the outliers are the new sample. Regardless of what we call it, this method reduces the sampling risk significantly.

Crosley and Anderson go on to speak of the modern-day computer's computational power, including the aptitude to identify anomalies and patterns (Anderson and Crosley 1). According to Tom Fawcett and Foster Provost's "Adaptive Fraud Detection," this technology could be used to find and analyze patterns and behaviors in the client's data in the fraction of the time a human could (Fawcett & Provost, 1997). On the other hand, Crosley and Anderson say, "AI can analyze and draw conclusions," (Anderson and Crosley 2) which may overstate the

intelligence of AI. Though they make a valid point in saying that AI can analyze data, existing studies have not yet proved that AI can draw conclusions, at least at a consistent rate. Just as Watson failed to correctly understand and answer all of the Jeopardy questions, it is premature to expect AI to be able to analyze a data set and report a conclusion.

Crosley and Anderson end the column with a statement to all firms, big and small, to become thought leaders - another word for innovators - in the field (Anderson and Crosley 2). The problem with the thought that everyone should want to use artificial intelligence and big data is that it may not be appropriate for all forms and sizes of business. Smaller businesses may not have the budget, nor the knowledge or client-base, to implement such advanced technology. Forbes reported CPA practices as the most profitable small businesses in 2010, with an average pretax margin of 17.1%. This margin, though considerably higher than the 10.1% of the next most profitable communication carriers, may not be able to support the drastic increase in budget AI would create (Nelson & Farrell). It is important to consider the increase of overhead, including implementation and support, that would occur, but that is not to say that the initially high costs of the technology will never be affordable for the smaller firms.

“The Emergence of Artificial Intelligence: How Automation is Changing Auditing” by Kokina and Davenport connects their research in artificial intelligence with the audit process. Kokina and Davenport adapted a breakdown of the audit tasks by structure using an earlier study from M. J. Abdolmohammadi. The table below illustrates their adaptation, which shows how we can implement artificial intelligence into auditing (Kokina & Davenport 1).

Mary Shacklett, the president of Transworld Data, a technology research firm, describes the difference between structured and unstructured data as it pertains to big data in her article,

“Unstructured data: A cheat sheet.” Her descriptions of the two categories are a helpful aid in understanding Kokina and Davenport’s table (table 1) (Kokina & Davenport 2).

**TABLE 1**  
**Aggregate Task Structure**  
**Adapted from Abdolmohammadi (1999)**

<b>Audit Phase</b>	<b>No. of Tasks</b>	<b>Task Structure</b>		
		<b>Structured</b>	<b>Semi-Structured</b>	<b>Unstructured</b>
Orientation	45	7 (16%)	14 (31%)	24 (53%)
Control Structure	75	10 (13%)	58 (77%)	7 (10%)
Substantive Tests	171	114 (67%)	54 (32%)	3 (1%)
Forming an Opinion and Financial Statement Reporting	41	0 (0%)	9 (22%)	32 (78%)
<b>Total</b>	<b>332</b>	<b>131 (39%)</b>	<b>135 (41%)</b>	<b>66 (20%)</b>

Under the “Audit Phase” column, the two authors list orientations, control structure, substantive tests, and forming an opinion and financial statement reporting. To clarify, orientation would be the initial stages of the audit, when the auditor is identifying potential risks and weaknesses in the company’s controls. Next, the auditors test the control structure itself by testing how each control operates and its effectiveness. Then, the auditors test samples of transactions to see the control from a quantitative view by looking at the financial statements and transactions for errors that could indicate a weakness or lack of controls. Finally, the auditor will form an opinion, stating whether they believe that the company was in accordance with GAAP and providing assurance that no significant misstatements exist.

According to Shacklett, structured data fields “are aligned side-by-side in fixed record lengths, with specific data fields appearing at static locations within each record. (Shacklett).” In audit, this could mean standard invoices, checks, and purchase requisitions (Shacklett).

According to Kokina and Davenport, these tasks represent 39% of the average audit. This research is influential in that it indicates there is already an opportunity for artificial intelligence to assist in almost half of the audit. Because structured tasks involve data the artificial intelligence can collect and analyze on its own, it would allow for low human involvement in routine tasks (Kokina & Davenport 2).

Alternatively, as described by Shacklett, unstructured data has no set format. Examples of unstructured data includes pictures, social media, and videos. Unstructured tasks, similarly, vary from task to task (Shacklett). Kokina and Davenport pass over using artificial intelligence for unstructured tasks, implying AI will have no role in these functions. I would argue, on the other hand, AI is helpful in reading unstructured data, as emails and phone conversations would reveal important anomalies not captured by the company's accounting information systems and other financial records.

For the purposes of this paper, it may have been more illustrative if Kokina and Davenport had elaborated on the tasks they considered structured and unstructured. Rather than assigning a number to each category, listing the tasks under each respective area would have allowed for additional analysis by themselves and their peers. Because semi-structured is a relatively vague term, it would be helpful to know how structured these tasks are to analyze how effective AI would be in completing them. Assuming all semi-structured tasks can partially be applied to AI, the technology could then automate up to 80% of audit tasks. This would effectively leave 20%, or 66 tasks, for the auditors to complete (Kokina & Davenport 2).

Kokina and Davenport cover the entirety of the audit process, yet never mention how artificial intelligence may be used to identify a company's weaknesses that could result in

fraudulent acts. This would be an important addition to the technology they propose, as machine learning possesses the capability to examine data that is needed when investigating fraud.

### **A Description of Fraud**

Donald Cressey described three factors that influence fraud: opportunity, rationalization, and pressure. These three components combine to create the fraud triangle. According to Cressey, for fraud to occur all three of these factors must be present. First, the opportunity for fraud arises when the employee notices a deficiency of internal controls for a process (Albrecht, Wernz, and Williams 21). Next, rationalization occurs when the employee feels justified to commit fraud. For example, some employees may believe they deserve more money, or that the company owes them, so they are entitled to the money they steal (Albrecht, Wernz, and Williams 46). The final factor, pressure, can be internal or external. In the case of misappropriation, the pressure is most likely financial. Common examples would be medical bills, gambling costs, or an addiction of some sort. On the other hand, employees may face an internal pressure from management to commit financial statement fraud. Financial statement fraud includes overstating revenue or understating expenses to increase the company's net income and earnings (Albrecht, Wernz, and Williams 20).

Jonathan Marks expands upon Cressey's theory of the fraud triangle with his own interpretation, the fraud pentagon. The fraud pentagon includes Cressey's original three components, rationalization, pressure, and opportunity, but includes competence and arrogance as additional components. Marks explains arrogance and competence account for human elements which correlate with the profiles of infamous fraudsters, such as Bernie Madoff and Mickey Monus. Arrogance, in Marks terms, is an attitude of superiority and overconfidence. These people believe they are above their company's internal controls. Competence is the

intelligence required to successfully commit and conceal the fraud. Competence may include the social skills to deceive coworkers into breaking company policy to further conceal the fraud (Marks). One example provided by Albrecht, Wernz, and Williams in their book “Fraud: Bringing Light to the Dark Side of Business” described an employee who abused company policy stating invoices under \$500 did not need secondary approval (Albrecht, Wernz, and Williams 22). He created a shell company that he used to charge his employer with false invoices under the \$500 threshold. Eventually, to speed the process he convinced a coworker any invoices under \$750 did not need to be approved by a second source. Although the coworker knew the policy called for amounts over \$500 to be approved, he trusted the employee’s judgement. This not only showed the fraudster’s arrogance that he could get around the \$500 authorization, but also competence to convince another employee to break the rules (Albrecht, Wernz, and Williams 22).

The Report to the Nations found that a staggering 89% of the frauds were considered asset misappropriation, a term to describe employee theft, costing the average victim \$130,000 (ACFE 4). To make matters worse, 46% of PWC’s respondents said the costs of the investigation into their fraud was equal to or greater than the loss from the fraud (PWC 10).

Detecting fraud can be difficult if the employee conceals what they embezzled. In 97% of cases reported in 2016, the fraudster used some form of concealment. Although a critic may ask why the auditors did not find the fraud, only 15% and 4% of frauds were discovered by internal or external audits, respectively (ACFE 16). The American Institute of Certified Public Accountants’ Statement on Auditing Standard No. 99 states that auditors must consider fraud, identify risks of fraud, and assess these risks using appropriate audit evidence (PCAOB). Coenen, a certified fraud examiner who wrote an article called “Why Didn’t the Auditors Find the

Fraud?” argues there are reasons an auditor may not discover a fraud. In addition to the limited amount of exposure an audit has to the population due to sampling, the fraudster may have altered supporting evidence to conceal the discrepancy (Cohen 1).

The most common alert of fraud comes from tips, 40% of cases. Other forms of detection include internal audit (15%), management review (13%), by accident (7%), account reconciliation (5%), document examination (4%), external audit (4%), notified by law enforcement (2%), surveillance and monitoring (3%), IT controls (1%), and confession (1%). In cases in which a tip was given, 53% of the time it came from an employee of the company, while 21% of the time it came from a customer (ACFE 16)

To address the issue of fraud, 54% of firms performed a general fraud risk assessment. 10% were on the opposite end of the spectrum, performing no risk assessments in their firms whatsoever (PWC 6).

### **Using Artificial Intelligence to Detect Fraudulent Activity**

Although the accounting industry is slow in improving its technology, it can learn from the banking industry. According to Kassner, AI can use algorithms, along with past data from cardholders, to create a model that detects fraudulent activity in real-time. Rather than flagging transactions as “fraudulent” and “not fraudulent,” the system assigns each a probability of being fraudulent. Using this method, any transactions over a certain risk threshold will immediately be rejected at the point of sale (Kassner). First of all, I believe Kassner’s application is more likely machine learning rather than AI. The difference being that the algorithm used to determine whether the transaction is fraudulent is based on past examples rather than the machine using human-like judgement. Norvig emphasizes the human-like capabilities as being artificial



intelligence's competitive advantage (Norvig 2). Similar to a human, the goal of AI is for it to be able to not only recognize a problem but be able to competently solve it without set rules. In machine learning, the algorithm would recognize that, for example, the cardholder is using their card in California when they used the card a few hours before in Pennsylvania. This would be a simple application of machine learning, which would recognize the sudden change in pattern and flag the transaction as fraudulent.

Information the system may use includes "cardholder purchasing behavior, buying history, recent activity, and information stored in cookies." This system could be applied to an accounting information system using a similar structure. For example, payments to vendors could be checked for accuracy using payment history, vendor trustworthiness, and vendor location (Kassner).

Apex Analytix already uses consecutive invoice numbers as an indicator of fraud in their risk analysis service (Apex Analytix). Deloitte also recommends a search of the following to spot fraudulent invoices:

- The company name listed on the invoice is not a registered company;
- No physical address is listed (do not solely rely on email addresses);
- The contact information listed on the invoice may not be legitimate. i.e. the PO Box number or telephone number might not actually exist;
- Incorrect/invalid dates may be present, such as 31 February 2013 for example;
- Invalid goods and services tax (GST) numbers or incorrectly formatted GST numbers;
- The GST value on the invoice may be incorrectly calculated;
- Often a very brief description is listed that is insufficient to adequately detail the goods or services being invoiced, such as "services as requested" or "supply goods as requested";
- Casual or sloppy grammar, spelling mistakes etc.;
- No tax invoice details;
- No remittance details; and
- The invoice is created using Microsoft Word.

The factors above are based on structured data, which can be used by AI in its predictive analysis (Deloitte).

According to Business Insider's Matthew Cochrane, Mastercard is working to protect its customers from fraud as well, using AI to be a real-time decision-maker. The tool, which uses machine learning, assigns each transaction a score that is later used to judge future payments. The first problem Mastercard was hoping to solve using the machine learning was false declines, which stopped legitimate transactions being made by the customer. In addition to being annoying for customers while trying to make a purchase, it can be even more irritating when the card is deactivated, requiring the customer to order a new credit card. Using machine learning, the tool can more accurately predict a transaction based on previous purchases, thus decreasing the frequency of these false declines.

Cochrane cites a 2015 study that showed 15% of cardholders experienced a false decline, leading to 40% of these subjects abandoning their credit card (Cochrane). Evan Schuman of Computerworld argues that though the new plan by Mastercard sounds intriguing, it is nothing new and has been established by companies such as Forter, Signifyd, Smyte, Stripe Radar, Sift Science, Ravelin, Riskified and Feedzai. Schuman finds the use of machine learning to be useless for Mastercard, as they do not have enough market share, nor transactions, to create an algorithm that can accurately score legitimate transactions (Schuman).

## II. My Proposal For a New Tool

As stated before, companies are focusing primarily on the opportunity component of the fraud triangle rather than pressure or rationalization. Although this could be attributed to the ease of eliminating opportunities for fraud by strengthening internal controls, it does not account for unknown control weaknesses. For example, should an employee mistakenly stumble upon a lack of segregated duties, Cressey's theory implies that the employee may be willing to commit fraud if they are facing a pressure and can rationalize their actions. For management to discover an opportunity can be difficult, as employees may find a lack of controls that management has not noticed. Pressure and rationalization, on the other hand, are often foreseeable. According to the 2016 PWC survey, only 34% of companies address rationalization and pressure components of the fraud triangle, while 50% of companies work to eliminate the opportunities for fraud (PWC 24).

I propose a tool that bridges the gap between fraud risk assessment and machine learning. To address the lack of checks on the rationalization and pressure components of the fraud triangle, the tool would review intercompany communication using machine learning to identify potential fraud risks. The communication channels to be utilized would include company emails, company instant messaging platforms, and the records of incoming and outgoing phone calls. Approximately 37% of companies the ACFE surveyed use some form of data monitoring (ACFE 26). This means companies are already recording emails and storing other records of communication.

Machine learning presents the opportunity to use prior cases of fraud to identify similar patterns and keywords within the monitored intercompany communication. The keywords the

company would be looking for would be those that indicate motive for fraud, including, but not limited to: living beyond their means, financial difficulties, family problems, issues with addiction, or feeling dissatisfied with the company for some reason.

Individuals can be under financial pressure for a multitude of reasons. Some people may encounter high amounts of debt due to a personal illness, a spouse or child with an illness, poor credit, college loans and mortgage payments, as well as an addiction to gambling, drugs, or alcohol. Others may simply live beyond their means, such as affording expensive homes, vehicles, and gifts for a secret lover (Albrecht et al. 2). The 2018 Report to the Nations found that 41% of fraudsters were living beyond their means, 29% faced financial difficulties, 14% were divorced or had family problems, and 10% had an addiction problem (ACFE, 44).

Living beyond an employee's means would describe a situation in which a person has a desire to spend more money to improve their lifestyle. Though it could be used to describe someone who lives paycheck-to-paycheck, the phrase would also describe someone living a wealthy lifestyle who wants to have an even higher standard of living. This could mean transitioning from living off \$100,000 to \$250,000, for example. Often, these types of individuals change their lifestyle rather suddenly, buying expensive cars, houses, and clothing. Though a machine cannot determine what an employee is wearing based on their emails, it could discover their new spending habits. If said employee sends an email to a coworker talking about a "new car", uses the email to speak with the dealer, sends a picture of the car, or talks to someone about the car on a company phone, the machine learning tool would understand the phrases used to describe their purchase of a car. It would be important for the machine to understand who is buying the car rather than simply the transaction occurring in general.

Financial difficulties may not be as obvious as the lifestyle changes in the previous section and as a result, they may be harder to detect. In my opinion, individuals facing financial burdens from illness, job loss, debt, etc. may feel pressured to commit fraud not only to alleviate their debt, but also to maintain their image. Someone in debt might feel their reputation would be ruined if their employer or coworker discovers the debt. The keywords the machine may look for in this instance could include any mention of “debt”, “loans”, and “borrowing” from others, such as family and friends, or in the case of medical pressures the keywords may include words such as “hospital,” “cancer,” and “chemotherapy.”

As it pertains to addiction, the employee could have dependencies on gambling, alcohol and drug use. In my readings, I have found many cases of gambling addictions resulting in millions of dollars in losses. The employee may start with losing their own money, then cover their own losses with embezzled funds. The employee rationalizes that those funds will be used in gambling to win back the initial losses, plus the amount embezzled. For example, the machine would be programmed to understand that mentions of trips to Las Vegas and Atlantic City could refer to gambling. For it to result in a high risk, though, the employee would need to use keywords associated with gambling during multiple occasions over a long period of time to separate those who go on infrequent trips and those who go often. Keywords may include “casino,” “Las Vegas,” “Atlantic City,” “over/under,” or any other terms that can be associated with gambling. For each of the examples provided, it is important to identify that the employee may be facing a financial strain as opposed to simply speaking about the topic. The difference is that, in the example of medical hardship, the former would likely mean the employee is a caretaker, while the latter situation could be an employee talking about a friend or distant relative in the hospital, which likely has no impact on the employee’s financial situation. The machine’s

algorithm would need to see specific patterns of usage for each situation to decide whether an employee meets the required criteria.

I propose using a measuring algorithm that would generate a “scorecard” which would highlight the factors I mention earlier. This, along with other indicators of potential fraud, considered together point to a higher risk. At the end, the scorecard should be able to accurately assign each employee a likelihood of committing fraud. Below I have included a depiction of the scorecard concept.

To train the machine, past examples of data that illustrate each of the scorecard’s criteria will need to be provided. This would mean showing the machine emails from many employees who committed fraud due to an addiction, for example, which will allow it to find keywords and phrases that were common between these employees. The primary goal is to give the machine enough data that it can differentiate between an employee who should be considered a positive result (an addict) and an employee who should be a negative result (not an addict). As the number of samples for the machine to use increases, the more accurate its algorithm will be.

# Sample Scorecard

Source	Factors	Meaning	Assessed Risk										
<b>HR database</b>													
Gender Orientation	Male or female	Male is more common for fraud	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
Marital Exemption	Change in status	Could indicate divorce or marriage											
DOB	Age	Certain ages more likely to commit fraud											
Salary													
Job title responsibilities	Financial/accounting	Access to more opportunities											
Level of authorization	Dollar amount												
Medical elections	Children/dependents?	Financial pressures											
Garnishments	Alimony or other payments	Financial pressures											
Completed trainings	Lack of anti-fraud training	May not know consequences of committing fraud											
<b>LexisNexis</b>													
National Crime file	Past legal issues	History of criminal acts	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
Employment history	Number of jobs	Not a good or trustworthy employee											
Borrowing history	Debt	Financial pressures											
Education verification	Do they have a degree												
Eviction record	Evicted	Financial pressures											
Rental payment history	Defaulted on payments?	Financial pressures											
Retail theft contributory database	Unethical past behaviors	History of criminal acts											
Sex offender registry	Unethical past behaviors	History of criminal acts											
<b>Journal entries</b>													
Amount	Around their authorization level	Possible frauds	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
Time	Before or after workday	Working to conceal fraud											
Day of the week	Weekends	Working to conceal fraud											
<b>Time log</b>													
Clock in	Clocking in late?	Lack of respect for employer or external pressures	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
Clock out	Clocking out early	Lack of respect for employer or external pressures											
Sick days	Too many?	Working to conceal fraud if none, may not like company or have medical issue if all used											
Vacation days	Any used?	Working to conceal fraud if none, may not like company if all used											
<b>Communication (email, phone, IM of company)</b>													
With vendors	Topic of conversation and number of communications	collusion	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
Negative emails to employees	Words used and frequency	defensive or hostile behaviors											
Mention of new purchases	Purchases discussed, price of items, and frequency	Lifestyle changes											
Negative email about denial of promotion/raise	Words used and frequency	rationalization											
Emails with a lawyer	Topic of conversation and frequency	Legal offenses											
<b>Communication (private email, phone, IM)</b>													
Email with prior employer	Topic of conversation	Reasons for termination	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
Topics and senders	Frequency and subjects of email	Could indicate frequent purchases that demonstrate lifestyle											
<b>Social Media</b>													
Pictures	Pictures of expensive items	Lifestyle change	<table border="1"> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> <tr><td> </td></tr> </table>										
	Pictures of trips	Lifestyle change											
	Pictures showing alcohol, drugs, casino	Addictions											
Posts about company	Negative posts	rationalization											

The sample scorecard I created on the previous page can be used to identify risks of fraud based on the four following columns:

1. Sources: I decided to incorporate this column into my scorecard to track where the information for each criterion can be obtained. The majority of the sources proposed are likely to be collected by the company, such as LexisNexis data and criminal history when doing a background check on new hires, while the human resources database and time logs are recorded internally. The column also specifies the specific record in the source provided. For example, the human resource database stores the *gender orientation*, from which the factors are shown in the next column.
2. Factors: This column describes the data being collected from the source specified. Continuing with the gender orientation example, the factors would be either male or female, which is then given a meaning in the next column.
3. Meaning: This column's purpose is to explain how the factor pertains to fraud. It will be important for the party who develops this technology to consider that some factors are more likely to be related to fraud than others. For example, gender orientation is demographic and would not be equally weighted to an attribute more common in fraudsters, like an eviction record, that is a behavioral indicator.
4. Assessed Risk: This column is simply used for the machine to "check" each category that is considered a risk. Therefore, at the end, the number of assessed risks can be added to calculate how likely the employee is to be committing fraud.



To decide the factors that would be included in addition to the communication between employees, I used the “red flags” the ACFE found to be most common in fraud cases and created a method for the machine to be able to determine if this red flag was met. Gender orientation is a useful indicator because 69% of fraud cases were committed by males compared to only 31% by females, showing that men are more likely to commit fraud (ACFE 38). Although this is an insightful factor, I think it should be weighted relatively lower because it does not account for an employee’s level of ethics and is biased towards men when women are also capable of committing fraud. Again, 41% of frauds are committed for the employee to live beyond their means, which is why the machine should receive information about the employee’s salary, their garnishments, and medical elections (ACFE 44). The machine cannot properly decide if an employee is living beyond their means if it does not know their means to begin with.

I also included LexisNexis as a source of the employee’s criminal background. I believe that a criminal background is indicative of the individual’s ethics. Even though a record in the retail theft database is different than embezzlement, it demonstrates the person’s capability to rationalize stealing. This is similar to other forms of crime, such as a traffic ticket. The person has the mindset that they are not held to the same rules and laws as their peers. Additionally, LexisNexis can provide prior employment history. A person with an extensive employment history could be explained by poor work performance or behavior while working for previous employers. In 15% of cases, the ACFE found that employees who committed fraud were either punished or terminated by prior employers (ACFE 42). These factors are difficult to track without explicitly contacting previous employers during the hiring process, however, in my opinion, it would be sufficient to use the number of previous employers as an indicator.

I believe incorporating the time and attendance log could be used to find anomalies of employee activity. An employee who is coming into work significantly earlier than their peers and posting journal entries could reveal that they are trying to conceal the entries from coworkers, while staying well past their ending time could reveal the same concern. The machine could also use its pattern recognition to identify changes in an employee's clock-in and clock-out times. If the employee typically leaves between 5pm and 6pm every evening, but suddenly begins leaving at 9pm, this could be a risk of fraud, though it could be also be attributed to other non-fraud workplace factors, such as preparing for the company's annual audit. The journal entry log can be used in conjunction with the time and attendance log. The journal entries will show if an employee posted outside of the normal work time, but can also show the amounts being entered. The human resource database should store the employee's authorization amount, meaning the dollar amount they can post in a journal entry without needing approval. If the employee is consistently posting just below this amount, it may show that they are trying to avoid the authorization controls and possibly posting fraudulent entries.

The list of factors on the scorecard is not comprehensive and should be expanded by the developer. Once the weighting is decided, the scorecard will use the criteria provided to generate a risk score that shows the employee's probability of committing fraud. One option would be to use percentage risk. For example, a "0%" risk would mean the employee is extremely unlikely to commit fraud, while a "100%" risk would be the employee is very likely to commit fraud. Another option could be to use a score out of 200, for example, with a higher score correlating to a higher risk. The distinction between a low, medium, and high-risk employee should also be decided by the developer, as using past data could establish the typical score for a fraudster. If

the average fraudster would be scored at a 70%, then a score around that range should be considered high-risk.

In the event of a high-risk employee, the company should increase their monitoring for the respective department. Because each department has different functions, the company must evaluate the most likely forms of fraud and test accordingly. Below I have provided an example for the accounts payable.

**Accounts Payable:** The most common frauds in the accounts payable department can be identified by examining the company's invoices and vendors. One of the first steps management should take is to look at the approved vendors and to essentially audit the list to ensure they are legitimate businesses. Vendors with unusual names or those that management does not immediately recognize should be investigated further, as this could mean the vendor is fictitious. The investigation should include comparing the listed address to those of employees, and then searching the company's location on a map, such as Google Maps. If the address looks similar to one of an employee or is located in a residential area, there is potential it is a fictitious vendor that the fraudster uses to send invoices for goods or services never received. Additionally, the company should look through the list of invoices for duplicates, which could be recognized by similar invoice numbers, dates, and payment amounts. Many of these activities could use artificial intelligence to make the process seamless and continuous.

It is difficult to predict who would be the initial developer of this technology. The Big Four accounting firms (Ernst & Young, PWC, Deloitte, and KPMG) could take the lead using their large client bases and vast amounts of data, especially because they would be able to incorporate the tool into their services. Mid-sized accounting firms, especially those with the largest revenues and a desire to be industry leaders, may also be frontrunners in creating the

technology. On the other hand, large technology companies like SAP and Oracle already have the tools and knowledge to create the described tool. In my opinion, the big four accounting firms would be the first because in addition to representing another source of revenue, the tool would also assist in the audit itself by presenting the firm with the departments that have the highest levels of risk.

I would then expect the tool to be licensed to small and mid-sized accounting firms to use for their client bases, as they likely do not have the capital, knowledge, and man-power to create a tool themselves. I find that leasing the tool, to clients and to smaller accounting firms, would be the best option for the eventual developer. Licensees then avoid the enhancement and maintenance costs associated with the tool. Instead, the licensor can push (automatically install) updates and offer maintenance services included in the license. The updates would not be specialized for each client, saving the accounting firm or developer money by only having to send one version of updates all at once.

Privacy is one of the most important concerns in successfully implementing the tool, as employees should be aware that they are being monitored, but also because their private information should be held confidentially. Therefore, a third-party should be employed to ensure this private information is being held securely. The accounting firm would benefit from receiving the licensing fees, and because not every company experiences fraud, the firm benefits from each of these clients who pays for the service, as the only variable cost for each licensee would be the cost of communicating the departments of interest. The company's law firm or an accounting firm that does not audit the company, would be the best choice due to the accounting firm's ability to alter their audit based on the tool's results and the law firm's attorney-client privilege.

An accounting firm cannot provide audit services and consulting services to the same client, which is why the company would have to hire another accounting firm.

In my opinion, a third-party firm would receive the results of the tool every time an employee moved from one risk level to another, such as low-risk to moderate-risk to show increased risk, or possibly high-risk to moderate-risk to show a decreased risk. Whenever an employee moves to a higher level of risk, the accounting firm would alert their client of the change in risk, however, they would not disclose the individual, but rather the department the individual works in. This prevents management from having a bias towards the employee, which could result in the employee realizing they are receiving different treatment than their peers. Instead, identifying the department of increased risk, such as accounts payable, purchasing, receiving, or payroll, the scope is small enough for management to monitor the transactions and controls.

Furthermore, by alerting the company's accounting or law firm of the areas with the highest risk of fraud according to the tool, it may accelerate the audit planning stage, resulting in less audit fees to be paid. The auditing firm may legally be able to rely on the tests run by the consulting accounting firm, as it is an independent source. Although, the firm may wish to run more tests or use a larger sample of transactions in its audit testing to mitigate risk.

Despite the benefits of using third parties, it is difficult to believe companies would willingly withdraw themselves from the process of directly receiving the information about fraud risk and identification of specific employees deemed to be risks. This certainly raises legal and ethical conflicts regarding the access to the details underlying the employee score. If the company is paying an additional cost for the tool, it is understandable that the company wants to see the employee at risk rather than get a broad response depicting a whole department as risky.

It would be up to law or a developer to decide that the tool cannot be used and monitored by the same source, which may decrease the value of the tool to companies. Instead, the tool could be bundled with additional consulting services. This way, customers can justify the slight increase in value of the bundle of services.

I would not recommend the company or the firm confront the employee about their level of risk. Although a company should inform employees about monitoring the network, the company should not disclose risk scores to the employees themselves. This disclosure could cause employees to feel targeted and provide further rationalization to commit fraud. In my opinion, disclosing scores to employees would also likely result in a lower level of productivity and higher rate of social isolation. My suggestion would be to limit those that could see the results to a third-party.

Critics may argue that employees will be more aware of their actions after hearing of the new technology, making it useless in discovering their fraud. Personally, I do not foresee employee awareness being an issue. In fact, I think that it could dissuade employees from committing fraud similar to a camera in stores discouraging customers from stealing.

The proposed tool would benefit companies of all sizes by increasing the monitoring of fraud indicators and risks, thus saving companies more than the current tools available. In some situations, I would expect this tool to prevent fraud. Because the tool identifies qualitative signs of someone who may commit fraud, it allows management to impose better proactive measures, such as improving or increasing internal controls. Otherwise, the tool would be best used to detect fraud earlier, thus decreasing losses and time spent on an investigation.

## Obstacles

The most significant issue with the tool would be the sensitivity of information used to determine the employee's score. As it pertains to privacy, I believe this will not only be the greatest obstacle for the tool to be successful, but also to being developed. There will need to be a focus on keeping the data safe and preventing unauthorized access. The machine should be the only party seeing the raw details of an employee's score. For example, I believe the employee has a right to know a human is not viewing their medical history or conversations over email about a hospital visit. Although a history of hospitalization is indicative of financial pressure, the results of the scorecard should only show broad details, such as "high financial pressure due to medical expenses," as opposed to "employee has been receiving chemo treatments for a cancer diagnosis." Then, if a third party is being used, they can inform management of the department with the elevated risk without disclosing the employee or the reasoning for their risk.

In addition to monitoring company-managed emails, the possibility exists to include personal emails if the data is being sent using the company server, meaning over the company's internet or on their equipment using a virtual private network (VPN). During the *Michael A. Smyth v. The Pillsbury Company* court case, the court set a precedent that a company has the right to search an employee's email sent through the company server if it is for a business purpose ("Michael A. Smyth v. The Pillsbury Company"). Despite the current legality of monitoring private emails, I consider this to be an invasion of privacy. In my opinion, accessing an employee's personal email is unethical, even if it is to protect the business, because private emails contain information that is typically not relevant to the company. On the other hand, if employees use their work email for personal reasons, I believe this was an inherent risk they decided to take. I understand the increased likelihood that employees discuss the factors included

on the scorecard in their private emails in place of their work email, though there are additional consequences that come with monitoring private emails. First, employees should be made aware of the fact they are being monitored. Monitoring communication in general is likely to evoke frustration from the employees, but monitoring private emails is imposing on the employee's privacy. I would imagine employees would feel betrayed and have resentment towards the company, as it reveals that management lacks trust in its employees.

On top of posing an ethical issue, collecting private information on employees can be considered a legal issue depending on how the information is used and if the company's security is compromised. According to Chron's J. Mariah Brown, employees are provided the right to privacy as it relates to health records. HIPAA requires that employers request permission from the employee before obtaining the employee's health records, or else they will not be released. It is legal, though, for an employer to require a doctor's note in the cases of sick leave, workers compensation, wellness programs or health insurance (HIPAA Within the Workplace). An employer risks a law suit if they discover their employee's medical condition through the machine learning. If the monitoring occurs over a work email, I think it is likely the courts would rule in favor of the employer due to their ownership of the email server, however, if the emails are sent through a private email, I think it is likely the courts would rule it a violation of HIPAA because there was no formal request for the information.

Should an employer terminate an employee, I believe it would be difficult to prove the termination was not wrongful based on what the employee has sent over email. Cornell Law School defines wrongful termination as, "a fired employee's claim that the firing breached an employment contract or some public law" ("Wrongful Termination"). If the employer has collected information from an employee, whether it is on a private or work email, there is the



possibility a terminated employee may claim the company was discriminating them based on emails they have sent. In a scenario when an employee tells a coworker over instant messaging about their pregnancy, the employee may claim this was the grounds for their termination if management cannot prove otherwise. Regardless of the reason for management's decision, employees may have the ability to prove, or at least argue, discrimination was a factor.

Ancillary to information privacy, it is important to address the concern of security. It is crucial for the success of the proposed machine that the information stored is secured. In addition to all the company data already being stored, now private employee information is threatened by unauthorized access of the database. Whether it is external hackers or internal intruders obtaining the data, the trust of employees, which could already have decreased with the implementation of the machine, will be lost if other parties access their information. It could ruin their chances of receiving jobs in the future, as well tarnish their reputation within and outside of the company. Before a full implementation, the developer or company involved would need to ensure the risk of being hacked is little to none.

False positives and negatives could become an issue as well. During the beginning stages as the machine learning is just starting to create a predictive model, there will be a question of how often the machine should generate a positive result. There will always be an effort for more positive results because false positives, when an individual who is not committing fraud but determined to be a higher risk, are easier to accept are false negatives, meaning a fraudster is not classified at a higher level of risk. The drawback to having many false positives is that it warrants more time from management to follow up on the report. Despite the fact a positive result allows management to address potential issues, the more often that the machine produces a false positive, the less likely, in my opinion, management will take the risks seriously. To

encourage uniformity of investigations, companies adopting this technology should provide a detailed outline of how management should approach the risk of fraud and enforce compliance with the set procedures.

To increase the machine's accuracy, I found in my research that the best option is to continuously train the algorithm by showing it positive and negative results, then testing whether it properly identifies certain situations. For example, a fictitious employee can be created as a test to determine who the machine will treat as a risk and who it will ignore. One test may be to send an email to another employee, saying "I can't believe they wouldn't give me a raise after all of the years I have worked for this company. You would think they would show some appreciation for all of the money I have made them." This is just one example, but it would be crucial that the machine have enough evidence to identify the employee's negative emotions towards the company and the subject revolving around their salary. If the machine does not identify the result as a potential risk, it would mean there is a deficiency in the machine's rating system for a specific category on the scorecard. In this case, the machine's effectiveness in determining rationalization looks to be inefficient.

A reason management may not properly investigate a report of fraud could be due to bias. The tool is designed to eliminate human bias as much as possible, but that cannot always be achieved. The flaw with the tool is that even though the process of obtaining the information and judging the individual lacks bias, the burden is on management to find or prevent the fraud. Management will only know the potential origins of the fraud based on the department, yet management can impose bias into the process by failing to monitor or investigate a specific employee in the department based on trust or favoritism. According to "Fraud: Bringing the Light to the Dark Side of Business," 70% of fraud cases occur after the employee's fourth year,

meaning these employees are likely to have relationships with their coworkers and possibly be viewed as people incapable of harming the company (Albrecht et al. 21). To fight this preference for bias, I believe no employee, including management, should be exempt from investigation or investigated differently from others.

On the other hand, management could exhibit a negative bias by further investigating an employee they expect could be the perpetrator. Using a uniform strategy of investigating also prevents management from exhibiting negative bias towards the employee. It is also important that management does not treat this employee hostilely through unfair actions or words that may indicate suspicion. Even if they are suspected to be the fraudster, they must be treated equal to other employees.

One interviewee, who asked to remain anonymous, provided the example of machine learning's role in hiring employees, basing its judgement of a fitting employee on prior hires. The company's employee base in the past had been primarily men, as women simply did not apply as often. Suppose a female applies for a position in the company along with equally experienced men. It is possible the machine would decide the female is not a suitable employee because she does not match the previous pattern of male employees (Anonymous). Although this is an important distinction, it could cause bias in creating a false negative or false positive result. A male and female facing identical financial issues may generate different results. Because a male is more likely to commit fraud, the male employee could be viewed as the more likely threat and falsely accused of fraud, whereas a female's probability of fraud could be decreased due to her gender.

### III. Conclusion

Many accountants are focused on the effort to automate audits and other areas of work, but are neglecting fraud, which continues to damage companies of all sizes. The tool I present offers the capability to continuously monitor for risks of fraud with minimal need for human intervention. The criteria used to measure the risk is comprised of data already stored by many companies, primarily inter-company communication, but also consist of additional risk factors that includes the company's time and attendance log, recorded journal entries, LexisNexis, and the human resource database. The benefit of security comes at a price, however, as privacy concerns would need to be addressed. The court system will need to provide additional guidance on the legality of employers monitoring private emails. Nonetheless, the tool offers an extra layer of security for companies while presenting additional revenue opportunities for a willing developer

## IV. Appendix

### Thoughts from Professionals

Eight experts from the accounting and intelligent automation fields were interviewed to provide a current perspective. The experts were asked an assortment of questions based on their field of study and the most prominent questions surrounding both fraud and artificial intelligence. I considered the following responses in my planning and analysis of the tool that I have proposed:

#### 1. Abhijit Akerkar –

Mr. Akerkar is an AI Strategist and Business Integrator at Lloyds Banking Group. My primary concern for this interview was discussing the security of AI as a result of the many companies who have been impacted by cybersecurity attacks. Mr. Akerkar says that the developer of the AI would need to have the confidence of their clients that their data is safe and their privacy is valued. This means it is imperative there is trust on both sides, for the client and the developer.

Because AI has grown in popularity due to “cheaper computational power and availability of open source algorithms,” it has the capability to make the technology more affordable, potentially for smaller companies and accounting firms. However, Mr. Akerkar believes the Big Four will have a considerable investment in this technology because they typically audit large, public companies that hold the most data. Despite the costs of integration and training, he believes that any firm who is an early adopter of artificial intelligence will likely be winners.

## 2. Anonymous Interviewee 1 –

This anonymous interviewee is a Data Scientist for a Big Four accounting firm. We discussed the use of AI for an audit setting rather than the specific use for fraud investigations. The interviewee believes privacy and confidentiality concerns have been addressed for the most part, though security threats are constantly evolving. We went on to discuss that many IT organizations will argue that managing data on-premises is safer than using cloud storage. For a Big Four accounting firm, their IT organization is the group that manages both cloud and on-premises storage. According to this interviewee, cloud technology is highly sought out for its ease of management and ability to rapidly develop the associated technology, such as the tool I suggest in this paper.

This person foresees many possibilities for who may develop and who may lease an AI tool. The Big Four firms may outsource pieces of AI from tech companies, such as Oracle and SAP to avoid the costs associated with managing the technology, however, they may also build their own, which presents the ability to create something innovative and new. If so, the tech companies would likely sell the tool to smaller firms as well. The smaller firms are much more difficult to predict. While some may have the resources to create such a technology, others may not. We could see smaller firms developing a specialized version that follows their business model, but again, this is difficult to predict.

The emphasis of creating this AI-based tool would be on increasing client value, meaning we offer increased value for the same price. In fact, if we automate, the AI should decrease the length of the audit, therefore decreasing the price the client would pay. As regulations are scaled-back to allow automated processes to replace or assist with regulated processes, it could allow the auditor to spend more time in their analytical role.

To describe the importance of data, they said “data is the true gold.” Companies will use data for a variety of tasks, including the capability of analyzing emotion using email archives, for example. The firm could use their clients Human Resources database to obtain the information, but this poses a privacy concern. It could be a concern for companies to allow third-parties access to private employee data.

### **3. Becky Walck –**

Ms. Walck is a Principal at Simon Lever. In her experience with Simon Lever and Ernst & Young (EY), she has been able to see the differences between audits in a Big Four firm as well as a regional firm. Simon Lever uses different programs than the Big Four, which require more manual work due to the difference in her client’s accounting systems. The larger companies, while she worked for EY, had more sophisticated accounting systems than the smaller firms she works with now. When her firm extracts the entries, they test material and round numbers using the consolidated audit trail (CAT). This will compare the categories assigned to accounts and whether the journal entries booked are unusual. Other forms of fraud assessment include authorization checks, dates and times of the entries, and a Benford analysis for the A/P records to show the distribution of numbers against the assigned tolerance. The focus of the authorization checks is to examine whether an employee was making entries outside of what the company allows them to post. The dates and times may show an employee who is posting an entry on an unusual date, such as late at night or during the weekend.

Signs of fraud also include the use of vacation days. An employee who uses no vacation days may demonstrate that they do not want someone else seeing their duties or prior work. This is one method an employee may use to conceal a fraud. Alternatively, it is also important to look at the employee’s physical surroundings. If they are making expensive purchases and have gifts

on their desk, this could mean they are living beyond their means or receiving kickbacks in some form from vendors.

Although some employees may be able to justify what looks suspicious, it is important to “trust, but verify.” Other times the discrepancy is due to the subjectivity of accounting principles. As it pertains to tracking employee monitoring, “Would employees appreciate? Probably not. But they should be aware the company owns the equipment.”

#### **4. Anonymous Interviewee 2–**

This interviewee said what we see being used right now in the business industry to process data is not considered AI but is rather automation. These automation programs read through employee emails, IM, and phone messages searching for certain keywords, then assign a score. AI, though, attempts to mimic human behavioral patterns, for example, to make decisions. The most helpful identifiers are behavioral changes that indicate lifestyle. Lifestyle changes may be increased spending habits, mood changes, changes in relationships, as well as time spent working.

One company, for example, searched their social media mentions for angry clients and employees. Their intention, however, was not to look for fraud, but to identify issues that needed to be solved internally (employees) and externally (customers). The company would constantly need to alter how the tech works to adhere to the PCAOB, so it would make more sense to allow a large company, such as Oracle and SAP, to do the work.

“The news media gives the perception AI does the job.” Accountants will remain highly involved, especially in high risk situations and in some areas of decision-making. AI on the other hand will pick up on cues to recognize patterns, then make an educated decision based on the



outcome of its analysis. For now, though, the human is still the decision-maker while AI is the decision aid.

## **5. Emily Bomberger –**

Ms. Bomberger is a CPA and CFE at RKL. In her experience with RKL, she finds that embezzlement is the most common fraud due to its frequency in smaller companies. Because embezzlement is so common, her firm often looks for missing checks and uses Benford's law on the first two numbers of the dollar amount, meaning they look at the frequency of these first two digits. Because "the results are only as good as the data you put in it," she believes AI will make an impact in their company one day, as it will more accurately analyze transactions based on prior data rather than pre-set thresholds.

RKL recommends to clients that they keep track of employee lifestyle choices. She believes a program that uses employee messaging for predictive analysis would "connect the dots," and that "to an extent, employees do not have an expectation of privacy. Personally, I do not have an expectation of privacy when I talk to coworkers over I/M." Companies only receive about 3% of lost fraud money, so a proactive tool would be making a difference.

When it comes to the rationalization for the fraud, "more often than not the fraud is not directed at the company. Their spouse may have lost a job or cannot make ends meet." This means that the fraud is a product of pressure, not usually an act of anger towards their company. The damage of fraud is not usually discovered until the employee leaves the company.

## **6. Christopher McGee –**

Christopher McGee is an advisory partner in risk management at KPMG. First of all, Mr. McGee raised the question of how I would recommend that a company address a positive result. This led to further questions, including: If I would use my approach of monitoring employee email, how high does the probability need to be for it to be worth confronting the employee? He continued by speaking of the importance of data quantity, as it must be enough for the AI to properly identify past instances of fraud. Because supervised learning uses historical data, there needs to be examples of identifiers the AI can use as a basis in its evaluation. This could include structured data, vacations, and the employee's credit score.

His analogy for the possibility of a large tech company outsourcing the tool was “the best salesmen sold the first phone.” Because outsourcing requires sharing the data, which is then used to strengthen the model for other clients of the outsourcer, companies would need to be onboard with their data being shared to others, including competitors. Although these companies will not see the data itself, it would be used to not only benefit your companies, but others.

## **7. Waqqas Mahmood –**

Mr. Mahmood is the Director of Advanced Technology at Baker Tilly. His view of AI used for audits and fraud detection is that there will be a security concern to keep all data behind closed doors. Should the tech use cloud computing, which is very possible, it will need to go through all of the protocols first. Companies will need to ensure their protection against scams and hacking if efficient to avoid the unauthorized access to private employee and company data. He believes the Big Four firms will be the major players in the race to create AI, as they have the money, the clients, and the data to do so.

One concept we discussed was creating a technology that truly thinks like a human. More importantly, I asked about the capability for AI to display human emotion that could be used to make a decision like a human and less like an objective machine. According to Mr. Mahmood, AI already has the capability to understand emotion through facial and voice recognition.

With the introduction of blockchain and voice recognition AI is very close to replacing humans. As long as the accounting adheres to the client's industry, "AI will stand for the digital way of life." Since the Big Four as the data, clients, and people, he believes there is the potential for 30-40% implementation of AI within the next five years and 90% in the next ten years. Low level jobs could soon be obsolete if the technology continues to automate simple and routine tasks, meaning half of the financial audit could eventually rely on digital support.

#### **8. David Hammarberg –**

Mr. Hammarberg is a CFE at McKonly and Asbury. In his experience, Benford's law is the most common tool in finding a fraud. Many clients know where the fraud occurred when the investigation begins, but they struggle to identify the fraud itself. AI could foster improvement of fraud investigations by understanding and searching for violations of company policy. Small details, like the time of day, could be included in the AI's search to identify risks that the fraud examiners could use as a guide for finding the fraud. For the tool I propose, SAP or Oracle would be the optimal developers for the tool, but some companies may want to develop the technology in-house to keep their data safe.

His company, McKonly and Asbury, audit 10% of emails per month, so the lack of privacy is assumed, as it is in other companies. Reading over emails would be best for the internal audit team and checking the time logs of when an employee logs in and out and their

search history would detect time fraud. Some other factors to look for include a lack of taking vacation time, doing the jobs of other people, new cars or other expensive technology, addictions, and potentially other data going through the network, including the employee's private email.

## V. References

Akerkar, Abhijit. Personal interview. 18 October 2018.

Albrecht, Steve W., Wernz, Gerald W., & Williams, Timothy L.

Anderson, Alan and Crosley, Gale. "The Audit of the Future: Daring, Disruptive, and Data-Driven but Poised to Add Significant Value to Firms and Clients." *Public Accounting Report*, Spring 2018. Retrieved from <http://www.crosleycompany.com/1747-2/>. Accessed 17 June 2018.

Anonymous. Personal interview. 12 November 2018.

Anonymous. Personal interview. 14 December 2018.

Barry, Jordan. "Employee Fraud: False Invoicing," *Deloitte Forensic Focus*, February 2015.

Retrieved from [www2.deloitte.com/nz/en/pages/forensic-focus/articles/employee-fraud-false-invoicing.html](http://www2.deloitte.com/nz/en/pages/forensic-focus/articles/employee-fraud-false-invoicing.html). Accessed 11 December 2019.

Bomberger, Emily. Personal interview. 19 December 2018.

Brown, Brown, and Rainey, Steve. "Driving faster, more accurate and more beneficial tax decisions," *IBM*, 9 April 2018. Retrieved from [www.ibm.com/blogs/watson/2018/04/driving-faster-more-accurate-and-more-beneficial-tax-decisions/](http://www.ibm.com/blogs/watson/2018/04/driving-faster-more-accurate-and-more-beneficial-tax-decisions/). Accessed 11 December 2019.

Brown, Mariah J. "HIPAA Within the Workplace," *Chron*. Retrieved from

<https://smallbusiness.chron.com/hipaa-within-workplace-4855.html>. Accessed 13 April 2019.

Chen, Te-Ping. "Workers Push Back as Companies Gather Fingerprints and Retina Scans." *The Wall Street Journal*, 27 March 2019. Retrieved from

[https://www.wsj.com/articles/workers-push-back-as-companies-gather-fingerprints-and-retina-scans-11553698332?mod=hp\\_lead\\_pos11](https://www.wsj.com/articles/workers-push-back-as-companies-gather-fingerprints-and-retina-scans-11553698332?mod=hp_lead_pos11). Accessed 22 April 2019.

Cochrane, Matthew. "How MasterCard is using AI to improve the accuracy of its fraud protection." *Business Insider*, 4 January 2017. Retrieved from <https://www.businessinsider.com/mastercard-artificial-intelligence-fraud-protection-2017-1>. Accessed 22 April 2019.

Coenen, Tracy. "Why Didn't the Auditors Find the Fraud?" *allBusiness*. Retrieved from <https://www.allbusiness.com/why-didnt-the-auditors-find-the-fraud-4967920-1.html>. Accessed 4 March 2019.

"Consideration of Fraud in a Financial Statement Audit," SAS No. 99, AU Section 316, Paragraph .01, *PCAOB*. Retrieved from <https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/AU316.aspx>. Accessed 21 April 2019.

Daniels, Sharon. "Arria's NLG Artificial Intelligence engine now powers Ernst & Young's Natural Language Generation global portal," *PR Newswire*. Retrieved from 9 October 2018, [www.prnewswire.com/news-releases/arrias-nlg-artificial-intelligence-engine-now-powers-ernst--youngs-natural-language-generation-global-portal-300727205.html](http://www.prnewswire.com/news-releases/arrias-nlg-artificial-intelligence-engine-now-powers-ernst--youngs-natural-language-generation-global-portal-300727205.html). Accessed 11 December 2019.

"Deloitte Harnesses the Power of Kira for Lease Accounting Contract Review," *Kira Systems*. Retrieved from [kirasystems.com/resources/case-studies/deloitte/](http://kirasystems.com/resources/case-studies/deloitte/).

Hammarberg, David. Personal interview. 10 January 2019.

Heller, Matthew. "Dems Propose Screening Algorithms for Bias." *CFO*, 11 April 2019. Retrieved from <http://www.cfo.com/technology/2019/04/dems-propose-screening->

algorithms-for-bias/?utm\_campaign=CFOWeekly&utm\_source=CFO-  
email&utm\_medium=email&utm\_content=CFOWeekly\_Friday\_2019-4-12&utm\_term=.  
Accessed 22 April 2019.

Hodges, Andrew. "Alan Turing and the Turing Test," *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*, edited by Robert Epstein, Gary Roberts, Grace Beber, Springer, 2018. Retrieved from [www.turing.org.uk/publications/testbook.html](http://www.turing.org.uk/publications/testbook.html). Accessed 10 December 2019.

Kassner, Michael. "How CallMiner uses analytics to secure customer data and ensure PCI compliance," *Tech Republic*. Retrieved from <https://www.techrepublic.com/article/how-callminer-uses-analytics-to-secure-customer-data-and-ensure-pci-compliance/>. Accessed 12 December 2019.

Kletzer, Lori. "The Question with AI Isn't Whether We'll Lose Our Jobs -- It's How Much We'll Get Paid," *Harvard Business Review*, 2018. Retrieved from <https://hbr.org/2018/01/the-question-with-ai-isnt-whether-well-lose-our-jobs-its-how-much-well-get-paid>. Accessed 30 June 2018.

Mahmood, Waqqas. Personal interview. 12 November 2018.

Manjoo, Farhad. "It's Time to Panic About Privacy." *New York Times*, 10 April 2019. Retrieved from [https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html?emc=edit\\_th\\_190414&nl=todayshadlines&nid=569320730414](https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html?emc=edit_th_190414&nl=todayshadlines&nid=569320730414). Accessed 22 April 2019.

Markoff, John. "Computer Wins on 'Jeopardy!': Trivial, It's Not," *NY Times*, 17 February 2011. Retrieved from [www.nytimes.com/2011/02/17/science/17jeopardy-watson.html](http://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html)

- Marks, Jonathan T. "Fraud Pentagon – An Enhancement to the Three Elements of Fraud," *Board and Fraud*, 21 September 2018. Retrieved from <https://boardandfraud.com/2018/09/21/the-fraud-pentagon-an-enhancement-to-the-fraud-triangle/>. Accessed 10 December 2018.
- Marr, Bernard. "What Is The Difference Between Artificial Intelligence And Machine Learning?" *Forbes*, 6 December 2016. Retrieved from <https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/#7c3a5612742b>. Accessed 17 June 2019.
- McGee, Christopher. Personal interview. 16 December 2018.
- Michael A. Smyth v. The Pillsbury Company. 914 F. Supp. 97. United States District Court, E.D. Pennsylvania. 1996. *Justia US Law*. Retrieved from <https://law.justia.com/cases/federal/district-courts/FSupp/914/97/2131293/>. Accessed 19 February 2019.
- Nelson, Brett and Farrell, Marueen. "The Most Profitable Small Businesses," *Forbes*, 15 April 2010. Retrieved from [www.forbes.com/2010/04/15/most-profitable-small-businesses-entrepreneurs-finance-sageworks.html?boxes=Homepagechannels#66eb9345784e](http://www.forbes.com/2010/04/15/most-profitable-small-businesses-entrepreneurs-finance-sageworks.html?boxes=Homepagechannels#66eb9345784e)
- Norvig, Peter. (2012, November 3). Artificial Intelligence. *New Scientist*, no. 2889.
- Pofeldt, Elaine. "This crime in the workplace is costing US businesses \$50 billion a year," *CNBC*. 12 September 2017. Retrieved from [www.cnbc.com/2017/09/12/workplace-crime-costs-us-businesses-50-billion-a-year.html](http://www.cnbc.com/2017/09/12/workplace-crime-costs-us-businesses-50-billion-a-year.html). Accessed 20 August 2018.
- Saloky, Tomas and Seminsky, Jaroslav. "Artificial Intelligence and Machine Learning," 2005. Retrieved from <http://conf.uni-obuda.hu/SAMI2005/SALOKY.pdf>. Accessed 17 June 2019.



Schuman, Evan. "With A.I. announcement, Mastercard goes for the hype." *Computerworld*, 6 December 2016. Retrieved from <https://www.computerworld.com/article/3146722/with-a-i-announcement-mastercard-goes-for-the-hype.html>. Accessed 22 April 2019.

Shacklett, Mary. "Unstructured data: A cheat sheet," *Tech Republic*, 14 July 2017. Retrieved from [www.techrepublic.com/article/unstructured-data-the-smart-persons-guide/](http://www.techrepublic.com/article/unstructured-data-the-smart-persons-guide/). Accessed 20 August 2018.

Taggart, A. & Nesfield, W. "DeNovo," *PWC*. Retrieved from [www.pwc.com/sg/en/financial-services/assets/fintech/denovo.pdf](http://www.pwc.com/sg/en/financial-services/assets/fintech/denovo.pdf). Accessed 11 December 2018.

Turing, Alan M. "Computing Machinery and Intelligence," *Mind*, 49, 1950, pp. 433-460. Retrieved from [www.csee.umbc.edu/courses/471/papers/turing.pdf](http://www.csee.umbc.edu/courses/471/papers/turing.pdf). Accessed 10 December 2018.

"Vendor Risk Analysis Service," *Apex Analytix*. Retrieved from [www.apexanalytix.com/controls-analytics-software/fraud-risk-monitoring/vendor-risk-analysis-fraud](http://www.apexanalytix.com/controls-analytics-software/fraud-risk-monitoring/vendor-risk-analysis-fraud). Accessed 10 December 2018.

Walck, Rebecca. Personal interview. 19 November 2018.

"Wrongful termination," *Cornell Law School*. Retrieved from [https://www.law.cornell.edu/wex/wrongful\\_termination](https://www.law.cornell.edu/wex/wrongful_termination). Accessed 13 April 2019.