An Exploration of the Impact of Increasing Internet Accessibility of IFAs.

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program University of Toronto

Prepared by Michael Ho

May 31, 2022

For Prof. Leonard Brooks

Table of Contents

1.0 Introduction

With the emergence of the internet and society's ever-growing dependence on the connectivity of the internet, nearly every aspect of daily life has been revolutionized and touched upon by the accessibility of internet connectivity. One area where this change is particularly noticeable would be in the field of forensic accounting; the internet has become more widespread, accessible, and more sophisticated, however alongside such monumental developments of the internet, fraud has evolved alongside it. As a result of this evolution, the role of an Investigative Forensic Accountant (hereinafter, IFA) has also been perpetually changing in order to withstand the evolution of internet fraud. Therefore, this research aims to explore what the future may look like for IFAs with a particular focus on how the internet exacerbates this change. In doing so, there will be a review and discussion on a few modern fraud cases, which have been enabled or amplified as a result of the connectivity of the internet - some examples of this would be phishing or money laundering. Following this, there will be a discussion revolving the future landscape of what IFA engagements may look like; this will be done through a thorough review of possible future IFA engagement areas which have arisen as a result of increased internet accessibility; some examples of these future engagement areas would be cryptocurrency fraud or artificial intelligence (hereinafter, AI) assisted fraud. Subsequently, a discussion on the skills, tools and techniques available to combat internet enabled fraud will be delved into, as well as, how advances in the connectivity of the internet can aid in the IFA profession and where additional training and the best practices will be, given the new landscape for IFA engagements due to increased internet access.

1.1 Objectives

This research project's primary objective is aimed at investigating the impact of increased internet accessibility and connectivity on the IFA profession as a whole. To achieve this primary objective, the following specific objectives will be explored:

- To provide a definition for the term "fraud."
- To identify how modern IFA engagement areas have been affected by the increase in internet accessibility and connectivity.
- To illustrate the amount of harm these fraudulent actions can cause.
- To explain the role in which IFAs serve in these modern internet enhanced IFA engagements.
- To present future IFA engagement areas as a result of increased internet accessibility and connectivity.
- To portray what the future of internet enhanced IFA engagements may look like.
- To indicate which skills will be the most important for responding to future IFA engagements.
- To examine tools which will be the most useful in combating internet enhanced fraudulent actions and behaviors.
- To convey how these tools can be effective for IFAs in forensic accounting engagements.
- To uncover the limitations of these tools in the context of an IFA engagement.
- To discuss techniques and methods of enhancing IFA training to handle internet enhanced engagements.

- To contribute suggestions and best practices for IFAs involved in engagements characterized by the increased internet accessibility and connectivity.

2.0 Defining Fraud

Fraud may appear to be a relatively easy and straightforward concept to understand, however depending on the different circumstances and scenarios, it may be apparent that there are several variations of what constitutes as definitions for fraud. In the Fraud Policy, FN-12 written by Steer et al. within the Chartered Professional Accountant Canada, it provides a definition of fraud, which states that it is any acts that are intended for financial or personal gain through deception using deliberate and intentional means[1]. Meanwhile, the American Institute of Certified Public Accountants (hereinafter, AICPA) defines fraud as "an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception that results in a misstatement in financial statements that are the subject of an audit"[2]. Additionally, the AICPA notes that there are two distinct characteristics which often characterize fraudulent actions: The first is whether the alleged perpetrator possessed the intent to misrepresent financial statements or records, while the second characteristic is the prevalence of financial misstatements as a result of either fraudulent financial reporting or the misappropriation of assets[3]. Fraud is stated in section 380(1) of the Criminal Code of Canada where any individual who obtains benefits through falsified or fraudulent means, whether uncertain or not within this act, continues

[1] Steer, P., Havey, P., Venneri, A., Olfert, R., Gosse, K, & Vasa, C, "Policy Document - FN-12- Fraud Policy," *Chartered Professional Accountants Canada*, November 24, 2022, p. 1, https://www.cpacanada.ca/-/media/site/operational/ex-executive/docs/02313-ex_fn-12-cpac-fraud-policy-nov-24-22-english.pdf. Accessed on April 21, 2023.
[2] American Institute of Certified Public Accountants, "AU-C Section 240 Consideration of Fraud in a Financial Statement Audit," *American Institute of Certified Public Accountants*, 2021, p. 165, https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-c-00240.pdf. Accessed on April 21, 2023.
[3] Ibid., p. 163.

to defraud any person and their valuable security[4]. Therefore, despite numerous definitions of what fraud can constitute, it is evident that there are a few common themes when it comes to defining fraud. One common theme appears to be that fraudulent actions involve the use of deception, concealment or purposeful misrepresentation of financial information, therefore it is apparent that fraudulent actions are ones that are done deliberately or with intention. On a similar note, the motivation for fraudulent behaviour is stemmed from the perspective of personal or financial gain of the perpetrator or to deprive the rightful owner of its use.

3.0 Modern Fraud

A review of the current IFA engagement areas is necessary in order to effectively portray the role in which IFAs currently serve and how increased internet connectivity has changed the landscape of IFA engagements. Additionally, the increase in the usage and accessibility of the internet can create potential implications for a variety of IFA engagements, therefore making it crucial in identifying the three types of areas within IFA engagements; the three types of areas that will be discussed are: phishing, money laundering and intellectual property theft and infringement. In identifying and reviewing such areas, the potential societal harms that result in these engagements will be discussed while also exploring the role forensic accountants play in order to address such concerns.

3.1 Phishing

Phishing is defined by Lastdrager as a deceitful act where a perpetrator attempts to gain sensitive or personal information from a specific target through impersonation methods. This act of deceit can be scaled accordingly[5]. In coming up with this definition

[4] Criminal Code, RSC 1985, c C-46, s 380(1).
[5] Lastdrager, Elmer E. H., "Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature," *Crime Science*, 2014, Vol. 3, Iss. 9, p. 8.

for phishing, which has been exacerbated as a result of the increased connectivity of the internet, Lastdrager reviewed 536 peer reviewed publications and analyzed 113 distinct definitions for what should be included in the constitution of the definition of phishing. They note that the most important elements to a phishing fraud would be the use of deception, impersonation, scalability of the fraudulent act, and a suitable target which includes information regarding the target[6]. Ali and Mohd Zaharon note that due to a rapidly increasing digital world where internet connectivity is available on numerous electronic devices simultaneously, people have become reliant on this easy access to the internet and as a result, this has increased the occurrence of cyber fraud activities. This poses a serious concern as users of the internet may be tricked or deceived by cyber criminals whose intention is to perpetrate fraud. Phishing attacks do not rely on technical attacks, such as hacking a system or a network, but rather rely on human psychology to coax and influence an internet user into providing their sensitive information to a potential fraudster[7]. James notes that the term "phishing" is derived from "fishing" and refers to the notion that cyber criminals are fishing for personal data from potential victims[8]. Typically, these fraudulent actions are presented from the perspective of an individual who is from a legitimate institution, such as an associate from the bank or a suspicious email regarding an unauthorized suspension on a subscription service, however phishing frauds can have far reaching impacts much greater than affecting one sole victim.

[6] Ibid., p. 1-8.
[7] Ali, Mazurina M. and Mohd Zaharon, Nur F., "Phishing—A Cyber Fraud: The Types, Implications and Governance," *International Journal of Educational Reform*, 2022, Vol. 0, Iss. 0, p. 1-2.
[8] James, Lance, *Phishing Exposed*, Waltham, Massachusetts: Syngress, 2006, p. 2.

3.2 Phishing - Case Study

Even the largest of technology companies are not immune to phishing attacks as according to Margolin & Biase, a Lithuanian man by the name of Evaldas Rimasauskas perpetrated a phishing fraud against two very large tech companies where a total of $120 million USD was wired to Mr. Rimasauskas. He was able to perpetuate this fraud against two large tech companies by creating a fake company with the same name as a legitimate computer hardware manufacturer, which had done business with the two tech companies prior. Mr. Rimasauskas then sent fraudulent phishing emails and fraudulent invoices requesting payment for goods or services provided. The false invoice scheme was not detected for about 2 years between the years of 2013 and 2015[9], and according to Fortin, these two tech companies were revealed to be Facebook and Google[10].

3.3 The Potential Harm of Phishing

The negative impacts that phishing frauds can inflict on everyday individuals with the growing evolution of the internet is astonishing. James notes in the year 2004 alone, over two million U.S citizens were victims of a phishing attack with a total aggregate loss of almost two billion USD and an average loss of approximately $1200 per incident[11]. The Anti-Phishing Working Group (hereinafter, APWG) is a non-profit that focuses on monitoring and reporting phishing attacks, which are reported by its member companies. According to the APWG, in the third quarter of 2022 alone, there were 1,270,883 total phishing attacks. This number represents the highest amount of phishing attacks ever

[9] Margolin, Jim and Biase, Nicholas, "Lithuanian Man Sentenced To 5 Years in Prison for Theft of Over $120 Million In Fraudulent Business Email Compromise Scheme," *United States Attorney Office: Southern District of New York*, December 19, 2019, https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business. Accessed on April 21, 2023, paras. 1-6.
[10] Fortin, Jacey, "He Tried to Bilk Google and Facebook Out of $100 Million With Fake Invoices," *The New York Times*, March 25, 2019. Accessed on April 21, 2023, from https://www.nytimes.com/2019/03/25/business/facebook-google-wire-fraud.html, paras. 1-2.
[11] Lance, p. 2.

recorded: Advanced fee email phishing frauds increased by 1000% in the third quarter while phishing attacks against business emails increased by 59% in the third quarter; in the second quarter of 2022, the AWPG reported a total of 1,097,811 total phishing attacks[12], therefore making it apparent that although phishing frauds have been around since the early onset of the internet, this type of fraudulent offending continues to increase and pose a significant threat to any individual that readily uses the internet.

3.4 The Role of IFAs in Phishing Engagements

Forensic accountants play a number of key roles in the mitigation and prevention of phishing frauds. One example from Richardson and Kelly who mentions that IFAs are usually called upon when there is a suspicion or an occurrence of fraud has already been detected[13]. An IFA's role would be relevant to determining fraudulent behaviour in relation to phishing schemes as they may be called to investigate a suspicious or potential fraudulent behaviour, and then determine whether the fraud had occurred as a result of a phishing scheme, which was demonstrated in the Mr. Rimasauskas case study. Additionally, Richardson and Kelly note that forensic accountants will attempt to reconstruct the entire fraud scheme like piecing together a puzzle in order to provide a quantifiable measure of the harm done or loss incurred. In doing so, they reconstruct the fraud while keeping in mind that ultimately, this case may end up before the courts, in which it would need to be able to endure critical analysis from the opposing party who would also be an expert in their field[14]. This is relevant as in the case involving Mr. Rimasauskas that was provided earlier, they were able to quantify the loss incurred, as

[12] Anti-Phishing Working Group, "Phishing Activity Trends Report 3rd Quarter," *Anti-Phishing Working Group*, December 12, 2022, https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf. Accessed on April 21, 2023, pp. 1-3.
[13] Richardson, Rachel and Kelly, Paul, "Cybersecurity: Can You Identify the Weakest Link?" *Accountancy Ireland*, August 2016, Vol. 48, Iss. 4, p. 45.
[14] Ibid., p. 45.

well as the case ultimately ending up before the courts as Mr. Rimasauskas was asked to forfeit $49,738,559.41 and to pay restitution in the amount of $26,479,079.24[15]. IFA's will also be able to conduct an assessment of an organization's overall fraud risk potential. This is particularly relevant after an instance of fraud occurs, such as a phishing scam, as a forensic accountant can recommend strategies to reduce the risk of future fraud.

4.0 Money Laundering

Money laundering is defined by MacQueen as the process of concealing the true origin and ownership of a source of income that is a result of criminal enterprises. If this process is able to be achieved successfully, the criminal organizations would be able to maintain control over their proceeds but under the guise of a legitimate business[16]. Furthermore, Turner adds to the discussion by contributing that the process of money laundering consists of a three part process: Placement, layering and integration. The first step is placement which is the process of actually generating the income; typically these funds would come through as a result of some sort of illegal activity or through the acceptance of improper payments. The second step is known as layering which involves transferring the funds through a number of financial institutions or through a variety of asset types, such as the buying and selling of an asset. The purpose behind this layering step is to add complexity so that the funds become harder to trace or to prove whether it originated from illegal means. Lastly, the final step is called integration which involves integrating this illegal or fraudulent obtained stream of income back into the individual's life, but in legitimate forms. For example, this could look like creating a fake company,

[15] Margolin and Biase, para. 8.
[16] MacQueen, Hector, *Money Laundering: Hume Papers on Public Policy 1.2*, Edinburgh, Scotland: Edinburgh University Press, 2019, p. 9.

which does not actually produce any goods or services, and then creating fake invoices that get paid out to the individual attempting to integrate the funds[17]. While money laundering is not a new concept, the escalation of internet connectivity has greatly intensified its prevalence.

Jones and Keasey states that the onset of the internet has brought forth numerous additional opportunities for money laundering activities[18]. In addition, Turner expands on this notion by contributing to the discussion that as technology advances, so do the opportunities to commit money laundering as well. An example provided would be that:

> Suppose a high-limit cash value policy is owned by an individual in the United States who is secretly the leader of an international art theft ring. As pieces are sold, his customers make payments to the insurance company where they add to the cash value of the account. The policy owner takes periodic loans against the policy value, creating fictitious invoices for services that match the amounts of the payments from the insurance company. Each party appears to be making legitimate transactions, with payments to and from an insurance company - and the underlying illicit funds, the payment for stolen art, is laundered[19].

Turner notes that although this example could have been performed prior to the onset of the internet, the creation of increased "online access and real-time payment verification" has amplified the possible schemes available to launder funds[20]. Therefore, money laundering presents a number of serious concerns; typically, the only funds that require laundering are those that are obtained illegally or through prohibited means. This would

[17] Turner, Jonathan E., *Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud*, Hoboken, New Jersey: John Wiley & Sons, 2011, p. 8-10.
[18] Jones, Rob and Keasey, Kevin, "Money Laundering and the Internet: A Challenge for Regulation," *Journal of Financial Regulation and Compliance*, 2000, Vol. 8, Iss. 1, p. 68.
[19] Turner, p. 99-100.
[20] Ibid., p. 100.

mean that the laundering of money promotes criminal behaviour, such as drug trafficking, bribery, corruption or fraud, which directly relates to an increase in crime and reduction of public safety. Furthermore, as Ashin notes, laundered funds may be utilized to increase the money laundering recipients' own wealth or political power. These funds may grant the ability to persuade or corrupt government officials, such as law enforcement or political figures, which in turn, results in further protection for themselves[21]. Lastly, as money laundering is a global problem, it can have far reaching impacts in terms of destabilizing entire financial institutions. As Ashin notes, money laundering activities pose a significant threat to a nation's ability to grow and their overall economy. Countries with money laundering concerns lack financial integrity and results in a lack of financial stability[22].

4.1 Money Laundering - Case Study

The Hong Kong and Shanghai Banking Corporation (hereinafter, HSBC) is a world renowned bank with over a century of history, however despite this, even a bank as significant as HSBC is not immune to money laundering concerns. As Naheem notes, HSBC allegedly assisted in money laundering activities for criminal enterprises and increased the potential risks of terrorism and drug trafficking within the United States[23]. As noted by Levin & Coburn after a thorough investigation, it was identified that HSBC perpetuated five key areas of concern that enabled potential criminal organizations to launder funds through its banking services: HSBC created U.S correspondent accounts without completing verification checks as these accounts were opened for individuals

[21] Ashin, Paul, "Dirty Money, Real Pain: Money Laundering Harms Innocent Individuals but Can Also Impose Serious Costs on National Economies," *Finance & Development,* June 2012, Vol. 49, Iss. 2, p. 38.
[22] Ibid., p. 40.
[23] Naheem, Mohammed A., "Risk of Money Laundering in the US: HSBC Case Study," *Journal of Money Laundering Control,* 2016, Vol. 19, Iss. 3, p. 226.

who would be considered as high risk clients; transactions were processed that directly hinder the US government's objective in limiting terrorism, drug smuggling activities and other potential criminal activities; they were supplying other banks who have potential connections to terrorist organizations with US correspondent services; disregarded any suspicious activities while processing bulk cheques; and promoting corporate accounts to those who may be deemed as a high risk clients[24].

4.2 The Potential Harm of Money Laundering

The adverse effect that money laundering can have on the global economy is substantial however as a result of greater connectivity afforded by the internet, the money laundering crisis has only been exacerbated. As Fausto notes, more and more modern criminals focus on the internet as a means of promoting criminal actions and this is due to three distinct advantages which come with online access: Anonymity, the ability to place transactions from remote locations, and an alleged perpetrator making as many transactions as they may desire. Moreover, this increased interconnectivity offers criminals more creative and opportunistic ways of laundering funds as there are no longer the days of laundering funds though roulette games[25].

The financial implications of money laundering are severe as according to Schneider who reviewed the International Monetary Fund and World Bank data determined that in the year 2000, approximately two to four percent of the world's gross domestic product (hereinafter, GDP) originated from illegitimate means. They further estimated that in the year 2006, international money laundering resulted in a figure

[24] Levin, Carl and Coburn, Tom, "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History Majority and Minority Staff Report," *United States Senate Permanent Subcommittee on Investigations Committee on Homeland Security and Governmental Affairs*, July 17, 2012, https://www.hsgac.senate.gov/subcommittees/investigations/library/files/report-us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history/. Accessed on April 24, 2023, p. 3-4.
[25] Fausto, Martin D. S., *Technology-Enhanced Methods of Money Laundering Internet as Criminal Means*, Cham, Switzerland: Springer Nature Switzerland AG, 2019, p. 2.

between 2 and 2.5 trillion USD or roughly between five to six percent of the global GDP for 2006[26]. Ultimately, as Otusanya and Lauwo note, the total figure of money laundered globally would be impossible to quantify; however it is believed that money laundering activities may constitute up to five percent of the global economy,[27] which has severe ramifications for the economy.

4.3 The Role of IFAs in Money Laundering Engagements

Forensic Accountants play a vital role in the fight against money laundering. As laundered funds may be concealed through many layers of deception, a key role for a forensic accountant would be to detect the occurrence of money laundering. An IFA may be contacted in regards to a company's suspicions on possible money laundering occurring within their company, however, possible money laundering may also be discovered while IFAs are engaged in other engagements. The versatility of IFAs and their ability to detect possible fraudulent acts, such as money laundering, greatly aids in investigations and can uncover fraudulent acts that would not have been discovered. For example, an IFA may be involved in an engagement where there is fraud occurring; however, in reviewing the financial data, such as transactions or invoices, the IFA may have already determined that the invoices were for a non-existent company, and the payments made to the company are actually funds being laundered fraudulently. Therefore, the IFA serves the role of identifying suspicious transactions, which may indicate money laundering activities. IFAs also possess special skills in identifying red flags and working with financial institutions to trace the flow of funds, which may be

[26] Schneider, Friedrich, "Turnover of Organized Crime and Money Laundering: Some Preliminary Empirical Findings," *Public Choice,* July 2010, Vol. 144, Iss. 3/4, p. 433-434.
[27] Otusanya, Olatunde J. and Lauwo, Sarah, "The Role of Offshore Financial Centres in Elite Money Laundering Practices: Evidence from Nigeria," *Journal of Money Laundering Control,* 2012, Vol. 15, Iss. 3, 336.

necessary for money laundering detection and prevention. Pacini et al. adds onto this notion and states that the key role of forensic accountants would be "tracking the movement of money, and investigating and recovering stolen assets in conjunction"[28]. Pacini et al. also note that due to the prolific use of shell companies, it can be very difficult for IFAs to ascertain the true identity of shell company ownership; this indicates an important role for IFAs, which is attempting to determining the natural owner of a shell company[29]. Finally, a key role for the IFA after the investigation would be to present the findings of their investigation in a well organized report as ultimately, the case may end up within the court systems and in front of a judge, in which there is an additional role of testifying in court as an expert witness.

5.0 Intellectual Property Theft/Infringement

The term intellectual property (hereinafter, IP) is defined by Prabu and Suriyaprakash as a form of property that is often taking shape as an intangible asset, which arises out of individuals' own intellect and creativity or is a result of cognitive function. The concept of intellectual property revolves around the notion that a creator's ideas are a representation of their own identity and therefore, should be protected[30]. As Wilding notes, oftentimes the most valuable asset to a company is not their physical properties or inventory, but rather their knowledge and information around a process[31]. Some common examples of IP are "copyright, trademarks, trade dress, patents, trade secrets, utility models, industrial designs, geographical indications, traditional knowledge and cultural expressions"[32]. Additionally, Wilding contributes to the discussion by

[28] Pacini, C., Hopwood, W., Young, G., & Crain, J., "The Role of Shell Entities in Fraud and Other Financial Crimes," *Managerial Auditing Journal*, 2019, Vol. 34, Iss. 3, p. 248.
[29] Ibid., p. 248-251.
[30] Prabu, Sakthivel L. and Suriyaprakash, T. N. K., *Intellectual Property*, London, United Kingdom: IntechOpen, 2022, p. 3-9.
[31] Wilding, Edward, *Information Risk and Security*, London, United Kingdom: Routledge, 2006, p. 47.
[32] Prabu and Suriyaprakash, p. 9.

stating that IP may simply be an idea, a manufacturing process, or anything which if were to be commercially developed, may possess value[33].

Due to the certain characteristics of the internet, theft of IP has been exponentially enhanced. Moid notes that due to the nature of internet files being quickly shared between users' computers and uploaded or downloaded at will, the only condition is that the file must exist on a server, which is connected to online access[34]. The effect of the internet on IP theft is evident as much of the internet consists of pirated material, such as music, movies, books and other forms of IP. However, intellectual property theft is a serious concern as Moid notes, more than ever are organizations needing to be cognizant of their IP safeguards and security procedures as the internet has made it easy for cyber criminals to commit corporate espionage. A possible example would be hacking into a corporation's database and stealing the documents that outline a company's research and development phase (hereinafter, R&D), which essentially would give the perpetrator a severe advantage against the company. Furthermore, the victim of the corporate theft may not become aware of this theft until counterfeit products have already been produced or where a patent was created by another company who stole the original company's R&D documentation[35]. Lastly, as Wilding notes, corporations and commercial business are not exposed to the risk of IP theft online, but also have to be cognizant of IP thefts risks, which can take the form of employee theft, the trading of protected company information for money or bribery, as well as the unintentional disclosure of information[36].

[33] Wilding, p. 47.
[34] Moid, Sana, "Fighting Cyber Crimes Using Forensic Accounting: A Tool to Enhance Operational Efficiency," *International Journal of Money, Banking and Finance, 2018,* Vol. 7, Iss. 3, p. 95.
[35] Ibid., p. 93-95.
[36] Wilding, p. 47.

5.1 Intellectual Property Theft/Infringement - Case Study

An excellent example of a potential harm that internet enabled IP theft can have would be the case of operation CuckooBees. According to Burgess, a private cyber security firm by the name of Cybereason had identified a cyber espionage operation, which had been previously undetected and running since 2019. It was determined that a group known as APT41/Winnti was behind the operation and had acquired several hundreds of gigabytes worth of IP and sensitive information[37]. According to Cybereason, the intended purpose of this attack was to steal proprietary information such as "R&D documents, source code and blueprints for various technologies"[38], from numerous technology and manufacturing companies located across the world[39]. As Burgess notes, this proprietary information would be split up and sold to various industries in both the private sectors, as well as public sectors; for example, R&D can be extremely valuable to competitors in their respective marketplaces as the need for completing their own R&D and potential patent design is alleviated[40]. Moreover, Sganga quotes from Cybereason's CEO Lio Div's who they had interviewed and stated that, "'Blueprint diagrams of fighter jets, helicopters, and missiles were [discovered],' [and in pharmaceuticals], '[they] saw them stealing IP of drugs around diabetes, obesity, depression.' The campaign has not yet been stopped"[41].

---

[37] Burgess, Christopher, "China's Cyber Espionage Focus: Intellectual Property Theft," *ProQuest,* May 17, 2022, https://www.proquest.com/docview/2665360049?accountid=14771&parentSessionId=yEN%2B5WCBfUk%2BQIHk2iWzMKhObxuhj7IitWph7YbQUww%3D. Accessed on April 26, 2023, p. 1.

[38] Cybereason, Nocturnus, "Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques," *Cybereason*, May 4, 2022, https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques. Accessed on April 26, 2023, para. 11.

[39] Ibid., para. 4.

[40] Burgess, p. 1.

[41] Sganga, Nicole, "Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies," *CBS News*, May 4, 2022, 12:01am, https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/#:~:text=A%20yearslong%20malicious%20cyber%20operation,manufacturing%2C%20energy%20and%20pharmaceutical%20sectors. Accessed on April 26, 2023, para. 3.

5.2 The Potential Harm of Intellectual Property Theft/Infringement

The harm intellectual property theft can have is apparent and significant as stated by Senator Casey from The U.S Congress Joint Economic Committee, not only does the theft and infringement of IP negatively affect the original IP holder, but has significant ramifications to an entire nation's economy. For example, he notes that on average, companies had experienced a loss of $101.9 million in lost revenues, as well as incurring additional costs to prevent further IP infringement. On average, these incurred additional costs have cost $1.4 million and have resulted in an average lost profit of $46.3 million for a single company. It was also noted that in 2011 alone, over 1.1 billion dollars' worth of counterfeit goods were seized by border officials[42].

In the current day and age of the internet where consumers directly shop online from international markets, it is extremely easy for these types of activities to create significant harm to the economy. Essentially, the $1.1 billion dollar figure only represents what was confiscated, therefore the magnitude of products coming in greatly exceeds this figure, which is a substantial amount of money that is not contributing to the local economy, but rather the economy of the country in which the counterfeit products shipped from. Additional harms that Casey notes are patent infringing products, which may create competition in pricing for the original patent holder, as well as intellectual property theft, which disproportionality affects small business since 79% of all American business are small businesses and it is likely that a smaller company will not have resources needed to fight the infringer[43].

[42] Casey, Bob, "The Impact of Intellectual Property Theft on the Economy," *The U.S. Congress Joint Economic Committee Chairman's Staff,* August 2012, https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf. Accessed on April 27, 2023, paras. 1-2.
[43] Ibid., p. 2-3.

5.3 The Role of IFAs in Intellectual Property Theft/Infringement Engagements

IFAs play a number of incredibly important functions in relation to IP theft or infringement. Most notably, as stated by Brennan & Hennessy, it would be the IFA's role to quantify the lost sales incurred and estimate the potential lost profit if IP infringement were to occur. If the lost profits could not be determined by the IFA, they would have the responsibility of determining an appropriate royalty to charge the patent infringer[44]. As well, if a patent infringement case were to end up in a court case, the IFA would have the responsibility of quantifying the total loss incurred and then providing testimony in court as an expert witness. As well, Brennan & Hennessy notes that in rare circumstances, IFAs may be required to value certain kinds of IP such as, trademarks or copyrights, which is another area where the skills of an IFA prove to be fruitful[45]. Lastly, a key role for an IFA would be supporting the legal counsel throughout the case as they will have a much greater understanding of the financial matters at hand and evidence to support the case.

6.0 Future Fraud

As advances in the internet have led to significant areas of change for modern day IFA engagements, it is important to consider the potential ramifications of this increased accessibility to the internet on future IFA engagement areas. This notion is verified by Trozze et al. as they state that the nature of many of these fraudulent actions are not a new phenomenon, but rather due to the increased cyber connectivity the methods of implementation for these frauds have evolved[46]. Therefore, a review of three types of

[44] Brennan, Niamh and Hennessy, John, "Forensic Accounting and Intellectual Property Infringement," *Commercial Law Practitioner,* 2001, Vol. 8, Iss. 5, p. 5-6.
[45] Ibid., p. 11.
[46] Trozze, A., Kamps, J., Akartuna E. A., Hetzel, F. J., Kleinberg, B., Davies, T. & Johnson, S. D., "Cryptocurrencies and Future Financial Crime," *Crime Science,* 2022, Vol. 11, Iss. 1, p. 12.

future engagement areas will be explored, which are: Artificial intelligence, cryptocurrency and synthetic identity theft. A discussion of each of these three types are crucial and will be in relation to the potential future fraudulent behaviour, where the direction of the forensic accounting profession may be heading towards and the skills which will be most valuable in the future.

6.1 Artificial Intelligence & Forensic Accounting

AI presents a number of exciting new advances which greatly aids the speed at which society undergoes significant transformations, however, this is not without compromises. A major concern is that in certain situations, the use of AI may actually help to perpetuate fraud and enable negative behaviours. For example, King et al. notes that with time, AI may begin to play a more substantial role in criminal offending[47]. According to Naqvi, AI has been defined by the Institute of Electrical and Electronics Engineers as "the combination of cognitive automation, machine learning, reasoning, hypothesis generation and analysis, natural language processing, and intentional algorithm mutation producing insights and analytics at or above human capability"[48]. Despite this, Naqvi notes that they prefer a more broader approach with the definition of technology, which is that it is capable of meeting objectives in ambiguous or unpredictable situations[49]. An example of a way in which AI can assist those who wish to perpetrate fraudulent behaviours is touched upon by Seymour and Tully who combined an AI neural network with a traditional phishing type scam, which then resulted in the creation of an AI model that had possessed the ability to target potential victims on

[47] King, Thomas C., Aggarwal, N., Taddeo, M. & Floridi, L., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions," *Science and Engineering Ethics,* 2020, Vol. 26, Iss. 1, p. 90.
[48] Naqvi, Al, *Artificial Intelligence for Audit, Forensic Accounting, and Valuation: A Strategic Perspective,* Hoboken, New Jersey: John Wiley & Sons, 2020, p. 42.
[49] Ibid., p. 42-43.

Twitter based on what the AI believes will be most attractive to the potential victim. This was achieved through carefully examining potential victims' Twitter profile, timeline posts or retweets[50]. As King et al. notes, this AI assisted phishing scam employs machine learning in which each message that is sent by the AI is tailored to particular victims, which is based on what the AI believes will be the most enticing for their victim to click on the intended phishing link[51]. This is particularly concerning as it indicates that moving forward in the future, fraudulent scams may become more and more difficult to detect. Oftentimes, a hallmark of phishing scams is the poor use of language and grammar as not only does AI resolve this issue entirely, but the phishing links are able to be even more specific and personalized, which increases the appearance of authenticity and believability, and may cause more people to fall victim to these types of fraudulent behaviours.

Another serious threat for the field of forensic accounting that is a result of the increased access and usage of the internet would be AI assisted financial market manipulation. As Martinez-Miranda notes, a reinforcement learning agent was employed in a study of market manipulation in an attempt to determine whether AI could learn the use of illegal and reproached trading tactics in order to maximize profit and whether it would artificially drive up the selling price of an asset[52]. According to King et al., the AI based artificial trading agents appeared to have learned through reinforcement about an illegal market manipulation technique of spoofing, which is the act of submitting an order

[50] Seymour, John and Tully, Philip, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter," *Blackhat*, n.d, https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf. Accessed on April 28, 2023, p. 1.
[51] King et al., p. 90.
[52] Martinez-Miranda, E., McBurney, P., & Howard, M. J. W., "Learning Unfair Trading: a Market Manipulation Analysis From the Reinforcement Learning Perspective," *2016 IEEE Conference on Evolving and Adaptive Intelligent Systems*, 2016, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7502499. Accessed on April 28, 2023.

but with no real intention to follow through with the order. The intention was to manipulate honest buyers in the marketplace and it was able to achieve this by "initially exploring the action space and, through exploration, placing false orders that became reinforced as a profitable strategy, and subsequently exploited for profit"[53]. This is very concerning as it highlights the potential for fraudsters to exploit financial trading systems and marketplaces with AI based software in the future. As King et al. notes, the use of AI powered trading agents may make it very difficult to discern how the financial market should appear as ultimately, perceptions will be warped by the use of this AI software[54] .

King et al. notes further concerns that arise out of AI based software and its influence on the financial market, which is that if AI software reaches a state of increased autonomy where it can access an individual's social media, it may be able to quickly learn all the details necessary to engineer the perfect and individually tailored pump and dump scheme. A pump and dump scheme is the act of spreading false news or information in an attempt to drive up the price of a stock. Once these prices have risen, the fraudsters will sell the stock for a profit while others who believed in the promotion will be left with what they had purchased but for an inflated price, which often crashes after the sale. Lastly, a serious concern that arises from the use of AI enabled trading agents is the fact that the AI is able to create new strategies and refine their abilities leading to an ever-increasing difficulty to detect the occurrence of unethical or illegal trading practices[55].

[53] King et al., p. 98.
[54] Ibid., p. 99.
[55] Ibid., p. 98-100.

6.2 Artificial Intelligence - The Future of IFA Engagements

The future landscape for IFA engagements appears to be incredibly intriguing as on one hand, AI poses a number of threats and can increase fraud risks however, on the other hand, AI possesses a number of extremely useful functions and likely will aid in the profession as a whole. As Nickerson notes, a survey was completed on 3000 executives and nearly 85% believe that AI technology would provide an advantage over that of humans completing the same task. As well, 79% of the surveyed participants believed that AI could increase productivity for its human counterparts.

Within every year, more and more businesses employ AI in their work streams to increase efficiency. For example, in 2016, only 38% of the businesses surveyed employed AI technology whereas in 2019, this figure increased to about 61%[56]. Molloy predicts that as AI use becomes more frequent and sophisticated, accountants will increasingly pass their monotonous duties onto AI based computers[57]. This notion is touched upon by Anand who voices the same perception and notes that future forensic accountants should have many of their traditional accounting duties, such as reviewing or collecting data, become automated by AI[58]. Despite this and as noted by Molloy, it is expected that accounting jobs will remain in high demand as Accounting Technicians Ireland currently has more members than ever recorded previously. It appears that AI is not replacing the human accountant workers, but rather is there to provide support[59]. This is also supported by Anand who notes that "while the goal of AI is to simulate

[56] Nickerson, Mark A., "AI: New Risks and Rewards," *Strategic Finance,* April 2019, Vol. 100, Iss. 10, p. 28.
[57] Molloy, Cian, "The Shape of Things to Come: What Lies in Store for the Accountancy Profession? Cian Molloy Investigates How the Profession Might Fare in the Years Ahead," *Accountancy Ireland,* February 2017, Vol. 49, Iss. 1, p. 31.
[58] Anand, Akriti, "Forensic Accounting and the Use of Artificial Intelligence," *Pennsylvania CPA Journal,* 2019, https://www.proquest.com/docview/2547074884/fulltextPDF/FE05ACD8191A40DFPQ/1?accountid=14771. Accessed on April 29, 2023, p. 27.
[59] Molloy, p. 31.

human abilities – and perform tasks more efficiently – the intention is to complement humans rather than replace them"[60]. Molloy notes that in this new era for accountants, it is expected that there will be an increased focus on the analysis of data rather than the more simplistic tasks such as, maintaining and creating financial statements[61]. Molloy notes that with the advances in the internet and increased AI use, accountants are able to analyze much larger samples of data and effectively "work smarter" as a result of the possibilities for AI. AI also possesses the ability to better represent results visually which in turn, results in improved decision making and a better end result for a client[62]. In this regard, Anand proposes that the analysis in which IFAs perform will shift from that of traditional spreadsheet analysis to a dashboard style where the IFA would instruct the software to analyze certain sections or areas[63]. Therefore, it is believed that many of these predictions for CPAs will hold true for IFAs in the forensic accounting field as well. It is possible in the future for forensic accountants to rely heavily on AI and other advanced tools to generate the data, however in this regard, the IFA will have a greater role in attempting to make sense of that data and work out any areas the AI software did not consider or analyze. Furthermore, the IFA in the future will be able to work faster as the use of AI permits analysis on larger sets of data and is able to better represent a pattern or trend. This notion is supported by Anand who voices similar opinions where she notes that "forensic accountants will spend the bulk of their time on interpreting results and performing higher-level analysis [rather than focusing on the more mundane tasks a forensic accountant is required to do]"[64].

[60] Anand, p. 26.
[61] Molloy, p. 31.
[62] Ibid., p. 33.
[63] Anand, p. 27.
[64] Ibid., p. 27.

Another potential area where the landscape for IFAs may change is noted by Molloy where CPAs may be able to expect that their role will be increasingly focused in making key judgements and adding value to services provided to the client[65]. This is another area where change will occur for forensic accountants as the software will free up valuable time for the IFA to get a good understanding of what the data means and whether fraud risks are present. This assumption is supported by Anand who references that while AI powered tools create efficiency and make large data sets more manageable, the role of the IFA will still be required in the future to "perform complex subjective evaluations, interpret and validate analysis, add technical expertise, and inform strategic decision-making"[66]. Therefore, the IFA still serves to be an integral factor when analyzing data and navigating through the numerous changes to future landscape for AI involved engagements.

6.3 Artificial Intelligence - IFA Skills for the Future

As new technologies such as AI revolutionize the way that IFA engagements may look like, there is a dramatic shift in the skills necessary to succeed in the future of the forensic accounting profession. One change noted by Molloy is that in the future, there will be less of a focus on technical skills, such as traditional accounting skills, and more focus on soft skills, such as the ability to speak to others in a clear and elaborate manner; for example, how a company can pitch for additional business or how a business can generate additional funds[67]. This is a result of AI being able to accommodate for many of the traditional accounting duties previously delegated to the CPA or IFA, therefore

[65] Molloy, p. 33.
[66] Anand, p. 27.
[67] Molloy, p. 31.

resulting in IFAs having more time to allocate towards conveying broad suggestions to their clients.

Another skill that will be crucial in the future for IFAs would be the ability to work with a wide variety of complex data types. As Anand notes, IFAs are increasingly dealing with data types that do not fit into traditional databases[68]. This may be relevant for the use of AI as in order for the AI software to conduct a review or analysis, it may require the data to be entered in a certain way or form factor, which highlights the need for IFAs to have a wide array of knowledge on data types and how it is to be structured. Additionally, in the future, IFAs need to possess excellent IT skills as most of the forensic accounting work will be performed using computers and complicated software, which will not be possible if a practitioner is not proficient in their IT skills. For example, Anand mentions that a business may suddenly decide to change directions in the course of an investigation; the practitioner must then be able to modify the software to reflect this change[69]. Molloy notes that as risk management and cybersecurity are the growing trends for forensic accounting firms, it can be inferred that valuable skills for IFAs to possess in the future would be those in risk management and cybersecurity. Additionally, it is noted that even those who are not accountants, but possess skills in cybersecurity or risk management may be valuable additions to a firm, which indicates that if a forensic accountant possessed those skills, they would have a larger advantage in targeting fraud within the internet and technological space[70].

Molloy discusses one skill that is particularly important which is the idea of perpetually learning and evolving a practitioner's skill toolbox or professional

[68] Anand, p. 26.
[69] Ibid., p. 27.
[70] Molloy, p. 32.

development. As the profession rapidly and perpetually changes in lieu of the increased access of the internet, practitioners need to be able to transition with the field[71]. Therefore, the ability to learn and find out what is needed for a particular engagement or field of study, as well as the ability to specialize one's knowledge further in a particular field is extremely important.

7.0 Cryptocurrency & Forensic Accounting

Cryptocurrency is a relatively new method of purchasing and selling assets digitally, and although it possesses a number of benefits, it has its limitations as well. Trozze et al. notes that given the recent trends and apparent direction cryptocurrency is heading towards, "the cryptocurrency space offers yet unexploited opportunities for crime"[72]. Cryptocurrencies are defined by Härdle et al. as being a form of digital assets which can be traded from one peer to another without the need for a "middle man;" typically this "middle man" would be some sort of financial institution such as a bank. By using cryptocurrencies, such as Bitcoin, a user is able to purchase something over the internet and almost pay the seller instantaneously without the need for a bank account, credit card or revealing one's true identity. Cryptocurrency transactions also allow users to directly transfer digital funds from one individual's wallet to another. Additionally, in any form of cryptocurrency, all transactions are listed in a cryptocurrencies blockchain, which is a public ledger of all the transactions. The factor of anonymity within the realm of cryptocurrencies is the key factor as to why cryptocurrencies are widely used, however also a key factor used for fraudulent behaviours[73].

[71] Ibid., p. 33.
[72] Trozze et al., p. 1.
[73] Härdle, W. K., Harvey, C. R., & Reule, R. C. G., "Understanding Cryptocurrencies," *Journal of Financial Econometrics*, February 2020, Vol. 18, Iss. 2, p. 181-183.

Trozze et al. completed a review of the literature and found that cryptocurrency possessed the potential to perpetuate 29 different types of fraud[74]. One type of harm from the 29 different types of fraud, which is caused by an ever-increasing cyber connected world, is that cryptocurrency provides a way for criminals and fraudsters to get paid in a form of currency that is anonymous. Additionally, the internet serves as a point of entry or access for many cyber criminals as for example, Akartuna et al. notes that cryptocurrency has significantly perpetuated ransomware and as a result, increased the occurrence of the criminal offense of extortion. Cyber criminals will employ malware to encrypt and essentially prevent a user from accessing the files on their hard drive. In order to be provided access to their files, the victims are typically required to pay a ransom through cryptocurrency due to the anonymous nature of cryptocurrency. This type of extortion can have devastating effects for various institutions held at ransom, especially if the victim does choose to pay the ransom, there is still no guarantee that the cyber criminals will actually decrypt the files after payment or demand further funds[75]. An example of the potential harm that ransomware can have is mentioned by Collier who notes that a newborn baby had passed away at the hospital as the hospital was unable to perform certain tests due to the hospital computers being shut down as a result of a ransomware attack[76].

This type of ransomware is still in its early onset as cryptocurrency is a relatively new concept, however the potential future implications of this type of criminal activity

[74] Trozze et al., p. 5.
[75] Akartuna, E. A., Hetzel, F. & Kleinberg, B., "Cryptocurrencies and Future Crime," *Dawes Centres for Future Crime at UCL,* February 2021, https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/ucl_cryptocurrencies_and_future_crime_policy_briefing_feb2021_compressed_1.pdf. Accessed on April 30, 2023, p. 3.
[76] Collier, Kevin, "Baby Died Because of Ransomware Attack on Hospital, Suit Says," *NBC News*, September 30, 2021, 10:51am, https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465. Accessed on April 30, 2023, paras. 1-6.

can be detrimental to society as a whole. For example, Dienst notes that a police station in New Jersey was recently held for ransom where 80-85% of the electronic files were looked at, many of which related to criminal investigations which had to be delayed[77]. This highlights a serious concern for future criminal prospects as it may be that this type of attack can be used for other nefarious purposes such as, rather than demanding funds and returning the files, a hacker could simply delete or encrypt the electronic files, which would be used to persecute those who are involved in criminal matters.

Another way in which cryptocurrency can enable criminal or fraudulent behaviors would be through cryptocurrency ATMs. As Akartuna et al. notes, an excellent way of laundering money is through cryptocurrency ATMs where an individual can deposit illegally obtained funds and exchange it for a cryptocurrency such as Bitcoin. This Bitcoin can then be used to purchase other goods or assets and due to the anonymous nature of cryptocurrency, no one would know whether these funds originated through illicit means or not[78]. This may become a larger and potential problem in the future as cryptocurrency use becomes more common, as well as the prominence of cryptocurrency ATMs given the lack of regulation and decentralization of cryptocurrencies. Akartuna et al. notes, many of the traditional fraud opportunities exist in the cryptocurrency space, for example, pump and dump schemes and phishing scams work in their traditional ways. However, with these new opportunities, some individuals will attempt to drive up the cost of certain securities by spreading misinformation, which can be done in the same way for cryptocurrencies and likewise, the concern for phishing scams is the same[79].

[77] Dienst, Jonathan, "Ransomware Attack at NJ County Police Department Locks Up Criminal Investigative Files," *NBC New York*, April 7, 2023, 7:11pm, https://www.nbcnewyork.com/investigations/ransomware-attack-at-nj-county-police-department-locks-up-criminal-investigative-files/4219341/. Accessed on April 30, 2023, p. 1-8.
[78] Akartuna et al., p. 3.
[79] Ibid., p. 3-4.

7.1 Cryptocurrency - The Future of IFA Engagements

The landscape of IFA engagements is changing drastically and cryptocurrencies play a significant role in exacerbating this change. A key reason for this change is because the characteristics of cryptocurrency often make it easier for nefarious individuals to commit fraudulent actions. These characteristics include: decentralization, anonymity and a nearly instant transfer speed. It is believed that the future landscape for IFA engagements will notably involve increased usage of cryptocurrencies.

One area of a future IFA engagement is identified by Millard who notes that a key concern is whether or not cryptocurrency exchanges are legitimate and genuine, especially taking into account the unregulated nature of cryptocurrencies[80]. According to Gara et al., in a recent case where a massive cryptocurrency exchange went bankrupt known as FTX, the exchange only possessed $900 million USD in assets despite nearly nine billion in liabilities. It is noted that typically, companies should have a roughly equal amount of assets to liabilities[81]. According to the US Securities and Exchange Commission (hereinafter SEC), the former CEO and co-founder Mr. Sam Bankman-Fried had been charged with defrauding investors as it was alleged that he misled investors and "built a house of cards on a foundation of deception while telling investors that it was one of the safest buildings in cryptocurrency"[82]. Therefore, IFAs will have a substantially increased role in identifying the legitimacy of crypto currency exchanges, as well as quantifying the harm caused and whether or not fraud was perpetrated by such

[80] Millard, Mark, "Forensic Investigations of Tomorrow," *Deloitte,* 2022, https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/an-ounce-of-prevention/forensic-investigations-of-tomorrow.html. Accessed on April 30, 2023, p. 4.
[81] Gara, A., Shubber, K. & Oliver, J., "FTX Held Less Than $1bn in Liquid Assets Against $9bn in Liabilities," *Financial Times,* November 12, 2022. Accessed on April 30, 2023, from https://www.ft.com/content/f05fe9f8-ca0a-48d5-8ef2-7a4d813af558, paras. 1-15.
[82] U.S. Securities and Exchange Commission, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX," *U.S. Securities and Exchange Commission,* December 13, 2022, https://www.sec.gov/news/press-release/2022-219. Accessed on April 30, 2023, paras. 1-13.

companies. Millard also notes that due to the sophisticated nature of cryptocurrencies in future engagements, IFAs will be required to "understand and unpick the true nature of the investment, identify and trace all the different cash flows relating to the fraud, and overlay this with email data and other evidence to understand how the fraud occurred"[83]. Additionally, as Millard notes, IFAs in the future may play a vital role in the recovery of funds which may have been embezzled by potential fraudsters; the aim of tracking these funds down is ultimately to return as much of the loss back to the victims as possible.

Another function for IFAs in the future landscape would be completing an IFA investigation report, which will serve as a major benefit to those who may not be an expert in the field of cryptocurrencies. Additionally, these reports will prove to be invaluable during court proceedings whether it be in civil or criminal court as an IFA has the responsibility to testify their findings as an expert witness in court[84]. Another area for potential IFA engagements in the future is mentioned by McClintock et al. which would be in the area of estate planning. Increasingly, estate planners are finding that some of their clients possess a wealth which includes or is composed of cryptocurrency assets[85]. Balla notes that a key role for IFAs in estate and trust matters is to value any assets which are to be included in one's estate or trust[86]. Therefore, a future engagement area for forensic accountants may be within the estate planning realm.

Hou notes that as technology progresses, it has become increasingly easy to hide assets from one's partner, which becomes extremely relevant when considering cryptocurrencies and divorce proceedings. Many spouses will attempt to hide their

[83] Millard, p. 5.
[84] Ibid., p. 5.
[85] McClintock, M.T., Kanaga, V. L., & Blattmachr, J. G., "Estate Planning in the Era of Digital Wealth," *Estate Planning,* May 2022, Vol. 49, Iss. 5, p. 5.
[86] Balla, Keith S., "The Forensic Accountant's Role in Estate and Trust Matters," *PKF O'Connor Davies,* n.d, https://www.pkfod.com/insights/the-forensic-accountants-role-in-estate-and-trust-matters.Accessed on May 1, 2023, para. 3.

digital assets such as their cryptocurrency in order to prevent them from being split equally within divorce proceedings; this role has been made easier by characteristics of cryptocurrencies such as anonymity[87]. Therefore, two potential engagement areas for IFAs in the future exist in relation to divorce proceedings. One potential engagement area that an IFA may be retained is to determine the value of a spouse's cryptocurrency fund, which would then be split equitably amongst the parties in a divorce proceeding. The other engagement area would be where an IFA may be retained to prove that one party possesses cryptocurrency, which they have not disclosed or are attempting to hide; the IFA may then have the role of attempting to locate or provide proof of the value of these hidden cryptocurrency assets.

7.2 Cryptocurrency - IFA Skills for the Future

There are numerous skills that will greatly benefit IFAs in the future in regards to cryptocurrency investigations. One beneficial skill would be the proficient use of a computer and excellent IT skills given the advanced nature of cryptocurrency trading. Additionally, an IFA involved in this type of work should have sufficient knowledge of the blockchain as it serves as the transaction ledger for cryptocurrencies. As Hares notes, an IFA likely would begin a cryptocurrency investigation at the blockchain since it serves as both the "entry and exit" points, which can provide IFAs with many clues to guide the rest of the engagement[88]. Therefore, a vital skill for future IFA engagements would be possessing knowledge around the use of the blockchain.

[87] Hou, Caline, "A Bit-ter Divorce: Using Bitcoin to Hide Marital Assets," *North Carolina Journal of Law & Technology*, 2015, Vol. 16, Iss. 3, p. 75-76.
[88] Hares, Sophie, "5 Ways Accountants Can Track Cryptocurrency," *Journal of Accountancy*, June 29, 2020, https://www.journalofaccountancy.com/newsletters/2020/jun/accountants-track-cryptocurrency.html. Accessed on May 1, 2023, paras. 11-12.

Another skill is identified by Millard who notes that an IFA should be familiar with tools such as data analytics as cryptocurrency frauds often possess copious amounts of financial information, which would be very difficult to analyze without software assistance. In addition, it is noted that a key skill would be the ability to collect, store and analyze extensive amounts of both electronic and hard copy data[89]. As well, Hares highlights the importance of traditional IFA skills in cryptocurrency investigations as an IFA may determine, through conducting a review of an alleged fraudsters email or personal electronic device, that there is valuable information in regards to how an individual was able to convert physical assets, such as cash, into virtual assets or even possibly the location of a cryptocurrency wallet. For example, in reviewing an alleged perpetrator's email, it may be that there is an email confirmation for the creation of a cryptocurrency wallet[90]. Millard notes that as these engagements may ultimately end up in either civil or criminal court, a necessary skill would be that they are able to write expert reports that clearly explains the content of the investigation in layman's terms, as well as the possible need to testify to the findings as an expert witness in court[91]. Therefore, it is also important for an IFA working in the cryptocurrency realm to possess sufficient knowledge and skills relating to legal processes and regulatory frameworks for cryptocurrency trading. An IFA would normally have legal assistance through legal counsel, however given the complex and international nature of cryptocurrency trading, this would be a very beneficial skill to have for IFA engagements. For example, Hares notes that in order to gather information on cryptocurrency trading exchanges, a subpoena

[89] Millard, p. 5.
[90] Hares, paras. 22-26.
[91] Millard, p. 5.

is typically required[92]. Therefore, by understanding what is required for an IFA engagement in terms of legal requirements, it can assist the IFA while they are planning their investigation.

Another potential skill that may be extremely important in future IFA engagements would be the knowledge and ability to obtain certain civil court orders, such as a Norwich order. According to Oliver, court orders may be used to trace stolen assets, such as cryptocurrencies, and if employed quickly enough, can stop the transfer of ill obtained cryptocurrency assets[93]. In addition, Rein notes that it may be possible to determine the identity of a cryptocurrency fraudster through a Norwich order as the court order requires "third parties to disclose information to potentially identify the wrongdoer, to trace funds and to assist prospective plaintiffs in determining whether a cause of action exists"[94].

Kilby mentions that despite the numerous new skills in which IFAs need in order to combat cryptocurrency frauds, the old basic investigative skills are more relevant than ever. It is noted that simply asking the right questions and receiving straight answers is an incredibly useful factor in cryptocurrency investigations[95]. Therefore, a valuable skill for IFAs to possess in the world of cryptocurrency frauds would be that of simply good interviewing and forensic investigative skills.

---

[92] Hares, paras. 14-15.
[93] Oliver, Joshua, "The Lawless World of Crypto Scams," *Financial Times*, September 18, 2022. Accessed on May 1, 2023, from https://www.ft.com/content/5987649e-9345-4eae-a4b8-9bfb0142a2ab, para. 16.
[94] Rein, Eric, S., "Challenges in Discovering Perpetrators of International Cryptocurrency Frauds," *American Bar Association.org*, April 23, 2018, https://www.americanbar.org/groups/litigation/committees/commercial-business/practice/2018/challenges-discovering-perps-international-cryptocurrency-fraud/. Accessed on May 1, 2023, para. 5.
[95] Kilby, Paul, "Taming Fraud in Crypto's Wild West," *Fraud Magazine*, March/April 2023, https://www.fraud-magazine.com/cover-article.aspx?id=4295020326. Accessed on May 2, 2023, paras. 21-22.

8.0 Synthetic Identity Theft & Forensic Accounting

With the increase in internet connectivity and accessibility, it appears that practically anything can be purchased over the internet and while this is a tremendous convenience for most individuals, it is not without its limitations. According to Montgomery, as a result of extensive computer and internet usage, a new form of identity theft has emerged. Although the concept of identity theft is not new, this new form of identity theft is known as synthetic identity (hereinafter, SID) theft and it can have far reaching impacts. SID theft can be defined as identity fraud where a perpetrator combines both real and false personal information in order to create a fake identity, which can then be used to defraud financial or governmental institutions[96]. In addition, Richardson and Waldron notes that the fraudulent action of "synthetic ID theft is the fastest growing financial crime in the United States"[97]. According to Miller et al., personal identifiable information (hereinafter, PII) can be found readily on the internet as a result of data breaches[98]. As well, Engel adds to the discussion by noting that fraudsters are able to obtain this personal information for ridiculously low prices on the "dark web;" it is noted that social security numbers can be bought for as little as a dollar or two. Additionally, there is an abundance of PII on the dark web as one marketplace alone had contained over 24 million social security numbers[99].

[96] Montgomery, Ken, "Synthetic Identity Fraud in the U.S. Payment System A Review of Causes and Contributing Factors," *The Federal Reserve*, July 2019, https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf. Accessed on May 2, 2023, p. 1-4.
[97] Richardson, Bryan and Waldron, Derek, "Fighting Back Against Synthetic Identity Fraud," *McKinsey & Company*, January 2, 2019, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/fighting-back-against-synthetic-identity-fraud. Accessed on May 2, 2023, para. 1.
[98] Miller, M., Budnik, R., & Chen, S., "The Changing Face of Identity Theft," *KPMG*, 2022, https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2022/synthetic-identity-fraud.pdf. Accessed on May 3, 2023, para. 1.
[99] Engle, Michael, "How To Combat Synthetic Identity Fraud," *Forbes*, November 3, 2022, 8:30am, https://www.forbes.com/sites/forbestechcouncil/2022/11/03/how-to-combat-synthetic-identity-fraud/?sh=691782d56673. Accessed on May 3, 2023, para. 3.

According to Richardson and Waldron, they note the process of SID theft works by taking a mix of real and fake information, and applying for credit under that identity; however, as this false identity will not match up with any records at the credit bureau, the credit application will likely fail. However, in the process of doing so, "the act of applying for credit automatically creates a credit file at the bureau in the name of the synthetic ID, so the fraudster can now set up accounts in this name and begin to build credit"[100]. As Miller et al. states, the alleged fraudster may then choose between two possible options for fraudulent gain: They can either use the credit, typically in the form of a credit card, to make purchases with no intention of paying back the financial institution. They could also slowly build credit under this false identity and once the credit is substantially increased, they would then decide to max out all credit available and not pay back the funds owed and on average, this amounts to about $15,000 USD[101]. Moreover, many government agencies have subsidies or aid relief funds that can be taken advantage of by fraudsters. As U.S. Attorney's Office, Southern District of Florida notes, two men allegedly created shell companies from their SID and applied for and received nearly three million dollars in relief money, which was intended to support small business during the coronavirus pandemic[102]. Engel notes that part of the reason why SID theft has become so pervasive and attractive is because traditional identity theft has become much more difficult and was a result of credit monitoring applications and fraudulent action alerts. On the other hand, in creating SID, the credit bureau has no means of establishing whether a submitted social security number, name or any other PII is real or

[100] Richardson and Waldron, para. 4.
[101] Miller, Budnik & Chen, p. 1.
[102] U.S. Attorney's Office, Southern District of Florida, "Two Men Who Allegedly Used Synthetic Identities, Existing Shell Companies, and Prior Fraud Experience to Exploit Covid-19 Relief Programs Charged in Miami Federal Court," *U.S. Attorney's Office, Southern District of Florida*, August 28, 2020, https://www.justice.gov/usao-sdfl/pr/two-men-who-allegedly-used-synthetic-identities-existing-shell-companies-and-prior-0. Accessed on May 4, 2023, para. 5.

not. As well, due to the increasing use of the internet, 16% of all retail sales now occur online, which means that the cardholder would not be present at the time of purchase and would be very convenient for a fraudster pretending to be someone else. Additionally, many governmental agencies contain processes in how applications can be applied for and received, however this is entirely through the internet, which also makes it easy for criminals to defraud the process[103].

Furthermore, another aspect that makes detection of SID even more difficult is stated by Richardson and Waldron who note that people who do not have credit histories, such as young people who are applying for credit the first time, often resemble SID and what complicates matters even further is that financial institutions are reluctant to impose significant identity verification checks out of fear they would inconvenience their customers and lead them to bank with a competitor[104]. According to Miller et al., as some of the PII contain social security numbers that are real, there may be an individual who is having their identity used for fraudulent purposes. It is noted that this type of fraud disproportionately affects those who are unable or unlikely to check their credit scores such as children, the elderly or homeless individuals[105].

8.1 Synthetic Identity Theft - The Future of IFA Engagements

The future landscape for IFAs in regards to SID theft appears to be quite promising and full of engagement opportunities. As Richardson and Waldron notes, SID theft growth in the United States has surpassed the growth rate of all other forms of financial crime[106]. Therefore, the future implications of the potential harm are significant

[103] Engle, paras. 6-7.
[104] Richardson and Waldron, paras. 4-7.
[105] Miller, Budnik & Chen, p. 1.
[106] Richardson and Waldron, para. 1.

and the engagement opportunities for IFAs are plentiful. Potential areas of engagements for IFAs in the future would be the prevention of cybersecurity attacks and the mitigation of harm following a cyber attack and in both of these scenarios, the occurrence and harm of synthetic identity theft may be lessened. As Bwerinofa-Petrozzello notes, forensic accountants play a key role in identifying potential cyber risks, vulnerabilities and preparing fraud risk assessments prior to the occurrence of a cyber attack[107]. Engle notes SID theft begins with a stolen social security number, which can be readily purchased over the internet for an incredibly low price[108]. Typically, this type of PII ends up on the internet as a result of malware or data breaches. Therefore, an IFA may prevent the occurrence of such malware installation or a potential data breach by helping companies become aware of their potential fraud risks and mitigating them before a cyber attack occurs, and where the PII becomes susceptible to theft. In addition, as Bwerinofa-Petrozzello states, IFAs can help develop a response plan in the event of a cyber attack that could limit the potential harm caused by the attack[109]. This may also help to reduce the occurrence of SID theft as the response plan may save valuable time and limit the amount of PII stolen, which in turn, could reduce the amount of SID theft that may be perpetuated.

Another area of future engagement for IFAs in relation to SID theft would be working with governmental agencies and financial institutions, such as banks to develop a model that can detect the occurrence of a fraudulently created SID. Currently, as Montgomery states "ID Analytics estimates that 85 percent to 95 percent of applicants

[107] Bwerinofa-Petrozzello, Rumbi, "Helping Clients Before a Cyberattack," *Journal of Accountancy*, September 2021, https://www.proquest.com/docview/2638778689/fulltextPDF/D6A7FD8999844BC8PQ/1?accountid=14771. Accessed on May 4, 2023, p. 27.
[108] Engle, paras. 2-3.
[109] Bwerinofa-Petrozzello, p. 27.

who were identified as synthetic identities were not flagged as high risk by traditional fraud models, such as those used to detect traditional identity theft"[110]. Therefore, as SID theft possesses different characteristics than traditional identity theft, the way in which fraudulently created identities are determined and deemed as high risk requires updating, which could be another future area of engagement for IFAs. According to Montgomery, it is estimated that in 2016 alone, costs of six billion USD was incurred as a result of SID theft[111]. This highlights another emerging area for IFAs, which is the quantification of loss or harm as a result of SID frauds. A financial institution, such as a bank, may employ an IFA to quantify the loss incurred due to SID theft; they may then use this figure to determine if adding additional verification steps to limit or prevent SID theft would be worth the investment. Moreover, the same could be said for governmental entities and the subsidies they may provide, such as welfare or disability payments that could be made to fraudulent SIDs.

Another potential area for future IFA engagements would be litigation support in SID theft litigation cases. Miller et al. notes that children are often the victims of SID theft as they likely do not possess credit, which makes them an ideal target. It is noted that children are 51 times more likely to be the victim of a SID fraud over an adult[112]. Moreover, as Montgomery notes, oftentimes these victims are not aware their identity has been compromised until they reach the age of majority and attempt to apply for credit[113]. Therefore, in the future, there may be many adults who fell victim to SID theft when they were children, who are seeking retribution for their new found inability to secure credit,

[110] Montgomery, p. 6.
[111] Ibid., p. 14.
[112] Miller, Budnik & Chen, p. 1.
[113] Montgomery, p. 17.

which can severely limit a young adult's life, for example, not being able to take out a mortgage or finance a car. Therefore, IFAs may have engagement opportunities in quantifying damages, which would be paid to the victims if litigation cases were to be successful. Furthermore, as PII is leaked online through data breaches and could result from negligence, in the future, there may be class action lawsuits that focus on seeking damages for an entire group of victims as a result a company's improper controls or PII regulation; if this were the case, IFAs would serve a crucial role in litigation support. Sanchez notes that if a case goes to litigation, the IFA would have the responsibilities of preparing the expert report in a way that is easily understood by the trier of fact and others, as well as testifying to the findings of the investigation, which would be an additional engagement area in the future for IFAs[114].

8.2 Synthetic Identity Theft - IFA Skills for the Future

In the fight against SID theft, IFAs bring a number of essential skills which can greatly aid an investigation. As Evans notes, the current framework for detection of identity theft is focused on the traditional form of identity theft and as a result, the internal controls and tools employed are not sufficient to detect and prevent SID theft[115]. This alludes to the necessity for a revised framework that can detect and prevent both the original form of identity theft, as well as the new approach. According to Evans, it is suspected that data analytics can be extremely useful in the fight against SID theft[116]. Meanwhile, Equifax mentions that machine learning can play a vital role in the detection

[114] Sanchez, Maria, "The Role of the Forensic Accountant in a Medicare Fraud Identity Theft Case," *Global Journal of Business Research*, 2012, Vol. 6, Iss. 3, p. 89.
[115] Evans, Lawrence, "Highlights of a Forum: Combating Synthetic Identity Fraud," *U.S Government Accountability Office*, July 2017, https://www.gao.gov/assets/gao-17-708sp.pdf. Accessed on May 5, 2023, p. 22.
[116] Ibid., paras. 22-23.

of SID[117]. Therefore, an incredibly important skill set for IFAs to possess would be the ability to work with companies to strengthen their internal controls and implement tools, such as data analytics and machine learning to mitigate the harm of SID theft. In terms of strengthening internal controls, this is an area where traditional IFA or fraud detection skills, such as an investigative mindset, would come in handy. An example is mentioned by Equifax where often these fraudulently created SIDs will use the same addresses as other fraudulently created identities and may update their addresses quite frequently[118]. An IFA who possesses an investigative mindset would determine that if there were two unrelated individuals with the same addresses, it would be a red flag, therefore this type of traditional forensic accounting knowledge and skills should be incorporated into the revised framework. Furthermore, many IFAs are experts in the use of data analytics and according to Equifax, this can be employed in SID fraud cases to "detect linkages and suspicious patterns indicative of phony or manipulated identities"[119]. Moreover, as Equifax adds, machine learning can be employed by IFAs to help determine inconsistencies or unique patterns that may indicate the possibility of SID[120]. Therefore, the skills of IFA can be used to help financial institutions or governmental entities to develop a more comprehensive framework for the detection of SID fraud. Another skill of IFAs that will aid in SID theft engagements in this regard is developing fraud response plans for companies who possess PII as Evans notes that hackers often attack public and private databases that may contain PII[121]. Therefore, companies may wish to have a plan in place prior to the occurrence of a hack, data breach or cyber attack. This way it may

[117] Equifax, "Synthetic Identity Fraud: A Look Behind the Mask," *Equifax*, 2019, https://assets.equifax.com/assets/usis/synthetic_identity_fraud_look_behind_mask_wp.pdf. Accessed on May 5, 2023, p. 12.
[118] Ibid., p. 13.
[119] Ibid., p. 12.
[120] Ibid., p. 12.
[121] Evans, p. 8-9.

mitigate the harm and potentially lessen the amount of PII that is stolen and uploaded to the internet, which in turn, reduces SID theft.

Another skill set of IFAs that can aid in SID theft engagements would be loss quantification skills, expert report writing and expert witness testimony skills. As Evans notes, the repercussions for those found guilty of SID theft are not strict enough and as a result, fraudsters are not deterred by the penalties[122]. This indicates a potential need for increased attention brought on this type of fraud. One way in which IFAs can aid in this would be to complete a loss quantification and their expert report, which would explain the fraud in simple terms so that people who are not experts in this field would understand. This piece of information combined with possible testimony in court would increase media attention and possibly increase attention to frauds of this nature.

According to Cunha, more information is required on how fraudsters are able to perpetuate this type of SID theft, which can then be used to improve the responsiveness of AI or machine learning algorithms[123]. This is another area where potentially the skills of an IFA may aid. For example, as IFAs are able to trace funds and explain how the fraud occurred, IFAs may be able to provide additional information on these types of frauds and how they are perpetuated; this data can then be used to train AI or machine learning algorithms.

IFA skills that include fund tracing and the ability to obtain court orders, such as the Norwich order, may help in SID engagement fraud cases as the IFA may be able to prove that it was not the alleged individual who incurred the charges, but rather a

[122] Ibid., p. 23.
[123] Cunha, Jim, "Mitigating Synthetic Identity Fraud in the U.S. Payment System," *The Federal Reserve*, July 2020, https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf. Accessed on May 6, 2023, p. 20.

fraudster stealing someone else's identity. For example, Mills discusses a case where a man received a $2,842 income tax bill for an employer he did not actually work for. It was found that this employer was entirely fraudulent, as well as it appearing that this man may have been a victim of SID theft[124]. However, if an IFA were to be retained, they may be able to prove that it was not this man who incurred those charges and that he is a victim rather than the perpetrator.

9.0 Investigative & Forensic Accounting Tools

With the rapid increase of internet accessibility, forensic accountants have been experiencing a new age of fraud engagements involved in the domains of the internet. However, with this new age of fraud engagements, brings forth new tools that utilizes the increased internet accessibility that are able to combat these new emerging IFA engagements; these tools are machine learning, data analytics and Benford's law. Therefore, it is important to define, critically examine, and discuss these new emerging tools stemming from the increased internet accessibility that are able to assist IFAs in the new age of fraud engagements. However, although it is important to discuss the benefits for all of the tools, it is also crucial to discuss the limitations of each so that there is a clear understanding of the tool itself and its usefulness in aiding IFAs in future engagements.

9.1 Machine Learning

Machine learning (hereinafter, ML) is a rapidly advancing field that serves as an emerging tool which has offered significant benefits to various industries, therefore it has

[124] Mills, Stu, "Ottawa Man's Mysterious Tax Bill May Shine Light on 'Synthetic Identity Fraud," *CBC News*, April 19, 2022, 1:00am, https://www.cbc.ca/news/canada/ottawa/mysterious-tax-bill-linked-to-synthetic-identity-fraud-1.6418589#:~:text=CBC%20News%20Loaded-,Ottawa%20man's%20mysterious%20tax%20bill%20may%20shine%20light%20on%20'synthetic,no%20one%20can%20track%20down. Accessed on May 7, 2023, paras. 1-21.

been explored as a tool that can be applied to forensic accounting and its engagements. ML is defined by Cho et al. as "a field of study that gives computers the ability to learn without being explicitly programmed"[125]. Primarily, machine learning is focused on how a computer can learn new behaviors and improve on its ability to predict future events without the necessity for direct instruction[126]. According to Brown, ML works by taking a set of data and treating this data as training data or information from which it can learn off of. This data can be in a variety of forms, such as transaction records, sensor data or even pictures of people or food items. Following this, a model of ML is selected and it will use the data provided to essentially teach itself to find patterns in the data or predict future events. Data from the training set will then be selected as a form of evaluation to determine the accuracy of the predictions of a ML based model. The programmers can adjust certain parameters of the model to increase the accuracy of its predictions[127]. Once a model is finalized, new sets of data can be fed to the computer algorithm and it should be able to produce similar results with other datasets. Typically, a ML model will attempt to produce results which are either "descriptive, meaning that the system uses data to explain what happened; predictive, meaning the system uses data to predict what will happen; or prescriptive, meaning the system will use the data to make suggestions about what action to take"[128]. Hence, it is apparent that machine learning could be a useful tool in the field of forensic accounting and its engagements.

[125] Cho, S., Vasarhelyi, M. A., Sun, T. Zhang, C., "Learning from Machine Learning in Accounting and Assurance," *Journal of Emerging Technologies in Accounting*, 2020, Vol. 17, Iss. 1, p. 1.
[126] Ibid., p. 1.
[127] Brown, Sara, "Machine Learning, Explained," *MIT Sloan School of Management*, April 21, 2021, https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained. Accessed on May 9, 2023 paras. 13-15.
[128] Brown, p. 17.

9.2 Machine Learning - Advantages in IFA Engagements

The prospective uses for ML applications in IFA engagements are widespread as Cho et al. notes, ML can help to automate many of the traditional monotonous duties of IFAs; for example, analyzing transactions or reviewing documents. Additionally, it is noted that ML can be particularly useful in situations where there is a lot of unstructured data, such as handwritten notes or scanned images as the computer is able to recognize and process this information if it were structured data, such as a dataset. The counting of physical inventory typically is a very tedious task, but ML can be combined with a drone that can not only quantify the amount of inventory, but also provide a rating of the condition of the inventory[129]. Despite these benefits, the true advantage afforded by ML is in its ability to increase the accuracy of results stemming from IFA engagements, expedite the process of investigating an IFA engagement, and bringing new functionality to the cases of other IFA tools. Fancher et al. adds to the discussion and notes that the combination of traditional forensic accounting skills and ML computer systems can work incredibly well in conjunction and will enable the IFA to not only respond to engagements in a more timely manner, but also the ML algorithms will learn throughout the process and will become better at detecting suspicious activity and ultimately prevent fraudulent actions[130]. For example, Ding et al. employed ML techniques to show that ML actually generated more accurate calculations of loss in insurance claims than what the managers were able to quantify based on financial statements alone[131]. Similarly,

[129] Cho, Vasarhelyi & Sun, p. 4-5.
[130] Fancher, D., Rial, E., Lalchand, S., & Balasubramanian, S., "The Evolution of Forensic Investigations," *Deloitte*, 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-forensic-analytics-series-the-evolution-of-forensic-investigations.pdf. Accessed on May 10, 2023, p. 1.
[131] Ding, K., Lev, B., Peng, X., Sun, T., & Vasarhelyi, M. A., "Machine Learning Improves Accounting Estimates: Evidence from Insurance Payments," *SSRN*, May 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3253220. Accessed on May 10, 2023, p. 2.

Fancher et al. notes that an advantage afforded to ML is that as it is AI powered, it will never miss a trend or suspicious transaction, which may not be the case for IFAs[132]. Badal-Valero et al. also notes that Benford's law, which is another IFA tool used in the detection of fraud activities was combined with a ML algorithm in an attempt to create a new tool where money laundering activities may be detected by ML through Benford's law[133]. As well, Castillo highlights the benefit of using a ML algorithm known as natural language processing, which "gives computers the ability to automatically read, understand, and derive meaning from human languages." This enables ML to separate textual data into patterns without the need of a human to read and categorize it first, which can be extremely useful for IFA engagements where there might be a great deal of information, as the computer would be able to separate all the data into themes and essentiality provide highlights on what is the most important information[134]. As Fancher et al. notes, a key advantage of ML is that it potentially enables the IFA to learn more about a fraudster's individual attributes as the ML computer can learn to identify these attributes, which may play a significant role in helping to identify and prevent fraudulent actions in the future. Furthermore, as AI and ML powered systems adapt, they become better at detecting possible fraudulent behaviours. This represents a shift in the "man vs. machine" team to more of a "man and machine" team." The hope is that it will shift the focus of fraud investigations as a whole to a more proactive approach rather than the current state of reactivity when fraud occurs[135], therefore this is another way in which ML can benefit IFAs in engagements.

[132] Fancher, Rial, Lalchand & Balasubramanian, p. 2.
[133] Badal-Valero, Alvarez-Jareño & Pavía, p. 24.
[134] Castillo, Andre, "Natural Language Processing," *The CPA Journal*, June/July 2021, Vol. 91, Iss. 6/7, p. 16.
[135] Fancher, Rial, Lalchand & Balasubramanian, p. 3.

9.3 Machine Learning - Limitations in IFA Engagements

Despite the numerous benefits of employing ML algorithms, there are a number of potential limitations to ML applications as well. For example, as Boukherouaa et. al mentions, a key concern with ML are the embedded biases; as ML forms its decisions based on the training data and historical performances, bias can be found, introduced and incorporated into ML decisions in a number of ways such as, through training data that is not representative or not having sufficient enough data. An example is provided where a company employed a ML based hiring system that excluded some female candidates. Historically, in past hiring scenarios, male candidates were preferred over their female counterparts. Additionally, the developers of a ML model may unknowingly or knowingly inject their own bias into a ML based system. A researcher may tweak a parameter, which results in the model favouring one characteristic more than others and could introduce bias[136].

Another limitation to ML applications that is particularly relevant to IFA engagements would be the notion stated by Kapoor et al. which is that often, it can be difficult for those who employ ML systems to explain how the model was able to achieve that result. Additionally, it may be even more difficult to validate the results from ML applications; this is known as the "black box" concern[137]. This poses a significant issue for IFAs as if an engagement ultimately ends up in court and the opposing counsel were to raise a concern around how the IFA achieved a certain result or how they were able to verify the accuracy of their result, and the response was simply that the ML software

[136] Boukherouaa, E. B., Shabsigh, G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., Mirestean, A. T., and Ravikumar, R., "Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance," *International Monetary Fund*, October 2021, https://www.imf.org/-/media/Files/Publications/DP/2021/English/PDEORAIFEA.ashx. Accessed on May 11, 2023, p. 14-15.
[137] Kapoor, I. S., Bindra, S., & Bhatia, M., "Machine Learning in Accounting & Finance: Architecture, Scope & Challenges," *International Journal of Business and Management*, April 2022, Vol. 17, Iss. 5, 13-22, p. 19-20.

calculated it, the opposing counsel would be able to use this information to discredit the expert witness during cross examination. What makes this concern even greater is that oftentimes, models employed in finance matters can become extremely complicated. For example, according to Kapoor et al., in predicting mortgage default rates, decision trees by the thousands were created by the ML model as a way of explaining how it was able to achieve the findings[138]. This makes it very difficult for an IFA to explain the results or findings to a judge and jury, which could pose major potential ramifications for an IFA engagement.

Another potential limitation is discussed by Boukherouaa et al., which is that ML approaches may be vulnerable to cyber threats. As ML is only as good as the data in which it relies upon, individuals looking to interfere in an IFA engagement may do so by manipulating the data employed by the model. An example is provided where in a data poisoning attack, the training data for the ML algorithm was corrupted and resulted in the model incorrectly learning information and then producing incorrect results. Furthermore, even if a model had been altered, the ML algorithm will still generate a result according to its set parameters; however, the result could be completely inaccurate and still remain undetected. This is because the algorithm accomplished what it was supposed to do, but the data which it was trained on was corrupted[139]. This could have negative implications for IFA engagements as alleged fraudsters may be able to potentially attack these algorithms and remove their wrongdoings from the model's parameters, which would then exclude the alleged fraudsters' actions. Lastly, Kapoor et al. notes that with the internet, ML models can be easily downloaded, installed and

[138] Ibid., p. 19-20.
[139] Boukheroouaa, Shabsigh, Alajmi, Deodoro, Farias, Iskender, Mirestean & Ravikumar, p.16-17.

employed for use in a number of scenarios. However, this leads to the possibility that they may be used incorrectly or the results produced will not be interpreted correctly[140]. This can have negative implications for IFA engagements, as well as the poorly interpreted or inaccurate findings, which may lead to significant miscarriages of justice given the serious nature of IFA engagements and may potentially discredit the IFA profession.

10.0 Big Data Analytics

According to Akinbowale et al., traditional approaches to data analytics have become outdated. In order for IFAs to remain at the forefront of the fraud detection and prevention field, new tools that can make the old ways seem slow, ineffective and monotonous need to be considered. One of these tools is the approach of big data analytics (hereinafter, BDA)[141]. Elgendy & Elragal notes that with the advancements in technology, significant volumes of data are becoming more and more widespread, which results in a necessity for new tools that can analyze substantial quantities of data in an efficient manner[142]. As Byrnes et al. notes BDA "is the science and art of improving knowledge about or gaining insights into some field of interest or subject matter by identifying and analyzing related patterns and correlations in Big Data[143]. As well, many researchers such as Gandomi & Haider and Elgendy & Elragal both note that the "big data" portion of BDA can be characterized by the three V's, which describe the

[140] Kapoor, Bindra & Bhatia, p. 19.
[141] Akinbowale, O. E., Mashigo, P. & Zerihun, M. F., "The Integration of Forensic Accounting and Big Data Technology Frameworks for Internal Fraud Mitigation in the Banking Industry," *Cogent Business & Management*, 2023, Vol. 10, Iss. 1, p. 2.
[142] Elgendy, Nada and Elragal, Ahmed, "Big Data Analytics: A Literature Review Paper," *Springer International Publishing Switzerland*, 2014, https://www.researchgate.net/profile/Ahmed-Elragal/publication/264555968_Big_Data_Analytics_A_Literature_Review_Paper/links/541e9b9a0cf203f155c0655a/Big-Data-Analytics-A-Literature-Review-Paper.pdf. Accessed on May 11, 2023, p. 215-216.
[143] Byrnes, P., Criste, T., Stewart, T., Vasarhelyi, M., Pawlicki, A. & McQuilken, D., "Reimagining Auditing in a Wired World," *AICPA*, August 2014, https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper-blue-sky-scenario-pinkbook.pdf. Accessed on May 12, 2023, p. 7.

characteristics of the data upon which BDA relies upon. The first V is for volume, which refers to the substantial amount of data present and available for analysis. The second V is variety, which refers to the diversity of the data present; this could be a mixture of structured and unstructured data. The third V stands for velocity, which refers to the rate at which data is created, changed or "analyzed and acted upon"[144]. However, as Gandomi and Haider note, this data is useless without a practical way of extracting the key tenets or finding the answers that researchers may be seeking from the data. This is where the most important role of analysis comes into play during the data analytics approach[145]. As Elgendy and Elragal note, "data analytics is the process of applying algorithms in order to analyze sets of data and extract useful and unknown patterns, relationships and information"[146]. Additionally, it is noted by Byrnes et al. that data analytics approaches can help create findings that are more robust and reliable as BDA can now potentially analyze the entirety of the data on the matter rather than just a small sample that could potentially become skewed[147]. Some examples of the types of BDA are provided by Gandomi and Haider; for example, text analytics that scours large sets of human generated text data in an attempt to create a valuable synopsis from the data, which typically is from emails, news sites, and corporate documents. Moreover, there are BDA techniques for analyzing audio, video, social media networks, and even predictive analytics which try to estimate what the future outcomes may look like based on the data available[148].

[144] Gandomi, Amir, and Murtaza, Haider, "Beyond the Hype: Big Data Concepts, Methods, and Analytics," *International Journal of Information Management*, 2015, Vol. 35, Iss. 2, p. 135; Elgendy and Elragal, p. 215-216.
[145] Ibid., p. 140.
[146] Elgendy and Elragal, p. 219.
[147] Byrnes, Criste, Stewart, Vasarhelyi, Pawlicki & McQuilken, p. 7.
[148] Gandomi and Murtaza, p. 140-143.

10.1 Big Data Analytics - Advantages in IFA Engagements

The BDA revolution appears to be well underway and offers numerous advantages to IFAs within the forensic accounting field. One benefit afforded to IFAs as a result of using BDA as a tool would be as Byrnes et al. notes, both the efficiency and effectiveness of fraud detection is enhanced by the use of BDA. This is a result of being able to analyze extremely large amounts of data in a relatively quick manner as it is noted that with data analytics, "patterns and connections that might never have been discovered in the past can be much more easily identified, analyzed, and visualized"[149]. This indicates that by employing BDA as a tool for IFAs, it can essentially make the role of an IFA easier or result in more meaningful fraud investigations. In addition, as Deloitte acknowledges, BDA technologies are able to reveal information which may not be found through traditional means at all; for example, information that is not explicitly stated but can be determined through looking at hidden meanings within the data[150]. As Chong mentions, a recent BDA trend is focused on combining security video recordings and data analytics algorithms to develop a deeper understanding of the ways in which people shop, which in turn, will allow store operators to gain valuable insights into how a store should be laid out for maximum profitability[151]. This type of analysis may be useful in IFA engagements as by looking at the hidden meanings within the data, it may reveal patterns which could indicate possible fraudulent behaviour such as, the moving of funds between accounts, which should not be occurring. This type of information can then help the IFA by providing clues as to what may be occurring. Another way in which BDA can aid the

[149] Byrnes, Criste, Stewart, Vasarhelyi, Pawlicki & McQuilken, p. 8.
[150] Deloitte, "Big Data Challenges and Success Factors," *Deloitte*, 2013, https://www2.deloitte.com/content/dam/Deloitte/it/Documents/deloitte-analytics/bigdata_challenges_success_factors.pdf. Accessed on May 12, 2023, p. 8.
[151] Chong, Phillip, "Protecting Privacy in the Age of Big Data and Analytics," *Deloitte*, n.d, https://www2.deloitte.com/th/en/pages/risk/articles/privacy-big-data-analytics.html. Accessed on May 13, 2023, para. 2.

IFA profession is that as Silva & Brizi mention that often times, companies will possess a wide variety of databases across different physical locations and it may be difficult for an IFAs to understand how all the information connects and travels between the databases; this is especially considering that it is likely both structured and unstructured data[152]. Silva & Brizi note that this instance is where BDA can help to reduce "the time investigators spend on low-value tasks, such as manually reconstructing connections between entities within tabular data or by gathering data from different systems. Having identified connections more quickly, this can leave more time for carrying out investigations themselves"[153]. An example provided by Silva & Brizi notes that what would have normally taken days to accomplish with older methods, was achieved in mere seconds with analytics software[154].

A major benefit to IFAs through the use of BDA is mentioned by Rezaee and Wang, who note that BDA can provide a risk rating for every single transaction, supplier, customer or employee; this helps with efficiency of engagements as the most risky transactions or employees can be focused on first. Additionally, as this risk score is calculated by data, it may be useful in court proceedings where an IFA can demonstrate to the trier of fact that their opinion is unbiased and that the evidence would be based on the risk score that was generated by BDA and its risk factors[155].

[152] Silva, Christophe, D., and Brizi, Leonardo, "Using Graph Data Analysis to Combat Financial Crime," *Deloitte*, n.d, https://www2.deloitte.com/ch/en/pages/financial-services/articles/graph-data-analysis-financial-crime.html. Accessed on May 13, 2023, paras. 1-7.
[153] Ibid., para. 7.
[154] Ibid., para. 8.
[155] Rezaee, Zabihollah and Wang, Jim, "Integration of Big Data into Forensic Accounting Education and Practice: A Survey of Academics in China and the United States," *Journal of Forensic and Investigative Accounting*, January–June 2022, Vol. 14, Iss. 1, p. 135.

10.2 Big Data Analytics - Limitations in IFA Engagements

Although BDA as a tool has significant positive advantages which have greatly aided the IFA profession, an examination of the limitations to the use and applicability of BDA is required as well. A limitation noted by The Institute of Chartered Accountants in England and Wales is that due to the fact that BDA relies entirely on the data provided, there is a possibility of generating unfair or biased results. This is because the analytic algorithms will attempt to classify the data in order to make predictions and it is noted that some of these factors may exacerbate this concern as the "opaque use of data, often using sensitive data that would otherwise not be allowed; confusing correlation with causation; and using data that is cheap and easily available, rather than data is most relevant but hard to capture"[156]. This is a significant limitation as based on the notion from The Institute of Chartered Accountants in England and Wales, relying on findings and predictions based on algorithms alone may disproportionately target certain groups in which the data represents and creates bias and unfair treatment[157]. Additionally, Howe & Elenberg note that BDA can infringe upon individuals' rights to privacy. An example that they provided was where BDA was used to rate potential hires' risk for a babysitting position, in which the data came from social media profiles. However, the concern was that none of the potential applicants were aware of this scoring process nor was consent ever obtained from the individuals[158].

A further limitation to BDA is noted by Akinbowale et al. who acknowledges that many IFAs do not possess the necessary skills and training to effectively use BDA for

[156] The Institute of Chartered Accountants in England and Wales, "Big Data and Analytics: The Impact on the Accountancy Profession," *ICAEW*, 2019, https://www.icaew.com/-/media/corporate/files/technical/technology/thought-leadership/big-data-and-analytics.ashx. Accessed on May 14, 2023, p. 8.
[157] Ibid., p. 8.
[158] Howe, Edmund, G., and Elenberg, Falicia, "Ethical Challenges Posed by Big Data," *Innovations in Clinical Neuroscience*, October–December 2020, Vol. 17, Iss. 10-12, p. 27.

investigative purposes, and this is an even greater concern in less developed countries[159]. Rezaee et al. who notes that "only three out of around 19 forensic accounting programs have a standalone big data course in China; in contrast, 43 out of 58 forensic accounting programs have a standalone big data course in the United States"[160]. This is a major limitation and concern as the inadequate or improper use of BDA can create further issues such as, creating bias or even possibly miscarriages of justice.

As Fancher et al. mentions, another limitation to the use of BDA as a tool in IFA engagements relates to the numerous data challenges. For example, due to the vast quantity of data needed for data analytics, storing all this data and keeping it safe while the investigation is ongoing is a very difficult process, which will only become more difficult as time goes on due to the continuous stream of data obtained during the investigation [161]. Additionally, Fancher et al. notes that "companies with decentralized operations and data sources that are siloed by geographies and departments may lack a master system to consolidate data globally"[162]. This also presents as another limitation as if an IFA were to be involved in an engagement such as this, Fancher et al. states that they would need to find some way of obtaining and merging this data together[163], which can create further issues such as, possibly requiring the need to transfer data across borders, which can present another set of concerns regarding legality and efficiency.

11.0 Benford's Law

Benford's Law (hereinafter, BL) is an incredibly fascinating phenomenon and a particularly useful tool for forensic accounting engagements. Although by no means is

[159] Akinbowale, Mashigo & Zerihun, p. 2.
[160] Rezaee, Z., Wang, J., and Lam, B. M., "Toward the Integration of Big Data into Forensic Accounting Education," *Journal of Forensic & Investigative Accounting*, January–June 2018, Vol. 10, Iss. 1, p. 89.
[161] Fancher, Rial, Lalchand & Balasubramanian, p. 6.
[162] Ibid., p. 6.
[163] Ibid., p. 7.

BL a recent discovery, this does not discount the usefulness of BL in fraud investigations. With the increase in internet accessibility, it may also increase the potential benefit for BL usage in IFA engagements. According to Durtschi et al., BL is a result of a discovery by Simon Newcomb in 1881, and then again by Frank Benford roughly 50 years later, where both had discovered that the logarithm books for academics to use in the library were more worn out on the earlier pages than the latter pages. This indicates that the earlier page numbers occurred more frequently hence showing that academics at the time were using the earlier pages more often leading to greater wear on the logarithm books[164]. This is an interesting phenomenon as general logic would note that the odds of getting any number from 1-9 should be equal however, as Collins states the following:

> The numeral 1 will be the leading digit in a genuine data set of numbers 30.1% of the time; the numeral 2 will be the leading digit 17.6% of the time; and each subsequent numeral, 3 through 9, will be the leading digit with decreasing frequency[165].

According to Gill, BL will apply to data sets that employ natural numbers which are defined as "numbers that are not ordered in a particular numbering scheme and are not human-generated or generated from a random number system"[166]. As Singleton notes, the idea behind BL is that as long as all the right conditions exist, such as a large enough data set, numeric data and presence of randomly generated numbers, BL should apply to a set of data. However, if an analysis is conducted and it appears that certain numbers

[164] Durtschi, C., Hillison, W. & Pacini, C., "The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data," *Journal of Forensic Accounting*, 2004, Vol. 5, p. 18-20.
[165] Collins, Carlton, J., "Using Excel and Benford's Law to detect fraud," *Journal of Accountancy*, April 1, 2017, https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html. Accessed on May 14, 2023, para. 3.
[166] Gill, John, "What Is Benford's Law and Why Do Fraud Examiners Use It?," *ACFE Insights*, March 14, 2023, https://www.acfeinsights.com/acfe-insights/what-is-benfords-law#:~:text=Fraud%20examiners%20use%20Benford's%20Law,invoices%20for%20%24900%20or%20%24800. Accessed on May 15, 2023, para. 4.

occur much more frequently than what should be expected and do not follow the distribution that is to be expected according to BL, it may indicate that those numbers did not naturally occur; this is in the event that those numbers were added in by a potential fraudster who may have been attempting to manipulate financial statements or records[167]. For example, as Singleton notes, if the cutoff for seeking secondary approval of a loan is $50,000, and by looking at just under this amount, it could possibly reveal whether there are fraudulent transactions. This is because according to BL, there should be less loans at over 40,000 dollars then at $30,000 or $20,000 dollar loans, but if there are significantly more transactions at $40,000 dollars, it may indicate that those numbers are not naturally occurring, but rather that a potential fraudster is increasing the amount of loans in the $40,000 dollar range to maximize their gain from fraudulent activity[168].

11.1 Benford's Law - Advantages in IFA Engagements

The principle of BL can provide a significant benefit to IFAs when conducting investigations. As Warshavsky states, the notion behind BL is that only naturally occurring numbers should be able to match the curvature or pattern of BL. As such, if humans select numbers that they have chosen themselves, these would no longer be naturally occurring and if all the other requirements for BL are met, fraudulent behaviour should stick out in the data and provide a significant clue to the IFA that something is not as it should be in regards to the data. It is noted that an IFA can apply analytical tests while working on an engagement to the accounting records, and then compare this result against the predicted results from BL, however if the shape of two representations are

[167] Singleton, Tommie, W., "Understanding and Applying Benford's Law," *ISACA*, May 1, 2011, https://www.isaca.org/resources/isaca-journal/past-issues/2011/understanding-and-applying-benfords-law. Accessed on May 15, 2023, paras. 8-14.
[168] Ibid., para. 8.

significantly different, then it may indicate concerns[169]. An example of a test using BL is noted by Warshavsky:

> First-Digit Test is a test for reasonableness that compares the actual first digit frequency distribution of a target company's data set to Benford's Law. At this test level, the data to be analyzed will be large and the test results would be used to identify obvious anomalies. This test will point a forensic accountant in the right direction, as fraudsters will tend to overuse certain digit patterns when inventing numbers[170].

Another benefit that BL can provide to IFAs is that as Singleton notes, the findings from BL is legally admissible evidence in criminal matters for the US[171]. This means that if an IFA were to find significant evidence of accounting records not matching up to the predictions as stated by BL, it may be what is needed to successfully prove that fraudulent behaviour has occurred. Moreover, as the criminal standard of proof is higher than the civil standard, this tool can provide major benefit to civil court proceedings as well. With the increase in internet accessibility, new functions in regards to BL have come about, all of which can aid the IFA in their engagements. For example, Li et al. note that BDA requires good quality data in order to produce accurate and unbiased results and as such, BL can serve as a tool to help ensure that the data employed for a BDA is of sufficient quality and free from anomalies[172]. As BL may be able to identify if

[169] Warshavsky, Mark, S., "Applying Benford's Law in Financial Forensic Investigations," *Gettry Marcus*, October/November 2010, https://www.gettrymarcus.com/wp-content/uploads/pdfs/MW-Applying-Benfords-Law-in-Financial-Forensic-Investigations.pdf. Accessed on May 15, 2023, p. 2-3.
[170] Ibid., p. 3.
[171] Singleton, para. 6.
[172] Li, F., Han, S., Zhang, H., Ding, J., Zhang, J., & Wu, J., "Application of Benford's law in Data Analysis," *Journal of Physics: Conference Series*, 2019, Vol. 1168, Iss. 3, p. 1.

numbers in the data are not naturally occurring, this in turn can help IFAs conduct more accurate and effective engagements.

Another significant benefit afforded to IFAs by using BL is that as Badal-Valero et al. (2018) notes, by combining ML approaches with BL, investigative resources can be used in the most efficient manner; for example, they note that by combining ML and BL, they were able to "uncover the largest number of fraudulent companies possible and, at the same time, reduce the likelihood of wrongly targeting companies"[173]. This is possible by using the information provided by police to build ML models, which then applied BL tests towards the accounting records of various suppliers in an attempt to determine whether certain suppliers were fraudulent or legitimate[174]. Therefore, BL can provide a number of benefits to IFAs which may greatly aid in a variety of engagements.

11.2 Benford's Law - Limitations in IFA Engagements

While BL can be an extremely useful tool for IFAs, it is equally important to consider the limitations associated with it. One limitation to BL is that as Collins notes, the application of BL is contingent on a few factors: The large sample sizes and "the data set [that] must contain data in which each number from 1 through 9, has an equal chance of being the leading digit, otherwise [BL] does not apply"[175]. An example of this is noted by Collins, as if a data set only contained sales prices, but the lowest sales price did not start with a 1 but rather a 5, then BL could not be applied[176]. This in itself is a limiting factor of BL, but beyond this, if an IFA were to mistakenly believe BL would apply to a set of data but in reality, it does not apply, it may make the data appear out of line with

[173] Badal-Valero, Alvarez-Jareño & Pavía, p. 25.
[174] Ibid., p. 25-26.
[175] Collins, para. 7.
[176] Ibid., paras. 5-7.

BL when in reality, the data wouldn't have fit BL regardless. This could be an extremely detrimental mistake to make as an IFA practitioner, especially if it were in the context of a court proceeding. Another shortcoming to the use of BL as a tool for IFA engagements is that as Goodman states, there is a lack of definition when it comes to stating whether or not a sample of data looks like the curve produced by BL. In other words, IFAs may say that the data does not appear how BL would predict it to be, but there is no measure of how much the data must deviate from the depiction for it to be considered not conforming to BL[177]. This concern can pose a significant problem for testifying IFAs as the opposing counsel cross examining the IFA could ask how the deviation of the data was determined, and what quantifiable measure was used to determine that the data set does not conform to the predictions made by BL. If the IFA is unable to provide a reasonable response to this notion, then it could potentially become an issue and harm the reputation of the IFA as a result.

Another potential drawback to the use of BL in IFA engagements is that if a fraudster is aware of BL, they may be able to create fraudulent actions in accordance with BL and then double check after inputting fraudulent numbers to ensure that the data matches the curvature of BL. This would essentially render BL useless as a tool for identifying fraudulent actions as it would be incapable of detecting fraudulent transactions or behaviors.

Lastly, as Goodman notes, there is a concern regarding the use of BL whereby it may be viewed as an "automatic fraud detector" and that any data that differs from BL is automatically fraudulent. Moreover, they note that the contribution of software tools,

[177] Goodman, William, "The Promises and Pitfalls of Benford's Law," *Royal Statistical Society*, June 6, 2016, https://rss.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1740-9713.2016.00919.x. Accessed on May 16, 2023, p. 41.

which provides a BL representation, could add to this concern as it may enhance the risk of mistakenly believing the data is fraudulent when in actuality, it is the contrary[178]. This is a dangerous trap for IFAs as it could be a potentially career destroying assumption to assume that someone perpetrated fraudulent actions when in actuality, they did not.

12.0 Methods of Enhancing IFA Training

As a result of increased internet accessibility, many areas within forensic accounting have been affected such as, new potential fraud risks, areas of engagements and new tools and techniques employed by IFAs in order to mitigate fraud risk and respond to IFA engagements. Therefore, it is crucial to outline how IFAs can stay informed and maintain adequate training, which will enable them to consistently deliver an exceptional quality of work and meet the high standards expected of IFAs.

12.1 Professional Development/Workplace Training

One approach to ensuring that IFAs receive adequate and consistently updated training is through workplace training or professional development courses offered through an employer. This type of training can be extremely valuable to IFAs as the employer can pick which types of training sessions are most relevant to their firm and the clients that they serve, or an employer can pick areas where they believe the most training is needed. For example, an employer may see that other firms are relying heavily on data analytics approaches but their own IFAs are still employing older and more traditional approaches. An excellent solution would be to contact an organization that can provide professional development courses, such as Lori and Chantrill who lists on their website a number of courses they offer. If an employer wished for their IFAs to learn more about

[178] Ibid., p. 38.

data analytics, the course offered by Deloitte will provide knowledge and practical skills on:

> How to apply data analytics, Techniques on data analytics (i.e., vendor spending, invoices, line items, duplicate payments, etc.), data reconciliation and data visualization focused on how to identify trends, outliers, and anomalies; the length, average cost per participant and method of instruction are provided[179].

12.2 University Undergraduate/Graduate Courses

Another approach to ensuring that IFAs obtain the necessary training to excel and be proficient in their fields is by offering courses to introduce these topics in undergraduate accounting courses. This allows the accountants to develop a basic understanding of IFA techniques and procedures prior to the IFA education and training opportunities. This could aid in creating a foundation of knowledge, which can make it easier for the accountants to learn IFA techniques and skills when the time comes. Additionally, it may pique their interest in IFA work and result in more accountants choosing to pursue a career as an IFA. An area identified by Rezaee and Wang which requires more training for IFAs is within the BDA field as there is shortage of IFAs who possess the necessary skills and techniques to employ big data approaches in forensic accounting engagements[180]. Additionally, Rezaee and Wang employed a survey and found that within the consensus of academics in both the U.S and China, it is believed that both big data and forensic accounting courses should be introduced to students in both the undergraduate level and graduate levels of university[181].

[179] Lori, Renée and Chantrill, Tanaquil, "Deloitte Training Services Building a Stronger Workforce," *Deloitte,* n.d, https://www2.deloitte.com/ca/en/pages/tax/articles/deloitte-training-services.html. Accessed on May 18, 2023, paras.19-22.
[180] Rezaee and Wang, p. 135.
[181] Ibid., p. 141.

12.3 Constructive Partnerships with Interrelated Industries

Another way of enhancing IFA training is by working closely with other industries related to forensic accounting, as well as law enforcement agencies; similar industries include cyber security firms and insurance companies. In developing good and positive collateral contacts with others working in such industries, IFAs may be able to gain information that indicates where emerging or future fraud risk may present, which then leads to the direction in which further training is required. For example, if a cybersecurity firm notices that there is a new exploit available that allows fraudsters to perpetuate fraud, they may be able to provide this information to an accounting firm so that the accounting firm can appropriately prepare its IFAs for the potential engagements and offer training opportunities. Additionally, it may be that these closely related industries would be the best people to contact in order to receive training on emerging fraud risks as they may be the only other companies or people who would have this type of knowledge and could train the IFAs on what they know.

12.4 Proactive Exploration of Future Industries

A way to enhance the training provided to IFAs is to explore new technological advances and fields of study, which may relate to forensic accounting and potential future fraud opportunities. In doing so, IFAs will be ready to combat the potential frauds as they occur and do not waste valuable time in learning about the new fields only after a fraud risk has emerged. An example of this could be the rise of cryptocurrency as Marr notes that Bitcoin was first introduced in 2008 through a paper that was posted online. Following this, in 2009, Bitcoin was created, and in 2010, for the first time ever, a value was placed on Bitcoin. By 2011, the price of Bitcoin began to rise and new forms of

cryptocurrency were emerging[182]. The idea is that an IFA may be able to follow along with these types of new technological advances and may be able to determine whether a field is likely to possess more fraud risks than others. In the case of cryptocurrency and given the characteristics of cryptocurrency, it appears pretty evident that fraud opportunities exist in this realm. If an IFA was carefully watching the progression of cryptocurrency from 2008 onwards, they may have been learning about cryptocurrencies prior to it becoming an area where fraudulent activity is a concern. This helps IFAs stay at the forefront of the fight against fraud and in learning about these industries, the IFAs are training themselves to deal with the possible fraud risk when they occur. A similar argument could be made regarding AI and future fraud opportunities today where currently, the potential for fraud is still quite limited. However, in the future, it is likely that AI perpetrated fraud will be quite common therefore, if IFAs immerse themselves in the knowledge around these emerging fields leading up to these fraud risks, they will have the necessary training and expertise to deal with such engagements when they inevitably occur.

12.5 Greater Research on Forensic Accounting

Lastly, a technique for improving the training of IFAs is through greater research. As forensic accounting is a relatively new field of study, greater research into how the profession can be improved as a whole will guide the training that is needed for IFAs. For example, in determining future fraud risks, new tools to fight financial crimes in which the profession is heading towards and ways of improving an engagement in terms of fraud detection and efficiency are required, therefore this relevant research will be able

[182] Marr, Bernard, "A Short History Of Bitcoin And Crypto Currency Everyone Should Read," *Forbes*, December 6, 2017,12:28am, https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=7fa22973f279. Accessed on May 18, 2023, paras. 5-8.

to change the way in which IFAs are trained and the areas upon which training should be focused. An example would be if through research, it is determined that a new emerging area of identity fraud is through the creation of fake personas with real identifying information, such as SID, then perhaps the training for IFAs should incorporate a component on how IFAs can work with organizations prior to a data breach to ensure that personal information is secured against hackers or cyber criminals.

13.0 Best Practices and Suggestions for IFA Engagements

Despite the many benefits brought forth by the advancement in accessibility and connectivity of the internet, it is important for IFAs to keep in mind that many of these new tools have limitations, and IFAs should not simply accept their findings as one hundred percent accurate. It is still the responsibility of the IFA to establish the legitimacy of the findings and verify through several different measures as ultimately, it may be the IFA testifying to those findings in a court of law. An example would be if an IFA applied a ML model incorrectly and the ML model incorrectly determined that fraudulent actions occurred when they may not have, this would be a serious concern for IFAs.

Given the advancement of technology and increased online access, the quantity of data produced from IFA engagements has been significantly exacerbated. IFAs should be mindful of whether they possess the means to store all the data emerging from an engagement, whether the data is safe and secure, how to access this data and what to do in the event that the data is leaked or hacked. In particularly challenging scenarios, IFAs should consult IT professionals, such as data storage companies to ensure their data is safely guarded and stored.

Many newly created fraud opportunities are simply new ways of committing old fraudulent behaviour or actions. For example, cryptocurrency fraud is essentially a Ponzi scheme, but with a new form of currency. Therefore, it is important to keep in mind the central tenets of traditional approaches to IFA engagements as well, such as, employing good interviewing skills and maintaining a skeptical mindset.

Since the majority of these new fraud opportunities exist within a realm where access to the internet and use of computer technologies are extremely prevalent, it may be wise for an IFA to possess sufficient IT skills in order to understand how a potential fraud may occur and how a fraudster may be able to circumvent controls to gain an advantage through this action. If an IFA does not possess the necessary IT skills or qualifications, bringing in an external IT company to serve as a consultant can be very beneficial.

As many of the new tools for aiding IFA work are emerging fields, there may not yet be regulatory bodies or industry regulations that govern their use. As such, IFAs should be mindful of the potentially changing landscape which could possibly limit the effectiveness or applicability of investigation in these respective areas. Additionally, it has yet to be seen whether some of these tools may be permitted for use in IFA engagements of the future. Therefore, IFAs should pay close attention to how these respective fields may be altered and whether any limitations will be imposed moving forward.

A central tenet to the role of an IFA is to maintain a high degree of objectivity and that the IFAs ultimate duty is to the court. It is extremely important that in these new engagement areas, this key tenet is not lost, especially taking into account how easily it may be to lose objectivity when employing these new tools. For example, AI powered

software can act in a biased manner if the data upon which it is trained upon is not representative. As such, IFAs must be mindful that this component of the IFA role is maintained.

There appears to be a shortage of forensic accountants, especially those who possess the skills necessary to employ the new approaches to combating financial crime, such as BDA or ML approaches. As a result, post-secondary institutions should offer additional courses or training programs so that the need for additional forensic accountants can be more readily fulfilled.

Given the complexity and specialized nature of many of these new engagement opportunities, it may be wise for IFAs to foster positive relationships with partners who work in similar industries. This could include cyber security professionals, data analysts and data scientists, securities professionals and cryptocurrency professionals. Knowing the right individuals who can provide assistance when needed can greatly accelerate and bring additional value to an IFA engagement.

14.0 Conclusion

The impact of increased internet accessibility and connectivity can be recognized and encountered in nearly every aspect of the IFA profession. As technology advances, traditional fraud risks are enhanced while providing new ways to perpetuate old fraudulent behaviours; meanwhile the increase in internet accessibility has also led to the creation of new types of fraudulent activities which further pose a significant risk. Despite this, the increase in the internet has also increased the tools in which are at the disposal of IFAs and has made much of the IFA work expedient and more effective in terms of fraud detection. With the addition of useful IFA tools, such as machine learning,

big data analytics and Benford's Law, it has created a new landscape in which IFA engagements are in, as utilizing the internet in targeting fraud engagements within the same scope has created an equal playing field for IFAs and potential fraudsters. This is crucial as in order to target those perpetuating fraudulent behaviours within the scope of increased internet accessibility, the IFAs and the tools they utilize must also be on par with such. In addition, this increase in online access and technology has led to the broadening of IFA skill sets to better respond to a wider variety of fraudulent actions. Therefore, the necessity for increased training opportunities and examination of best practices is highlighted by the changing face of the IFA profession which comes as a result of increased internet accessibility and connectivity.

References

Akartuna, E. A., Hetzel, F. & Kleinberg, B., "Cryptocurrencies and Future Crime," *Dawes Centres for Future Crime at UCL,* February 2021, https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/ucl_cryptocurrencies_and_future_crime_policy_briefing_feb2021_compressed_1.pdf. Accessed on April 30, 2023.

Akinbowale, O. E., Mashigo, P. & Zerihun, M. F., "The Integration of Forensic Accounting and Big Data Technology Frameworks for Internal Fraud Mitigation in the Banking Industry," *Cogent Business & Managemen*t, 2023, Vol. 10, Iss. 1, 1-22.

Ali, Mazurina M. and Mohd Zaharon, Nur F., "Phishing—A Cyber Fraud: The Types, Implications and Governance," *International Journal of Educational Reform,* 2022, Vol. 0, Iss. 0, 1-21.

American Institute of Certified Public Accountants, "AU-C Section 240 Consideration of Fraud in a Financial Statement Audit," *American Institute of Certified Public Accountants,* 2021, https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-c-00240.pdf. Accessed on April 21, 2023.

Anand, Akriti, "Forensic Accounting and the Use of Artificial Intelligence," *Pennsylvania CPA Journal,* 2019, https://www.proquest.com/docview/2547074884/fulltextPDF/FE05ACD8191A40DFPQ/1?accountid=14771. Accessed on April 29, 2023.

Anti-Phishing Working Group, "Phishing Activity Trends Report 3rd Quarter," *Anti-Phishing Working Group*, December 12, 2022, https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf. Accessed on April 21, 2023.

Ashin, Paul, "Dirty Money, Real Pain: Money Laundering Harms Innocent Individuals but Can Also Impose Serious Costs on National Economies," *Finance & Development*, June 2012, Vol. 49, Iss. 2, 38-41.

Balla, Keith S., "The Forensic Accountant's Role in Estate and Trust Matters," *PKF O'Connor Davies,* n.d, https://www.pkfod.com/insights/the-forensic-accountants-role-in-estate-and-trust-matters.Accessed on May 1, 2023.

Boukherouaa, E. B., Shabsigh, G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., Mirestean, A. T., and Ravikumar, R., "Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance," *International Monetary Fund*, October 2021, https://www.imf.org/-/media/Files/Publications/DP/2021/English/PDEORAIFEA.ashx. Accessed on May 11, 2023.

Brennan, Niamh and Hennessy, John, "Forensic Accounting and Intellectual Property Infringement," *Commercial Law Practitioner*, 2001, Vol. 8, Iss. 5, 103-109.

Brown, Sara, "Machine Learning, Explained," *MIT Sloan School of Management*, April 21, 2021, https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained. Accessed on May 9, 2023.

Burgess, Christopher, "China's Cyber Espionage Focus: Intellectual Property Theft," *ProQuest*, May 17, 2022, https://www.proquest.com/docview/2665360049?accountid=14771&parentSessionId=yEN%2B5WCBfUk%2BQIHk2iWzMKhObxuhj7IitWph7YbQUww%3D. Accessed on April 26, 2023.

Bwerinofa-Petrozzello, Rumbi, "Helping Clients Before a Cyberattack," *Journal of Accountancy*, September 2021, https://www.proquest.com/docview/2638778689/fulltextPDF/D6A7FD8999844BC8PQ/1?accountid=14771. Accessed on May 4, 2023.

Byrnes, P., Criste, T., Stewart, T., Vasarhelyi, M., Pawlicki, A. & McQuilken, D., "Reimagining Auditing in a Wired World," *AICPA*, August 2014, https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper-blue-sky-scenario-pinkbook.pdf. Accessed on May 12, 2023.

Casey, Bob, "The Impact of Intellectual Property Theft on the Economy," *The U.S. Congress Joint Economic Committee Chairman's Staff*, August 2012, https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf. Accessed on April 27, 2023.

Castillo, Andre, "Natural Language Processing," *The CPA Journal*, June/July 2021, Vol. 91, Iss. 6/7, 16-19.

Cho, S., Vasarhelyi, M. A., Sun, T. Zhang, C., "Learning from Machine Learning in Accounting and Assurance," *Journal of Emerging Technologies in Accounting*, 2020, Vol. 17, Iss. 1, 1-10.

Chong, Phillip, "Protecting Privacy in the Age of Big Data and Analytics," *Deloitte*, n.d, https://www2.deloitte.com/th/en/pages/risk/articles/privacy-big-data-analytics.html. Accessed on May 13, 2023.

Collier, Kevin, "Baby Died Because of Ransomware Attack on Hospital, Suit Says," *NBC News*, September 30, 2021, 10:51am, https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465. Accessed on April 30, 2023.

Collins, Carlton, J., "Using Excel and Benford's Law to detect fraud," *Journal of Accountancy*, April 1, 2017, https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html. Accessed on May 14, 2023.

Criminal Code, RSC 1985, c C-46, s 380(1).

Cunha, Jim, "Mitigating Synthetic Identity Fraud in the U.S. Payment System," *The Federal Reserve*, July 2020, https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf. Accessed on May 6, 2023.

Cybereason, Nocturnus, "Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques," *Cybereason*, May 4, 2022, https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques. Accessed on April 26, 2023.

Deloitte, "Big Data Challenges and Success Factors," *Deloitte*, 2013, https://www2.deloitte.com/content/dam/Deloitte/it/Documents/deloitte-analytics/bigdata_challenges_success_factors.pdf. Accessed on May 12, 2023.

Dienst, Jonathan, "Ransomware Attack at NJ County Police Department Locks Up Criminal Investigative Files," *NBC New York*, April 7, 2023, 7:11pm, https://www.nbcnewyork.com/investigations/ransomware-attack-at-nj-county-police-department-locks-up-criminal-investigative-files/4219341/. Accessed on April 30, 2023.

Ding, K., Lev, B., Peng, X., Sun, T., & Vasarhelyi, M. A., "Machine Learning Improves Accounting Estimates: Evidence from Insurance Payments," *SSRN*, May 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3253220. Accessed on May 10, 2023.

Durtschi, C., Hillison, W. & Pacini, C., "The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data," *Journal of Forensic Accounting*, 2004, Vol. 5, 17-34.

Elena Badal-Valero, E., Alvarez-Jareño, J. A., & Pavía, J. M., "Combining Benford's Law and Machine Learning to Detect Money Laundering. An Actual Spanish Court Case," *Forensic Science International*, 2018, Vol. 282, 24-34.

Elgendy, Nada and Elragal, Ahmed, "Big Data Analytics: A Literature Review Paper," *Springer International Publishing Switzerland*, 2014, https://www.researchgate.net/profile/Ahmed-Elragal/publication/264555968_Big_Data_Analytics_A_Literature_Review_Paper/links/541e9b9a0cf203f155c0655a/Big-Data-Analytics-A-Literature-Review-Paper.pdf. Accessed on May 11, 2023.

Engle, Michael, "How To Combat Synthetic Identity Fraud," *Forbes*, November 3, 2022, 8:30am, https://www.forbes.com/sites/forbestechcouncil/2022/11/03/how-to-combat-synthetic-identity-fraud/?sh=691782d56673. Accessed on May 3, 2023.

Equifax, "Synthetic Identity Fraud: A Look Behind the Mask," *Equifax*, 2019, https://assets.equifax.com/assets/usis/synthetic_identity_fraud_look_behind_mask_wp.pdf. Accessed on May 5, 2023.

Evans, Lawrence, "Highlights of a Forum: Combating Synthetic Identity Fraud," *U.S Government Accountability Office*, July 2017, https://www.gao.gov/assets/gao-17-708sp.pdf. Accessed on May 5, 2023.

Fancher, D., Rial, E., Lalchand, S., & Balasubramanian, S., "The Evolution of Forensic Investigations," *Deloitte,* 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-forensic-analytics-series-the-evolution-of-forensic-investigations.pdf. Accessed on May 10, 2023.

Fausto, Martin D. S., *Technology-Enhanced Methods of Money Laundering Internet as Criminal Means*, Cham, Switzerland: Springer Nature Switzerland AG, 2019, p. 1-181.

Fortin, Jacey, "He Tried to Bilk Google and Facebook Out of $100 Million With Fake Invoices," *The New York Times*, March 25, 2019. Accessed on April 21, 2023, from https://www.nytimes.com/2019/03/25/business/facebook-google-wire-fraud.html.

Gandomi, Amir, and Murtaza Haider, "Beyond the Hype: Big Data Concepts, Methods, and Analytics," International Journal of Information Management, 2015, Vol. 35, Iss. 2, 137-144.

Gara, A., Shubber, K. & Oliver, J., "FTX Held Less Than $1bn in Liquid Assets Against $9bn in Liabilities," *Financial Times,* November 12, 2022. Accessed on April 30, 2023, from https://www.ft.com/content/f05fe9f8-ca0a-48d5-8ef2-7a4d813af558.

Gill, John, “What Is Benford's Law and Why Do Fraud Examiners Use It?,” *ACFE Insights*, March 14, 2023, https://www.acfeinsights.com/acfe-insights/what-is-benfords-law#:~:text=Fraud%20examiners%20use%20Benford's%20Law,invoices%20for%20%24900%20or%20%24800. Accessed on May 15, 2023.

Goodman, William, “The Promises and Pitfalls of Benford’s Law,” *Royal Statistical Society*, June 6, 2016, https://rss.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1740-9713.2016.00919.x. Accessed on May 16, 2023.

Härdle, W. K., Harvey, C. R., & Reule, R. C. G., “Understanding Cryptocurrencies,” *Journal of Financial Econometrics*, February 2020, Vol. 18, Iss. 2, 181-208.

Hares, Sophie, “5 Ways Accountants Can Track Cryptocurrency,” *Journal of Accountancy*, June 29, 2020, https://www.journalofaccountancy.com/newsletters/2020/jun/accountants-track-cryptocurrency.html. Accessed on May 1, 2023.

Hou, Caline, “A Bit-ter Divorce: Using Bitcoin to Hide Marital Assets,” *North Carolina Journal of Law & Technology*, 2015, Vol. 16, Iss. 3, 74-105.

Howe, Edmund, G., and Elenberg, Falicia, “Ethical Challenges Posed by Big Data,” *Innovations in Clinical Neuroscience*, October–December 2020, Vol. 17, Iss. 10-12, 24-30.

James, Lance, *Phishing Exposed*, Waltham, Massachusetts: Syngress, 2006, p. 1-35.

Jones, Rob and Keasey, Kevin, "Money Laundering and the Internet: A Challenge for Regulation," *Journal of Financial Regulation and Compliance*, 2000, Vol. 8, Iss. 1, 67-77.

Kapoor, I. S., Bindra, S., & Bhatia, M., "Machine Learning in Accounting & Finance: Architecture, Scope & Challenges," *International Journal of Business and Management*, April 2022, Vol. 17, Iss. 5, 13-22.

Kilby, Paul, "Taming Fraud in Crypto's Wild West," *Fraud Magazine*, March/April 2023, https://www.fraud-magazine.com/cover-article.aspx?id=4295020326. Accessed on May 2, 2023.

King, Thomas C., Aggarwal, N., Taddeo, M. & Floridi, L., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions," *Science and Engineering Ethics*, 2020, Vol. 26, Iss. 1, 89-120.

Lastdrager, Elmer E. H., "Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature," *Crime Science*, 2014, Vol. 3, Iss. 9, 1-10.

Levin, Carl and Coburn, Tom, "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History Majority and Minority Staff Report," *United States Senate Permanent Subcommittee on Investigations Committee on Homeland Security and Governmental Affairs*, July 17, 2012, https://www.hsgac.senate.gov/subcommittees/investigations/library/files/report-us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history/. Accessed on April 24, 2023.

Li, F., Han, S., Zhang, H., Ding, J., Zhang, J., & Wu, J., "Application of Benford's law in Data Analysis," *Journal of Physics: Conference Series*, 2019, Vol. 1168, Iss. 3, 1-8.

Lori, Renée and Chantrill, Tanaquil, "Deloitte Training Services Building a Stronger Workforce," *Deloitte*, n.d, https://www2.deloitte.com/ca/en/pages/tax/articles/deloitte-training-services.html. Accessed on May 18, 2023.

MacQueen, Hector, *Money Laundering: Hume Papers on Public Policy 1.2*, Edinburgh, Scotland: Edinburgh University Press, 2019, p. 1-75.

Margolin, Jim and Biase, Nicholas, "Lithuanian Man Sentenced To 5 Years in Prison for Theft of Over $120 Million In Fraudulent Business Email Compromise Scheme," *United States Attorney Office: Southern District of New York*, December 19, 2019, https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business. Accessed on April 21, 2023.

Marr, Bernard, "A Short History Of Bitcoin And Crypto Currency Everyone Should Read," *Forbes*, December 6, 2017,12:28am, https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=7fa22973f279. Accessed on May 18, 2023.

Martinez-Miranda, E., McBurney, P., & Howard, M. J. W., “Learning Unfair Trading: a Market Manipulation Analysis From the Reinforcement Learning Perspective,” *2016 IEEE Conference on Evolving and Adaptive Intelligent Systems*, 2016, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7502499. Accessed on April 28, 2023.

McClintock, M.T., Kanaga, V. L., & Blattmachr, J. G., “Estate Planning in the Era of Digital Wealth,” *Estate Planning*, May 2022, Vol. 49, Iss. 5, 4-18.

Millard, Mark, “Forensic Investigations of Tomorrow,” *Deloitte*, 2022, https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/an-ounce-of-prevention/forensic-investigations-of-tomorrow.html. Accessed on April 30, 2023.

Miller, M., Budnik, R., & Chen, S., “The Changing Face of Identity Theft,” *KPMG*, 2022, https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2022/synthetic-identity-fraud.pdf. Accessed on May 3, 2023.

Mills, Stu, “Ottawa Man's Mysterious Tax Bill May Shine Light on 'Synthetic Identity Fraud,” *CBC News*, April 19, 2022, 1:00am, https://www.cbc.ca/news/canada/ottawa/mysterious-tax-bill-linked-to-synthetic-identity-fraud-1.6418589#:~:text=CBC%20News%20Loaded-,Ottawa%20man's%20mysterious%20tax%20bill%20may%20shine%20light%20on%20'synthetic,no%20one%20can%20track%20down. Accessed on May 7, 2023.

Moid, Sana, “Fighting Cyber Crimes Using Forensic Accounting: A Tool to Enhance Operational Efficiency,” *International Journal of Money, Banking and Finance, 2018,* Vol. 7, Iss. 3, 92-99.

Molloy, Cian, “The Shape of Things to Come: What Lies in Store for the Accountancy Profession? Cian Molloy Investigates How the Profession Might Fare in the Years Ahead,” *Accountancy Ireland*, February 2017, Vol. 49, Iss. 1, 30-33.

Montgomery, Ken, “Synthetic Identity Fraud in the U.S. Payment System A Review of Causes and Contributing Factors,” *The Federal Reserve*, July 2019, https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf. Accessed on May 2, 2023.

Naheem, Mohammed A., “Risk of Money Laundering in the US: HSBC Case Study,” *Journal of Money Laundering Control*, 2016, Vol. 19, Iss. 3, 225-237.

Naqvi, Al, *Artificial Intelligence for Audit, Forensic Accounting, and Valuation: A Strategic Perspective*, Hoboken, New Jersey: John Wiley & Sons, 2020, p. 1-306.

Nickerson, Mark A., “AI: New Risks and Rewards,” *Strategic Finance*, April 2019, Vol. 100, Iss. 10, 26-31.

Oliver, Joshua, “The Lawless World of Crypto Scams,” *Financial Times,* September 18, 2022. Accessed on May 1, 2023, from https://www.ft.com/content/5987649e-9345-4eae-a4b8-9bfb0142a2ab

Otusanya, Olatunde J. and Lauwo, Sarah, "The Role of Offshore Financial Centres in Elite Money Laundering Practices: Evidence from Nigeria," *Journal of Money Laundering Control*, 2012, Vol. 15, Iss. 3, 336-361.

Pacini, C., Hopwood, W., Young, G., & Crain, J., "The Role of Shell Entities in Fraud and Other Financial Crimes," *Managerial Auditing Journal*, 2019, Vol. 34, Iss. 3, 247-267.

Prabu, Sakthivel L. and Suriyaprakash, T. N. K., *Intellectual Property*, London, United Kingdom: IntechOpen, 2022, p. 1-138.

Rein, Eric, S., "Challenges in Discovering Perpetrators of International Cryptocurrency Frauds," *American Bar Association.org*, April 23, 2018, https://www.americanbar.org/groups/litigation/committees/commercial-business/practice/2018/challenges-discovering-perps-international-cryptocurrency-fraud/. Accessed on May 1, 2023.

Rezaee, Z., Wang, J., and Lam, Brian, M., "Toward the Integration of Big Data into Forensic Accounting Education," *Journal of Forensic & Investigative Accounting*, January–June 2018, Vol. 10, Iss. 1, 87-99.

Rezaee, Zabihollah and Wang, Jim, "Integration of Big Data into Forensic Accounting Education and Practice: A Survey of Academics in China and the United States," *Journal of Forensic and Investigative Accounting*, January–June 2022, Vol. 14, Iss. 1, 133-150.

Richardson, Bryan and Waldron, Derek, "Fighting Back Against Synthetic Identity Fraud," *McKinsey & Company*, January 2, 2019, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/fighting-back-against-synthetic-identity-fraud. Accessed on May 2, 2023.

Richardson, Rachel and Kelly, Paul, "Cybersecurity: Can You Identify the Weakest Link?" *Accountancy Ireland*, August 2016, Vol. 48, Iss. 4, 44-45.

Sanchez, Maria, "The Role of the Forensic Accountant in a Medicare Fraud Identity Theft Case," *Global Journal of Business Research*, 2012, Vol. 6, Iss. 3, 85-92.

Schneider, Friedrich, "Turnover of Organized Crime and Money Laundering: Some Preliminary Empirical Findings," *Public Choice*, July 2010, Vol. 144, Iss. 3/4, 473-486.

Seymour, John and Tully, Philip, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter," *Blackhat*, n.d, https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf. Accessed on April 28, 2023.

Sganga, Nicole, "Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies," *CBS News*, May 4, 2022, 12:01am, https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/#:~:text=A%20yearslong%20malicious%20cyber%20operation,manuf

acturing%2C%20energy%20and%20pharmaceutical%20sectors. Accessed on April 26, 2023.

Silva, Christophe, D., and Brizi, Leonardo, "Using Graph Data Analysis to Combat Financial Crime," *Deloitte*, n.d, https://www2.deloitte.com/ch/en/pages/financial-services/articles/graph-data-analysis-financial-crime.html. Accessed on May 13, 2023.

Singleton, Tommie, W., "Understanding and Applying Benford's Law," *ISACA*, May 1, 2011, https://www.isaca.org/resources/isaca-journal/past-issues/2011/understanding-and-applying-benfords-law. Accessed on May 15, 2023.

Steer, P., Havey, P., Venneri, A., Olfert, R., Gosse, K, & Vasa, C, "Policy Document - FN-12- Fraud Policy," *Chartered Professional Accountants Canada*, November 24, 2022, https://www.cpacanada.ca/-/media/site/operational/ex-executive/docs/02313-ex_fn-12-cpac-fraud-policy-nov-24-22-english.pdf. Accessed on April 21, 2023.

The Institute of Chartered Accountants in England and Wales, "Big Data and Analytics: The Impact on the Accountancy Profession," *ICAEW*, 2019, https://www.icaew.com/-/media/corporate/files/technical/technology/thought-leadership/big-data-and-analytics.ashx. Accessed on May 14, 2023.

Trozze, A., Kamps, J., Akartuna E. A., Hetzel, F. J., Kleinberg, B., Davies, T. & Johnson, S. D., "Cryptocurrencies and Future Financial Crime," *Crime Science,* 2022, Vol. 11, Iss. 1, 1-35.

Turner, Jonathan E., *Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud*, Hoboken, New Jersey: John Wiley & Sons, 2011, p. 1-204.

U.S. Attorney's Office, Southern District of Florida, "Two Men Who Allegedly Used Synthetic Identities, Existing Shell Companies, and Prior Fraud Experience to Exploit Covid-19 Relief Programs Charged in Miami Federal Court," *U.S. Attorney's Office, Southern District of Florida*, August 28, 2020, https://www.justice.gov/usao-sdfl/pr/two-men-who-allegedly-used-synthetic-identities-existing-shell-companies-and-prior-0. Accessed on May 4, 2023.

U.S. Securities and Exchange Commission, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX," *U.S. Securities and Exchange Commission*, December 13, 2022, https://www.sec.gov/news/press-release/2022-219. Accessed on April 30, 2023.

Warshavsky, Mark, S., "Applying Benford's Law in Financial Forensic Investigations," *Gettry Marcus,* October/November 2010, https://www.gettrymarcus.com/wp-content/uploads/pdfs/MW-Applying-Benfords-Law-in-Financial-Forensic-Investigations.pdf. Accessed on May 15, 2023.

Wilding, Edward, *Information Risk and Security*, London, United Kingdom: Routledge, 2006, p. 67-86.