PalArch's Journal of Archaeology
of Egypt / Egyptology

The Impact of Digitalization on Occupational Fraud Opportunity in Telecommunication Industry: A Strategic Review

[1]Arman Hj. Ahmad, [2]Ridzuan Masri, [3]Chang Mui Zeh, [4]Mohd. Farid Shamsudin,
[5]Rizal Ula Ananta Fauzi

[1,4]Department of Marketing, Universiti Kuala Lumpur Business School, Malaysia
[2]School of Management and Business, Manipal International University, Malaysia
[3]School of Business and Law, International University of Malaya-Wales, Malaysia
[5]Management Study Program, Faculty of Economics & Business, Universitas PGRI Madiun, Indonesia

Email: arman@unikl.edu.my

Arman Hj. Ahmad, Ridzuan Masri, Chang Mui Zeh, Mohd. Farid Shamsudin, Rizal Ula Ananta Fauzi: The Impact of Digitalization on Occupational Fraud Opportunity in Telecommunication Industry: A Strategic Review -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x

Keywords: Digitalization, Fraud, Occupational Fraud, Telecommunication

ABSTRACT

The objective of this conceptual paper is to evaluate the impact of digital anti-fraud measures on the occurrence of occupational fraud, specifically in telecommunication industry. The research was designed as a case study specifically in telecommunication industry involving underpinning theories and models. The paper discusses the identification of elements associated with fraud, effectiveness of digitalized anti-fraud controls and suggests appropriate recommendations for telecom practitioners. The paper has identified in view of digital disruption; the presence of technology advancement reduces the fraud opportunity element by internal fraudster yet broaden the fraud landscape for external fraud at the same time. The findings of the research are yet to be verified by certified fraud examiners as secondary data is the main source used and normally more occupational fraud occurrences are either uncovered or not reported taking into consideration of organization reputation. More scholar studies required to further investigate the actual cost of losses and effectiveness of recommended measures. The paper is a pioneer effort to associate benefit of technology advancement whilst decoupling the fraud elements in the telecommunication context.

1. Introduction

Corporate fraud has been on a rise ever since the emergence in digital era. The traditional fraud type identified include theft of funds or goods, bribery and corruption, regulatory non-compliance, supply chain fraud, money laundering

(AML), merger and acquisition (MA) fraud, financial misconduct, capital market fraud, asset misappropriation etc. Apart from that, among some technology led new fraud type are social media fraud, e-commerce fraud, cyber- crime, counterfeiting, cloud computing fraud and crypto-currency fraud (Deloitte, 2014). Telecommunication fraud has not been spared from fraudulent activities covering from network, billing, CRM, financial system, and procurement (Ghosh, 2010). Mark (2013) mentioned that the traditional telecoms fraud may be classified under four broad categories: hacking, contractual, technical, and procedural fraud. He has categorized mobile fraud type into subscription, system access (including Direct Inward System Access and PBX hacking), call selling, artificial inflation of traffic, revenue share, payphone, bypass and occupational fraud (including dealers/sales fraud, packet splitting, unauthorized credit adjustment, voucher fraud, leaking of credit card information and selling billing information). Among all fraud type, occupational fraud represents the largest threat within the organization as it is committed by internal employees who are entrusted to run the organization business. Since the launch of 4G LTE technology in 2009, the internet usage has growth tripled from 1,596 million users in March 2009 to 4,536 million in June 2019 (IWS, 2019). According to GSMA (GSMA, 2019), it is estimated that there 3.5 billion mobile internet subscribers globally in 2019. This translates to half of a million of the world population is in fact using mobile data. (Leftronic, 2019) claimed that 52.2% of internet usage around the globe originated from smartphones, and the number is growing and mushrooming! E-commerce has grown 3 times faster brick-and-mortar businesses; having said that with the exponential increase of mobile internet usage, m-commerce is predicted to soon taking over e- commerce model in daily life consumption. In view of the new digital services like mobile banking, e-commerce and IoT third-party services, this has opened new emerging fraud type, in which put security and data privacy at greater risks (Yelland, 2013).

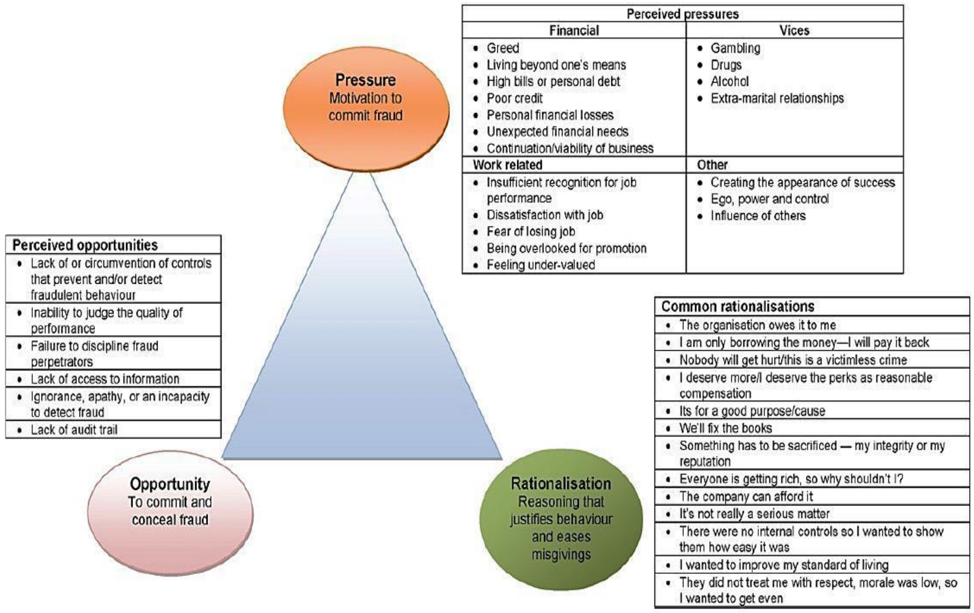
2. Problem Statement

Occupational fraud has been a prevalent threat to organization across the globe, with steady increase in frequency and cost of losses over the past decades. Past studies have yet to show any significant association between technology application and elements of fraud motivation. Addressing this problem will have practical benefits to all industries practitioner in all regions and contribute to re-align the anti-fraud control strategies. The objective of this paper is to provide deeper insights on how to better eliminate or reduce fraud from technology, organizational culture and processes perspectives. This will be contextualized with a review of recent literature on the how digital revolution impacts various telecom operators and current statistical analysis of fraud landscape.

3. Literature Review

Underpinning fraud theories or models

The Fraud Triangle by Donald R. Cressey tells that three reasoning elements must be present at the same time when people commit fraud, namely pressures or incentives to commit fraud, perceived opportunity, and ability to rationalize fraudulent activities. Pressures or incentives to commit fraud come in negative form when confronted with financial, work or personal factors that could lead to undesirable activities (Mohd-Sanusi, Haji Khalid, & Mahir, 2015). Some of the example are individual financial crisis, drug or gambling addiction, expectation to meet sales or productivity targets and desire for privilege social status due to greed etcetera (Wells, 2018). The next critical element is perceived opportunity comes in two aspects: the conditions in the organization that allow fraud to occur and the inheritance of organization to manipulation. In other words, a perpetrator sees some way to abuse a position of trust when there is a possibility or opportunity in weak internal controls. (ACPEN, 2010) PwC 2009 Global Economic Crime Study and EY 2009 European Study Survey also indicated that employee reduction may cause higher fraud risks due to lack of attention in monitoring control procedures. In the other hand, perpetrators often time construct mindset to excuse or rationalize their acts. First-time offenders with lack of personal integrity and no criminal past normally justify their crimes as being caught in undesirable circumstances for instance meeting financial goals under extreme pressures, feeling dissatisfy being underpaid or unappreciated by the employer etc. According to ACFE (2018) report, up to 85% of occupational fraudsters were first time offenders as they had neither been convicted nor terminated due to any fraud-related offenses.


Pressure
Motivation to commit fraud
Opportunity
To commit and conceal fraud
Rationalisation
Reasoning that justifies behaviour and eases misgivings

Perceived pressures	
Financial	Vices
• Greed • Living beyond one's means • High bills or personal debt • Poor credit • Personal financial losses • Unexpected financial needs • Continuation/viability of business	• Gambling • Drugs • Alcohol • Extra-marital relationships
Work related	Other
• Insufficient recognition for job performance • Dissatisfaction with job • Fear of losing job • Being overlooked for promotion • Feeling under-valued	• Creating the appearance of success • Ego, power and control • Influence of others

Perceived opportunities
• Lack of or circumvention of controls that prevent and/or detect fraudulent behaviour
• Inability to judge the quality of performance
• Failure to discipline fraud perpetrators
• Lack of access to information
• Ignorance, apathy, or an incapacity to detect fraud
• Lack of audit trail

Common rationalisations
• The organisation owes it to me
• I am only borrowing the money—I will pay it back
• Nobody will get hurt/this is a victimless crime
• I deserve more/I deserve the perks as reasonable compensation
• Its for a good purpose/cause
• We'll fix the books
• Something has to be sacrificed — my integrity or my reputation
• Everyone is getting rich, so why shouldn't I?
• The company can afford it
• It's not really a serious matter
• There were no internal controls so I wanted to show them how easy it was
• I wanted to improve my standard of living
• They did not treat me with respect, morale was low, so I wanted to get even

Fig. 1. The fraud triangle.

Source: (Dellaportas, 2013)

Over time, there are some limitations of the Fraud Triangle highlighted by other scholars. Firstly, it does not apply to predatory employees who deliberately take up a job for the sake of performing fraud (Wells, 2018). Secondly, some studies show that rationalization is a in fact a grey area in which it should be a pre-requisite before a fraud occurs instead of ex post facto of justification (Ravisankar et al., 2011). Thirdly, according to interviews with Swiss and Austrian offenders, the finding shows perceived opportunity factor is the most critical element even in the absence of the other two elements (Schuchtera & Levi, 2015). As such, the idea of "Fraud Diamond" model in 2004 has been suggested by Wolfe and Hermanson. An additional element called capability portraying the perpetrator must be consciously aware of his/her own ability and 6 distinct traits for committing fraud, which encompass of: (i) influential position within the organization, (ii) adequate intelligence in exploitation the weakness in internal controls, (iii) strong confidence and ego in believing his/her act able to go undetectable over long time, (iv) strong and persuasive personality to convince others to collude or conceal fraud, (v) effective liar with consistent story of lies and (vi) ability to manage extreme stress while taking the risk of being detected (Giles, 2012).

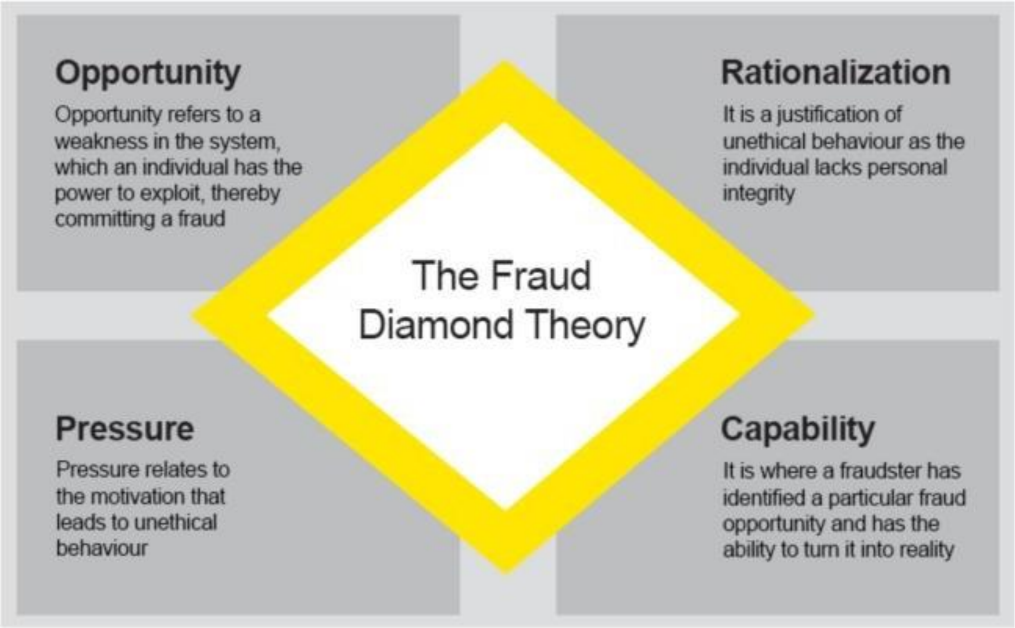

Opportunity
Opportunity refers to a weakness in the system, which an individual has the power to exploit, thereby committing a fraud
Rationalization
It is a justification of unethical behaviour as the individual lacks personal integrity
The Fraud Diamond Theory
Pressure
Pressure relates to the motivation that leads to unethical behaviour
Capability
It is where a fraudster has identified a particular fraud opportunity and has the ability to turn it into reality

Fig. 2 The Fraud Diamond

Subsequently, Marks (2012) developed the Pentagon Fraud theory on top of Fraud Triangle by adding two new elements called capability and arrogance. It is developed on the basis of 89% of fraud cases are carried out by owners or top executives for example C-level; as well as 70% caused by individual pressure, greed and arrogance elements (Christian, Basri, & Arafah, 2019).

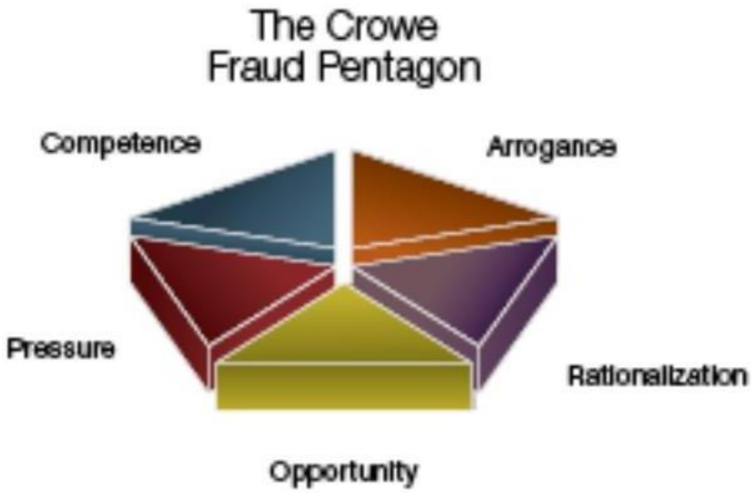


Fig. 3 The Pentagon Fraud

With more complex fraud schemes uncovered, there are more new theories suggested. (Biegelman & Baltow, 2012) suggested that, among those include:

(i) Tip of the Iceberg Theory – true extend of actual amount of loss when first instance discovered will only be revealed upon further investigation conducted over time
(ii) Potato Chip Theory – addictiveness leads to other avenue or branch of possible fraud
(iii) Rotten Apple Theory – due to either imitation of fraudulent observed carried out by superiors themselves or lack of direction and overseeing in job integrity
(iv) Low-Hanging Fruit Theory – overlook of simple and lower-risk fraud
(v) Addition by Subtraction Theory – lack of implementing zero tolerance for fraud policy will deter the immediate removal of perpetrator before causing greater loss when he/she is promoted to higher corporate level
(vi) Fraudster as Employee Theory – once commit fraud with bad track record, the perpetrator should no longer be considered as employee

Occupational fraud trending worldwide since digital disruption

According to ACFE 2018 report, across 23 industry categories in 23 countries worldwide, the survey findings show 2,690 cases of occupational fraud had contributed total losses of over $7 billion (ACFE, 2019). With the estimation of 5% of typical organization losses of revenue each year, it represents an increase reaching $ 4 trillion using the 2017 estimated Gross World Product, as opposed to approximately $ 3.7 trillion in 2014 (ACFE, 2015) and 2015 (ACFE, 2017). Of the three primary categories defined by ACFE, asset misappropriations is the most commonly detected fraud scheme; however the 89 percent of the study cases only contributed the least median loss of $ 114,000. Of which, 97 percent of the fraudster attempt in concealment in the form of create, alter or delete, which could take up between 12 to 30 months before being uncovered.

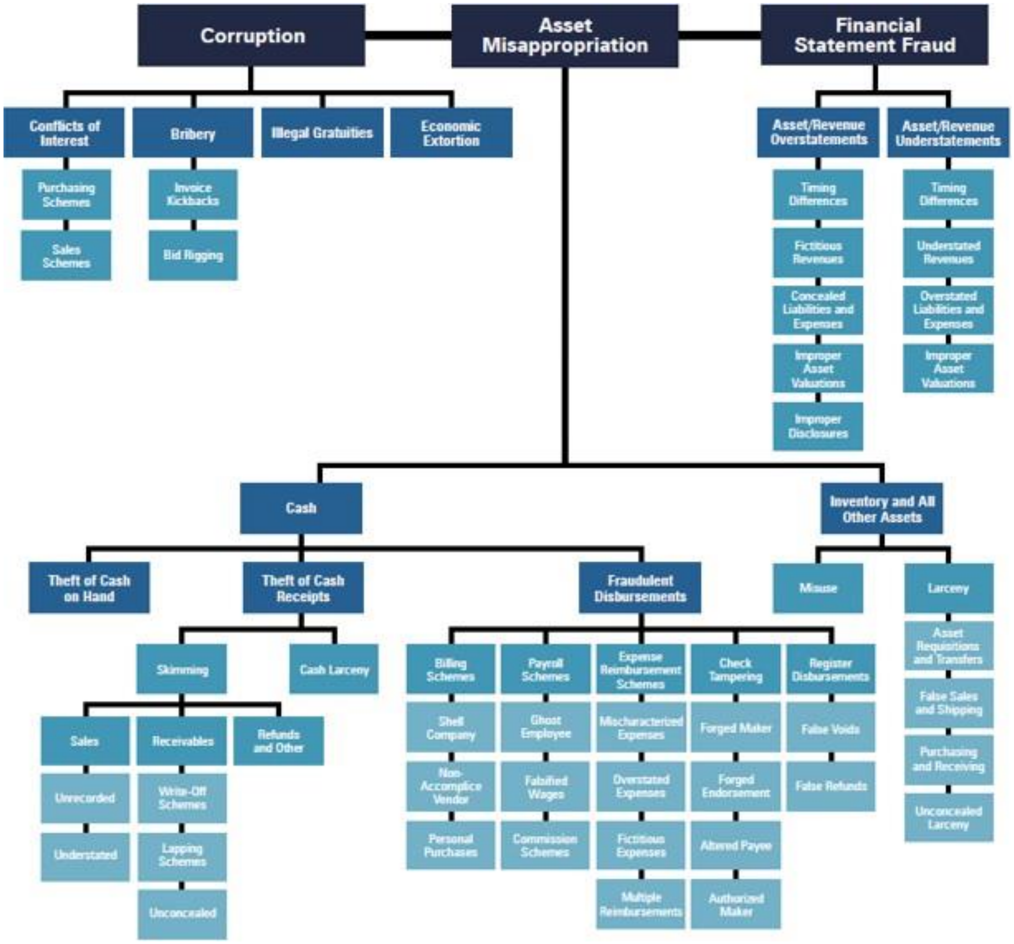


Fig. 4 Fraud Tree

Bologna and Lindquist (1995) has categorized corporate fraud or abuse into internal and external fraud, in which external perpetrators could be suppliers or contractors whereas internal fraudster would be employees, executives, managers or business owners themselves. In some cases, there could be a mixture of both occupational and external fraud. (Jans, Lybaert, & Vanhoof, 2009) Further breakdown of occupational fraud classification is between fraud for and fraud against the organization as well as fraud between management versus non-management. Above perspective is like Davia *et al.* (2000) using different dimension of classification based on the intention of the act: statement and transaction fraud. The former statement fraud intends to misstate financial values to deceived shareholders on organization profitability, whereas the latter intends to embezzle organizational assets. Example of the statement fraud case studies in some of the largest institutions in US, among them are Enron, Worldcom, Aldelphia , Quest and ImClone (E.Lokanan, 2015) and Dieselgate scandal in Volkswagen (Donning, Eriksson, M., & OM, 2019). This is in-line with the study conducted by PriceWaterhouseCoopers (“PWC”) in a Global Economic Crime Survey (GECS) that the increase of accounting fraud has posed a serious threat to corporate business (PWC, 2014).

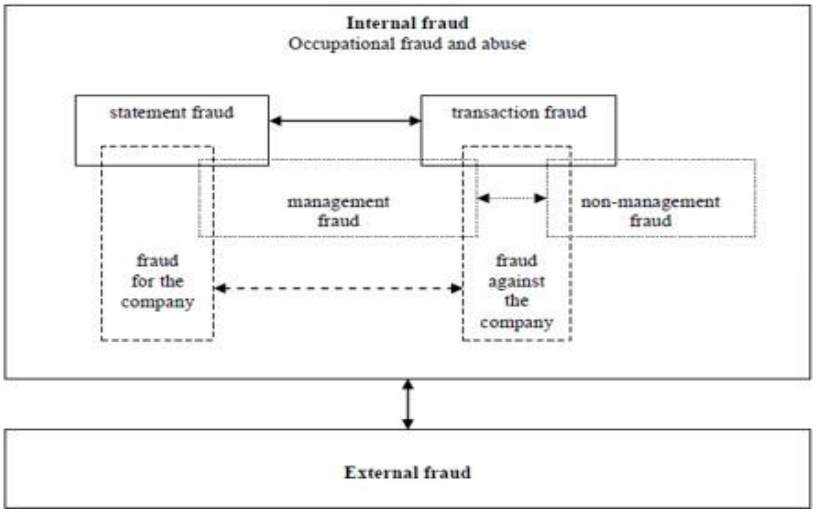


Fig. 5 Fraud Classification Overview

(Reints, 2018) Former Tesla employee, Salil Parulekar, had allegedly embezzle around $ 9.3 million from the company between 2016 and 2017, by falsifying invoices and bank documents with instructions to wire payments to his accounts instead of Hote Industrial Manufacturing supplier. (Brook, 2018) In another occupational fraudulent incident earlier in 2018, another employee, Martin Tripp, managed to sabotage by accessing the Tesla Manufacturing Operating System's (MOS) backend source code using false user ids and subsequently making direct changes to the codes and exporting highly sensitive industry data to unknown third parties.

4. Discussion

Figure 6 below is the model of the research framework in this paper. This conceptual framework illustrates the effect of digitalization as moderating variable on the independent variables associated to the occupational fraud in telecommunication industry.

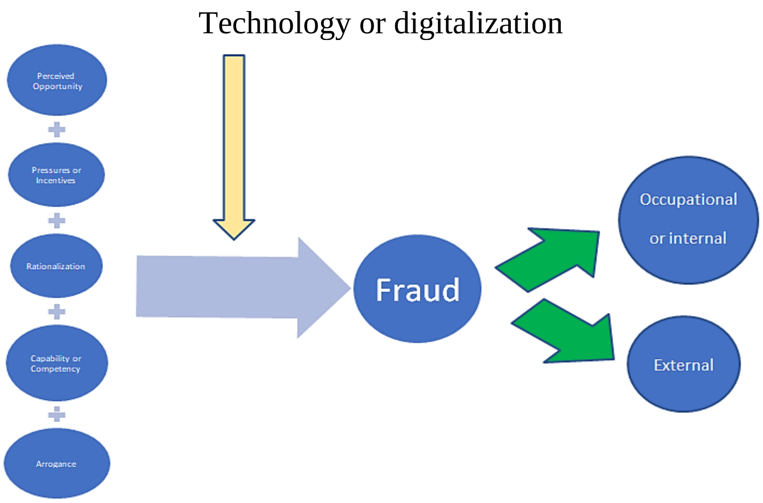


Fig. 6 Conceptual Framework (source: Author)

Reducing fraud opportunity

Telecommunication industry was ranked 17th among all industries participated in the study, with 50 reported cases and medium loss of $ 100,000. The higher risk schemes for telecommunication industry are corruption, skimming and billing. Although the reported median loss in telecommunication is no way near the occurrence risk factors examined in other top industries e.g. "Banking and Financial Services", "Government and Public Administration", "Manufacturing'" and "Health Care", it's observed the percentage of distribution in telecommunication has an amazing decreased from 3.1 in 2012 to merely 1.9 in 2017.

Asset Misappropriation Sub-categories	**2012**	**2014**	**2016**	**2018**
SCHEMES on THEFT OF CASH RECEIPTS				
Skimming	14.6	11.8	11.9	11
Cash Lacerny	11	8.9	8.4	11
SCHEMES on FRAUDULENT DISBURSEMENTS OF CASH				
Cash Register Disbursements	3.6	2.8	2.7	3
Check Tampering	11.9	10.9	11.4	12
Claims Reimbursement	14.5	13.8	14	14
Billing	24.9	22.3	22.2	20
Payroll	9.3	10.2	8.5	7
SCHEMES on FRAUDULENT DISBURSEMENTS OF CASH				
Cash On-hand	10.8	10.9	11.5	15
Non-Cash	17.2	21	19.2	21
Total cases	**1,388**	**1,483**	**2,410**	**2,690**

Table 1 Sources: ***(ACFE, 2013), (ACFE, 2015), (ACFE, 2017), (ACFE, 2019)***

The present ACFE studies over past recent years consistently showing an increase in occupational fraud. However, what it fails to highlight is the fraudulent activities' breakdown from the landscape of both type of perpetrators and element of fraud derived from Fraud Triangle/Fraud Diamond/Pentagon Fraud theories. Previous studies mostly focus on fraud opportunity due to weak internal fraud controls and low chances of being detected or reprimanded (Dorminey et al., 2012). In accordance to the analysis in Table 1 above, we can summarize that with the technology advancement in digital era, perceived opportunity element has been significantly decreased when associated with occupational fraud instead of external fraud. Numerous counter-effort activities have been put in place to combat the fraudulent occurrence, mainly in prevention and detection instead of investigation. Statistical evidence above revealed that certain fraud type had negatively reduced with increase of fraud management tools used. Reduction in fraudulent frequency of skimming, billing and payroll tells that digital way of anti- fraud detection able to reduce (if not eliminate) the fraud opportunity/ The main factors are paperless procedures and improved transaction tracking via end-to-end value chain journey.

(i) Skimming – depicts any scheme whereby cash is stolen e.g. payment accepted from customers, yet sale not recoded
(ii) Billing – depicts any scheme whereby invoices issued for fictitious goods or services in order to receive payments intended for personal purchases e.g. a shell company for billing services not rendered (similar to 1MDB fraud case)
(iii) Payroll – depicts any scheme whereby false claims submitted for compensation e.g. invalid overtime claims and ghost employees added to the payroll

As pointed out earlier, some fraud type occurrence is gradually increased due to motivation of other fraud elements, namely capability, pressures and arrogance. These are the acts performed physically hence difficult to be detected by the system alone as perpetrators are leveraging on their position in the organization. As such, other anti-fraud controls would be more appropriate to be imposed: code of conduct, internal audit, tips, hotlines, rewards for whistleblowing, fraud training, job rotation and proactive monitoring in unexpected area using more effective methods (see Recommendation chapter).

(i) Cash larceny – depicts any scheme whereby cash is stolen upon transactions being recorded in bookkeeping e.g. cash and checks physical theft from daily receipts before bank deposits
(ii) Check tempering – depicts any scheme whereby checks' forgery or alteration prior to check deposit e.g. physical outgoing checks theft into own account (similar to Tesla fraud case)
(iii) Cash on hand – depicts any scheme whereby physical cash theft from victim organizations' premises e.g. stealing from a company vault or petty cash box
(iv) Non-cash – depicts any scheme whereby non-cash assets physical theft or misuse involved e.g. inventory theft and authorized usage of confidential customer financial information

Findings from total of 54 responses from Communications Service Providers across a range of diversified network industries globally correspond that 30 percent increase in using fraud management maturity model and continuous investment in tools e.g. Fraud Management System (FMS), Test Call Generator (TCG), signaling probes, business intelligence (BI), Revenue Assurance System (RA), queries on top of Data Warehouse, Data Mining System, Depth Packet Inspection System (DIP), Link Analysis etcetera (TMForum, 2019). Again, these tools have successfully proven reducing fraud opportunity element towards internal resources itself effectively.

The impact of collusion

It is observed that occupational fraud has encouraged involvement of two or more perpetrators since digital era. The combine efforts of fraudster across multiple parties, sectors or functions are proven more harmful and enabled higher chance of overriding anti-fraud measures in organization. The studies from ACFE show a drop of single perpetrator from 58 percent in 2012 to 52 percent in 2017; in other words, a dramatic increase in the frequency scheme relate to two or more perpetrators, with exceeding 35.6 percent jump in terms of median loss over the span of 5 years studies. Notably, the misappropriation of non-cash assets would be more common in collusion schemes compared to single-perpetrator frauds as it makes sense to involve different parties from other team functions to steal larger amount. In that case, since there is higher payout expected to more individuals involved in the act, greater losses are observed.

Telecom Fraud cases cross borders and industries

Telecom is one of the industries impacted tremendously due to digital disruption on the Internet of Things (IoT), changing subscribers' behaviors and technology advancement to 5G. Given telecom companies control critical infrastructures and store personal information, it is compelling for both external and internal perpetrators to commit fraud. In China mainland, cross-border telecommunications network fraud cases have seen a worrying trend (Yingchao, 2017). With collaboration with authorities in other countries e.g. Malaysia, Kenya, Cambodia, Indonesia, Laos etc., the Ministry of Public Security had successfully solved over 3000 cases, diminished 58 foreign fraud dens and arrested 975 fraudsters since 2016. It is notable that the intelligence means of cross-border telecom fraud activities have evolved by constantly shifting the fraud dens between Southeast Asia to Europe, South America, and Africa (ZX, 2019). The latest syndicate was busted when China police in Chongqing arrested 69 suspects with help from Myanmar counterpart, with fraud cost amounting to nearly 10 million yuan or USD 1.4 million. Taking advantage on the nature of globalization, it's considerably fast to setup fraud dens in other international countries in a more organized and financed fashion. In some cases, victims' personal information including bank account or bank card numbers, could be easily obtained via online purchases or deliberate occupational fraud act. (Yin, 2018) A perpetrator Xu illicitly leaked victims' personal information (identity fraud) upon managed to conveniently purchase more than 20,000 pieces of personal information, resulting in 146,000-yuan loss in telecom fraud.

In the event of cross-border fraud cases, we should not forget about direct financial loss impact to the telecommunication organization itself. There are interconnect and roaming cost incur between operators for voice and data network services connectivity. Telecom arbitrage fraud indicates differences in settlement rates exploited between countries (AYAMGA, 2018). In the Communication Fraud Control Association (CFCA) 2015 survey, telecom arbitrage fraud amounted to $ 2.94 billion of revenue loss. According to survey conducted, most of the corporate executives are aware of the cross-border fraud risks however only 41 percent of the CFOs are taking cybercrime seriously (EY, 2016). Among some internal controls recommended are strategic market-entry in countries with different cultural expectation and behaviors tolerance, better fostering third party partners relationship, implement positive organization culture in encouraging whistleblowing etc. In terms of occupational fraud across industry, at times it's a challenge to compromise between telecom operators own internal policies with other parties e.g governments, banking and financial institutes, payment gateway channels etcetera in the event of conflict of interest. Consequently, the end-to-end security measures in entire ecosystem unable to be implemented in full force. Some occupational fraud type has been observed by scholars and industry practitioners as following (AYAMGA, 2018):

(i) M-banking fraud – In 2015 and 2016 itself, 278 and 388 mobile money fraud cases were recorded respectively in Ghana.
(ii) Telephone banking fraud – using social engineering technique, victims are tricked into disclosing personal information via cold calling or fake emails.
(iii) Slamming fraud – telecom operators illegally change customers' telephone service without consent, normally switch from local to international service to charge high termination call rates.
(iv) Cramming fraud – telecom operators illegally add charges to customers' bills for services without authority e.g. promotions.
(v) Negative option marketing fraud – telecom operators deceive customers into signing up certain marketing materials.
(vi) Toll Free Number fraud – occupational fraudsters deliberately collaborate with external party allowing high volume of calls routed to toll free number. The intention is to increase the bills and in return, profit sharing scheme with the external party.
(vii) Pricing Confusing fraud – operators use multiple and confusing pricing plan to deceive customers in signing up, however quickly change the prices thereafter.
(viii) False Answer Supervision (FAS) fraud – collaboration with other interconnect/roaming operators or business partners to increase revenue for each call by performing short-stopping fraud (intentionally divert call to machine recorded message), early answer (intentionally playing fake ringing tone to increase call duration), late disconnect (intentionally delay the call termination).
(ix) International Revenue Share Fraud (IRSF) fraud – collaboration between operators and third party to collect illegal payout from premium rate number company, in which the range of numbers advertised in various parts of the world might belong to legit victim, hence causing huge bill amount.

Digital evolution and telecom fraud threats in e-commerce and m-commerce

Worldwide, we are seeing an increase of telecom and MVNOs steering towards e-commerce and m-business as part of the move to reduce distribution or supply chain costs and increase efficiency in personalized customer service. Merging of both online and offline marketing (physical stores) has merged cohesively to stay competitiveness. SaaS cloud service providers, social media platform, OTTs are becoming more crucial in this new business strategy model. Such telecom internal digitalization capabilities have attracted small e-commerce start-ups into partnerships on key areas of e-store, e-care, IoT and M2M, media content and video, and mobile payment. These new way of proposition services on data monetization is a win-win situation for all parties to capture adjacent business opportunities (EY, 2017). One example, with the help of TIE Kinetix and The Online Company, T-Mobile today is leveraging on its e-commerce system for consumer acquisition, soon focusing on business acquisition and consumer renewals/upgrades.

(ROFIQ, 2012) It’s important to note that e-commerce involve sellers, buyers and the medium (including telecom, financial services etc.). The role of telecom is mainly to establish internet network for transferring transaction data, provide websites as Marketplace UI as well as media of payment gateway (Lee & Turban 2001). Surveys reveal that online business revenue losses were estimated $ 2.7 billion in the US and Canada, £ 300 million in UK and $ 220 million in Australia respectively (CyberSource, 2011; US College Search, 2011; Ecommerce Report, 2010). Furthermore, 86% of Indonesian Internet users had lost average cost of $ 1,265 per month in lieu cyber-crime (Norton 2010). Stakeholders of transactions using e-commerce in fact consists of sellers, buyers, and the media (Lee & Turban 2001). The media used would be either Internet network for data transmission, websites for UI interfaces and credit cards for payments. The e-Commerce market in Malaysia is growing with contribution of 6.3% to gross domestic product (GDP) in 2017 in which translated to value added increase from RM75.0 billion in 2016 to RM85.8 billion in 2017 (MCMC, 2018). However, the security and privacy related issues are largely related to 53.4 percent survey respondents raise concern on identity fraud e.g. cards fraudulent, fake online retailers etc. and 59.0 percent worry on privacy issues e.g. misused of information, customers’ behaviors pattern tracking etcetera (Zhang, Bian, & Zhu, 2013).

The renowned e-commerce platform, eBay, has put some stringent measures in its customer feedback system to minimize the falsified manipulation of trust rating (Brown and Morgan 2006). However, this is not the case in Taobao. According to Chen and Yang, (2009), based on their research findings, up to 47 percent of the rated transactions are once detected as fraud as super sellers tend to commit trust fraud in order to boost their business and attract more customers. It is estimated about an astounding 80 percent of Taobao sellers have committed this type of fraud (Money Week, 2011). To make things worse, there are about 1,000 active trust fraud external companies who work closely with internal fraudster to artificially boost reputation within the Taobao ecosystem, in which a few of them in return making profits in millions of RMB every year (Beijing Youth Daily, 2009). Meanwhile, m-commerce is relatively new, however judging by the mobile usage penetration and data consumption explosion rate, it's a future trending replacing e-commerce (Middleton, 2011). Some success stories from Safaricom in Kenya, paybox in Austria, Compass Bank in the US and in Germany serve as good references. In Malaysia, Celcom's AirCash enables mobile e- Wallet services. Similar initiatives taken up with other operators e.g. vCash by Digi, m-payment by Germany's Mobilecom, Orange Money by Orange Group, m-banking by Finland's Sonera, Easypaisa by Telenor Pakistan, wireless services and m-billing by US's Sprint PCS (with collaboration with telecom TelecomOne), just to name a few (Tamturk, 2016). Both e-commerce and m-commerce present higher fraud exploitation risk especially in card-not-present (CNP) transactions (Basset, 2013). Future technology adoption of cloud services amongst mobile internet and smartphone devices lead to more challenges in combating fraud threats. The most common next generation networks cyber vulnerabilities for smartphones are identified as: (i) Data leakage resulting from device loss or theft, (ii) Unintentional disclosure of data, (iii) Attacks on decommissioned smartphones, (iv) Phishing attacks via mobile app or websites, (v) Spyware attacks via mobile app, (vi) Network Spoofing Attacks, (vii) Surveillance attacks, (viii) Dialler ware attacks, (ix) Financial malware attacks and (x) Network congestion. In which (i), (ii), (iii) and (ix) are relevant to occupational fraud.

5. Recommendation

Future mode of anti-fraud controls – Technology

Technological advancements in digital evolution has provided more effective methods in prevention, detection, investigation, and correction, consequently meaning additional challenges to the perpetrators (be it single or multiple) when committing fraud and concealment. In most of the typical organization, some common anti-fraud controls are being implemented, associating the reduce fraud losses and shorter fraud duration. Today, information age represents big data which would be beneficial to perform statistical analysis on data characteristics. Inspired by the fact of increase in fraud collusion between two or more perpetrators, some sophisticated anti-fraud controls have evolved recently, namely Knowledge Discovery in Databases (KDD), data mining, link analysis and Social Network Analysis (SNA). On top of that, other useful means such as machine learning algorithms, data mining and meta-learning are proven effective based on current development of innovative in other industries (West and Bhattacharya, 2015; Data Science, 2017 and Abbasi et al., 2012).

According to Michalski et al., (1998) Knowledge Discovery in Databases (KDD) is used to manage huge amount of data using data mining as the core activity between data input (for raw data pre-processing) and output result (knowledge). Witten and Frank (2000) cites that data mining is *"…the process of discovering patterns in data. The process must be automatic or (more usually) semi-automatic. The patterns discovered must be meaningful in that* *they lead to some advantage, usually an economic advantage. The data is invariably present in substantial quantities*.”. Data mining comes in various form of techniques in the past empirical research focusing in financial fraud detection including decision trees, neural networks, K-means clustering, FR² framework (Jans, Lybaert, & Vanhoof, 2009) etc. Two main tasks undertaken by data mining, namely predictive and descriptive. The former predicts the values by establishing predictive observation on the underlying relationships between attributes. Whereas the latter task provides the holistic view of entire data sets by using pattern recognition, anomaly analysis and correlations findings on unsupervised data (Tan et al., 2006). (Bach, Dumičić, Žmuk, Ćurlin, & Zoroja, 2018) analyzed one case study of suspicious working- hour claims in a project-based company in Croatia, and they found that data mining techniques had again confirmed the accuracy of past researches on the data mining model in occupational fraud detection. In the said case study, the CHAID decision tree was adopted by applying sequence of functions from various areas including data science, machine learning, statistics etc., resulting in an automatic fraud-detection software with precision rate as high as 80%. Similar positive result findings was shared in the study made over the effect of the unbalanced data in telecommunication context using Naive Bayes model with extension of anomaly detection, resulting in an accurate and distinct segregation output between normal classifiers and fraud classifiers (Sousa, 2014). Social Network Analysis leverages on the fact that organizations are networked between all entities e.g. employees, customers, suppliers etcetera (Lookman & Nurcan). It represents a dynamic analysis of occupational fraud behaviors and characteristics as opposed to conventional rule-based algorithms. Today, most of the telecommunication organizations have fraud management system (FMS) as the basic tool to detect patterns in transactions (data from financial statement, inventory and supply chain, network, claims from HR etc.). However, certain extend of human intervention, monitoring and judgement are still required when reviewing this huge amount of information. Furthermore, another disadvantage of traditional FMS automated tool is the limitation of rule- based algorithm without holistic view of other related transactions by the same entities. SNA has the capabilities to combine human ability to combine with computer’s intelligence to detect fraud cases iteratively, resulting in eliminating labor intensive tasks and providing better illustration of potential risky cases in a more holistic graphical view. Machine learning is particularly useful when it comes to big data involved in fraud detection and prevention (Donning, Eriksson, M., & OM, 2019). Machine learning algorithms intentionally automate the discovery of patterns and it usually comes in two approaches: supervised and unsupervised. The former is more predictable due to pre-defined guidelines and possible outputs already known prior. Whereas the latter involve manual human intervention to identify complex processes or data patterns without guidelines (Data Science, 2017). Meanwhile, meta-learning is an extension of machine learning leveraging on information obtained from prior data mining or machine-learning method. In other words, purpose of meta-learning is to improve the quality of results for future applications via auto self-learn on top of the process and algorithms itself (Abbasi, Albrecht, Vance & Hansen, 2012).

Future mode of anti-fraud controls – Organizational culture

As previously mentioned in the Discussion chapter, there is so much so that technology can only help in detecting and preventing fraud. Hence the organizational environment and culture play a crucial role thereafter. Positive and effective measures would be able to tackle the loopholes in organizational culture of high pressure. Building a fraud prevention culture by top executives will set a firm tone at the top and send a clear signal to employees, shareholders and stakeholders that they take zero tolerance in fraud crime. According to Dr. Joseph T. Wells (founder of ACFE), top executives must ‘walk the talk’ in maintaining work profession integrity, accountability and responsibility by setting good example in being honest and serious in taking necessary disciplinary actions against convicted perpetrators (Biegelman & Baltow, 2012). Moreover, a strong and independent Audit Committees within an organization will ensure compliance and foster “checks and balances” mindset culture to executive leadership. Apart from that, by having constant communication and interactive, scenario-based trainings will ensure a culture of compliance within organization and the anti-fraud controls stay relevance to the emerging complex fraud in the digital era.

Future mode of anti-fraud controls – Processes

As we are moving towards digital society, all forms of digital platforms are connectivity to each other in the ecosystem encompassing close interaction between customers, suppliers, third party players, businesses, governments, advertisers, telecommunication operators, infrastructures and Internet of Things (IoT). Collaboration is the crucial component in staying competitive and sustainable in rapid evolution of mobile broadband networks (5G and Fourth Industrial Revolution) era. Digital identities serve as unique identifier across all digital platforms. Telecommunication companies would benefit much in revenue growth by working with other service providers to reduce fraud. A good example would be BICS, a provider of wholesale carrier services, manages a global anti-fraud crowdsourcing platform with collaboration with telecom operators by leveraging on intelligence from mobile phone numbers and compliances in both local and international data privacy laws (Stryjak & Ulrich, 2019). Grab of Singapore and Go-Jek of Indonesia consistently apply stringent monitoring of customers’ identities and risk profiles in their apps as part of anti-fraud controls. Meanwhile, siloed organizational structures and outmoded IT systems is no longer relevant in today business. A digital-driven omnichannel strategy is important by promoting organizational change and process improvement to expand fraud management capabilities. Collaboration between fraud management teams and other departments, regions or countries would tremendously improve the decision-making and detection efficiency. In some cases, simplification of processes would result in faster response and action time against fraudulent attacks, for example fraud alerts should be sent to customers for pre-approval. A good business processes will ensure that accounts are completed correctly, and policies are followed. A comprehensive risk assessment processes will significantly reduce the loopholes in business ecosystem. That includes identifying, measuring and mitigating fraud risks, subsequently implementing appropriate oversight internal controls e.g. behaviors red flags checks, hotlines and tip. According to GLF (GLF, 2018), metrics and processes to manage fraudulent traffic are in place in most of the network carriers, unfortunately, there is a lack of consistency in tracking and implementation has not been followed through. Furthermore, survey showed less than 70% of fraud incidents were reported to the CEO's level.

6. Conclusion

It's believed that high number of occupational frauds remains hidden due to constraint in staff resources and budget on anti-fraud measures especially in the case of smaller scale organizations (Suh, Nicolaides, & Trafford, 2019; Johansson & Carey, 2016; Bussmann & Werle, 2006). For some larger organization, the information on fraud incidents are regarded as confidential simply taking into consideration of possible reputation damage to the organizations and loss of trust from customers (Button, 2008). As such, the statistics illustrated in this paper might be imperfect. Contextually, the studies from ACFE have triggered me to challenge the overall relevance to the Fraud Triangle, Fraud Diamond and Pentagon Fraud theories. It is arguable that the results do not explain the positive improvement in certain fraud sub-categories upon applying technology advancements in anti-fraud internal controls. The statistics in fact has the tendency to lead the readers into believing occupational fraud is the most prevalent threat and challenging to be addressed despite we have seen organizations making tremendous strides in terms of awareness and internal ability advancements to combat these crimes. At the same time, digitalization has changed the landscape of fraud activities globally, hence there is a need for telecom operators to
have controls as close to the risks as possible to e-fraud, collusion and emerging trending of m- commerce fraud. This paper puts forward some recommendations to combat occupational fraud in telecommunication industry. At present, a lot of attention is put on the technology advancement to prevent and detect fraud. Despite reduction of some fraud type observed thanks to the new technologies and techniques, this industry is still suffering from increase of telecom fraud. Given the mentioned situation, it is crucial for organization leaderships and governance bodies to continue reinforcing the right organizational culture and processes.

Acknowledgement

This research was supported by the Centre for Research & Innovation, Universiti Kuala Lumpur, and Universiti Kuala Lumpur Business School, Malaysia. We would also like to show our gratitude to the Management of Universiti Kuala Lumpur, the Dean of Universiti Kuala Lumpur Business School, the Management of School of Management and Business, Manipal

International University Malaysia, the Management of International University of Malaysa-Wales, Malaysia as well as all citizen of the above said universities, for their endless support and assistance towards the completion of this research. Our special thanks also go to the publication editors and everyone in the impact hub. Thanks for all your support and encouragement! Finally, to Mak (Hjh. Normah Hj. Hashim) and Bak (Hj. Ahmad Hj. Akib), may Allah grant both of you with His Jannah. Aamiin Ya Rabb.

References

Acfe. (2013). *Report To The Nations On Occupational Fraud And Abuse: 2012 Global Fraud Study.* Association Of Certified Fraud Examiners. Retrieved From Https://Www.Acfe.Com/Uploadedfiles/Acfe_Website/Content/Rttn/2012-Report-To-Nations.Pdf

Acfe. (2015). *Report To The Nation On Occupational Fraud And Abuse: 2014 Global Fraud Study.* Usa: Association Of Certified Fraud Examiners. Retrieved From Https://Www.Acfe.Com/Rttn/Docs/2014-Report-To-Nations.Pdf

Acfe. (2017). *Report To The Nations On Occupational Fraud And Abuse: 2016 Global Fraud Study.* Associate Of Certified Fraud Examiners. Retrieved From Https://Www.Acfe.Com/Rttn2016/Docs/2016-Report-To-The-Nations.Pdf

Acfe. (2019). *Report To The Nation On Occupational Fraud And Abuse: 2018 Global Fraud Study.* Usa: Association Of Certified Fraud Examiners. Retrieved From Https://Www.Acfe.Com/Report-To-The- Nations/2018/Default.Aspx

Acpen. (2010, November 10). *Business Fraud, Internal Controls, And Forensic Analysis For The Accountability Professional.* Retrieved From Pdfdrive: Https://Www.Pdfdrive.Com/Business- Fraud-Internal-Controls-And-Forensic-Analysis-For-The-Accountability-Professional- E19172324.Html

Ayamga, D. (2018). Telecommunication Fraud Prevention Policies and Implementation Challenges. Luleå University Of Technology.

Bach, M. P., Dumičić, K., Žmuk, B., Ćurlin, T., & Zoroja, J. (2018). Internal Fraud In A Project-Based Organization: Chaid Decision Tree Analysis. *Procedia Computer Science* , 138, 680–687.

Basset. (2013). *Basset Telecom Report: Following The Money – The Drivers Of Fraud.* Sweden: Basset.Retrieved From Https://Www.Gsma.Com/Membership/Wp-Content/Uploads/2012/03/Following_The_Money_The_Drivers_Of_Fraud.Pdf

Biegelman, M. T., & Baltow, J. T. (2012). *Executive Roadmap To Fraud Prevention And Internal Control Second Edition: Creating A Culture Of Compliance.* New Jersey, Usa: Wiley.

Brook, C. (2018, June 21). *Tesla Data Theft Case Illustrates The Danger Of The Insider Threaat*. Retrieved From Digital Insider: Https://Digitalguardian.Com/Blog/Tesla-Data-Theft-Case-Illustrates-Danger-Insider-Threat

Christian, N., Basri, Y., & Arafah, W. (2019). Analysis Of Fraud Triangle, Fraud Diamond And Fraud Pentagon Theory To Detecting Corporate Fraud In Indonesia. *The International Journal Of Business Management And Technology*, 3(4), 1-6.

Dellaportas, S. (2013). Conversations With Inmate Accountants: Motivation, Opportunity And The Fraud Triangle. *Accounting Forum* , 37, 29– 39.

Deloitte. (2014). *India Fraud Survey Edition I.* Deloitte. Retrieved From Https://Www2.Deloitte.Com/Content/Dam/Deloitte/In/Documents/Finance/In-Finance-Annual- Fraud-Survey-Noexp.Pdf

Donning, H., Eriksson, M., M., E. M., & Om, L. (2019). Prevention And Detection For Risk And

Fraud In The Digital Age – The Current Situation. *Acrn Oxford Journal Of Finance And Risk Perspectives*, 8, 86-97.

E.Lokanan, M. (2015). Challenges To The Fraud Triangle: Questions On Its Usefulness. *Accounting Forum*, 39, 201-224.

Ey. (2016). *Corporate Misconduct - Individual Consequences.* Ernst & Young. Retrieved From Https://Www.Ey.Com/Publication/Vwluassets/Ey-Corporate-Misconduct-Individual- Consequences/$File/Ey-Corporate-Misconduct-Individual-Consequences.Pdf

Ey. (2017). *Global Digital Telecom Playbook: Telcos Reinvent Themselves In The Digital Age.* Ernst & Young. Retrieved From Https://Www.Ey.Com/Publication/Vwluassets/Ey-Global-Digital-Telecom-Playbook/$File/Ey-Global-Digital-Telecom-Playbook.Pdf

Ghosh, M. (2010, July). Telecoms Fraud. *Computer Fraud & Security*, Pp. 14-17.

Giles, S. (2012). *Managing Fraud Risk: A Practical Guide For Directors And Managers.* West Sussex, Uk: Wiley.

Glf. (2018). *Taking Action Against Fraud: Demonstrating The International Wholesale Industry's Leadership Against Telecoms Fraud.* Itw Global Leaders' Forum (Glf). Retrieved From Https://Www.Deltapartnersgroup.Com/Sites/Default/Files/Glf%20-%20taking%20action%20against%20fraud%20-%20october2018_0.Pdf

Gsma. (2019). *Mobile Internet Connectivity 2019: Global Factsheet.* United Kingdome: Gsma. Retrieved From Https://Www.Gsma.Com/Mobilefordevelopment/Wp-Content/Uploads/2019/07/Mobile- Internet-Connectivity-Global-Factsheet.Pdf

Iws. (2019, November 11). *Internet Growth Statistics*. Retrieved From Internet World Stats: Usage And Population Statistics: Https://Www.Internetworldstats.Com/Emarketing.Htm

Jans, M., Lybaert, N., & Vanhoof, K. (2009). A Framework For Internal Fraud Risk Reduction At It Integrating Business Processes: The Ifr² Framework. *The International Journal Of Digital Accounting Research*, 9, 1-29.

Leftronic. (2019). *21+ Amazing Mobile Internet Usage Statistics In 2020*. Retrieved From Leftronic.Com: Https://Leftronic.Com/Mobile-Internet-Usage/

Lookman, S., & Nurcan, S. (N.D.). A Framework For Occupational Fraud Detection By Social Network Analysis.

Mcmc. (2018). *E-Commerce Consumer Survey 2018.* Malaysian Communication And Multimedia Commission. Retrieved From Https://Www.Mcmc.Gov.My/Skmmgovmy/Media/General/Pdf/Ecs- 2018.Pdf

Middleton, J. (2011, August 2). *Ten Lessons For M-Commerce Implementation*. Retrieved From Telecoms.Com: Https://Telecoms.Com/31442/Ten-Lessons-For-M-Commerce-Implementation/

Mohd-Sanusi, Z., Haji Khalid, N., & Mahir, A. (2015). An Evaluation Of Clients' Fraud Reasoning Motives In Assessing Fraud Risks: From The Perspective Of External And Internal Auditors. *Procedia Economics And Finance*, 31, 2-12.

Reints, R. (2018, November 9). *Former Tesla Employee Allegedly Embezzled Over $9 Million*. Retrieved From Fortune: Https://Fortune.Com/2018/11/09/Tesla-Employee-Embezzlement/

Rofiq, A. (2012). Impact Of Cyber Fraud And Trust Of E-Commerce System On Purchasing Intentions: Analysing Planned Behaviour In Indonesian Business.

Schuchtera, A., & Levi, M. (2015). Beyond The Fraud Triangle: Swiss And Austrian Elite Fraudsters. *Accounting Forum*, 39, 176-187.

Sousa, J. V. (2014, June 30). Telecommunication Fraud Detection Using Data Mining Techniques.

Purto. Stryjak, J., & Ulrich, P. (2019). *Collaborative Platforms For Digital Societies In Asia Pacific.* Gsma. Retrieved From Https://Www.Gsmaintelligence.Com/Research/?File=A74992c36833ae7881a 7fb9bcf2288c9&Dow Nload

Suh, J. B., Nicolaides, R., & Trafford, R. (2019). The Effects Of Reducing Opportunity And Fraud Risk Factors On The Occurrence Of Occupational Fraud In Financial Institutions. *International Journal Of Law, Crime And Justice*, 56, 79–88.

Tamturk, V. (2016, August 24). *Mobile Commerce Is On The Rise, So Is Fraud*. Retrieved From Cmscmedia: Https://Www.Cms-Connected.Com/News-Archive/August-2016/Mobile-Commerce-Is-On-The- Rise-So-Is-Fraud

TMforum. (2019). *Tm Forum Technical Report: Fraud Survey Report 2019.* Malaysia: Tmforum.

Retrieved From Https://Www.Tmforum.Org/Resources/Technical-Report/Tr246-Fraud-Survey- Report-2019-R19-0-0/

Wells, D. J. (2018). *International Fraud Handbook.* Wiley. Retrieved From Pdfdrive: Https://Www.Pdfdrive.Com/International-Fraud-Handbook-E187423160.Html

Yelland, M. (2013, March). Fraud In Mobile Networks. *Computer Fraud & Security*, Pp. 5-9. Yin, C. (2018, August 4). *40 telecom fraud criminals penalized*. Retrieved from ChinaDaily.com.cn: http://www.chinadaily.com.cn/a/201808/04/WS5b64e633a3100d951b8c8914. html

Yingchao, G. (2017). Research on How to Deal with the Dilemma of Global Cooperative Governance of Cross-Border Telecom Network Fraud in China. *Chinese Studies*, 6, 249-263

Zhang, Y., Bian, J., & Zhu, W. (2013). Trust fraud: A crucial challenge for China's e-commerce market. *Electronic Commerce Research and Applications* , 12, 299–308

ZX. (2019, September 20). *69 arrested for cross-border telecom fraud in SW China*. Retrieved from XinhuaNet: http://www.xinhuanet.com/english/2019-09/20/c_138408235.html