Whistleblowing and fraud in digital era

Santi Widhiyanti*, Yustrida Bernawati

Airlangga University, Jalan. Airlangga No.4 - 6, Surabaya, 60115, East Java, Indonesia

ABSTRACT

Whistleblowing of fraud in the digital era in Indonesia has shifted from the traditional way into a digital system. Digital whistleblowing allows someone to reveal a number of information accompanied by photos/ videos through social media/ other online sources. It is assumed that there is a possibility that the information is inaccurate. This study discusses financial statement fraud using artificial intelligence (AI) technology. The analysis was done by firstly using a literature study. Besides that, observation of the phenomenon of fraud cases that recently hit SOEs in Indonesia was also done. Then, it was increasingly discussed in depth by reading the media (online, either website or social media). In the next step, this study looked for references such as journals, books, and news in electronic media related to this paper. Results showed that Fraud often happens that the customer initially only gives a complaint through the company's social media, but in the end, it is used as whistleblowing by external parties. Therefore, suggestions can be by open complaints on social media, which can spread quickly, should be handled by the company well so that the company's image can be maintained. Furthermore, whistleblowers require commitment from management starting from the lowest management to the highest management because it is related to whistleblower protection rules that include a guarantee of security, fairness, and continuity of work in the organization. An effective Whistleblowing system requires the right system/ management and procedures so that the reporters and the witnesses feel safe and their safety is guaranteed.

ABSTRAK

Whistleblowing terhadap fraud di era digital di Indonesia telah bergeser dari cara tradisional menjadi sistem digital. Whistleblowing digital memungkinkan seseorang mengungkap sejumlah informasi disertai foto/ video melalui media sosial / sumber online lainnya. Diasumsikan bahwa ada kemungkinan informasi tersebut tidak akurat. Penelitian ini membahas tentang penipuan laporan keuangan dengan menggunakan teknologi kecerdasan buatan (AI). Analisis dilakukan dengan terlebih dahulu menggunakan studi pustaka. Selain itu, observasi terhadap fenomena kasus fraud yang belakangan ini melanda BUMN di Indonesia juga dilakukan. Kemudian semakin dibahas secara mendalam dengan membaca media (online, baik website maupun sosial media). Selanjutnya penelitian ini mencari referensi berupa jurnal, buku, dan berita di media elektronik yang berkaitan dengan makalah ini. Hasil penelitian menunjukkan bahwa fraud sering terjadi di mana pelanggan awalnya hanya menyampaikan pengaduan melalui media sosial perusahaan, namun pada akhirnya dijadikan whistleblowing oleh pihak eksternal. Oleh karena itu, saran yang dapat berupa keluhan terbuka di media sosial yang dapat menyebar dengan cepat sebaiknya ditangani oleh perusahaan dengan baik agar citra perusahaan dapat terjaga. Lebih lanjut, whistleblower membutuhkan komitmen dari manajemen mulai dari manajemen terendah hingga manajemen tertinggi karena terkait dengan aturan perlindungan whistleblower yang mencakup jaminan keamanan, keadilan, dan kelangsungan pekerjaan dalam organisasi. Sistem Whistleblowing yang efektif membutuhkan sistem / manajemen dan prosedur yang tepat agar pelapor dan saksi merasa aman dan terjamin keselamatannya.

* Corresponding author, email address: santi.widhiyanti@gmail.com

1. INTRODUCTION

In 2016, the Association of Certified Fraud Examiners (ACFE), in collaboration with the Center for Research and Prevention of White Collar Crime (P3K2P) Perbanas Surabaya and sponsored by Ernst and Young (EY) Indonesia, conducted a survey aimed at obtaining an overview of fraud in Indonesia. Based on the survey results, the most common fraud in Indonesia is corruption with an average loss of IDR 100,000,000 - IDR 500,000,000 per case (ACFE-INDONESIA, 2017: 9).

There are three types of fraud: financial statement fraud, misuse of assets, and corruption (Tuanakotta, 2014: 195 - 204). First, financial statement fraud is fraud committed intentionally by intelligent people. Using their intelligence, they manipulate the trust through political persuasion or intimidation for their own benefit or the organization depending on whether the crime is a work or organizational crime (Krambia-Kapardis, Christodoulou, and Agathocleous, 2010). Second, misuse of assets is unauthorized use of company property for personal gain, which includes theft, embezzlement, or misappropriation of cash or supplies and other assets (Wells, 2017: 45 – 46). Finally, it is corruption that is the use of their impact or power in business activities illegally for personal benefits, which is contrary to their responsibility to the employer or the rights of others such as accepting bribes or being involved in conflicts of interest (Wells, 2017: 245).

There have been some frauds commited by the companies in Indonesia. At the end of 2019, the mass media was enlivened by the news about PT. Asuransi Jiwasraya (Persero) which was reported by the Ministry of SOEs to the Attorney General's Office due to allegations or indications of fraud that caused Jiwasraya to experience liquidity problems resulting in delayed payment of customer claims (CNBCIndonesia, 2019). In mid-2019, the Indonesian people were shocked by the news that BPJS Health experienced a deficit. The news was reinforced by Iqbal Anas Ma'ruf, Head of BPJS Health Public Relations, who acknowledged that the fraud had contributed to the deficit in BPJS Health. However, the fraud was not the main cause in the health insurance program (Kontan, 2019a). Indications of fraud in the National Health Insurance (JKN) program have long been detected. The Corruption Eradication Commission (*Indonesia: Komisi Pemberanasan Korupsi / KPK)*

even detected that up to mid-June 2015, as many as 175,774 claims of advanced referral health facility (FKRTL) were suspected fraud. And until mid-2016, more than 1 million problematic claims were found (Kontan, 2019b). Fraud can be done by JKN participants, BPJS Health officials, health service providers, and providers of drugs and medical devices (Kontan, 2019b). One of the acts of fraud committed by BPJS Health officials is to withhold payments to health facilities or partners for the purpose of personal gain (Kontan, 2019b). There is a public perception stating that educated individuals certainly know that fraud is prohibited, but in fact this does not apply to the two examples of cases above.

The results of a survey conducted by ACFE-INDONESIA (2017) provide evidence that the phenomenon of the rise of fraud apparently has nothing to do with the level of education. In fact, most corruptors in Indonesia are bachelor and master graduates. In other words, bachelor, master, or doctoral graduates (ACFE-INDONESIA, 2017: 9) have the opportunity to become perpetrators of fraud. Then, ACFE-INDONESIA (2017: 43) raised a big question: "who" and "what" is wrong? Higher education in Indonesia has always been demanded to promote honesty, integrity, and so on so as to reduce the level of fraud, but the fact is actually reversed.

The case above was responded by the regulator by issuing regulation that must be obeyed by various agencies including government agencies, banks, and other commercial companies. The intended regulation is a whistleblowing system. National Committee on Governance Policy (KNKG, 2008: 2) confirms that the whistleblowing system is part of the internal control system in preventing the practice of irregularities and fraud as well as strengthening the application of good governance practices.

Some studies conclude that whistleblowing system is the most effective way to prevent or reduce fraud because the time required for action is shorter and involves the reputation of the organization so that the handling must begin from the internal (Erkmen, Özsözgün Çalışkan, and Esen, 2014; Francis, Armstrong, and Foxley , 2015; Karatuna and Başol, 2018; Pamungkas, Ghozali and Achmad, 2017; Peltier-Rivest, 2018; Said, Alam, Mohamed and Rafidi, 2017; Scott-Young, 2014).

The definition of whistleblowing is

clear. For example, KNKG (2008: 3) defines wrongdoing as acts that violate statutory regulations; relevant industry regulations/ standards and internal regulations of the organization, and can be reported. Besides that, whistleblowing is a disclosure of violations or a disclosure of other acts that can harm the organization and stakeholders.

The Enron and WorldCom financial scandals in the 2000s became a momentum of change for the implementation of whistleblowing. In the past, whistleblowing was done internally by employees, or externally by external parties such as information from the media (news) or government agencies (Lam and Harcourt, 2019). However, in line with current technological advances, whistleblowing through social media or other online sources has increased where the reporter's identity can be anonymous and the speed or ease of sharing information widely can be accompanied by photos or videos (Lam and Harcourt, 2019). However, the information submitted along with the photographic or video evidence needs to be investigated further to find out the truth because the ease of reporting allows the information submitted in the report to be inaccurate.

Technological advances in the current digital era have an impact on whistleblowing and fraud so that those who wish to convey or detect fraud have been facilitated. They no longer need to go through complicated processes or be reluctant to meet face to face because of a fear of reporting. Technology also facilitates many parties in fraud prevention, one of which is through artificial intelligence (AI) technology, which is artificial neural network (ANN) in the detection of fraudulent financial statements.

With technological advances, information related to whistleblowing systems and fraud can be easily known by many parties so that the principles of mutual reminding and mutual openness simultaneously and gradually encourage community participation and company employees to be more willing to act to prevent fraud and corruption by speaking up and reporting to the parties who can handle it. But how is the role of technology in whistleblowing and fraud in Indonesia today that will be examined by the author through a literature study?

This article was developed based on the research conducted by Lam and Harcourt (2019) which discussed virtual whistleblowing and its characteristics and implications, with references from the United States, Canada, the United Kingdom, and Australia. The authors believe that the information submitted along with the photographic or video evidence needs to be investigated further to find out the truth because the ease of reporting allows the information submitted in the report to be inaccurate. This article discusses whistleblowing and fraud in the current digital era in Indonesia in the form of a literature study. The contribution of this research is that there is still not much discussion about whistleblowing and fraud in the digital era in Indonesia so it is hoped that this paper can add to the literature on whistleblowing and fraud in the digital era.

2. THEORITICAL FRAMEWORK AND HYPOTHESIS

Financial Scandals and Regulations

In 2019, there was a polemic related to the 2018 financial statements published by PT Garuda Indonesia (GIA). The polemic began during the Annual General Meeting of Shareholders (AGM - 24 April 2019). Two GIA commissioners Chairul Tanjung and Dony Oskaria were reluctant to sign the 2018 financial statements because they felt there were irregularities stemming from the transaction in the Aviation Connectivity Services Delivery Cooperation Agreement between PT Mahata Aero Teknologi and Citilink Indonesia worth US $ 239.94 million or around IDR 2.98 trillion. This fund had been recognized as income even though in reality it was still in the form of receivables so the company actually suffered losses in the previous period but was recorded profits (Detik.com, 2019).

In the past, financial scandals, such as Enron (2001), WorldCom (2002), and Lehman Brothers (2008) cases, occurred due to fraud perpetrated by internal parties through fraudulent financial statements or corrupted company assets/ equity (Anindya and Adhariani, 2019). Long before that, in 1970s there was a fraud scandal that made the Securities and Exchange Commission (SEC) finally issued regulations with the aim to ensure fair, accountable and transparent business behavior.

A few years later or in the 1990s, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued an Enterprise Risk Management (ERM). Since then, ERM has been worldwide and it is recommended or even mandatory to apply to

both private and public companies to minimize or prevent risk. ERM becomes a strategy or effort to evaluate and manage the risks that exist in the agency in order to increase the value or profit of the agency.

Young (2016) provides an example of the Sarbanes Oxley Act (SOX Title III Section 301), and states that public companies should implement formal communication channels for employees to report problems related to accounting, internal control, and questionable audits. KNKG (2008: 17) adds that information regarding the existence of this channel and the procedures for its use must be widely disseminated to all employees. Young (2016) concludes the research conducted by Hooks, Kaplan, & Schultz (1994) and Ponemon (1994) that whistleblowers play an important role in the organization's internal control structure.

The National Committee on Governance Policy (KNKG 2008: 2) reaffirms that whistleblowing system is part of the internal control system in preventing the practice of irregularities and fraud as well as strengthening the application of good governance practices. Although the laws and regulations do not yet fully regulate the whistleblowing system, Indonesia has several laws and regulations that partially deal with reporting violations and reporter protections, among others (KNKG, 2008: 5):

a. Law No. 28 of 1999 concerning the Administration of the State that is Clean and Free from Corruption, Collusion and Nepotism article 9

b. Law No. 31 of 1999 concerning Eradication of Corruption Crime article 31 and article 41 paragraph (2) point e

c. Law No. 15 of 2002 in conjunction with Law No. 25 of 2003 concerning Money Laundering Acts articles 39 to 43

d. Law No.13 of 2003 concerning Labor article 153 paragraph (1) letter I and article 158 paragraph (1) letter i

e. Law No.7 of 2006 concerning the Ratification of the United Nations Convention Against Corruption (UNCAC), Section 33 of UNCAC

f. Law No.13 of 2006 concerning the Protection of Witnesses and Victims article 10 paragraph 1

g. Government Regulation No.71 of 2000 concerning Procedures for the Implementation of Community Participation and the Awarding of Corruption Prevention and Eradication article 6

h. Government Regulation No.57 of 2003 concerning Procedures for Special Protection for Reporters and Witnesses for Money Laundering

i. Police Chief Regulation Number 17 of 2005 concerning Special Protection Procedures for Reporters and Witnesses for Money Laundering.

The regulations regarding whistleblowing apply not only to public companies, but also to banks. Bank Indonesia requires banks to have and implement an anti-fraud strategy through the Bank Indonesia Circular Letter No.13/ 28/ DPNP dated 9 December 2011 concerning the Implementation of Anti-Fraud Strategy for Commercial Banks. This Circular covers the main provisions, in which in the application, the anti-fraud strategy consists of 4 pillars of the fraud control system: (1) prevention, (2) detection, (3) investigation, reporting, and sanctions (4) monitoring, evaluation, and follow-up. Bank Indonesia also firmly states that any violations of these provisions will be subject to administrative sanctions in accordance with Bank Indonesia Regulation No. 5/8/ PBI/ 2003 dated May 19, 2003 concerning the Application of Risk Management for Commercial Banks which was later amended in accordance with the provisions contained in Bank Indonesia Regulation No. 11/25/ PBI/ 2009 dated July 1, 2009.

Whistleblowing

The word whistleblowing comes from English Language. In the past, the police 'blew' or 'whistled' as hard as possible when there was a crime to warn the nearest police and the surrounding community (Bell, 2011). Whistleblowing is the practice of someone reporting inappropriate, unethical or illegal actions in an organization to those who can correct these actions (Bell, 2011).

The National Committee on Governance Policy (KNKG 2008: 6) outlines 3 aspects of the violation reporting system: (1) structural aspects which contain elements and infrastructure of the violation reporting system; (2) operational aspects related to the mechanism and working procedures of the violation reporting system; and (3) treatment aspects which ensure that the violation reporting system is sustainable and increases its effectiveness. Some people often think that witness is the same as reporter. But actually they are completely different. Witness is someone who sees, hears or experiences the

violation committed by the reported party and is willing to provide information before a court hearing; while reporter or whistleblower is a person who reports a violation but he / she may not see or hear the conduct of the violation himself but has evidence in the form of records, pictures, etc. that a violation has occurred (KNKG, 2008: 4).

Nurhidayat and Kusumasari (2018) argue that from the very beginning of its emergence, whistleblowing has been a behavior based on ethical issues. In other words, it is related to ethical behavior. Pamungkas et al. (2017) defines ethical behavior as the suitainability of one's behavior/ actions, generally complied with correct and good norms so that dignity and respect increase. According to Nurhidayat and Kusumasari (2018), the ethical values that underlie whistleblowing are the values of integrity, transparency, public interests protection, and rejection of any deviations from the rules of conduct and code of ethics. Furthermore, whistleblowing which is an ethical dilemma can be described as to the following: where an individual is faced with two options, that is, maintaining the integrity of an individual and being a member of an organization whose loyalty is demanded to protect the wider public interest.

According to Merchant and White (2017), ethics is closely related to management control system (MCS). By linking these two things, the organization can establish a framework that promotes good behavior to contribute to the achievement of organizational goals in addition to being able to to follow the principles of organizational ethics . The MCS is created with the aim of ensuring that employees do the best for the interests of the organization, in which the employees apply the business strategy as intended by the organization (Merchant and White, 2017).

According to Lam and Harcourt (2019), in order to prevent whistleblowing by employees, the company should have a culture of ethics, accountability, and transparency so that employees are not shrouded in fear to report or criticize. In order for the whistleblowing system to work effectively, tones and ethical behavior must "seep" from above, down through the middle, under the organization and back again (Scott-Young, 2014), as illustrated in Figure 2 in next page.

Scott and Young (2014), propose structural elements that are important in creating a healthy and safe ethical ecosystem that builds and maintains trust and openness in organizations:
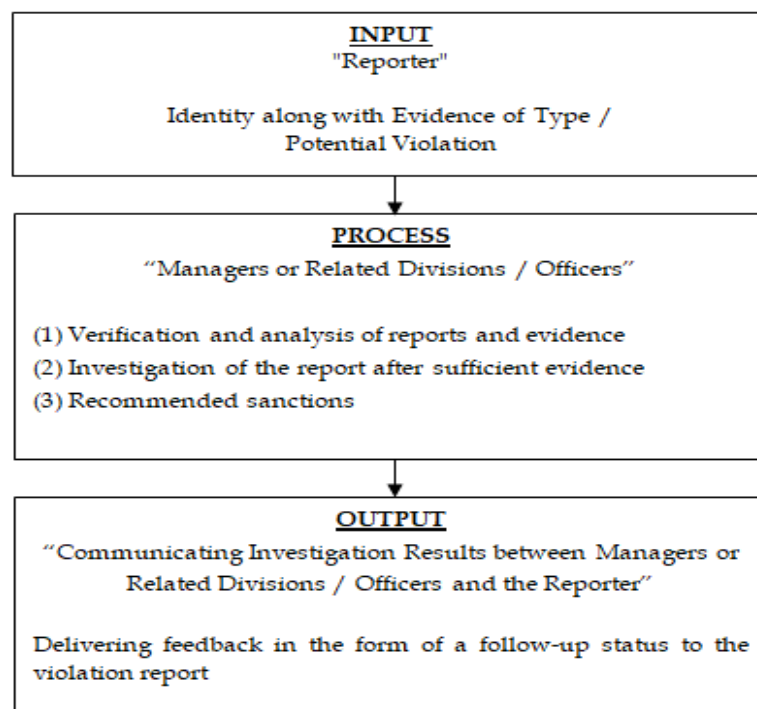

Figure 1
Whistleblowing System Flow

Source: Processed by Researchers (2019)

a. Creating a code of conduct
b. Providing training for code of ethics awareness
c. Providing training to reframe attitudes towards whistleblowers
d. Creating a mechanism for getting advice / support
e. Providing management training in listening and responding skills
f. Providing training for moral courage and voice values
g. Providing several reporting channels, including anonymous hotlines
h. Establishing protocols for investigative and corrective actions
i. Giving feedback about actions to reporters and organizations
j. Appreciating the courage to speak; listen to management awards and actions
k. Speaking and enabling voices in KPIs for performance appraisal
l. Quarterly reporting of employee votes and actions produced.

There are two things that are highlighted related to the whistleblowing: (1) a healthy and good environment, where whistleblowers are protected from acts of retaliation by organizations and perpetrators, can encourage the spirit to blow the whistle, and (2) ethical education in accounting programs need to be developed so that ethical reasoning for Accounting graduates can grow (Liyanarachchi and Newdick 2009).

According to Nurhidayat and Kusumasari (2018), based on their research conducted in Indonesia, developing a more effective and systematic whistleblowing system is deemed necessary and urgent to develop good governance and create integrity in all public institutions in Indonesia. In addition, the whistleblowing system must also provide more guarantees of protection by considering and including key elements categorized into several aspects that include human culture and ethics, policy, legal protection, and organizational structure as with processes and structures that are aligned with special/ appropriate characters in Indonesia. This opinion is supported by Erwin and Ramsay (2015) that whistleblower must be protected by regulations that guarantee fair treatment and continuity of work as a consequence of whistleblowing in the public interest.

Research conducted by Nawawi and Salin (2018) implies that some employees still do not believe in the whistleblowing mechanism even though the existing mechanism is correct. Nawawi and Salin (2018) argue that this indicates the need for continuous guarantees for staff regarding the confidentiality of their reports without feeling afraid to submit the report. Clear and specific rights of the whistleblower must be explained in the employment contract so that the company does not abuse the power to take revenge on the whistleblower by unfair dismissal and
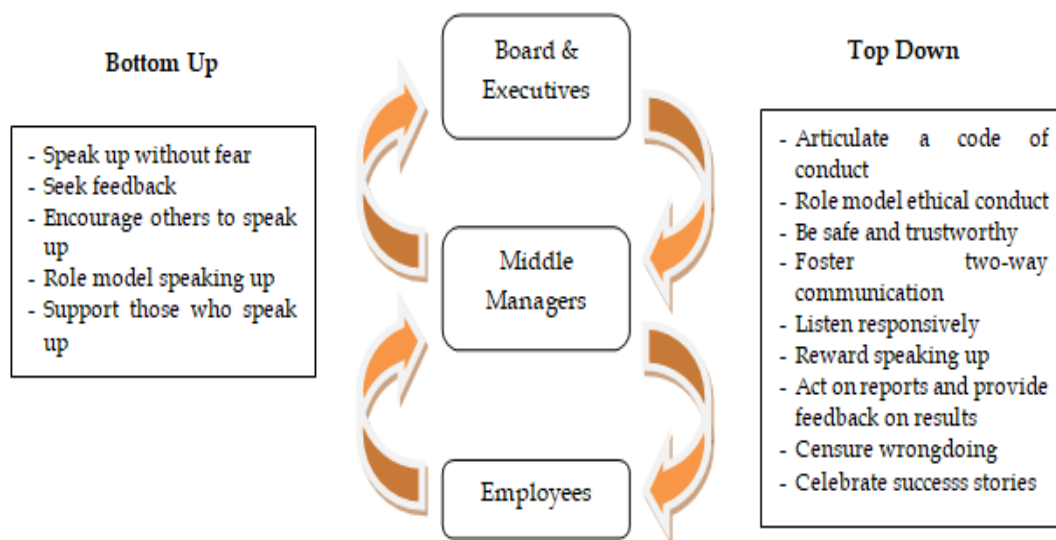

Figure 2
Building Ethical Ecosystems

Source: Scott-Young (2014)

good business culture by recognizing and appreciating the whistleblower's actions as good deeds and needs to be improved (Nawawi and Salin, 2018).

On one hand, Yeoh (2014) argues that whistleblowers are influenced by someone's extraordinary personal, social, and economic factors. On the other hand, they may be motivated by the desire to do things right or because of altruistic concerns, the need to avoid personal responsibility. In some cases in the United States, they are more motivated by inducements for financial rewards.

There are strong factors that can encourage and prevent employees from conducting whistleblowing (disclosure). Social justice, professional ethics, morals, and regulations that provide guidance and protect whistleblowers are the factors that encourage employees to do whistleblowing. In addition, the factors that inhibit employees to do whistleblowing include the legal system and internal control of the company, media coverage, and the fear of retaliation by the company or perpetrators (Erwin and Ramsay, 2015).

Scott and Young (2014) provide a new paradigm in whistleblowing, as seen in Figure 3 above. It can be done by reframing the speak-up in a more positive way, the term that further emphasizes 'employee voice' that can be used to replace the term 'internal complaints or internal whistleblowing'.

Whistleblowers can report without including credible evidence. In this way, whistleblowers can keep their identity confidential or report as anonymous in order to avoid retaliation from the organization or perpetrators but having risk of losing their effectiveness for three reasons (Near and Miceli, 1995): (1) members of the organization can ignore the concerns of whistleblowers who are not willing to face their target of allegations (unscrupulous perpetrators), (2) if the whistleblowers do not provide sufficient evidence of error, the recipient of the complaint cannot obtain additional information from them, and (3) if the whistleblowers are seen as credible complainants because of their characteristics, the anonymous status will reduce their credibility even though it can increase or does not affect the effectiveness of those who have lower credibility characteristics. Furthermore, Near and Miceli (1995) propose five main factors that influence termination of wrongdoing: (a) whistleblower characteristics, (b) complaint recipient characteristics, (c) wrongdoer characteristics, (d) wrongdoing characteristics, and (e) organizational characteristics. These five factors affect individual variables (regarding whistleblowers, complaint recipients, and wrongdoers) and situational variables (regarding organization and wrongdoing) (Near and Miceli, 1995).

Fraud
A correct definition about fraud needs to be discussed as well. Albrecht (2009: 6) defines fraud in a general term and includes all the ways human ingenuity that can be designed and forced by individuals in order to get benefit from others by using false information. Pamungkas et al. (2017) argues that there are no definite and volatile rules that can be defined as general propositions in defining fraud because it includes surprises, fraud, cunning, and other unfair ways committed by fraudsters. Furthermore, Pamungkas et al. (2017) adds that the only limitation that can define it is the boundary that limits human dishonesty.

The Association of Certified Fraud Examiners (ACFE), in Tuanakotta (2014: 195 - 204), divides fraud into 3 (three) types according

Old Paradigm : Whistleblowing	New Paradigm : Pro-Social Voice
Informer; disgruntled traitor	Loyal corporate citizen
Risk creator	Risk identifier
Negative threat	Positive opportunity
Source of problem	Stimulus to solution
External protection required	Internal protection provided
Silence the voice	Listen
Ignore	Respond; act; feedback
'Shoot the messenger'; punish	Encourage; reward

Figure 3
Reframing Internal Whistleblowing as a Pro-Social Employee Voice
Source: Scott-Young (2014)

to the actions taken by the perpetrators: financial statement fraud, misuse of assets, and corruption. Merchant and White (2017) explain that there are three most common reasons, called the fraud triangle, why someone commits fraud or behaves unethically: (1) the existence of an opportunity to commit fraud, for example because of ineffective internal control system, (2) rationalization, for example "I did not get the bonus that I should get", (3) the existence of motivation due to pressure from outside (such as debt / greed) and internal pressure (such as workload).

However, Wolfe and Hermanson (2004), in Free (2015), state that the fraud triangle has now been replaced by the fraud diamond as described in figure 4). Wolfe and Hermanson (2004) describe considerations in the context of "capability" such as position, intellectual capacity, confidence, resilience to stress and guilt, and the ability to coerce and persuade others.

The case of sexual harassment that hit PT. Garuda Indonesia (GIA) originated from the tweet of Twitter users who revealed the case of sexual harassment committed by officials at the airline. As reported by Bisnis.com (2019), flight attendants who opposed acts of sexual harassment would get sanctions in the form of route changes (unpleasant) or one-sided dismissal. If the allegation turns out to be true, it means that the perpetrator has committed fraud by abusing his position. The authors believe that the information submitted along with the photographic or video evidence needs to be investigated further to find out the truth because the ease of reporting allows the information submitted in the report to be inaccurate. In this paper, the authors discuss financial statement fraud using artificial intelligence (AI) technology.

3. RESEARCH METHOD

This paper discusses whistleblowing and fraud in the current digital era in Indonesia in the form of a literature study. Observation of the phenomenon of fraud cases that recently hit SOEs in Indonesia becomes the idea of this paper. It is then increasingly deepened and by reading the media (online, either website or social media). The next step is to look for references such as journals, books, and news in electronic media related to this paper.

4. DATA ANALYSIS AND DISCUSSION
Digital Whistleblowing

There is a shift of doing the disclosure in the past and in the current condition. In the past, disclosure or whistleblowing was
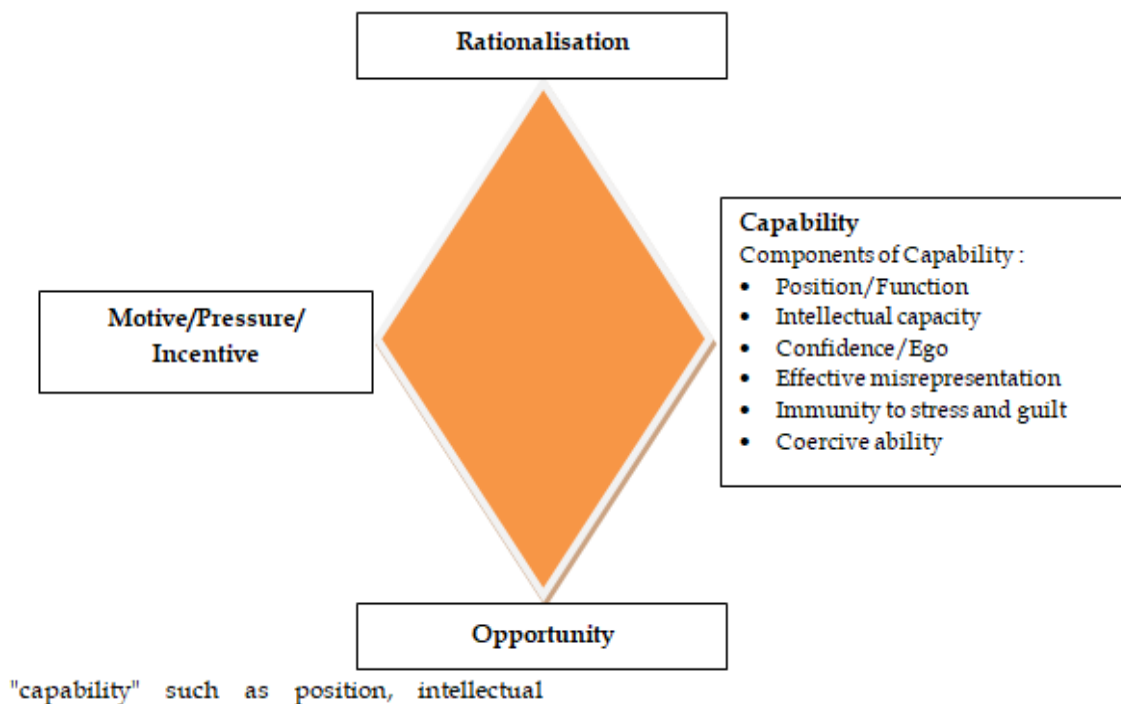

Figure 4
Diamond Fraud

Sources: Wolfe and Hermanson (2004) in Free (2015)

done internally by employees or externally by information from the media (news) or government agencies specifically handling whistleblowing (Lam and Harcourt, 2019). Current technological advances make whistleblowing easy to do such as through social media or other online sources. The reporter's identity can be anonymous and the information shared widely can also be accompanied by photos or videos (Lam & Harcourt, 2019). The definition of whistleblowing through internal organizations, according to Lam and Harcourt (2019), is too restrictive or inappropriate in the current digital era, because accessibility of information is not always limited to internal organizations. The discussion in this article highlights digital whistleblowing as whistleblowing through social media or other online sources.

There are two kinds of delivering information about whistleblowing in the past and nowadays. In the past, traditional whistleblowing is delivered in printed form or electronic media through newspaper, television or radio. Conventional investigative journalists at that time faced various difficulties, such as restrictions by media owners in investigating and reporting, because media owners were afraid of being abandoned by big advertisers (large nominal advertisements) as well as threats of lawsuits from organizations accused of wrongdoing (Lam and Harcourt, 2019). Nowadays in the digital age, the internet has become commonplace and social media is easily accessible with low cost, thus making whistleblowing in this way preferred (Lam and Harcourt, 2019).

Disclosure by WikiLeaks in 2010 and Snowden in 2013 had a big impact on journalistic aspect, decision-maker, and public (Brevini, 2017). According to Dreyfus, Lederman, and Bosua (2011), WikiLeaks gives four changes to the media: (1) challenging traditional media, which so far have only been sleepwalking, to be more courageous and want to ask more difficult questions, (2) revolutionizing traditional media especially newspapers by collaborating in new and creative ways, (3) illustrating how sophisticated analysis of large data sets to reveal the bigger picture through a series of stages starting with collecting, filtering, to visualizing data derived from large data sets based on statistical methods of data analysis, (4) WikiLeaks has started a new era of media into digital or online media which gives birth to a new type of media, that is, leaks

publishers (publishers who leak confidential/ limited matters). WikiLeaks disclosure is a sign that whistleblowing is entering a new era with the help of media and technology in the digital age.

In Indonesia, at the end of 2019 PT Garuda Indonesia (GIA) was once again in the spotlight due to smuggling of luxury goods which led to the opening of cases of sexual harassment after GIA had previously received widespread attention from the polemic of the 2018 Financial Report case. It was Twitter user @digeeembok (identity unknown), on December 3, 2019, who initially responded to the news about the smuggling of a large motorbike which dragged four GIA directors (Bisnis.com, 2019). The next day, this account began to dismantle one by one GIA high-ranking crimes ranging from sexual harassment, unilateral dismissal of employees, to corruption at the airline company accompanied by evidence in the form of screenshot photos (Bisnis.com, 2019). The author believes that the information submitted along with the photographic or video evidence needs to be investigated further to find out the truth, because the ease of reporting allows the information submitted in the report to be inaccurate.

Brevini (2017) argues that disclosure done by WikiLeaks is made possible due to the available infrastructure of social media sites and cloud technology, a mechanism that is useful for movements to grow and define the relationship between these two aspects with their observers but it is also an important technical asset such as when WikiLeaks utilized the cloud as an encrypted platform provider for disclosure and extracting information that might otherwise remain hidden. The phenomenon of disclosure or whistleblowing is still under debate between online privacy and transparency (Brevini, 2017). Lam and Harcourt (2019) explain things that can affect the decision of online whistleblowers to report or not and the results of the report in an online whistleblowing model that summarizes the antecedents and whistleblowing results in Figure 5.

According to Bell (2011), modern digital fingerprinting technology makes it possible to track user (human) identification associated with certain copies of leaked digital files. Bell (2011) defines digital fingerprinting today, referring to modern technology, as digitally marking documents and data that can be uniquely identified and associated with

individuals. Fingerprinting technology has been developed for media that has copyright so that in the future if there are people who share access illegally, they can be identified (Bell, 2011).

Bell (2011), proposes three methods that can be used by whistleblower working in a restricted organizational environment to detect changes in digital documents or softcopy files:
a. Method 1 - Comparing file sizes. This

method is easy but can sometimes detect formal techniques and ad hoc fingerprinting.
b. Method 2 - Comparing the size of zipped files. This method is a bit more complicated but far more effective and uses file compression directly to allow file comparisons.
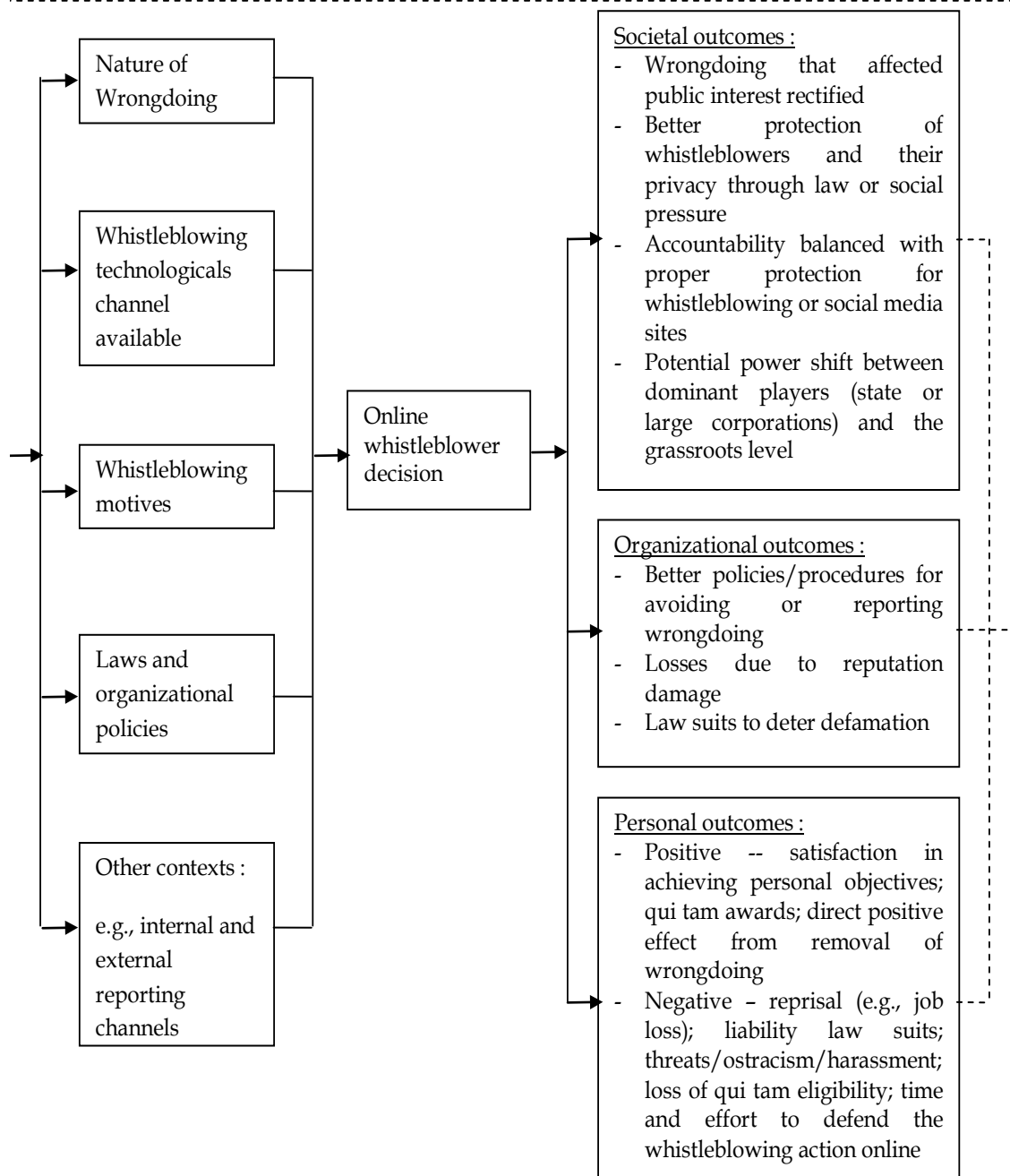c. Method 3 - Comparing the previous text and the size of zipped files. This method

```
┌────────────────────┐                    ┌─────────────────────────────────┐
│ Nature of          │                    │ Societal outcomes :             │
│ Wrongdoing         │                    │ - Wrongdoing that affected      │
└────────────────────┘                    │   public interest rectified     │
                                          │ - Better protection of          │
┌────────────────────┐                    │   whistleblowers and their      │
│ Whistleblowing     │                    │   privacy through law or social │
│ technologicals     │                    │   pressure                      │
│ channel available  │                    │ - Accountability balanced with  │
└────────────────────┘                    │   proper protection for         │
                     ┌──────────────┐     │   whistleblowing or social media│
┌────────────────────┐│ Online       │    │   sites                         │
│ Whistleblowing     ││ whistleblower│    │ - Potential power shift between │
│ motives            ││ decision     │    │   dominant players (state or    │
└────────────────────┘└──────────────┘    │   large corporations) and the   │
                                          │   grassroots level              │
┌────────────────────┐                    └─────────────────────────────────┘
│ Laws and           │                    ┌─────────────────────────────────┐
│ organizational     │                    │ Organizational outcomes :       │
│ policies           │                    │ - Better policies/procedures for│
└────────────────────┘                    │   avoiding or reporting         │
                                          │   wrongdoing                    │
┌────────────────────┐                    │ - Losses due to reputation      │
│ Other contexts :   │                    │   damage                        │
│                    │                    │ - Law suits to deter defamation │
│ e.g., internal and │                    └─────────────────────────────────┘
│ external reporting │                    ┌─────────────────────────────────┐
│ channels           │                    │ Personal outcomes :             │
└────────────────────┘                    │ - Positive -- satisfaction in   │
                                          │   achieving personal objectives;│
                                          │   qui tam awards; direct positive│
                                          │   effect from removal of        │
                                          │   wrongdoing                    │
                                          │ - Negative – reprisal (e.g., job│
                                          │   loss); liability law suits;   │
                                          │   threats/ostracism/harassment; │
                                          │   loss of qui tam eligibility; time│
                                          │   and effort to defend the      │
                                          │   whistleblowing action online  │
                                          └─────────────────────────────────┘
```

Figure 5
Online Whistleblowing Model

Source: Lam and Harcourt (2019)

is the most complicated because it involves actions that might be considered unusual in some workplaces thereby reducing reasonable denial and attracting attention to whistleblowers.

Heumann et al. (2013) in Lam and Harcourt (2019) classifies whistleblowers based on the aims and motives into five categories: (1) 'altruists' means to make disclosures to obtain justice because this figure has high ethical standards, (2) 'avengers' means to retaliate for injustice obtained from the organization against whistleblowers or other victims, (3) 'alarmists' means to emphasize the consequences of the organization's actions which they disclose even without substantive evidence, (4) 'bounty hunters' means to make disclosure to obtain rewards, (5) organization men (or persons) are career loyalists who want to put pressure to drive change for the better so that they can improve the organization where they have given most of their lives to serve (for example in the military and religion).

In digital whistleblowing, Lam and Harcourt (2019) divide whistleblowers into four types: (1) spontaneous actors make spontaneous disclosures after observing unexpected errors and are deemed appropriate for disclosing information either photos or videos online just to produce interaction and entertainment because they do not understand their actions as whistleblowing, (2) reserved complainers make disclosure of organizational mistakes online only to trusted people due to emotional outlet (angry / frustrated / looking for sympathy) or get advice in which the information is then taken and spread more widely by third parties, (3) attention seekers make disclosures through social media based on naive motives because they want to get attention or recognition in a hope of becoming a celebrity (social climber) or getting praise as a hero, and (4) covetous competitors are companies that do seek commercial profit from false information that is revealed either real or imaginative by competing companies so that information in the form of malicious issues can be spread anonymously and without strong evidence.

According to Francis et al. (2015), there are two directions that should be done before conducting whistleblowing: presenting self-questions and taking practical actions.

Self-questions
Ask yourself this question:

a. Is this the most appropriate response?
b. Is it serious enough to guarantee this report?
c. Are there better ways to reduce this type of corruption?

Reconfirm your facts and make sure that the lawsuit does not have bad motivation.

Practical actions
Some practical pre-actions that can be taken are as follows:
a. Consult with family for support
b. Consult with a lawyer (for privileged communication)
c. Copy all documents before whistleblowing
d. Get an oath before doing whistleblowing so that the supporters do not withdraw their statement
e. Ensuring that you can survive financially if the worst possibility happens, that is, to lose a job at the company
f. Be aware of your career costs (the cost of losing income if the worst possibility happens, that is, to lose your job).

Francis et al. (2015) proposes the application of reward and punishment for those in the work environment, by not making rewards or awards to reporters as the main motive but rather to be a benefit. The link between incentive and corruption systems is explained in research conducted by Teichmann, Sergi, Teichmann, and Sergi (2018) as follows:
a. Conventional incentive system can encourage corruption in multinational companies. Employees are rewarded for their productivity only, not for compliance. So the employees often bribe public officials to increase sales in order to get bonuses. The company considers that the employee's compliant behavior in the company is normal or as it should be. Therefore, compliant behavior does not guarantee to get additional payment.
b. Incentive system can help prevent corruption. Incentive systems can help align interests between agents and principals by rewarding both productivity and adherence to anti-bribery rules.
c. Incentive system should be adjusted to ensure compliance with more effective formal anti-bribery rules through a performance matrix that measures compliance and productivity. Employees are given bonuses not only for productivity, but also for compliance and are subject to malus due to non-compliance.

d. The incentive system through the provision of bonuses from the percentage of the amount of fines that should be imposed on the company can foster anti-bribery to the company. For example, because of reports from employees, the company is protected from fines and investigations of a certain nominal value. Therefore, the company can provide these employees with a certain percentage or nominal determined by the company. It is recommended that the criteria for awarding bonuses in such cases be determined in advance with the nominal terms and amounts.

e. The biggest challenge faced when introducing anti-bribery incentives is appropriate measurement of performance.

According to Eichmann et al. (2018), alternative tools are needed to combat bribery. In addition, there should be additional bonus for traditional productivity. Multinational companies should introduce a bonus-malus system, that is, a bonus for compliance and malus for non-compliance.

According to Erwin and Ramsay (2015), an open-door policy from management is needed to get feedback from employees. The open-door policy is a good policy for several reasons: (1) allowing employees to express unusual activities / actions that can lead to fraudulent activities / actions, (2) fostering trust and mutual respect so that employees feel that their opinions are heard and encourage them to blow the whistle in the future.

Dilemmas always arise with internal whistleblowers, especially employees. They want to do whistleblowing but are constrained by the company's code of confidentiality which requires the confidentiality of confidential or sensitive organization information (Lam and Harcourt, 2019). Therefore, companies should provide a place to express their employees' conscience to avoid whistleblowing. With technology, whistleblowing is easy to do, but it is worth watching out whether the identity of the whistleblower and witnesses can be safe. Management or audit committee is responsible for the development and implementation of internal disclosure regulations (KNKG, 2008: 11).

Artificial Neural Network for Detecting Fraud
According to Omar, Nawawi, and Puteh Salin (2016), the most popular type of fraud is the misuse of assets, including cash and inventory theft, which mostly comes from the operations

and sales departments. The majority of fraudsters in the case study are men, new employees, and young adults who are motivated because of a lack of understanding of fraud behavior, opportunities to commit fraud, lifestyle, and financial pressures. Robinson, Robertson, and Curtis (2012) investigate the effect of the characteristics of fraud itself and the organizational context on the intention of employees to do whistleblowing. The results are consistent with the hypothesis that employees tend to report: (1) financial statement fraud rather than theft; (2) immaterial fraud rather than material fraud; (3) when the perpetrators realize that the employee has knowledge about fraud; and (4) when other people are not aware of fraud rather than when others know or are aware of fraud

In the research conducted by Karatuna and Başol (2018), "The Association of Certified Fraud Examiners' (ACFE) 2014 Report to the Nations on Occupational Fraud and Abuse" states that employee whistleblowing is the most important source of information to reveal the existence of potential fraud in the organization.

A survey conducted by the Association of Certified Fraud Examiners (ACFE) Indonesia, in collaboration with the White Collar Crime Research and Prevention Center (P3K2P), shows that corruption is the most common fraud case in Indonesia (ACFE-INDONESIA, 2017). Based on the survey, the biggest type of fraud in Indonesia is corruption, or 67%, followed by misuse of assets 31%, and financial statement fraud 2%.

In the last four decades, artificial intelligence (AI) has created major changes through a more modern approach that involves the development of computers with architectural and processing capabilities making it possible to mimic human thought/brain and thought processes (Chatterjee, Ayadi, & Boone, 2000). The process produces knowledge representation based on massive processing power, rapid decision making based on large amounts of data, and the ability to recognize patterns based on experience called neural computing or artificial neural networks. In other words, this AI technology is called Artificial Neural Network (ANN) (Chatterjee et al., 2000).

Cerullo and Cerullo (1999) explain that the concept of a neural network consists of many processing elements that work together to form a network that makes it possible to process multiple operations simultaneously so that the
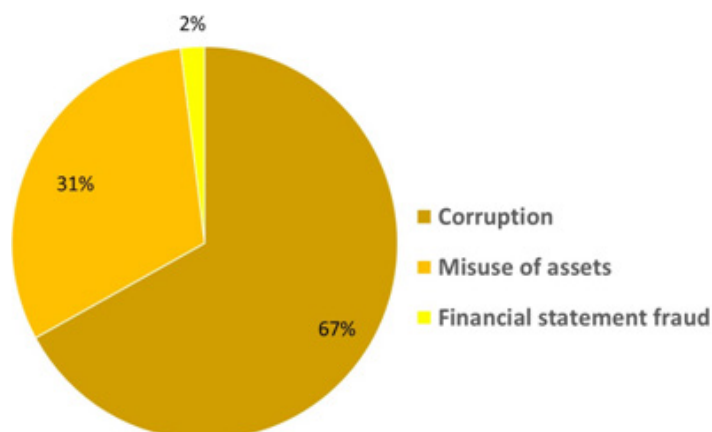
Figure 6
Most Fraud in Indonesia

Source: ACFE-INDONESIA (2017)

operations can be carried out faster than the traditional methods that process one operation at one time. Neural networks solve problems through the recognition of patterns in data that are very complex for humans or even with other computer methods because basically neural networks use a database of historical examples of input and output values to create a mathematical model so that the patterns can be recognized (Cerullo and Cerullo, 1999).

Cerullo and Cerullo (1999) provide reasons why neural networks are more suitable to be applied than expert systems, among others are:
a. Requires complex pattern recognition
b. Large decision domain size
c. Unstructured application
d. The problem situation is difficult to reduce to an if-then rule
e. To solve the problems need intuition
f. Requires a large number of variables to detect patterns or correlations.

The advantage of ANN is that the statistical training required is less formal than logistic regression and is able to detect complex non-linear relationships indirectly between dependent variable and independent variables (Omar et al., 2017). For example, ANN is able to process large amounts of data in a short time although the predicted results from ANN cannot be explained or interpreted properly which makes this a big problem for ANN (Koskivaara, 2004; Omar et al., 2017). In the research conducted by Omar et al. (2017), based on previous literature, however, ANN can be used to (1) detect and predict financial statement fraud; (2) detect and predict financial distress; (3) detect and predict fraud

cases; (4) forecast credit risk management; and (5) predict stock market prices. N. Omar et al. (2017) provides an illustration of the process for establishing a fraud prediction model in financial statements using ANN (Figure 7).

Omar et al. (2017) explains that the ANN structure consists of three main layers: input layer, hidden layer, and output layer. The following techniques can be used to detect and predict fraud on financial statements, namely logistic regression, decision tree, ratio analysis, support vector machines (SVM), Benford's Law, Altman Z-Score, and Beneish Model which later will become the input layer in the ANN model (Omar et al., 2017).

Cerullo and Cerullo (1999) describe some specific accounting applications that are appropriate using neural network software, where most of the problems can be categorized into prediction, classification, and pattern recognition as follows:
a. Fraud detection on credit cards
b. Fraud detection on employees
c. Fraud management
d. Detection of weaknesses in the internal control structure
e. Interpretation of audit evidence
f. Interpretation of audit quality
g. Interpretation of employee evaluations
h. Bankruptcy prediction
i. Risk prediction
j. Inventory estimation
k. Product costs estimation
l. Sales estimation
m. Budget estimation
n. Earnings estimation
o. Earnings per share (EPS) prediction

p. Employee performance prediction
q. Loan risk prediction
r. Stock price prediction
s. Give advice on merger decisions
t. Give advice on personal financial planning.

ANN is not only used in the accounting sector, but also in auditing sector. Based on previous literature, according to Koskivaara (2004), ANN can be applied in are seven areas of auditing sector, such as material errors, management fraud, support for going concern decisions, internal control, risk assessment, audit fees, and financial distress problems.

Like the use of AI technology in the detection of fraud in the accounting and auditing sector through the ANN system, although the ANN system provides many conveniences for auditors through a promising alternative approach to the AR (analytical review) procedure, the system is still unable to replace professional judgment. This is caused by the prediction results from ANN that cannot be explained or interpreted properly, making this a big problem for ANN (Koskivaara, 2004; N. Omar et al., 2017).

5. CONCLUSION, IMPLICATION, SUGGESTION AND LIMITATION

Current technological advances allow whistleblowing through social media or other online sources to increase because the reporter's identity can be anonymous and the speed or ease of sharing information widely can be accompanied by photos or videos (Lam
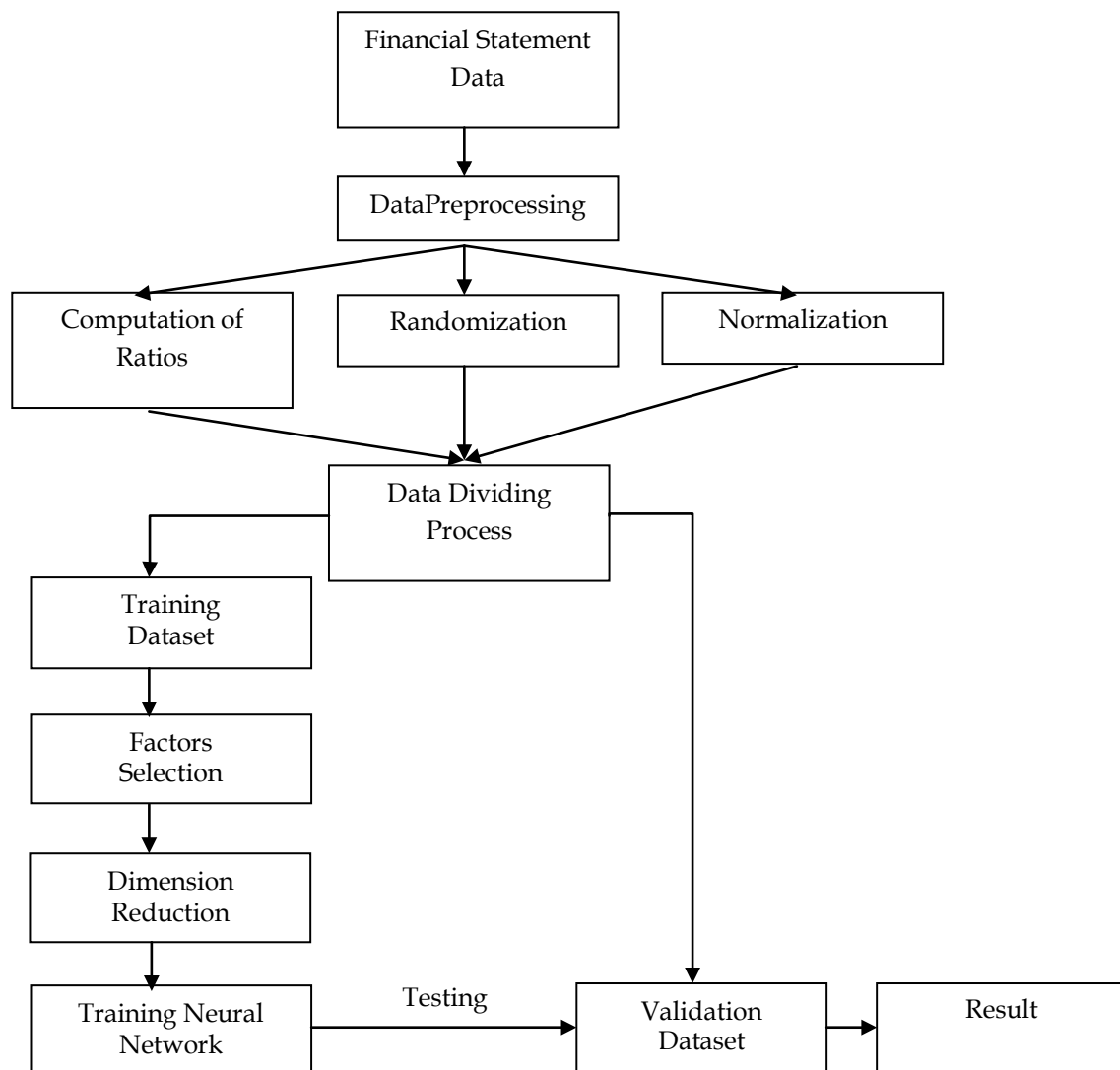

Figure 7
Process for Establishing Prediction Model of Financial Statement Fraud

Sources: Omar, Johari, and Smith (2017)

and Harcourt, 2019). However, the information submitted along with the photographic or video evidence needs to be investigated further to find out the truth, because the ease of reporting allows the information submitted in the report to be inaccurate. Inaccuracy of information through digital whistleblowing may occur because there is no process to check and confirm the truth of information. In addition, digital whistleblowing allows someone to disclose as much information as possible because there is no stipulation of the maximum amount of information distributed to social media.

Social media is now widely used by companies to interact with customers and prospective customers. It often happens that the customer initially only gives a complaint through the company's social media, but in the end it is used as whistleblowing by external parties. Open complaints on social media, which can spread quickly, should be handled by the company well so that the company's image can be maintained. Even though the company has handled complaints well, customers are not necessarily satisfied with the company's solutions/ apologies that can eventually trigger negative comments. Besides, there is also possibility that the comments are not true (false/ hoax) so as to tarnish the good name of the company. Therefore, legal advisor needs to be prepared by the company.

Companies should have a culture of ethics, accountability, and good transparency to prevent whistleblowing by employees (Lam and Harcourt, 2019). Whistleblowing is closely related to one's moral or ethical actions. This proves that the morale of an employee is very important starting from the selection process to training and ethics programs. Merchant and White (2017) explain the importance of the process of selection and training of personnel needed to align individual differences in the tendency to behave ethically, the importance of communication links between superiors and their subordinates, and the importance of ethical behavior which is higher than the achievement of goals. Clark (2003) in Merchant and White (2017) asserts that corporate ethics programs (CEP) positively influence employee initiatives and willingness to report any violations. Whistleblowers require commitment from management starting from the lowest management to the highest management because it is related to whistleblower protection rules that include a guarantee of security, fairness, and continuity of work in the organization. The new whistleblowing paradigm makes reporters dare to speak up about wrong doing in the organization because they feel that they are contributing to make the organization better and their reports are responded to and then given feedback so that solutions can be sought together and the organizations protect their speak-up actions.

An effective whistleblowing system requires the right system/ management and procedures so that the reporters and the witnesses feel safe and their safety is guaranteed, such as their property, lives and family, as stipulated in Law No. 13 of 2006 concerning Protection of Witnesses and Victims Article 10 paragraph 1. It is not only the system / management and procedures, but the environment must also participates in the creation of an effective whistleblowing system. Whistleblowing system requires the participation of various parties in order to be effective in preventing or minimizing fraud because the time required for enforcement is shorter and this involves the reputation of the organization, so the handling should be from the internal first. Information technology is used in running a whistleblowing system and detecting fraud. The case that happened to one of the SOEs in Indonesia started from tweeting on a Twitter account to the allegations of fraud in the form of abuse of position. This an example of the role of technology in digital whistleblowing and fraud.

Artificial Neural Network (ANN) provides major changes that make it possible to process large amounts of data to produce fast decision making in its ability to recognize patterns (from prior experience). ANN is useful for detecting fraud in financial statements. ANN provides convenience in terms of detection, interpretation, estimation, and prediction. This paper is expected to enrich insights related to the use of information technology in the field of whistleblowing and fraud in the digital age.

REFERENCES

Albrecht, W. Steve. 2009. Fraud Examination, Fourth Edition. Ohio: Cengage Learning.

ACFE-INDONESIA, (2017). Survai Fraud Indonesia 2016 (Vol. Agustus 2017). Jakarta: ACFE (Association Certified of Fraud Examiners) Indonesia Chapter.

Anindya, J. R., & Adhariani, D. (2019). Fraud Risk Factors and Tendency to Commit Fraud : Analysis of Employees' Perceptions. International Journal of Ethics and Systems. doi:https://doi.org/10.1108/IJOES-03-2019-0057

Bell, G. B. (2011). Digital Whistleblowing in Restricted Environments. Journal of digital information, 12(3), 1-14.

Bisnis.com. (2019). 'Akun Twitter @ digeeembok Beberkan Pelecehan Seksual Pramugari Garuda Indonesia'. Retrieved from https://kabar24.bisnis.com/read/20191212/16/1180608/akun-twitter-digeeembok-beberkan-pelecehan-seksual-pramugari-garuda-indonesia, access, 25 January 2020

Brevini, B. (2017). WikiLeaks : Between Disclosure and Whistle-blowing in Digital Times. Sociology Compass, 11(3), 1-11.

Cerullo, M. J., & Cerullo, V. (1999). Using Neural Networks to Predict Financial Reporting Fraud : Part 1. Computer Fraud & Security, 1999(5), 14-17.

CNBCIndonesia, (2019). 'BUMN Lapor Dugaan Fraud & Kecurangan Jiwasraya ke Kejagung!'. Retrieved from https://www.cnbcindonesia.com/market/20191115093006-17-115442/bumn-lapor-dugaan-fraud-kecurangan-jiwasraya-ke-kejagung access, 25 January 2020

Chatterjee, A., Ayadi, O. F., & Boone, B. E. (2000). Artificial Neural Network and the Financial Markets : A Survey. Managerial Finance, 26(12), 32-45.

Detik.com. (2019). 'Kisruh Garuda : Laporan Keuangan Cacat, Direksi Didenda Rp 100 Juta'. Retrieved from https://finance.detik.com/bursa-dan-valas/d-4604799/kisruh-garuda-laporan-keuangan-cacat-direksi-didenda-rp-100-juta/1. access, 25 January 2020Dreyfus, S., Lederman, R., & Bosua, R. (2011). Can We Handle the Truth? Whistleblowing to the Media in the Digital Era. Global Media Journal-Australian Edition, 5(1), 1-6.

Erkmen, T., Özsözgün Çalışkan, A., & Esen, E. (2014). An Empirical Research about Whistleblowing Behavior in Accounting Context. Journal of Accounting & Organizational Change, 10(2), 229-243. doi:10.1108/JAOC-03-2012-0028

Erwin, J., & Ramsay, B. (2015). Whistleblowing Environment in Indonesian Financial Institutions. International Journal of Business and Social Research, 5(11), 28-35.

Francis, R., Armstrong, A., & Foxley, I. (2015). Whistleblowing : A Three Part View. Journal of Financial Crime, 22(2), 208-218. doi:10.1108/JFC-03-2014-0011

Free, C. (2015). Looking Through the Fraud Triangle : A Review and Call for New Directions. Meditari Accountancy Research, 23(2), 175-196. doi:10.1108/MEDAR-02-2015-0009

Karatuna, I., & Başol, O. (2018). To Blow the Whistle or Not: The Roles of Perceived Organizational Retaliation and Upward Communication Satisfaction in Employee Responses to Observed Wrongdoing Redefining Corporate Social Responsibility (pp. 217-233): Emerald Publishing Limited.

Kontan. (2019a). 'BPJS Kesehatan : Fraud Bukan Penyebab Utama Defisit'. Retrieved from https://nasional.kontan.co.id/news/bpjs-kesehatan-fraud-bukan-penyebab-utama-defisit?page=3. access, 25 January 2020

Kontan. (2019b). 'Catat, Ini Daftar Tindakan Kecurangan alias Fraud dalam Pelaksanaan Program JKN'. Retrieved from https://nasional.kontan.co.id/news/catat-ini-daftar-tindakan-kecurangan-alias-fraud-dalam-pelaksanaan-program-jkn?page=all. access 25 January 2020

Koskivaara, E. (2004). Artificial Neural Networks in Analytical Review Procedures. Managerial Auditing Journal, 19(2), 191-223.

Krambia-Kapardis, M., Christodoulou, C., & Agathocleous, M. (2010). Neural Networks : the Panacea in Fraud Detection? Managerial Auditing Journal, 25(7), 659-678.

Lam, H., & Harcourt, M. (2019). Whistle-blowing in the Digital Era : Motives, Issues and Recommendations. New Technology, Work and Employment, 34(2), 174-190.

Liyanarachchi, G., & Newdick, C. (2009). The Impact of Moral Reasoning and Retaliation on Whistle-blowing : New Zealand Evidence. Journal of business ethics, 89(1), 37-57.

Merchant, K. A., & White, L. F. (2017). Linking the Ethics and Management Control Literatures Advances in Management Accounting (Vol. 28, pp. 1-29): Emerald Publishing Limited.

Nawawi, A., & Salin, A. S. A. P. (2018). Whistle Blowing Intentions–Evidence from Malaysian PLC. International Journal of Law and Management, 60(5), 1111-1125.

Near, J. P., & Miceli, M. P. (1995). Effective-whistle Blowing. Academy of Management Review, 20(3), 679-708.

Nurhidayat, I., & Kusumasari, B. (2018). Strengthening the Effectiveness of Whistleblowing System : A Study for the Implementation of Anti-Corruption Policy in Indonesia. Journal of Financial Crime, 25(1), 140-154. doi:10.1108/JFC-11-2016-0069

Omar, M., Nawawi, A., & Puteh Salin, A. S. A. (2016). The Causes, Impact and Prevention of Employee Fraud : A Case Study of an Automotive Company. Journal of Financial Crime, 23(4), 1012-1027. doi:10.1108/JFC-04-2015-0020

Omar, N., Johari, Z. A., & Smith, M. (2017). Predicting Fraudulent Financial Reporting using Artificial Neural Network. Journal of Financial Crime, 24(2), 362-387.

Pamungkas, I. D., Ghozali, I., & Achmad, T. (2017). The Effects of the Whistleblowing System on Financial Statements Fraud : Ethical Behavior as the Mediators. International Journal of Civil Engineering and Technology, 8(10), 1592-1598. doi:DOI 10.1108/ JFC-04-2015-0020

Peltier-Rivest, D. (2018). The Battle Against Fraud : Do Reporting Mechanisms Work? Journal of Financial Crime, 25(3), 784-794. doi:10.1108/JFC-05-2017-0048

Robinson, S. N., Robertson, J. C., & Curtis, M. B. (2012). The Effects of Contextual and Wrongdoing Attributes on Organizational Employees' Whistleblowing Intentions Following Fraud. Journal of business ethics, 106(2), 213-227. doi:https://doi.org/10.1007/s10551-011-0990-y

Said, J., Alam, M. M., Mohamed, D. I. B., & Rafidi, M. (2017). Does Job Satisfaction, Fair Treatment, and Cooperativeness Influence the Whistleblowing Practice in Malaysian Government Linked Companies? Asia-Pacific Journal of Business Administration, 9(3), 220-231. doi:10.1108/APJBA-06-2017-0053

Scott-Young, C. M. (2014). Empowering Employee Voice to Reduce Ethical Risk Achieving Ethical Excellence (pp. 133-151): Emerald Group Publishing Limited.

Teichmann, F. M., Sergi, B. S., Teichmann, F. M., & Sergi, B. S. (2018). Bribery and Corruption Today: Practices and Challenges', Compliance in Multinational Corporations (pp. 1-29): Emerald Publishing Limited.

Tuanakotta, T. M. (2014). Akuntansi Forensik & Audit Investigatif. Jakarta: Salemba Empat.

Wells, J. T. (2017). Corporate Fraud Handbook: Prevention and Detection. New Jersey: John Wiley Sons.

Yeoh, P. (2014). Whistleblowing : Motivations, Corporate Self-Regulation, and the Law. International Journal of Law and Management, 56(6), 459-474. doi:10.1108/IJLMA-06-2013-0027

Young, R. (2016). An Empirical Examination of Psychological Climate and Internal Disclosure Policy Compliance Advances in Accounting Behavioral Research (pp. 127-154): Emerald Group Publishing Limited.